TESIS DE MAGISTER EN INGENIERIA DEL SOFTWARE

Asistente para la realización de auditoría de sistemas en organismos públicos o privados

Autor: Lic. Horacio Daniel Kuna

Directores de Tesis: Dr. Ramón García Martínez

M.Ing. María Alejandra Ochoa

Año 2006

A mi mujer Graciela,
A mis Hijas Paula y Andrea,
Por su amor, comprensión y apoyo.

Resumen

La revolución tecnológica, la globalización de la economía, han convertido a la información en uno de los activos más importantes a proteger que tienen las empresas.

La auditoría de sistemas tiene una función central en esta tarea, centrándose en la prevención de riesgos. En general se observa un escaso desarrollo de las técnicas de auditoría asistidas por computadora (CAATs).

El sistema que se desarrolla en este trabajo es un asistente metodológico al proceso de auditoría en lo relacionado a cada una de las tareas que realiza el auditor de sistemas considerando los estándares internacionales.

Abstract

The technological revolution, the globalization of the economy, they have transformed to the information into one from the most important assets to protect that they have the companies.

The systems audit has a central function in this task, being centered in the prevention of risks. In general a scarce development of the audit techniques is observed attended by computer (CAATs).

The system that is developed in this work is a methodological assistant to the audit process in the related to each one of the tasks that the auditor of systems carries out considering the international standards.

Agradecimientos

- Al Instituto de Tecnología ORT, por haberme dado una profesión.
- A la Universidad de Morón, por haberme dado la oportunidad de continuar mis estudios.
- A todo el personal de CAPIS, por su calidad, calidez y eficiencia.
- Al Doctor Ramón García Martínez, por su apoyo, capacidad y paciencia.
- A la M.Ing. María Alejandra Ochoa por su apoyo y orientación.
- Al ITBA por posibilitarme concretar un sueño.

INDICE

Capítulo 1

Introducción

1. INTRODUCCIÓN

1.1. El tema de la Tesis

La tesis que se presenta trata sobre el desarrollo de una herramienta de software que asiste al auditor de sistemas en su tarea. El desarrollo de la misma se basa en herramientas Open Source como el PHP y el Firebird y se utiliza la metodología Métrica V3 [Métrica V3,2004].

El trabajo tiene como objetivo fundamental el de brindar una herramienta software que asista al auditor de sistemas desde el punto de vista metodológico, en todas las fases de su trabajo, contemplando los estándares internacionales, un objetivo secundario es la utilización de la metodología Métrica V3 en un desarrollo completo.

1.2 A quiénes está dirigido el texto

El trabajo esta dirigido fundamentalmente a ingenieros del software, auditores de sistemas, profesionales del área de sistemas, y cátedras universitarias vinculadas a la auditoría de sistemas y la ingeniería del software. Esta tesis puede tomarse como material de referencia para la adopción de buenas practicas en la auditoría de sistemas.

1.3 Descripción de la composición del presente trabajo

El documento esta organizado en 12 capítulos y anexos:

- Capítulo **1. Introducción**. Presenta el tema de la tesis, los destinatarios de la misma y la manera en que esta organizado el documento.
- Capítulo **2. Estado de la cuestión.** Incluye un panorama de la actual situación relacionada con la auditoría de sistemas, especificando el contexto en el que se desarrolla la tesis.
- Capítulo **3. Problema**. Comprende una descripción del problema a resolver y una explicación del objetivo de la tesis.
- Capítulo **4. Solución**. Que incluye las siguientes secciones:

  - ✓ Sección **4.1. Planificación del Sistema de Información.** Incluye la documentación que resulta del proceso “PSI: Planificación del Sistema de Información” de la Metodología Métrica en su versión III. La documentación incluye un marco de referencia para el desarrollo de sistemas de información que corresponde a los objetivos estratégicos de la organización.
  - ✓ Sección **4.2. Desarrollo del sistema de información**

- ✓ Sección **4.2.1 Estudio de Viabilidad**. Comprende el alcance del sistema, la situación actual, la descripción general del sistema, las alternativas de solución y la selección de la alternativa mas optima. Incluye actividades relacionadas con la gestión, la planificación, la calidad del proyecto como así también con la gestión de configuración
- ✓ Sección **4.2.2. Análisis del sistema de información.** Comprende el análisis del sistema actual, la obtención de requisitos del sistema, los modelos de datos y requisitos.
- ✓ Sección **4.2.3. Diseño del sistema de información.** Comprende la definición de la arquitectura del sistema, el diseño de la interfaz y de las clases.
- ✓ Sección **4.2.4. Construcción del sistema de información.** Comprende la descripción del entorno de construcción y el resultado de las pruebas.
- ✓ Sección **4.2.5. Implementación y aceptación del Sistema**. Comprende las actividades relacionadas con puesta en funcionamiento del sistema
- ✓ Sección **4.3. Mantenimiento del Sistema de Información.** Comprende todas las tareas relacionadas con el mantenimiento del sistema.
- ✓ Sección **4.4. Gestión del proyecto.** Comprende todas las actividades relacionadas con la gestión del proyecto
- ✓ Sección **4.5. Seguridad.** Comprende las actividades relacionadas con garantizar los aspectos relacionados con la seguridad del sistema.
- ✓ Sección **4.6. Gestión de Configuración**. Comprende todas las actividades relacionadas con garantizar la integridad de cada uno de los productos que se generan.
- ✓ Sección **4.7. Interfaz de aseguramiento de la calidad.** Comprende todas las actividades que se realizan a lo largo de todo el ciclo de vida del sistema, que se relacionan con la calidad.

❖ Capitulo **5. Experimentación.** Comprende la descripción de un caso real de estudio

❖ Capitulo **6. Conclusiones y futuras líneas de investigación.** Comprende las conclusiones a las que se llegó después de haber finalizado el trabajo de tesis, junto con las futuras líneas de trabajo a abordar.

❖ Capitulo **7. Referencias.** Comprende las referencias bibliográficas utilizadas a lo largo del texto.

❖ Capitulo **11. Bibliografía.** Comprende la bibliografía utilizada en la elaboración del documento.

❖ **Anexos.** Comprende la documentación anexa al contenido principal del texto, incluye las guías de auditoría de COBIT, el resumen de dominios y procesos de COBIT, cuestionarios, seudorreglas obtenidas, checklist e interfaces del sistema.

Capítulo 2

Estado de la cuestión

2. ESTADO DE LA CUESTION

En este capitulo se desarrollan los fundamentos de la auditoría de sistemas (Sección 2.1) y las conclusiones del estado actual de la cuestión (Sección 2.2)

2.1. Fundamentos de la Auditoría de Sistemas

2.1.1. Conceptos básicos de Auditoría.

La palabra auditoría proviene del latín y etimológicamente significa “oír”, en sus comienzos la auditoría de los SI estaba relacionada con detectar errores en los procedimientos vinculados con el procesamiento de la información, esta actividad ha evolucionado y en la actualidad se entiende al auditor como un consultor especializado en riesgos.

La auditoría de sistemas es el conjunto de técnicas, actividades y procedimientos, destinados a analizar, evaluar, verificar y recomendar en asuntos relativos a la planificación, control, eficacia, seguridad y adecuación de los sistemas de información en la empresa [Rivas, 1988].

La auditoría de sistemas es fundamental para garantizar el correcto funcionamiento de los Sistemas de Información al proporcionar los controles necesarios que permiten garantizar la seguridad, integridad, disponibilidad y confiabilidad de los mismos.

Los auditores de sistemas de información [ISACA, 2002] examinan y evalúan el desarrollo, implementación, mantenimiento y operación de los componentes de sistemas automatizados y sus interfaces con sistemas externos y no automatizados.

2.1.2. Objetivos de la Auditoría de Sistemas.

Para la Sindicatura General de la Nación los objetivos de la auditoría de sistemas son [SIGEN, 2004]

Los organismos públicos deben contar con sistemas que tengan incorporados instrumentos idóneos de control interno, a fin de favorecer el cumplimiento de sus metas y objetivos, provean la emisión de información financiera y operativa oportuna y confiable, que coadyuve a la eficacia, eficiencia y economía de las operaciones, el cumplimiento de la normativa y la protección adecuada de activos y recursos, incluyendo acciones tendientes a la detección y disuasión de fraudes y otras irregularidades.

Por lo tanto, la auditoría del control interno de los sistemas tiene por objeto examinar y evaluar la calidad y suficiencia de los controles establecidos por el ente para lograr el mejor funcionamiento de aquellos. El auditor deberá formarse opinión e informar acerca de la razonabilidad de tales controles, dando cuenta de los apartamientos observados y recomendando las propuestas para su mejoramiento.

Es importante señalar que, a diferencia de otras auditorias -donde el conocimiento del control interno es un medio para su concreción-, para la labor de auditoría del control interno de los sistemas, el examen, y las propuestas a efectuar para el logro del funcionamiento adecuado del mismo, será el objeto principal de la labor.

La auditoría del control interno debe aplicar procedimientos tendientes a evaluar sus componentes, a saber:

a. Ambiente de control
b. Apreciación del riesgo
c. Actividades de control
d. Información/comunicación
e. Supervisión

Se debe analizar y comprobar el funcionamiento del sistema, teniendo en cuenta los objetivos del control interno que se incluyen a continuación:

f. La emisión de información financiera y operativa confiable, íntegra, oportuna y útil para la toma de decisiones.
g. El cumplimiento de las leyes y normas aplicables.
h. La protección de los activos y demás recursos, incluyendo actividades para la disuasión de fraudes y otras irregularidades.
i. El conocimiento, por parte de la Dirección Superior, del grado de consecución de los objetivos operacionales, sobre la base de la aplicación de criterios de eficacia, eficiencia y economía.

La tarea tendrá por objeto, fundamentalmente, determinar y concluir si el referido Sistema se ha estructurado de tal manera que proporcione un grado razonable de seguridad para el cumplimiento de los mencionados objetivos.

En todos los casos, el auditor deberá informar aquellas cuestiones que se apartan de un razonable funcionamiento y que, por ende, deberían ser subsanadas por las autoridades, efectuando recomendaciones en tal sentido y sugiriendo los métodos de corrección de las deficiencias.

Cuando el objeto de la auditoría del control interno se relacione con los sistemas computadorizados de información, se contemplarán, además, tareas específicas sobre este particular, tales como:

j. La planificación, el desarrollo y la implantación de los sistemas utilizados para programar, organizar, ejecutar y controlar las operaciones.
k. La información producida por los sistemas y su pertinencia, confiabilidad y oportunidad.
l. La reglamentación básica de cada sistema, su implantación y la divulgación de la misma entre los usuarios.
m. Los mecanismos de control interno previo y posterior incorporados en los sistemas.
n. Los recursos idóneos identificados y disponibles para garantizar la continuidad de las operaciones en casos de contingencias o desastres.
o. El programa de adiestramiento al personal de sistemas de información, sus usuarios y los auditores internos.
p. La satisfacción que los sistemas brindan a los usuarios.

2.1.3. Los bienes a proteger.

Los bienes a proteger son [COBIT, 1996]:

- Datos, que son todos los objetos de la información.
- Aplicaciones, son el conjunto de sistemas de información.
- Tecnología, es el conjunto de hardware y software de base
- Instalaciones, son los recursos necesarios para alojar a los sistemas de información.
- Recursos Humanos, es el personal relacionado directamente con el desarrollo y producción de los sistemas de información.

2.1.4. Funciones de los auditores de sistemas.

Se establecen tres tipos de funciones para los auditores de sistemas [Piattini, 2003]:

- Participar en la revisión del diseño, realización, implantación y explotación de las aplicaciones informáticas
- Revisar y evaluar los controles implementados en los sistemas informáticos.
- Revisar y evaluar la eficacia, utilidad, fiabilidad y seguridad de los equipos e información.

2.1.5. Metodología de desarrollo de Auditoría de sistemas

Diferentes autores proponen metodologías de desarrollo de auditorias de sistemas, en general la mayoría de ellos coinciden en las siguientes fases:

- *Fase 1. Identificar el Alcance y los Objetivos de la Auditoría Informática (A.I.)*

En esta fase se determinan los limites y el entorno en que se realizara la auditoría, es el momento donde se determina hasta donde debe llegar la tarea, debe existir un acuerdo muy preciso entre autoridades y clientes sobre las funciones (seguridad, dirección, etc.), las materias (sistemas operativos, bases de datos, etc.) y los departamentos o áreas a auditar (sistemas, comunicaciones, etc.). El éxito del proceso de auditoría depende de una clara definición de esta fase.

- *Fase 2. Realizar el Estudio Inicial del entorno a auditar*

Para realizar dicho estudio es necesario examinar las funciones y actividades generales de la organización a auditar y en particular de las relacionadas con las tecnologías de la información, se deberá obtener información sobre:

ORGANIZACIÓN

- Se debe definir la estructura organizativa del Departamento o área de Informática a auditar.
- Organigrama, se trata de la estructura formal de la organización a auditar.
- Departamentos, entendiendo como departamentos a las áreas que siguen a la dirección, en el estudio inicial se deberá definir la función de cada uno de ellos.
- Relaciones funcionales y jerárquicas entre las distintas áreas de la organización, el auditor verificará si se cumplen las relaciones funcionales y jerárquicas previstas, o por el contrario, detectará, cualquier anomalía como por ejemplo, si algún empleado tiene dos jefes.
- Flujo de información, la calidad de este flujo tiene un enorme impacto sobre la eficacia y eficiencia de la gestión, deberá investigar sobre posibles canales alternativos o no formales de comunicación.
- Numero de puestos de trabajo y personas por puesto de trabajo
- Distribución de recursos ineficiente
- Necesidad de reorganización

ENTORNO OPERATIVO

El equipo de auditoría informático debe poseer antes de comenzar la tarea una información fiable del entorno en el que se va ha desarrollar las actividades. Se debe considerar:

- Situación Geográfica de las áreas de sistemas a auditar, verificando la existencia de los responsables y la estructura interna del área informática, así como el uso de estándares de trabajo formales o informales, los planes de capacitación y las políticas de ingreso de personal a las áreas de sistemas.
- Arquitectura y Configuración Hardware y Software
- Inventario completo del hardware y software, incluyendo CPUs, procesadores, periféricos, software de base y aplicación, legalidad del mismo, etc.
- Telecomunicaciones, topología, proveedores, servicios que se brindan, seguridad, etc.
- Aspectos relacionados con la seguridad y planes de contingencia.

APLICACIONES INFORMÁTICAS, BASES DE DATOS Y ARCHIVOS

- Se deben determinar los sistemas informáticos implementados en la empresa.
- Volumen, Antigüedad y Complejidad de las aplicaciones
- Metodología de desarrollo de aplicaciones
- Metodología de mantenimiento de las aplicaciones.
- Documentación de aplicaciones
- Cantidad y complejidad de bases de datos, tamaño y características de bases de datos, número de accesos a BD, frecuencia de actualización
- Planes de desarrollo
- Políticas de backup.

Muchos autores sugieren que en el final de esta etapa es necesario realizar un Análisis de Riesgo, que será el que guié el proceso de auditoría.

- *Fase 3. Determinación de los recursos necesarios para realizar la auditoría de sistemas.*

Después de realizar el estudio preliminar se debe determinar los recursos materiales y humanos necesarios para implementar el plan de auditoría

Recursos Materiales

- Software: paquetes de auditoría del equipo auditor, compiladores
- Hardware: PCs, impresoras, líneas de comunicación.
- Se debe establecer quien provee estos recursos

Recursos Humanos

La Auditoría de sistemas en general suele ser ejercida por profesionales universitarios y por otras personas de probada experiencia multidisciplinaria y en algunos casos se requiere que los profesionales estén certificados por ISACA (Information System audit. And Control Association).

- *Fase 4. Elaborar el Plan de Trabajo*

En esta fase se definen el calendario de actividades a realizar, formalizando el mismo para la aprobación por parte de las autoridades.

El plan de la auditoría en muchos casos es guiado por las recomendaciones que brinda ISACA a través de sus guías y contempla:

- Conocimiento de la organización y de sus procesos, para identificar problemas potenciales, alcance, etc.
- Programa de auditoría: Calendario de trabajo (tareas y recursos) y su seguimiento
- Evaluación interna del control, mediante pruebas de cumplimiento de los controles

- *Fase 5. Realizar las Actividades de Auditoría*

Es el momento donde se efectivizan las actividades planificadas en la fase anterior, aplicando distintas técnicas y utilizando herramientas que garanticen el cumplimiento de los objetivos planteados, se documenta esta etapa, monitoreando las posibles desviaciones que se detecten en relación con la planificación original.

- *Fase 6. Realizar el Informe Final*

El objetivo final del auditor es entregar por escrito un informe, en donde constarán las conclusiones y recomendaciones. El auditor justifica personalmente su auditoría en forma documentada. La elaboración del Informe Final es la única referencia constatable de toda auditoría, y el exponente de su calidad. Por lo tanto es muy importante que su contenido sea claro y estructurado de tal manera que responda a las expectativas del cliente en cuanto al cumplimiento de los objetivos planteados.

Modelo de Estructura de un Informe Final:

- Definición de objetivos y alcance de la auditoría.

- Enumeración de temas considerados
- Cuerpo expositivo

a) Situación actual. Cuando se trate de una Revisión periódica.

b) Tendencias. Se tratarán de hallar parámetros de correlación.

c) Puntos débiles y amenazas.

d) Recomendaciones y Planes de Acción. Constituyen, junto con la exposición de puntos débiles, el verdadero objeto de la auditoría informática. Es importante considerar que el objetivo final debe ser el de crear un ambiente de control dentro de la empresa y las recomendaciones deben estar orientadas en este sentido.

En el informe final deben quedar claramente formalizados los siguientes puntos:

- ✓ Alcance
- ✓ Objetivos
- ✓ Período de cobertura
- ✓ Naturaleza y extensión del trabajo de auditoría
- ✓ Organización
- ✓ Destinatarios del informe
- ✓ Restricciones
- ✓ Hallazgos
- ✓ Conclusiones
- ✓ Recomendaciones

- *Fase 7. Carta de Presentación.*

Es la última etapa de la auditoría consta de un resumen de 3 ó 4 folios del contenido del informe final, dirigido a las autoridades de la empresa u organización donde se realizó la auditoría, es conveniente que los responsables máximos de la empresa certifiquen que la tarea fue realizada de acuerdo a lo previsto, este documento debe incluir los siguientes elementos:

– Incluye los datos generales de la auditoría como los limites de la misma, los objetivos y alcance de la auditoría
– Cuantifica las áreas analizadas
– Proporciona una conclusión general, puntualizando las áreas de gran debilidad
– Presentar las debilidades y riesgos en orden de importancia
– Proporciona un resumen de las recomendaciones realizadas.

2.1.6. Técnicas y herramientas utilizadas en el proceso de auditoría.

➔ Técnicas:

- Revisión: análisis de la información obtenida tanto en el estudio inicial como en la propia auditoría, en general esta información es obtenida a través de cuestionarios y entrevistas.

- Entrevistas: se trata de una de las actividades personales más importantes que realiza el auditor, esta técnica se basa fundamentalmente en la elaboración de preguntas al entrevistado, las entrevistas pueden tener diferentes estructuras (preguntas abiertas, cerradas, etc.) que dependerán de los objetivos de la entrevista y el perfil del entrevistado. En muchos casos desencadena en checklist: cuestionario minucioso, ordenado y estructurado por materias
- Observación, donde el auditor observa en forma pasiva como se realizan las tareas.
- Simulación de situaciones.
- Muestreos

➔ **Herramientas**

- Cuestionario general
- Cuestionario-Checklist, se trata de un conjunto de preguntas cerradas muy utilizadas en el proceso de auditoría que permiten obtener información tanto cualitativa como cuantitativas, destinadas a determinar las fortalezas y debilidades de los sistemas de control.
- Simuladores (generadores de datos)
- Paquetes de Auditoría (generadores de programas)

2.1.7. Auditoría asistida por computadora

La norma SAP 1009 (Statement of Auditing Practice) denominada Computer Assisted Audit Techniques (CAATs) o Técnicas de Auditoría Asistidas por Computador (TAACs), plantea la importancia del uso de TAACs en la auditoría de sistemas.

La norma SAP 1009 los define como programas de computador y datos que el auditor usa como parte de los procedimientos de auditoría para procesar datos de significancia en un sistema de información.

Las TAACs pueden ser usadas en:

➔ Pruebas de detalles de transacciones y balances (Recálculos de intereses, extracción de ventas por encima de cierto valor, etc.)
➔ Procedimientos analíticos, por ejemplo identificación de inconsistencias o fluctuaciones significativas.
➔ Pruebas de controles generales, tales como configuraciones en sistemas operativos, procedimientos de acceso al sistema, comparación de códigos y versiones.
➔ Programas de muestreo para extractar datos.
➔ Pruebas de control en aplicaciones.
➔ Recálculos.

Existen diferentes tipos de software:

Paquete de Auditoría. Son programas generalizados de computadora diseñados para desempeñar funciones de procesamiento de datos que incluyen leer bases de datos, seleccionar información, realizar cálculos, crear archivos de datos e imprimir informes en un formato especificado por el auditor. Son usados para control de secuencias, búsquedas de registros, detección de duplicaciones, detección de gaps, selección de datos, revisión de operaciones lógicas y muestreo, algunos de ellos son el IDEA, ACL, etc.

Software para un propósito específico o diseñado a la medida. Son programas de computadora diseñados para desempeñar tareas de auditoría en circunstancias específicas. Estos programas pueden ser desarrollados por el auditor, por la entidad, o por un programador externo contratado por el auditor. Por ejemplo programas que permitan generar check-list adaptados a las características de la empresa y de los objetivos de la auditoría.

Los programas de utilería. Son usados por la organización auditada para desempeñar funciones comunes de procesamiento de datos, como clasificación, creación e impresión de archivos. Como por ejemplo planillas de cálculo, procesadores de texto, etc.

Los programas de administración del sistema. Son herramientas de productividad sofisticadas que son típicamente parte de los sistemas operativos sofisticados, por ejemplo software para recuperación de datos o software para comparación de códigos. Como en el caso anterior estas herramientas no son específicamente diseñadas para usos de auditoría. Existen en el mercado una gran variedad de este tipo de herramientas como por ejemplo los que permiten controlar las versiones de un sistema (Ej. Subversión)

Rutinas de Auditoría embebidas en Programas de aplicación. Módulos especiales de recolección de información incluidos en la aplicación y diseñados con fines específicos. Se trata de módulos que permiten obtener pistas de auditora en muchos casos generados a través de trigers programados en las propias bases de datos

2.1.8. Estado de la tecnología

A nivel internacional y nacional existen diferentes normas que intentan estandarizar el proceso de la auditaría de sistemas, algunas de ellas son:

2.1. 8.1. COBIT (*Control Objectives for Information and related Technology)*

La misión y Objetivos de COBIT es investigar, desarrollar, publicar y promover un conjunto de objetivos de control en tecnología de la información (TI) con autoridad, actualizados, de carácter internacional y aceptados generalmente para el uso cotidiano de gerentes de empresas y auditores.

La Information Systems Audit and Control Foundation y los patrocinadores de COBIT, han diseñado este producto principalmente como una fuente de instrucción para los auditores de sistemas.

COBIT ha sido desarrollado como estándares para mejorar las prácticas de control y seguridad de las TI que provean un marco de referencia para la Administración, Usuarios y Auditores.

COBIT define los siguientes elementos:

✓ Dominios: Agrupación natural de procesos. Se definen 4: Planificación y organización, Adquisición e implementación, Prestación y soporte, Monitoreo *(ver anexo 2)*
✓ Procesos: Conjuntos o series de actividades unidas con delimitación o cortes de control. En cada proceso se definen objetivos de control. *(ver anexo 2)*
✓ Actividades: Acciones requeridas para lograr un resultado medible. *(ver anexo 1)*

Se definen 34 objetivos de control generales, uno para cada uno de los procesos de las TI. Estos procesos están agrupados en cuatro grandes dominios.

2.1.8.2. ISACA

La Information Systems audit. And Control Association (ISACA) estableció un conjunto de normas generales para los sistemas de auditoría de la información [ADACSI, 2004], las mismas son:

010 Título de auditoría

- 010.010 Responsabilidad, autoridad y rendimiento de cuentas

020 Independencia

- 020.010 Independencia profesional
- 020.020 Relación organizativa

030 Ética y normas profesionales

- 030.010 Código de Ética Profesional
- 030.020 Atención profesional correspondiente

040 Idoneidad

- 040.010 Habilidades y conocimientos
- 040.020 Educación profesional continua

050 Planificación

- 050.010 Planificación de la auditoría

060 Ejecución del trabajo de auditoría

- 060.010 Supervisión
- 060.020 Evidencia

070 Informes

- 070.010 Contenido y formato de los informes

080 Actividades de seguimiento

- 080.010 Seguimiento

2.1.8.3. SIGEN

A nivel nacional la SIGEN (Sindicatura General de la Nación) establece un Conjunto de normas y procedimientos generales relacionados con el proceso

de Auditoría financiera, no encontrándose ninguna específica relacionada con la Auditoría de Sistemas.

2.1.9. Marco Legal

Existen diferentes instrumentos legales en la Argentina que enmarcan la tarea de la auditoría, aunque para muchos expertos estos instrumentos aun son insuficientes e incompletos, la tabla 2.1 es un resumen de los mismos:

Tema	Ley o decreto	Observaciones
Propiedad Intelectual	Ley N° 11.723	Propiedad Intelectual. Régimen legal.
	Dto. N° 165/94	Se establece un marco legal de protección para las diferentes expresiones de las obras de software y base de datos, así como sus diversos medios de reproducción.
	Ley N° 25.036	Modifica la ley 11.723, incluye la protección de la propiedad intelectual sobre programas de computación fuente y objeto, las compilaciones de datos o de otros materiales. Penaliza la defraudación de derechos de propiedad intelectual.

	Ley N° 25.326	Protección de Datos Personales. Regula sobre principios generales relativos a la protección de datos, derechos de los titulares de dato de usuarios y responsables de archivos, registros y bancos de datos.
Confidencialidad	Ley Nº 24.766	Establece la obligación de abstenerse de usar y revelar la información sobre cuya confidencialidad se hubiera prevenido.
Archivos Digitales	Dec.Administrativa Nº 43/96 - JGM	Reglamenta los archivos digitales. Establece como órgano rector a la Contaduría Gral. de la Nación.
	Ley Nº 24.624 (Art.30)	Autoriza el archivo y conservación en soporte electrónico u óptico indeleble de la documentación financiera, de personal y de control de la Administración Pública Nacional.

COMPETENCIA DE LA SUBSECRETARIA DE LA GESTION PUBLICA	Dto. Nº 889/01	Aprueba la estructura organizativa de la Secretaría para la Modernización del Estado en el ámbito de la Subsecretaría de la Gestión Pública, creando la Oficina Nacional de Tecnologías de la Información y otorgándole competencias en materia de firma digital.

	Dto. Nº 673/01	Crea la Secretaría para la Modernización del Estado en el ámbito de la Jefatura de Gabinete de Ministros, asignándole competencia para actuar como Autoridad de Aplicación del régimen normativo que establece la Infraestructura de Firma Digital para el Sector Público Nacional y para la aplicación de nuevas tecnologías informáticas en la Administración Pública Nacional.

	Dto. N° 78/02	Estructura organizativa de la Jefatura de Gabinete de Ministros. Dispone que la SUBSECRETARIA DE LA GESTION PUBLICA ejercerá todas aquellas facultades que le fueran oportunamente atribuidas a la ex SECRETARIA DE GABINETE Y MODERNIZACION DEL ESTADO, en lo referente a los temas de su competencia
FIRMA DIGITAL	Disp. Nº 5/02 - ONTI	Documentación técnica de la Autoridad Certificante de la ONTI.
	Res. Nº 176/02 - JGM	Habilita en Mesa de Entradas de la Subsecretaría de la Gestión Pública el Sistema de Tramitación Electrónica para la recepción, emisión y archivo de documentación digital firmada digitalmente.

	Res. Nº 17/02 - SGP	Establece el procedimiento para solicitar la certificación exigida al Registro del Personal acogido al Sistema de Retiro Voluntario, habilitando la modalidad de tramitación mediante el empleo de documentación digital firmada digitalmente.
	Ley Nº 25.506	Ley de Firma Digital - Boletín Oficial del 14/12/2001
	Dto. Nº 2628/ 02	Ley de Firma Digital - Reglamentación
	Dto. Nº 1023/01	En su artículo 21 permite la realización de las contrataciones comprendidas en el Régimen en formato digital firmado digitalmente.

	Dto. Nº 677/01	Otorga a los documentos digitales firmados digitalmente remitidos a la Comisión Nacional de Valores de acuerdo a las reglamentaciones dictadas por ese organismo, similar validez y eficacia que los firmados en soporte papel.
	Dec.Administrativa Nº 102/00 - JGM	Prorroga por DOS (2) años a partir del 31 de diciembre de 2000 el plazo establecido en el artículo 1° del Decreto N° 427/98.
	Ley Nº 25.237	Establece en el artículo 61 que la SINDICATURA GENERAL DE LA NACION ejercerá las funciones de Organismo Auditante en el régimen de empleo de la firma digital en la instrumentación de los actos internos del Sector Público Nacional.

	Res. Nº 212/98 - SFP	Establece la Política de Certificación del Organismo Licenciante, en la cual se fijan los criterios para el licenciamiento de las Autoridades Certificantes de la Administración Pública Nacional
	Res. Nº 194/98 - SFP	Establece los estándares sobre tecnología de Firma Digital para la Administración Pública Nacional.
	Dto. Nº 427/98	Autoriza la utilización de la firma digital en la instrumentación de los actos internos del Sector Público Nacional, otorgándole los mismos efectos que la firma ológrafa y estableciendo las bases para la creación de la Infraestructura de Firma Digital para el Sector Público Nacional.

	Dto. Nº 283/03	Firma Digital - Emisión de Certificados Digitales
	Res. Nº 45/97 - SFP	Establece pautas técnicas para elaborar una normativa sobre firma digital que permita la difusión de esta tecnología en el ámbito de la Administración Pública Nacional.
	Dto. 160/04	Designa a los integrantes de la Comisión Asesora para la Infraestructura de Firma Digital creada por la Ley Nº 25.506.
PAUTAS PARA SITIOS WEB ESTATALES	Res. Nº 97/97 - SFP	Pautas de integración para las páginas web de la Administración Pública Nacional.

PROCEDIMIENTOS ADMINISTRATIVOS	Dec. Administrativa N° 118/01- JGM	Crea el Proyecto de Simplificación e Informatización de Procedimientos Administrativos (PRO-SIPA), en el contexto del Plan Nacional de Modernización y en el ámbito de la Jefatura de Gabinete de Ministros.
SEGURIDAD EN REDES	Res. Nº 81/99 - SFP	Creación del ArCERT, Coordinación de Emergencias en Redes Teleinformáticas de la Administración Pública Argentina.

Tabla 2.1 : Marco legal

2.2. Software de Auditoría de sistemas existentes en el mercado

❖ ***Software: Meycor COBIT CSA (Control Self-Assessment)***

Procedencia del Software: Datasec – Uruguay

Descripción del software:

Es una herramienta de software que automatiza la evaluación de una organización contra los objetivos de control del marco COBIT, generando un diagnóstico y recomendaciones que facilitan la implementación de esos objetivos de control.

El producto está basado en la 3ra. edición de los objetivos de control de COBIT. No incluye las guías de auditoría de COBIT; pero provee un Módulo de

Auditoría (MEYCOR-AUDIT COBIT (CSA)) que permite la verificación de la veracidad y fiabilidad de las respuestas a los cuestionarios incorporados respecto del grado de cumplimiento con cada uno de los objetivos de control de COBIT.

El producto puede ser utilizado como una herramienta de autoevaluación enfocado a la Gerencia de TI, y permite obtener un diagnóstico de su situación actual y una serie de recomendaciones a seguir a fin de alcanzar un nivel deseable en cuanto a seguridad, calidad, eficacia y eficiencia de sus sistemas de información.

También puede ser utilizado como una herramienta para que la Auditoría -ya sea interna o externa- evalúe las fortalezas y debilidades de los controles de TI existentes en los sistemas de información de la organización, en base al estándar mundial COBIT y las mejores prácticas de cada una de las plataformas tecnológicas.

Este producto se comercializa a todo el mundo a través de la ISACA, en la dirección www.isaca.org.

Meycor Cobit CSA permite:

- Incluye metodológicamente un enfoque de proyecto que guiará al administrador a través de los distintos pasos del proceso de evaluación.
- Permite definir diferentes niveles de acceso para cada usuario, posibilitando un acceso selectivo para cada uno de los 34 procesos de COBIT.
- Incluye dos útiles rutinas para facilitar la comprensión y propender a la concienciación de la Alta Gerencia (extraídas de COBIT Implementation Tool Set):
  - Planilla de autoevaluación para la gobernabilidad en TI (IT Governance Self-Assessment)
  - Planilla de diagnóstico de las inquietudes en materia de TI de la Dirección (Management's IT Concerns Diagnostic)
- Genera automáticamente un ranking de los procesos de acuerdo al resultado obtenido.
- Permite ampliar la granularidad en la evaluación de algunos objetivos de control de COBIT al conectarlos con cuestionarios relacionados con riesgos específicos como seguridad física y lógica, incendio, daños causados por agua, controles ambientales, etc.
- Permite la administración de la ponderación interna que puede utilizar el software para cada objetivo de control, a efectos de personalizarlos respecto de las peculiaridades de cada organización

bajo medición. Como resultado del procedimiento de ponderación, se puede obtener un valor cuantitativo para cada proceso.

- Permite identificar diferentes niveles de restricciones (relativas a los 5 recursos de TI) que obstaculizarán la implementación de los objetivos de control a menos que se efectúe un gran cambio de mentalidad, de inversión en infraestructura o de prioridad en control y seguridad por parte de quienes establecen las políticas de la organización.
- Permite calcular el costo de implementación de cada recomendación asociada a objetivos de control, generando un cronograma para su implementación en varios períodos.
- Permite analizar, en conexión con los objetivos de control correspondientes, el estatus de control y seguridad de plataformas específicas (Windows®, UNIX®, Novell®, AS/400®), Bases de Datos (Oracle®, Informix®), etc., incluyendo cuestionarios adicionales para evaluar esas plataformas.
- Permite evaluar grandes corporaciones con recursos de TI distribuidos en diferentes ubicaciones, a través de la creación de varios centros de análisis, con la posibilidad de consolidar los resultados en forma global o local.
- Permite una revisión periódica de la evolución de las decisiones efectuadas por la Dirección a través de gráficas de comparación de los diagnósticos de los diferentes períodos evaluados.

❖ ***Software: Meycor COBIT MG (MANAGEMENT GUIDELINES)***

Procedencia del Software: Datasec – Uruguay

Descripción del software:

COBIT en su 3ra edición incorpora las Guías de Gerenciamiento (Management Guidelines), que incluyen un conjunto de herramientas formado por el Modelo de Maduración, los Factores Críticos de Éxito (CSFs), los Indicadores Clave de Meta (KGIs) y los Indicadores Clave de Desempeño (KPIs).

Estas herramientas se integran, bajo el estilo formal de la metodología MEYCOR, para analizar en forma mensurable y controlar los 34 procesos de TI que identifica COBIT, asegurando así, su gobernabilidad y su alineación con los objetivos del negocio.

Contiene un enfoque que permite ubicar en que nivel de control sobre la TI se encuentra la organización y definir adonde se quiere llegar. MEYCOR COBIT - Guías de Gerenciamiento (MG) ofrece un conjunto de

elementos genéricos, orientados a ejecutar acciones concretas que permitan a la Dirección y a la Gerencia obtener respuestas a las siguientes interrogantes:

- ¿Hacia donde va la organización en el uso de la tecnología?
- ¿Se cumple una adecuada relación costo-beneficio en esos avances?
- ¿Cuáles son los indicadores de desempeño?
- ¿Qué es realmente lo importante que debe hacerse?
- ¿Cuáles son los factores críticos de éxito?
- ¿Cuáles son los riesgos de no alcanzar los objetivos?
- ¿Qué hacen otras organizaciones similares en la materia?

HERRAMIENTAS QUE PROVEE MEYCOR COBIT - GUÍAS DE GERENCIAMIENTO (MG)

1. MODELO DE MADURACIÓN

El Modelo de Maduración es una forma excelente de medir el grado de evolución de los procesos de la organización. Este modelo identifica el perfil de avance de las empresas, en relación a los temas de la gobernabilidad, de la seguridad y del control en TI.

Define estados que permiten ubicar donde se encuentra la organización y a donde quiere llegar en esos temas, así como poder identificar en que nivel se encuentran las organizaciones líderes del área. Fija niveles discretos que crean los umbrales que se transforman en metas a alcanzar. MEYCOR COBIT - Guías de Gerenciamiento (MG) asiste al usuario para definir su estado actual, así como cuales son las recomendaciones requeridas para evolucionar al estado fijado como meta. Es posible analizar en forma gráfica la brecha entre el estado actual y la meta.

2. FACTORES CRÍTICOS DEL ÉXITO (CSFs)

Un Factor Crítico de Éxito es una acción o una condición que debe ocurrir necesariamente para conseguir ciertos objetivos básicos de la organización. Requiere la atención de todos los sectores involucrados para poder llevar a cabo las acciones que cada factor implica.

Además:

- proveen a la Dirección de una adecuada guía para el control en TI.
- definen las cosas más importantes a ser efectuadas para contribuir a que los procesos de TI alcancen sus objetivos.

- sus actividades pueden ser de tipo estratégico, técnico, organizacional o de procedimiento.
- deben ser concretos y orientados a la acción, enfocados hacia los recursos más importantes para cada proceso en desarrollo.

MEYCOR COBIT - Guías de Gerenciamiento (MG) además de incorporar los factores críticos de éxito que define COBIT, permite que se agreguen otros específicos para la organización.

3. INDICADORES CLAVE DE META (KGIs)

Definen medidas numéricas que informan a la Dirección - luego del hecho - si el proceso tecnológico ha alcanzado los requerimientos del negocio. Usualmente se expresan en términos de criterio de información:

- Disponibilidad de la información necesaria para atender las necesidades del negocio.
- Ausencia de integridad y riesgos de confidencialidad.
- Relación costo-eficiencia de los procesos y operaciones.
- Confirmación de la veracidad, eficacia y cumplimiento. El poder comparar un valor actual con un valor a alcanzar, permite medir la aproximación al objetivo general de lograr que la tecnología de la información brinde información acorde a los criterios de COBIT y sea útil para lograr los objetivos del negocio. MEYCOR COBIT - Guías de Gerenciamiento (MG) además de incorporar los indicadores que define COBIT, permite que se agreguen otros específicos para la organización.

4. INDICADORES CLAVE DE DESEMPEÑO (KPIs)

- Son medidas de la eficiencia y eficacia con que un proceso de TI está logrando los requerimientos del negocio. Monitorean el desempeño de los participantes del proceso, pronosticando las probabilidades de éxito para el futuro.
  Mientras los Indicadores Clave de Meta (KGI) se enfocan en “que”, los Indicadores Clave de Desempeño (KPI) se enfocan en “como”. Son a menudo una medida de los Factores Críticos de Éxito (CSF) y pueden identificar oportunidades para mejorar los procesos.

MEYCOR COBIT - Guías de Gerenciamiento (MG) además de incorporar los indicadores que define COBIT, permite que se agreguen otros específicos para la organización.

5. RECOMENDACIONES DE MEJORA

Las recomendaciones de mejora sirven para organizar las acciones a priorizar con el fin de eliminar las brechas detectadas entre los valores actuales y los valores a alcanzar. Las recomendaciones se agrupan en proyectos a efectos de dar un marco de acción coordinado, temporal y financiero. MEYCOR COBIT - Guías de Gerenciamiento (MG) además de las facilidades para clasificar los proyectos que define COBIT, permite asociar un costo financiero a cada recomendación, de modo de obtener una primera aproximación a la comparación de los costos de proyectos con el presupuesto anual disponible, reconociendo así una restricción importante.

- ***Software: Gesia 2000***

Procedencia del Software: Audinfor S.L. - España

Descripción del software:

Las directrices y objetivos del GESIA 2000 no han sido otros que el de poner al alcance de los profesionales de la auditoría, y de forma muy especial de los responsables de despachos y firmas de auditoría, una herramienta que, acorde con las nuevas tecnologías, facilite su labor de organizar y controlar los trabajos.

La normalización de los papeles de trabajo es otro de los aspectos contemplados en el desarrollo del GESIA 2000, al potenciar el diseño de diferentes modelos de organización de papeles acorde con el sector, tamaño, complejidad, grado de control interno, etc. en los que esté inmerso el auditor. La informática brinda una excelente oportunidad para reducir tiempos en los trabajos repetitivos y sobre todo modelizar los papeles y la documentación a cumplimentar.

No se impone ningún esquema preconcebido, solamente se exige que sea cual fuere el sistema utilizado, su diseño y definición responda a una determinada lógica que pueda ser trasladable al sistema informático.

- ***Software: ACL Edición de Escritorio / Red***

Procedencia del Software ACL Services Ltd. -

Descripción del software:

ACL es la herramienta de software de auditoría preferida por la comunidad de auditoría interna internacional, para la extracción y el análisis de datos, la detección de fraudes y el control continuo. Al proporcionar una exclusiva y eficiente combinación de acceso a los datos, análisis y elaboración integrada de reportes, ACL permite transformar los datos en información significativa y asistirlo en el logro de objetivos comerciales para agregar valor a su organización.

- Independientemente del origen de los datos (bases de datos planas o relacionales, hojas de cálculo, archivos de reportes), ACL lee y compara los datos y permite que los datos de origen permanezcan intactos, lo que ofrece una calidad e integridad total. ACL le permite captar de inmediato la información sobre las transacciones fundamentales para su organización.

  Los comandos están programados previamente para el análisis de datos (una variedad completa de eficiencia analítica, que abarca desde clasificaciones simples hasta pruebas complejas). Automatice su análisis a través del control continuo y la notificación en tiempo real. **Con ACL se puede:**

- Efectuar análisis más veloces, independientemente del departamento de tecnología, con una interfaz de usuario intuitiva, menús desplegables, barras de tareas y comandos tipo "apuntar y hacer clic".
- Aprovechar la capacidad de tamaño ilimitado de archivo y la velocidad sin precedentes de ACL para procesar rápidamente millones de transacciones, asegurar una cobertura al 100 por ciento y una confianza absoluta en los resultados.
- Producir informes claros. Diseñar, generar una vista previa y modificar los resultados en una forma fácil, en pantalla, con formato tipo "arrastrar y soltar".
- Identificar tendencias, determinar excepciones y destacar áreas potenciales de interés.
- Ubicar errores y fraudes potenciales al comparar y analizar los archivos, de acuerdo con el criterio del usuario final.
- Identificar temas de control y asegurar el cumplimiento de las normas.
- Permite realizar estadísticas según la necesidad del usuario.
- La posibilidad de correr un servidor ACL (con OS/390) y clientes ACL (con Windows) que se conectan al servidor, mejorando el rendimiento de procesamiento. Con lo cual las empresas con grandes volúmenes de datos

pueden realizar análisis a sus datos de forma rápida, gracias a la arquitectura Cliente/Servidor.

En una forma sólida pero sencilla, ACL extiende la profundidad y el espacio para el análisis, aumenta la productividad personal y brinda confianza en los resultados. Además, no se necesita ser un especialista técnico para usarlo. Con ACL, las organizaciones pueden lograr una rápida recuperación de la inversión, reducir el riesgo, asegurar la conformidad con las normas, minimizar las pérdidas y mejorar la rentabilidad.

❖ ***Software: 3 RD EDITION Management Advisor***

Procedencia del Software: : MethodWare – Costa Rica

Descripción del software:

COBIT 3 RD EDITION Management Advisor soporta análisis de brecha multi-nivel, permitiendo realizar un "benchmark" efectivo de los procesos de TI y analizar resultados de evaluaciones actuales versus anteriores en una base de datos única. Con su sofisticada función de alerta, provee un rastreo instantáneo de las áreas que requieren seguimiento, asegurando la disposición de la máxima cantidad de información con el toque de un botón.

- Está basado en Windows ®, amigable para el usuario y fácil de aprender.
- Tiene capacidad intranet/internet.

COBIT 3 RD EDITION Management Advisor le permite:

- Incorporar sólo aquellas partes de la estructura COBIT que son relevantes para la revisión actual.
- Aplicar en forma consistente las Guías Gerenciales de TI en toda su organización, utilizando como modelo base la estructura COBIT.
- Responder a la necesidad de los gerentes de controlar y medir a TI, proveyéndoles la información que necesitan en la forma que desean.

- Determinar y monitorear el nivel apropiado de seguridad y control de TI de su organización mediante las guías gerenciales.
- Contar con una interfaz completa con Microsoft ® Word y Excel para informes y análisis, y la habilidad de vincular cualquier documento existente, COBIT 3RD EDITION Management Advisor es una herramienta completa para los profesionales de TI.
- Proveer de facilidades para elaborar informes y gráficos ad-hoc y estándar en todas las etapas del proceso de auditoría.

❖ ***Software: COBIT Advisor 3 RD EDITION (Audit)***

Procedencia del Software: MethodWare – Costa Rica

Descripción del software:

COBIT Advisor 3 RD EDITION (Audit) provee una aplicación consistente de la estructura COBIT; aplicable a todo tipo de empresas. Entre sus muchos beneficios se tiene:

- Seguir guías de las mejores prácticas para una administración efectiva de TI en la organización; aplica estas Guías de Auditoría de COBIT en un proceso comprensivo y consistente. Y asegura que éstas tienen como objetivo los procesos, criterios de información y recursos de TI más relevantes.
- Permitir incorporar sólo aquellas partes de la estructura COBIT que son relevantes para la revisión actual.
- Gastar más tiempo auditando y menos tiempo registrando.
- Está basado en Windows es amigable para el usuario y fácil de aprender.
- Tiene capacidad para intranet/internet.
- interfaz completa con Microsoft ® Word y Excel para la generación de informes y gráficas.
- Cuenta con informes Word tipo Formulario, que permiten el input directo del documento al sistema por parte de los usuarios y de la gerencia.
- Provee informes estándar y ad-hoc y facilidades de graficación en todas las etapas del proceso de auditoría.
- COBIT Advisor 3 RD EDITION (Audit) posibilita consolidaciones a múltiples niveles, lo que permite comparar resultados de las auditorias a través de la organización y en el tiempo,
- Administrar las observaciones y recomendaciones de auditoría de SI en una base de datos única.
- Permite analizar y comprender los resultados de la auditoría mediante funciones de filtrado y ordenamiento

❖ ***Software: Idea Data Analysis Software***

Procedencia del Software: CaseWare IDEA -

Descripción del software:

CaseWare IDEA (www.caseware-idea.com) es un software de PC bajo Windows en Español, muy fácil de usar, que permite que el Analista de datos o Auditor de Negocios acceda virtualmente a cualquier archivo de datos de cualquier entorno y analice el cien por ciento de miles o millones de

transacciones en segundos detectando la totalidad de las excepciones y construyendo las propias bases de datos de Análisis de datos o Auditoría con datos completamente flexibles y de entornos diversos. IDEA representa un cambio total en la labor de Análisis de Análisis de Datos y Auditoría, ya que elimina - donde esto sea posible - el riesgo estadístico de las muestras y es una herramienta para apoyar el pensamiento creativo del Analista de Datos y del Auditor, a través de una serie de funciones de análisis predefinidas y gráficos interactivos, permite navegar sobre los datos o sobre los resúmenes estadísticos descubriendo potenciales problemas o identificando vulnerabilidades operativas, financieras o de negocios. Asimismo tiene funciones de soporte para los costosos análisis físicos (Inventarios, firmas, carpetas, documentos), que permiten o bien realizar muestras para pruebas sustantivas o de cumplimiento, o bien realizar ABCs de los datos para detectar el grupo de casos mas valioso para aplicar el análisis, y numerosas funciones de análisis de datos y detección de fraude. Finalmente IDEA automatiza en forma natural y en un lenguaje abierto, los programas de Análisis de Datos y Auditoría desarrollados y permite crear la biblioteca propia de programas de Análisis, y hasta integrar los procesos de Análisis y Auditoría con aplicaciones de negocios para el desarrollo de Alertas en línea y Monitoreo continuo.

2.3. Conclusiones.

Como resultado del análisis del estado actual de la Auditoría de sistemas se observa que existe un pobre desarrollo de la Auditoría de Sistemas Asistida por computadora. En relación al Software encontrado se encuentran las siguientes limitaciones y dificultades:

- Todos los paquetes de software analizados son de tipo comercial, con un alto costo que en muchos casos es inaccesible para los auditores.

- No se detectan paquetes que aborden de manera integral todos los pasos necesarios para realizar una auditoría, en general abordan una o algunas de las actividades necesarias para realizar esta tarea.

- Los paquetes relevados tienen un bajo nivel de adaptabilidad, por lo tanto su utilización en general se relaciona con las grandes empresas, quedando las pequeñas y medianas fuera del alcance de los mismos.

Capítulo 3

Problema

3. PROBLEMA

En este capítulo se desarrolla la descripción del problema (sección 2.1) de los auditores de sistemas a la hora de llevar adelante su tarea; y se define el objetivo del presente trabajo de tesis (sección 2.2).que resuelve la problemática detectada.

3.1. Descripción del problema

La auditoría de sistemas se puede definir como el proceso de revisión y evaluación, parcial o completo de los aspectos relacionados con el procesamiento automatizado de la información [ISACA, 2002].

En este proceso se aplican métodos, técnicas y procedimientos para evaluar los recursos de la tecnología de la información.

La auditoría de Sistemas comprende la evaluación formal y sistemática de todos los elementos relacionados con la tecnología de la información (TI), como: los datos, los sistemas de aplicación, la tecnología, las instalaciones, la gente; con el objetivo de garantizar el cumplimiento de las normas y procedimientos establecidos por la empresa en todo lo relacionado con la información y la tecnología de la información, de manera de minimizar los riesgos que amenacen la efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad de la información.

A la hora de realizar una auditoría de sistemas los profesionales responsables de esta actividad se encuentran con algunos de los siguientes problemas:

- ✓ Un importante porcentaje de profesionales que realizan esta tarea no son expertos en la misma, muchos de ellos realizan sus actividades en forma aislada, sin contacto con otros profesionales especialistas en la actividad.
- ✓ Desconocimiento de metodologías, técnicas y herramientas utilizadas para el proceso de auditoría de sistemas.
- ✓ Desconocimiento de estándares utilizados en el proceso de auditoría de sistemas.
- ✓ De acuerdo a estudios realizados la gran mayoría de auditorias de sistemas que se realizan en la actualidad no utilizan herramientas software que asistan integralmente a los auditores de sistemas en su tarea.

Los problemas descriptos provocan en muchos casos auditorias de baja calidad que no cubren los objetivos previstos.

3.2. Objetivo de la tesis

El objetivo del proyecto es diseñar la primer versión de una herramienta que asista desde el punto de vista metodológico al proceso de auditoría en lo relacionado con la determinación de alcances y objetivos, estudio preliminar, determinación de recursos necesarios, planificación, desarrollo, y presentación de conclusiones y permita la generación automática de documentación, considerando lo estándares existentes y adecuándolos al entorno a auditar.

La herramienta que se desarrollará permitirá resolver el siguiente problema detectado:

- ✓ La inexistencia de una herramienta software integrada y basada en la filosofía Open Source, que los asista desde el punto de vista metodológico, a los profesionales que realizan auditorías de sistemas.

Capítulo 4

Solución

Sección 4.1 - Planificación del Sistema de Información

4.1 PLANIFICACIÓN DEL SISTEMA DE INFORMACION

4.1.1. ACTIVIDAD PSI 1 - Inicio del Plan de Sistemas de Información

4.1.1.1. TAREA PSI 1.1 Análisis de la necesidad del Plan de Sistemas de Información.

- ***Descripción general del Plan de Sistemas de Información. Aprobación de inicio de PSI***

Este plan de Sistemas de Información tiene el objetivo de posibilitar al tesista la obtención del título de Magíster en Ingeniería del Software.

Un elemento crítico para el éxito y la supervivencia de las organizaciones, en esta sociedad global es la administración efectiva de la información y de la Tecnología de Información (TI) relacionada. Esta criticidad surge de:

- La creciente dependencia que tienen las organizaciones en la información que manejan y en los sistemas que proporcionan dicha información.
- La creciente vulnerabilidad y la gran cantidad de amenazas a las que se exponen los Sistemas de Información.
- El costo y la escala de las inversiones actuales y futuras en información y en Tecnología de información.
- El enorme potencial que tienen las tecnologías de la Información y las Comunicaciones para cambiar radicalmente las organizaciones y las prácticas de negocio.

Para muchas organizaciones, la información y la tecnología que la soporta, representan los activos más importantes y valiosos de la empresa.

En este marco se considera conveniente y necesario el desarrollo de un Software que asista al Auditor de Sistemas a desarrollar su tarea y de esta manera garantizar que la información cumpla con requerimientos de calidad, de reportes fiduciarios y de seguridad.

4.1.1.2. TAREA PSI 1.2 - Identificación del alcance del Plan de Sistemas de Información.

- ***Descripción general del Plan de Sistemas de Información, alcance y objetivos***

Los objetivos estratégicos relacionados con el PSI son:

- ✓ Lograr un estándar de calidad en el proceso de Auditoría de Sistemas, que posibilite a las organizaciones obtener información que les permitan minimizar los riesgos relacionados con el gobierno de la Tecnología de la Información.
- ✓ Lograr que el proceso de auditoría de Sistemas se adapte al entorno a auditar.
- ✓ Brindar una plataforma que permita independizar el sistema de las licencias comerciales.

Los Factores Críticos de Éxito son:

- ✓ Conocer en profundidad el Estándar COBIT
- ✓ Conocer las distintas alternativas tecnológicas relacionadas en el desarrollo de productos basados en la filosofía Open Source.
- ✓ Conocer en profundidad la metodología de desarrollo de Auditorías de Sistemas.
- ✓ Tener contacto permanente con Auditores para poder actualizar y mantener el sistema

4.1.1.3. TAREA PSI 1.3 Determinación de los responsables

- ***Descripción general de PSI - Responsables del Plan de Sistemas de Información***

Para la realización del presente proyecto se asigna como responsables a:

- ❖ Dr. Ramón García Martínez y M.Ing. María Alejandra Ochoa, quienes como Director y Directora adjunta del proyecto de tesis, serán los responsables de verificar y controlar el desarrollo del mismo.
- ❖ Lic. Horacio Daniel Kuna, quien como tesista, será el responsable de llevar adelante el proyecto en todas sus etapas.

4.1.2. ACTIVIDAD PSI 2 - Definición y Organización del Plan de Sistemas de Información

4.1.2.1. TAREA PSI 2.1. Especificación del ámbito y alcance

El presente Plan de Sistemas de Información tiene como objetivo el desarrollo de un sistema integral, desarrollado con herramientas Open Source, que asista desde el punto de vista metodológico al Auditor de Sistemas y que incorpore el estándar COBIT (Control Objectives for Information and related Technology), de la Fundación de Auditoría y Control de Sistemas de Información, que actualmente se utiliza en esta actividad.

Para esto se desarrollará un prototipo que funcionará en un entorno Web.

- ***Descripción General de los procesos afectados***

Objetivos generales

- Automatizar el proceso de auditoría informática
- Orientar al auditor en el proceso de auditoría de sistemas
- Incorporar los estándares existentes para la realización de auditorías de sistemas
- Adaptar el proceso de auditoría al entorno donde se desarrolla

4.1.2.2. TAREA PSI 2.2. – Organización del PSI

- ***Equipo de trabajo***

En la tabla 4.1. se especifica el equipo de trabajo.

Responsable del proyecto	Lic. Horacio Kuna
Seguimiento y control	Dr. García Martínez
Seguimiento y control	Ma.Ing. Alejandra Ochoa

Tabla 4.1.: Equipo de trabajo

4.1.2.3. TAREA PSI 2.3 - Definición del Plan de Trabajo

- ***Plan de Trabajo***

El plan de trabajo para el desarrollo del prototipo se lleva a cabo en base a la metodología Métrica III, la figura 4.1. detalla los tiempos estimados para la construcción del sistema.

ID	Task Name	Duration	Start	Finish
1	**Fases**	**284 days**	Mon 25/04/05	Thu 25/05/06
2	Planificación de Sistemas de Información	12 days	Mon 25/04/05	Tue 10/05/05
3	Estudio de viabilidad del Sistema	13 days	Wed 11/05/05	Fri 27/05/05
4	Analisis del sistema de Información	72 days	Mon 30/05/05	Tue 06/09/05
5	Diseño de Sistemas de Información	54 days	Wed 07/09/05	Mon 21/11/05
6	Construcción del sistema de Información	100 days	Tue 22/11/05	Mon 10/04/06
7	Implementación del Sistema de Información	33 days	Tue 11/04/06	Thu 25/05/06
8	**Interfaces**	284 days	Mon 25/04/05	Thu 25/05/06
9	Gestión de proyectos	284 days	Mon 25/04/05	Thu 25/05/06
10	Gestión de Configuración	259 days	Mon 30/05/05	Thu 25/05/06
11	Seguridad	247 days	Wed 15/06/05	Thu 25/05/06
12	Aseguramiento de la calidad	259 days	Mon 30/05/05	Thu 25/05/06

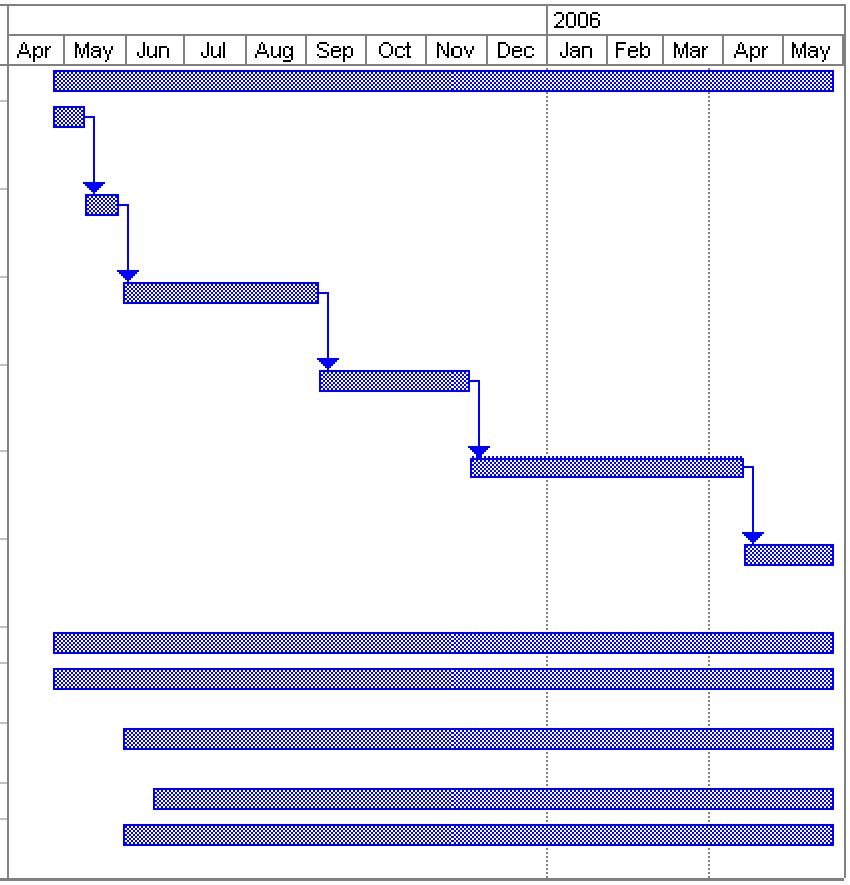


Figura 4.1.: Planificación del Sistema

Aclaración:

El plan de trabajo que se detalla en la Figura 4.1, es el resultado de haber realizado, utilizando las técnicas de Punto de Función y COCOMO, en la Interface de Gestión de proyectos.

4.1.2.4. TAREA PSI 2.4 Comunicación del Plan de Trabajo

- ***Aceptación del plan de trabajo***

Se ha realizado una reunión entre el tesista, cuya función es la de llevar adelante el presente desarrollo, y el Director, responsable de controlar el desarrollo del mismo, se ha aprobado y aceptado el plan de trabajo detallado en el punto anterior.

4.1.3. ACTIVIDAD PSI 3 - Estudio de la información relevante.

4.1.3.1. TAREA PSI 3.1 - Selección y Análisis de antecedentes

- ***Análisis de los antecedentes***

Se ha utilizado como antecedente del presente trabajo las tesis de Magíster en Ingeniería del Software presentadas por el Lic. Enrique Fernández [Fernández, ,2006], Ing. Alejandro Sueldo [Sueldo, 2006] y el Ing. Mario Peralta [Peralta, 2004], donde se aplicó en un proyecto concreto la metodología Métrica III. En estas tesis se ha observado que fases son necesarias de la metodología para el desarrollo de un proyecto de Tesis que no se enmarca en una empresa u organización en particular.

Las fuentes de Información de las que se basa este proyecto son:

- ✓ Código de Etica Profesional de la ISACA (Information Systems Audit and Control Association)
- ✓ Normas Generales de Auditoría de Sistemas de Información de la ISACA.
- ✓ Directivas de Auditoría de SI de la ISACA.
- ✓ Lineamientos de Auditoría de SI de la ISACA.
- ✓ Resumen ejecutivo de COBIT
- ✓ Descripción de la estructura COBIT
- ✓ Objetivos de Control COBIT
- ✓ Guías de Auditoría COBIT

4.1.3.2. TAREA PSI 3.2 - Valoración de los antecedentes

- ***Catálogo de Requisitos- Requisitos generales***

En este punto se detallan los requisitos generales del sistema.

- El sistema deberá servirle al auditor como un asistente en el proceso de auditoría informática.
- Deberá contemplar en forma completa la metodología que se utiliza en la auditoría de sistemas.
- Deberá considerar el estándar COBIT
- Deberá considerar las auditorías por áreas.
- Deberá desarrollarse en un entorno WEB
- Deberá desarrollarse con herramientas Open Source.

4.1.4. ACTIVIDAD PSI 4 - Identificación de Requisitos

4.1.4.1. TAREA PSI 4.1 – Estudio de los Procesos del PSI

Se estudia cada proceso de la organización incluido en el ámbito del Plan de Sistemas de Información. Para cada uno de ellos, es necesario identificar las actividades o funciones, la información implicada en ellas y las unidades organizativas que participan en el desarrollo de cada actividad.

Para obtener esta información es necesario llevar a cabo sesiones de trabajo con los usuarios implicados en cada uno de los procesos a analizar. Una vez contrastadas las conclusiones, se elabora el modelo correspondiente a cada proceso. Si existe relación entre los distintos modelos, se unifican en la medida de lo posible, con el fin de proporcionar una visión global en el contexto de la organización y facilitar una identificación de requisitos más objetiva.

Al tratarse de un proyecto que no se implementa sobre una organización en particular, esta tarea no se realiza. Pero se desarrolla para auditar el Proceso de Desarrollo de SI de cualquier organización, ya sean internos o externos. El proceso de la organización que se ve afectado es el de Desarrollo de SI.

4.1.4.2. TAREA PSI 4.2. – Análisis de las necesidades de Información

Mediante sesiones de trabajo, se identifican las necesidades de información de cada uno de los procesos analizados en la actividad anterior. Se elabora un modelo de información que refleje las principales entidades y relaciones existentes entre ellas. Todo esto se realiza con la perspectiva de lo que debe ser el proceso en cuanto a sus actividades y funciones, así como a la información de entrada y salida para cada una de ellas.

Los resultados del análisis realizado en esta tarea son la base para la identificación de requisitos.

Al tratarse de un proyecto que no se implementa sobre una organización en particular, esta tarea no se realiza. La información que se requiere en este proyecto es la de determinar si los procesos de desarrollo de SI se ajustan a algún estándar de calidad.

4.1.4.3 TAREA PSI 4.3 – Catalogación de Requisitos

- ***Catálogo de Requisitos – Requisitos de los procesos afectados por el PSI***

Los criterios utilizados para la asignación de las prioridades para los diferentes requisitos son los siguientes:

- Importante: aquellos requisitos para los que van a determinar la funcionalidad dada al sistema de información.
- Regular: son los requisitos que no definen la funcionalidad del sistema, pero sirven para realizar soporte a las actividades principales.
- No Importante: son aquellas funcionalidades que pueden ser canalizadas mediante la utilización de otras herramientas y que no se contempla en la creación del Sistema de Información.

En la tabla 4.2. se describen los principales requisitos que debe cumplir el sistema.

Número	Descripción	Importancia
1	El Sistema deberá emitir en forma automática una primer versión del informe final de auditoría	Importante
2	Permitir que usuarios remotos puedan operarlo utilizando como cliente un navegador	Importante
3	Deberá ser desarrollado con herramientas gratuitas basadas en la filosofía Open Source	Importante
4	El sistema deberá correr sobre diferentes sistemas operativos	Importante
5	El sistema deberá soportar el estándar COBIT	Importante

Número	Descripción	Importancia
6	El sistema deberá posibilitar el desarrollo de auditorías por áreas	Importante
7	El sistema deberá permitir definir el alcance de cada proyecto de auditoría	Importante
8	El sistema deberá permitir la carga de las tablas básicas	Importante
9	El sistema deberá registrar el estudio inicial	Importante
10	El sistema deberá proponer los recursos necesarios para realizar la auditoría	Importante
11	El sistema deberá sugerir la planificación de la auditoria de acuerdo al alcance.	Importante
12	El sistema deberá asistir al auditor en el desarrollo de la auditoría sugiriendo los distintos checklist.	Importante
13	El sistema deberá permitir el resguardo de la información	Regular
14	El sistema deberá controlar los accesos de los distintos perfiles de usuarios	Regular
15	El sistema deberá impedir que usuarios no autorizados accedan a información confidencial.	Regular
16	El sistema podrá integrarse con otras herramientas software que se utilizan en la auditoría de sistemas utilizadas en la auditor	No importante

Tabla 4.2.: Principales requisitos del sistema

4.1.5. ACTIVIDAD PSI 5 – Estudio de los Sistemas de Información Actuales

4.1.5.1 TAREA PSI 5.1 – Alcance y Objetivos del Estudio de los Sistemas de Información Actuales

- ***Catálogo de objetivos de PSI. Objetivos del estudio de los sistemas de información actuales***

Todos los sistemas que estén en producción y desarrollo dentro de la organización, serán sometidos a la evaluación mediante el software que se esta desarrollando.

4.1.5.2. Tarea PSI 5.2: Análisis de los Sistemas de Información Actuales

- ***Descripción general de SI actuales***

La auditoría de Sistemas debe realizarse sobre el conjunto de áreas y procesos relacionadas con la Tecnología de la Información que se desarrollan en una organización tanto pública como privada, incluyendo todos los Sistemas de Información que se encuentran en desarrollo o en producción.

4.1.5.3. Tarea PSI 5.3: Valoración de los sistemas de Información Actuales

- ***Valoración de la situación actual***

Con la excepción de los Bancos, las empresas internacionales y las grandes empresas de capital nacional se observa que el proceso de Auditoría de Sistemas no se realiza o se realiza sin tener en cuenta los estándares internacionales relacionados con la tarea, atentando esto con la calidad de los resultados que se obtiene.

4.1.6. ACTIVIDAD PSI 6 – Diseño del Modelo de Sistemas de Información

4.1.6.1. Tarea PSI 6.1: Diagnóstico de la situación actual.

- ***Diagnóstico de la situación Relación de sistemas de información que se conservan y mejoras necesarias***

Este Plan de Sistemas de Información no tiene como objetivo el reemplazo de ningún SI específico, sino someter el desarrollo, producción y gestión de los mismos a un proceso de auditoría.

4.1.6.2. Tarea PSI 6.2: Definición del Modelo de Sistemas de Información

- ***Modelo de Sistemas de Información.***

Se espera que los Sistemas de Información se vean mejorados después de aplicar el software a desarrollar, la figura 4.2. muestra el modelo al que se quiere arribar:

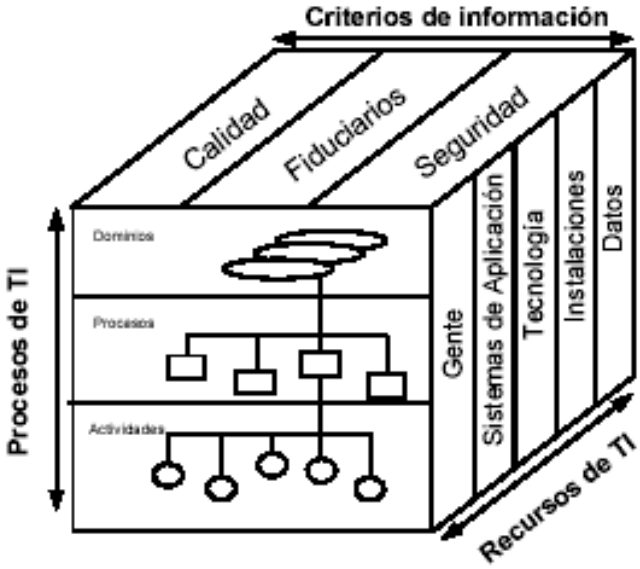


Figura 4.2.: Puntos estratégico de los SI

Donde los procesos relacionados con la Tecnología de la Información deben tener:

- Determinados criterios de información relacionados con la seguridad, calidad y fiduciarios.
- Relación con recursos de la TI como los sistemas de aplicación, las instalaciones, los datos, etc.
- Actividades que implican obtener Objetivos de Control, entendiendo a los mismos como una definición del resultado o propósito que se desea alcanzar implementando procedimientos de control en una actividad de TI particular.

4.1.7. ACTIVIDAD PSI 7 - Definición de la Arquitectura Tecnológica

4.1.7.1. TAREA PSI 7.1 - Identificación de las Necesidades de Infraestructura Tecnológica

Alternativas de Arquitectura Tecnológica

Alternativa 1 : Arquitectura WEB

Una aplicación web es aquella en que los usuarios acceden a un servidor web a través de Internet o de una intranet. Las aplicaciones web son populares debido a la practicidad del navegador web como cliente ligero, La habilidad

para actualizar y mantener aplicaciones web sin distribuir e instalar software en miles de potenciales clientes es otra razón de su potencialidad

Una ventaja mas importantes a considerar para la construcción de aplicaciones web, es que los browsers o navegadores funcionan igual independientemente de la versión del sistema operativo instalado en el cliente. En vez de crear clientes para Windows, Mac OS X, GNU/Linux, y otros sistemas operativos, la aplicación es escrita una vez y es mostrada casi en todos lados.

Una aplicación web está comúnmente estructurada con una arquitectura en tres-capas. Donde el web browser es la primer capa, un motor usando alguna tecnología web dinámica (ejemplo: CGI, PHP, Java Servlets o ASP) es la capa de en medio, y una base de datos como última capa. El web browser manda peticiones a la capa media, que la entrega valiéndose de consultas y actualizaciones a la base de datos generando una interfaz de usuario.

Alternativa 2: Arquitectura distribuida

Se caracteriza porque aparecen entornos informáticos departamentales adecuados a las necesidades de cada departamento en concreto. Sus características funcionales principales son :

- Cada usuario trabaja con su terminal local inteligente, con lo que obtiene mejores tiempo de respuesta.
- Los recursos necesarios que no estén disponibles sobre el terminal local pueden tomarse del ordenador central a través de la red de telecomunicaciones.

Características físicas

- ✓ Sistemas informáticos distribuidos en los que los ordenadores a través de la organización están conectados por medio de una red de telecomunicaciones.
- ✓ Cada ordenador sobre la red tiene capacidad de tratamiento autónomo que permite servir a las necesidades de los usuarios locales.
- ✓ También proporciona acceso a otros elementos de la red o a servidores centrales.
- ✓ Toma importancia la red de comunicación de datos.

Características lógicas

- Cada tarea individual puede ser analizada para determinar si puede distribuirse o no. En general, las tareas más complejas o de carácter estratégico para la organización se mantienen en el ordenador central. Las tareas de complejidad media o específicas para un determinado grupo de usuarios se distribuyen entre las máquinas locales de ese grupo.
- La plataforma física seleccionada puede ajustarse a las necesidades del grupo de usuarios, con lo que surgen los ordenadores especializados para determinados tipos de tareas.

4.1.7.2. TAREA PSI 7.2 - Selección de la Arquitectura Tecnológica

- ***Arquitectura Tecnológica***

Analizadas las dos propuestas y evaluadas las necesidades y el entorno en el cual el sistema se utilizará se opta por la Arquitectura WEB por las siguientes razones:

  - Las características técnicas de esta arquitectura se adaptan al entorno donde se espera se aplicará el sistema
  - No requiere instalaciones en los clientes.
  - Se puede desarrollar con herramientas Open Source.
  - No requiere en los clientes un sistema operativo en especial.
  - Soporta la arquitectura en tres capas
  - Es mas económica que la arquitectura distribuida
  - Su implementación es más sencilla.

4.1.8. ACTIVIDAD PSI 8 - Definición del Plan de Acción

4.1.8.1. TAREA PSI 8.1 Definición de proyectos a realizar

- ***Plan de proyectos***

No se incorpora a este trabajo de Tesis otro proyecto que no sea el “Asistente para la realización de auditoría de sistemas en organismos Públicos o Privados”, por esta razón este será el proyecto a implementar.

4.1.8.2. TAREA PSI 8.2 ELABORACION DEL Plan de Mantenimiento del PSI

- ***Plan de mantenimiento del PSI***

Se estableció entre el tesista y los directores , para que se realice la tarea de supervisión del proyecto, un mecanismo de comunicación cotidiano a través de los distintos servicios que brinda Internet, esto se debe a que el tesista reside en la provincia de Misiones a 1.100 Km. de la Ciudad de Buenos Aires; el

tesista enviará a los Directores la última versión de cada capítulo, que será evaluada y corregida.

Se establece un mecanismo de encuentros presenciales cada 30 días, donde se realizará un seguimiento general del proyecto.

Será responsabilidad del tesista el mantenimiento del versionado de la tesis a través de procedimientos que se aplicarán en la fase de Gestión de configuración de la metodología Métrica III.

4.1.9. ACTIVIDAD PSI 9 - Revisión y Aprobación del Plan de Sistemas de Información

4.1.9.1. TAREA PSI 9.1 - Convocatoria a la presentación

- ***Plan de presentación.***

Para la presentación del Plan de Sistemas de Información, se recopilan los resultados de las actividades desarrolladas en esta fase, Identificación de Requisitos, Definición de la Arquitectura Tecnológica y Definición del Plan de Acción. El Plan de Sistemas de Información es presentado a los Directores del proyectos para su estudio y aprobación.

4.1.9.2. TAREA PSI 9.2 - Evaluación y mejora de la propuesta.

- ***Evaluación y mejora.***

Se realizó una evaluación del proyecto con los Directores de la Tesis, donde se analizaron propuestas de mejoras relacionadas con la necesidad de acotar el prototipo a un tipo de auditoría en particular de manera de confirmar la efectividad y eficiencia del sistema, para en futuras etapas completar el desarrollo.

4.1.9.3. TAREA PSI 9.3 - Aprobación del PSI

- ***Aprobación Formal del plan de Sistemas de Información.***

En una reunión presencial realizada entre el tesista y los Directores del proyecto, estos últimos informaron la aprobación del presente PSI, para que de esta manera el tesista continúe con la fase siguiente del proyecto.

Capítulo 4

Solución

Sección 4.2 – Desarrollo del Sistema de Información

Capítulo 4

Solución

Sección 4.2.1 – Estudio de Viabilidad del Sistema

4.2.1. ESTUDIO DE VIABILIDAD

4.2.1.1. Actividad EVS 1. Establecimiento del alcance del sistema.

4.2.1.1.1. Tarea EVS 1.1. Estudio de la Solicitud

- ***Descripción General del Sistema***

El objetivo del sistema es asistir al auditor de sistemas en cada una de las fases de la tarea de auditoria.

- ***Catálogo de objetivos de EVS***

Los objetivos del Estudio de Viabilidad del sistemas son:

- ❖ Identificar el alcance del sistema
- ❖ Analizar las necesidades concretas del sistema
- ❖ Proponer una solución concreta
- ❖ Determinar la justificación económica del proyecto.
- ❖ Evaluar los riesgos del proyecto
- ❖ Evaluar las alternativas de solución.
- ❖ Seleccionar la mejor solución.

- ***Catálogo de requisitos***
  - ✓ Construir una herramienta software que permita facilitar, orientar y asistir al auditor en la determinación del alcance y los objetivos de la auditoría, en el estudio preliminar, en la determinación de los recursos necesarios, en el plan de trabajo, en el desarrollo de la auditoría y la elaboración del informe final.
  - ✓ Construir una herramienta que incorpore los estándares existentes en el mercado.
  - ✓ Contar con una herramienta que se adapte al contexto.

4.2.1.1.2 Tarea EVS 1.2. Identificación del Alcance del Sistema

- ***Descripción General del Sistema***
  - ✓ ***Contexto del sistema:*** Areas relacionadas con la Tecnología de la Información y Comunicaciones de las empresas, pudiéndose aplicar en cualquier entorno de desarrollo y producción.
  - ✓ ***Estructura organizativa:*** las unidades organizativas que se verán afectadas por el uso del nuevo sistema serán las relacionadas con la seguridad y calidad de los procesos y productos software.

- ***Catálogo de Requisitos. Requisitos Relativos a Restricciones o Dependencias con Otros Proyectos***

No existen restricciones, sincronización o dependencias con otros proyectos, como se explico en el Plan de Sistemas de Información solo se contempla el desarrollo de un solo proyecto.

- ***Catálogo de Usuarios***

Los posibles usuarios serán los auditores internos y externos de cualquier empresa u organismo, estatal o privado, en el caso de empresas que no realicen ningún tipo de auditoría de sistemas podrá utilizarse el asistente para realizar un autodiagnóstico relacionado con el ambiente de control de los Sistemas de Información, este autodiagnóstico no será una salida del asistente, sino que podrá ser sencillamente deducido a partir de los distintos check list que propondrá el sistema.

4.2.1.1.3.Tarea EVS 1.3: Especificación del Alcance del EVS

- ***Catálogo de los objetivos del EVS***
  - ✓ ***Objetivos del Estudio de la Situación Actual:*** El objetivo es investigar si existen en el mercado productos software que resuelven en forma integral los requisitos del sistema a construir de manera de determinar si se justifica el desarrollo propuesto.
- ***Catálogo de usuarios***

El estudio de viabilidad será desarrollado por el maestrando y supervisado y controlado por los directores de la Tesis.

- ***Plan de trabajo***

El Estudio de Viabilidad del Sistema contempla las siguientes actividades:

1. Estudio de las necesidades del sistema.

2. Relevamiento del estado del arte relacionado con las herramientas de Auditoría Asistidas por Computadora en el mercado local e internacional

3. Análisis de la viabilidad del sistema propuesto

4. Elaboración de las conclusiones.

5. Aprobación del EVS por parte de los directores de la Tesis

4.2.1.2. Actividad EVS 2. Estudio de la situación actual.

4.2.1.2.1.Tarea EVS 2.1.: Valoración del estudio de la situación actual.

- ***Descripción de la situación actual***

  - ***Contexto del sistema actual:*** La situación actual se caracteriza por sistemas de información cada vez más complejos, integrados y con uso intensivo de las nuevas tecnologías de la Información y comunicación que implican riesgos relacionados con la seguridad y calidad de la información que se genera y administra.
  - ***Descripción de los Sistema de Información actuales:***

Parte de esta actividad se desarrolló en el punto 2.6. “Auditoría asistida por computadora”.

A continuación se amplía esta información con la descripción funcional de sistemas relacionados con la Auditoría de sistemas:

❖ Software: Meycor COBIT CSA (Control Self-Assessment)

Es una herramienta de software que automatiza la evaluación de una organización contra los objetivos de control del marco COBIT, generando un diagnóstico y recomendaciones que facilitan la implementación de esos objetivos de control.

❖ Software: Meycor COBIT MG (MANAGEMENT GUIDELINES)

COBIT en su 3ra edición incorpora las Guías de Gerenciamiento (Management Guidelines), que incluyen un conjunto de herramientas formado por el Modelo de Maduración, los Factores Críticos de Éxito (CSFs), los Indicadores Clave de Meta (KGIs) y los Indicadores Clave de Desempeño (KPIs).

❖ Software: Gesia 2000

Las directrices y objetivos del GESIA 2000 no han sido otros que el de poner al alcance de los profesionales de la auditoría, y de forma muy especial de los responsables de despachos y firmas de auditoría, una herramienta que, acorde con las nuevas tecnologías, facilite su labor de organizar y controlar los trabajos.

❖ Software: ACL Edición de Escritorio / Red

ACL es la herramienta de software de auditoría preferida por la comunidad de auditoría interna internacional, para la extracción y el análisis de datos, la detección de fraudes y el control continuo. Al proporcionar una exclusiva y eficiente combinación de acceso a los datos, análisis y elaboración integrada de reportes, ACL permite transformar los datos en información significativa y asistirlo en el logro de objetivos comerciales para agregar valor a su organización.

❖ Software: 3 RD EDITION Management Advisor

COBIT 3 RD EDITION Management Advisor soporta análisis de brecha multi-nivel, permitiendo realizar un "benchmark" efectivo de los procesos de TI y analizar resultados de evaluaciones actuales versus anteriores en una base de datos única. Con su sofisticada función de alerta, provee un rastreo instantáneo de las áreas que requieren seguimiento, asegurando la disposición de la máxima cantidad de información con el toque de un botón.

❖ Software: COBIT Advisor 3 RD EDITION (Audit)

COBIT Advisor 3 RD EDITION (Audit) provee una aplicación consistente de la estructura COBIT; aplicable a todo tipo de empresas, permitiendo seguir las mejores prácticas para una administración efectiva de TI en la organización.

❖ Software: Idea Data Analysis Software

CaseWare IDEA (www.caseware-idea.com) es un software de PC bajo Windows en Español, muy fácil de usar, que permite que el Analista de datos o Auditor de Negocios acceda virtualmente a cualquier archivo de datos de cualquier entorno y analice el cien por ciento de miles o millones de transacciones en segundos detectando la totalidad de las excepciones y construyendo las propias bases de datos de Análisis de datos o Auditoría con datos completamente flexibles y de entornos diversos.

4.2.1.2.2.Tarea EVS 2.2: Identificación de los Usuarios Participantes en el Estudio de la Situación Actual

- ***Catalogo de usuarios***

Los responsables de realizar el Estudio de Viabilidad del Sistemas son:

- Maestrando: Lic. Horacio Kuna.
- Director de la Tesis. Dr. Ramón García Martínez.
- Codirectora: M.Ing. María Alejandra Ochoa.

4.2.1.2.3. Tarea EVS 2.3: Descripción de los Sistemas de Información Existentes

- ***Descripción de la situación actual:***

No se desarrolla un estudio detallado de los sistemas mencionados en el punto anterior por no considerar se necesario para realizar el estudio de Viabilidad del Sistema al no tener ninguno de ellos las características que se esperan del desarrollo que se propone realizar.

4.2.1.2.4. Tarea EVS 2.4: Realización del Diagnóstico de la Situación Actual

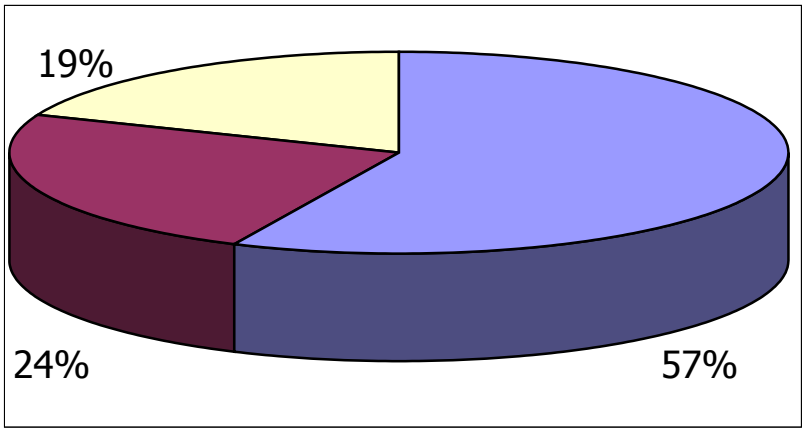
- ***Descripción de la situación actual***
  - ***Diagnóstico de la situación actual***

Se puede encontrar el diagnóstico en la tarea PSI 6.1: Diagnóstico de la Situación Actual, del Plan de Sistemas de Información, es importante agregar que en el ámbito nacional no se ha detectado asistentes integrados para la realización de auditoría de sistemas.

En lo relacionado con el desarrollo de auditorías de Sistemas un estudio, que se muestra en la figura 4.3. reciente de la Auditoría General de la Nación dio el siguiente resultado:

Situación General
Auditorías Internas Informáticas
Organismos Públicos de la Argentina

Auditores no especializados en TI



No se realizan Auditorías Internas de TI

Auditores especializados

Figura 4.3.: Auditorías De acuerdo a los resultados de Circ. 01-2002 –

Este estudio permite inferir que el desarrollo de Auditorías de Sistemas en la administración Pública nacional es muy bajo, casi el 60% de los organismos no realizan ningún tipo de auditoría.

En cuanto a la actividad privada de acuerdo a un relevamiento inicial realizado los porcentajes son aun más amplios en cuanto a la falta de auditoría de sistemas.

En lo relacionado al software relacionado con la auditoría de sistemas, se observa por un lado que no existe un software que asista al profesional en todas las fases del proceso de auditoría, si se detectan algunos que si abordan el análisis de una empresa desde los objetivos de control que se establecen en COBIT.

En lo relacionado al porcentaje de empresas que realizan esta tarea, sorprende el bajo porcentaje que lo realiza y que solo el 24% es realizado por profesionales formados en la materia.

Se detecta que ninguna herramienta software son desarrollados con productos Open Source.

4.2.1.3. Actividad EVS 3. Definición de los requisitos del sistema

4.2.1.3.1. Tarea EVS 3.1: Identificación de las Directrices Técnicas y de Gestión

- ***Catalogo de Normas:***

La tabla 4.3. muestra el conjunto de normas relacionadas con la auditoría de sistemas que se tienen en cuenta para este proyecto.

Nombre	Origen
Estándares de Auditoría – S1 a S9	ISACA
Directrices de Auditoría – G1 a G32	ISACA
Procedimientos de Auditoría – P1 a P9	ISACA
COBIT (Control Objectives for Information and related Technology)	Fundación de Auditoría y Control de Sistemas de Información.

Tabla 4.3.: Normas de auditoría

4.2.1.3.2. *Tarea EVS 3.2: Identificación de Requisitos*

- **Identificación de requisitos**
  - Asistir al auditor en el proceso de **determinación del alcance y objetivos**, guiándolo a través de cuestionarios específicos, de acuerdo al tipo de organización que se trate, que permitan orientarlo metodológicamente en el proceso de definición del alcance y los objetivos generales y específicos.
  - Asistir al auditor en el **estudio preliminar**, proponiéndole cuestionarios que permitan definir, considerando el alcance y objetivos definidos en el punto anterior, la estructura interna del Área de Informática a auditar, las aplicaciones existentes, el personal relacionado con la tarea, el inventario y arquitectura del hardware y software, la documentación existente, las características de las telecomunicaciones, la cantidad y características de las bases de datos, etc.

- El asistente en función de los objetivos, alcance y el estudio preliminar deberá sugerirle al auditor **los recursos** necesarios para realizar la tarea.
- Asistir al proceso de **planificación** adaptando la misma a la organización específica donde se intenta realizar la tarea, proponiendo de acuerdo a los pasos anteriormente desarrollados un plan de trabajo tentativo.
- Asistir en el **desarrollo** de la auditoría, sugiriendo distintos cuestionarios y cheklist para cada una de las áreas a auditar (desarrollo, producción, redes, gestión, etc.), definiendo los objetivos de control de acuerdo a las características de la organización.
- El asistente deberá orientar al auditor en la elaboración del **informe final** considerando las tareas realizadas anteriormente.
- Se analizará la factibilidad de integrar el asistente con otros software específicos como por ejemplo el IDEA [IDEA, 2004], Magerit [MAGERIT, 2004]. MSPROJECT, etc.
- La herramienta se desarrollará dentro del ambiente OPEN Source, ejecutable en cualquier sistema.
- El sistema deberá impedir el acceso no autorizado a los datos.
- La velocidad de acceso deberá ser razonable
- Se deberá desarrollar en un entorno web.
- Deberán existir perfiles de usuarios.

4.2.1.3.3. *Tarea EVS 3.3: Catalogación de Requisitos*

- ***Catalogo de requisitos***

La tabla 4.4 muestra el catalogo de requsitos:

Requisito	Tipo	Prioridad
Asistir al auditor en el proceso de **determinación del alcance y objetivos**	Funcional	Alta
Asistir al auditor en el **estudio preliminar**	Funcional	Alta
El asistente en función de los objetivos, alcance y el estudio preliminar deberá sugerirle al auditor **los recursos** necesarios para realizar la tarea.	Funcional	Alta

Asistir al proceso de **planificación** .	Funcional	Alta
Asistir en el **desarrollo** de la auditoría	Funcional	Alta
El asistente deberá orientar al auditor en la elaboración del **informe final** considerando las tareas realizadas anteriormente.	Funcional	Alta
Se analizará la factibilidad de integrar el asistente con otros software específicos como por ejemplo el IDEA, MAGERiT. MSPROJECT, etc.	No Funcional	Baja
La herramienta se desarrollará dentro del ambiente OPEN Source, ejecutable en cualquier sistema.	No Funcional	Alta
El sistema deberá impedir el acceso no autorizado a los datos.	No Funcional	Alta
La velocidad de acceso deberá ser razonable	No Funcional	Baja
Se deberá desarrollar en un entorno web.	No Funcional	Alta
Deberán existir perfiles de usuarios.	No Funcional	Baja

Tabla 4.4.: Catalogo de requisitos

4.2.1.4. Actividad EVS 4: Estudio de alternativas de solución.

4.2.1.4.1. *Tarea EVS 4.1: Preselección de Alternativas de Solución*

- ***Descomposición inicial del sistema en subsistemas***

Los subsistemas que se espera que tenga el Software son:

Alternativa 1:

- Subsistema de **Alcance y Objetivos,** donde se realiza la parametrización general del sistema y se inicia la auditoría.
- Subsistema de **Estudio preliminar**: donde se realiza el estudio inicial del entorno a auditar.

- Subsistema de **recursos**: donde se determinan los recursos necesarios para hacer la auditoría.
- Subsistema de **planificación**: Donde se realiza el plan de trabajo
- Subsistema de **desarrollo**: Donde se realiza la auditoría.
- Subsistema de **interface:** Donde se integra en forma automática con otras herramientas software como el IDEA, o el MS Project.
- Subsistema de **informe final**: donde se elabora el informe final.

Alternativa 2:

- Subsistema de **Alcance y Objetivos,** donde se realiza la parametrización general del sistema y se inicia la auditoría.
- Subsistema de **Estudio preliminar**: donde se realiza el estudio inicial del entorno a auditar.
- Subsistema de **recursos**: donde se determinan los recursos necesarios para hacer la auditoría.
- Subsistema de **planificación**: Donde se realiza el plan de trabajo
- Subsistema de **desarrollo**: Donde se realiza la auditoría.
- Subsistema de **informe final**: donde se elabora el informe final.

- ***Alternativas de solución a estudiar***

De acuerdo a lo investigado en relación a sistemas existentes en el mercado vinculados con la asistencia integral al auditor de sistemas desde el punto de vista metodológico, no se ha encontrado ningún sistema que tenga las características funcionales y no funcionales esperadas, en particular no se ha encontrado en el mercado una herramienta que abarque toda la metodología de desarrollo de auditorías de sistemas en un entorno WEB y basado en herramientas Open Source. Por tal motivo la única alternativa viable para cubrir la necesidad planteadas en este proyecto es la construcción de un Software a tal efecto.

4.2.1.4.2. Tarea EVS 4.2: Descripción de las Alternativas de Solución

- ***Alternativas de solución a estudiar.***

Se definió como única alternativa viable la construcción de un nuevo sistema, para ello se han definido los requisitos funcionales y no funcionales que componen el mismo, a continuación se detallan dos alternativas de solución posibles para el producto:

- ❖ Alternativa 1: Construir un producto que se integre en forma automática con las herramientas ya existentes en el mercado como el MsProject de Microsoft, IDEA o el ACL.
- ❖ Alternativa 2: Construir un producto que no se integre, en esta primer versión con otros productos ya existentes en el mercado.

4.2.1.5. Actividad EVS 5: Valoración de las alternativas

4.2.1.5.1. Tarea EVS 5.1: Estudio de la Inversión

- ***Valoración de alternativas:***
  - ***Impacto en la organización de alternativas:***

    Alternativa 1: En el proceso de Auditoría se utilizaría una única herramienta software para asistir al Auditor de sistemas en su tarea.

    Alternativa 2: En el proceso de Auditoría se utilizaría más de una herramienta software para asistir al auditor de sistemas en su tarea.

  - ***Costo /Beneficio de las alternativas.***

    ❖ Alternativa 1: Construir un producto que se integre en forma automática con las herramientas ya existentes en el mercado como el MsProject de Microsoft, IDEA e el ACL. La tabla 4.5. muestra los costos y beneficios de esta alternativa:

Costo	*Beneficio*
Mayor tiempo de desarrollo	Mayor funcionalidad
Licencias de productos comerciales	
Estudio de las alternativas de integración de herramientas	

Tabla 4.5.:Costo beneficio alternativa 1

❖ Alternativa 2: Construir un producto que no se integre, en esta primer versión con otros productos ya existentes en el mercado. La tabla 4.6. muestra los costos y beneficios de esta alternativa:

Costo	*Beneficio*
Menor funcionalidad	Menor tiempo de desarrollo
	Software basado completamente en herramientas open source, por lo

	tanto no hay costo de licencias.

Tabla 4.6.:Costo beneficio alternativa 2

4.2.1.5.2. Tarea EVS 5.2: Estudio de los Riesgos

- ***Valoración de alternativas***
  - ❖ ***Valoración de Riesgos***

La valoración se establece de 0 a 5, donde 5 es el máximo valor del riesgo. La tabla 4.7. representa los riesgos de las dos alternativas evaluadas.

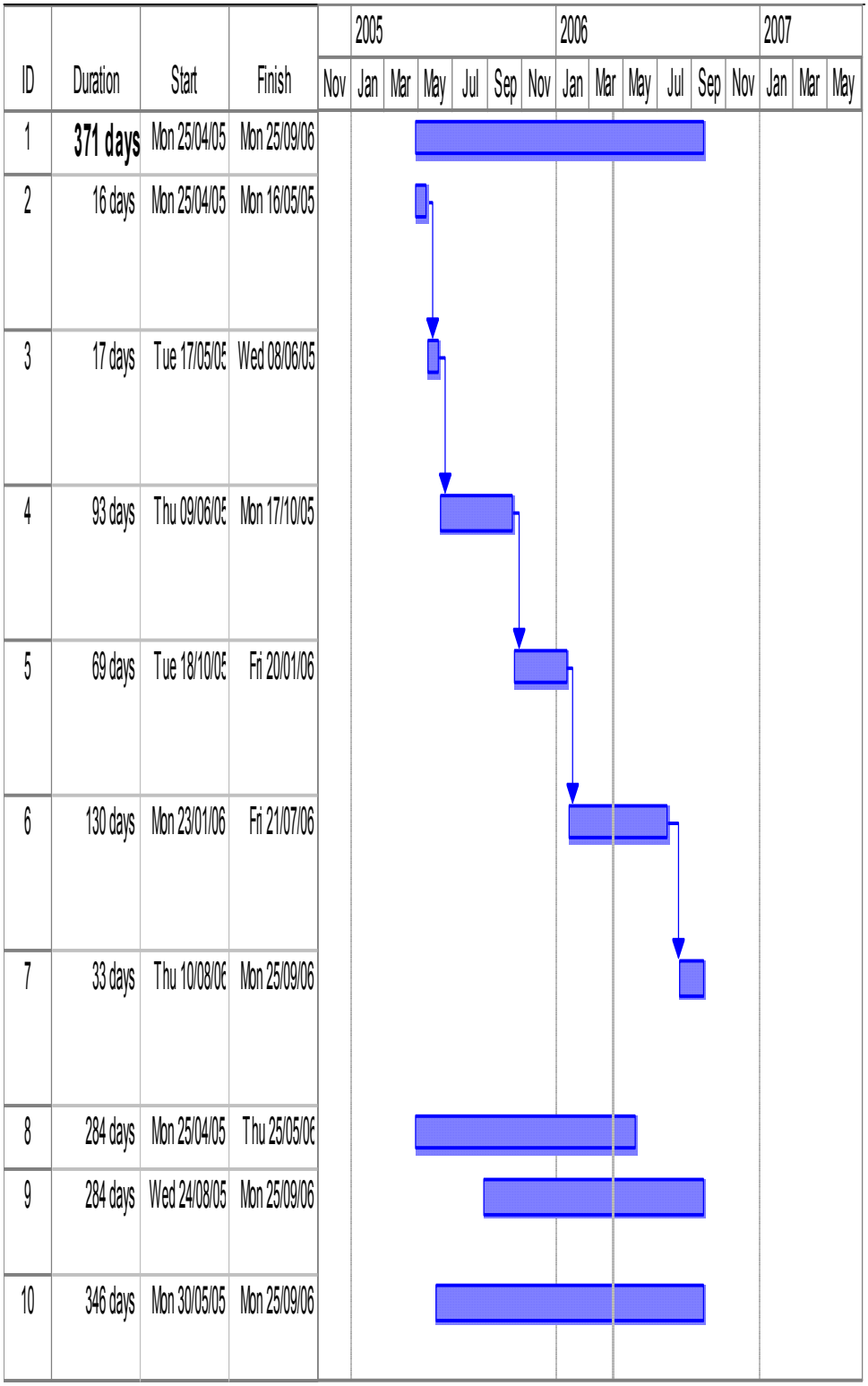
Riesgo	Valoración Alternativa 1	Valoración Alternativa 2
Falta de financiamiento para la adquisición de licencias para el desarrollo.	5	0
Problemas de integración entre módulos	4	1
Tiempo de desarrollo que excede la planificación	4	2
Curva de aprendizaje importante	5	2
Utilización de otras herramientas en el proceso de auditoría	3	5
Total	**21**	**10**

Tabla 4.7.:Riesgos de las alternativas

4.2.1.5.3. Tarea EVS 5.3: Planificación de Alternativas

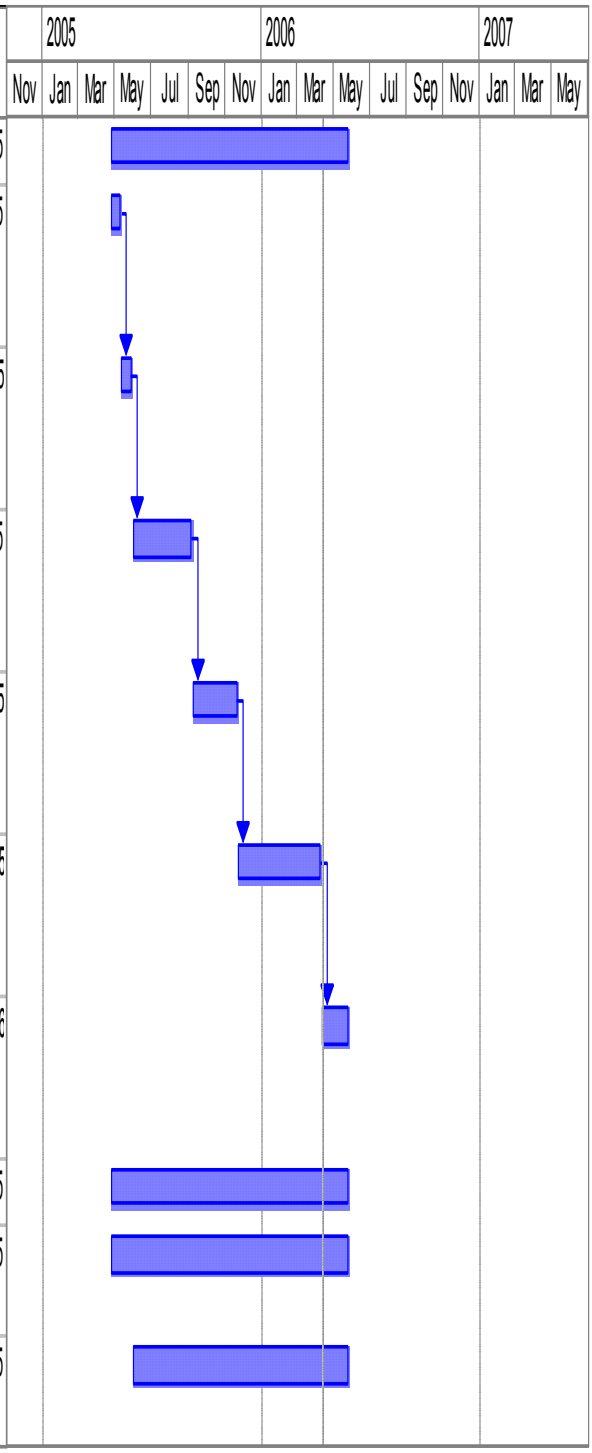
- **Plan de trabajo de cada alternativa**

Alternativa 1:



Alternativa 2:

ID	TaskName	Duration	Start
1	**Fases**	**284 days**	Mon 25/04/05
2	Planificación de Sistemas de Información	12 days	Mon 25/04/05
3	Estudio de viabilidad del Sistema	13 days	Wed 11/05/05
4	Analisis del sistema de Información	72 days	Mon 30/05/05
5	Diseño de Sistemas de Información	54 days	Wed 07/09/05
6	Construcción del sistema de Información	100 days	Tue 22/11/05
7	Implementación de Sistema de Información	33 days	Tue 11/04/06
8	**Interfaces**	284 days	Mon 25/04/05
9	Gestión de proyectos	284 days	Mon 25/04/05
10	Gestión de Configuración	259 days	Mon 30/05/05



4.2.1.6. ACTIVIDAD EVS 6: SELECCIÓN DE LA SOLUCIÓN

4.2.1.6.1. Tarea EVS 6.1: Convocatoria de la Presentación

- ***Plan de presentación de alternativas***

Se convocó a una reunión entre el tesista y los Directores del , en donde el tesista explicó las dos alternativas de solución posibles, con sus riesgos, costo/beneficio y plan de trabajo.

4.2.1.6.2. Tarea EVS 6.2: Evaluación de las Alternativas y Selección

- ***Solución propuesta***

Después de realizarse la reunión entre el tesista y los Directores del proyecto, se ha resuelto, para el primer prototipo a construir, a la alternativa dos, construir un producto que no se integre con software comercial ya existente. Esto es debido a que se considera a la misma como la más viable considerando que es la que tiene menor riesgo, menor tiempo de desarrollo, menores costos y que cubre las necesidades iniciales del proyecto. Se establece que esta integración podrá realizarse en futuras versiones.

4.2.1.6.3. Tarea EVS 6.3: Aprobación de la Solución

- ***Tarea EVS 6.3: Aprobación de la Solución***

Se realizó una reunión entre el tesista y los directores donde se da su aprobación formal a la alternativa que propone desarrollar un producto que en esta instancia no se integra en forma automática con otros software comerciales.

Capítulo 4

Solución

Sección 4.2.2. – Análisis del Sistema de Información

4.2.2. ANÁLISIS DEL SISTEMA DE INFORMACIÓN

4.2.2.1. Actividad ASI 1: Definición del Sistema

4.2.2.1.1.Tarea ASI 1.1: Determinación del Alcance del Sistema

- ***Catálogo de requisitos***

Se evaluaron los requisitos especificados en la tarea EVS 3.3. y se consideró que los requisitos especificados son los adecuados, dándose por válidos el catálogo de requisitos definido en el Estudio de Viabilidad.

- ***Contexto del sistema***

La figura 4.5 muestra el contexto del sistema

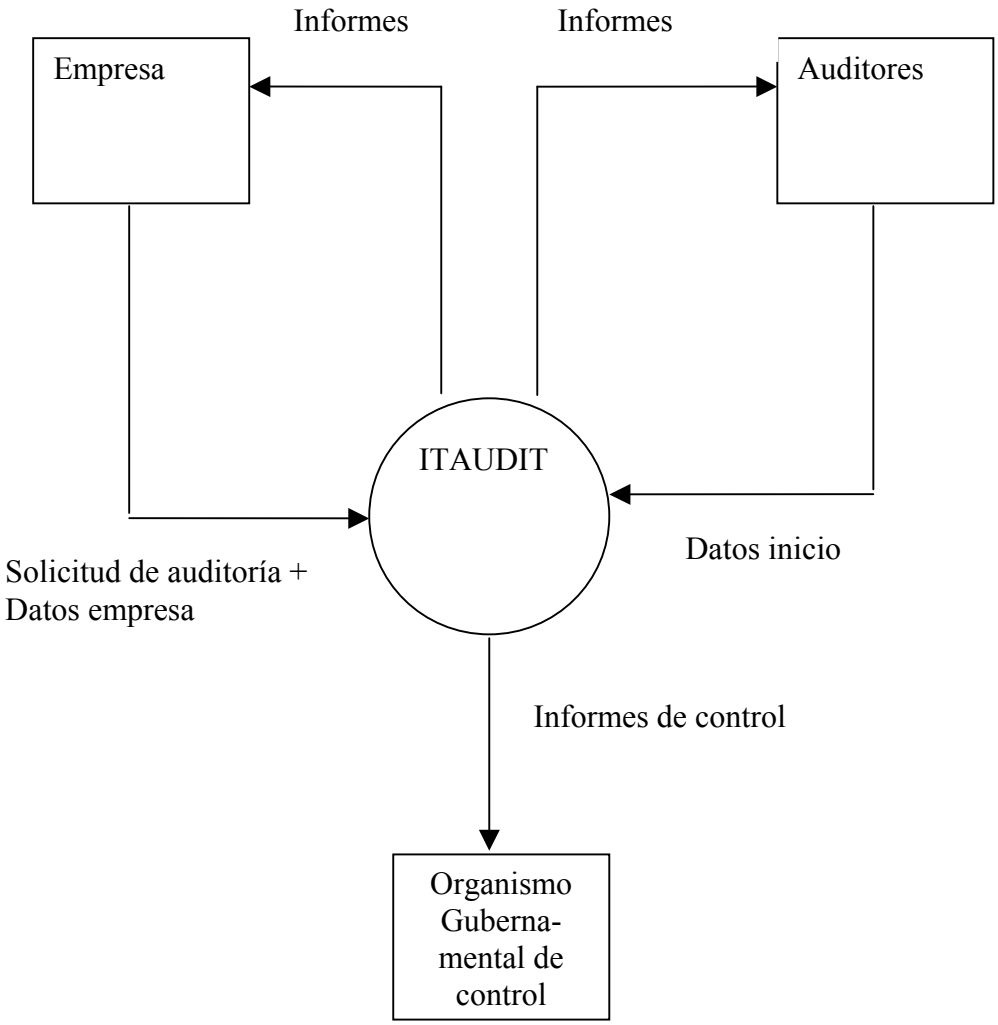


Figura 4.5. Diagrama de contexto

La metodología se utilizará es la estructurada, por lo tanto las tareas específicas asociadas a la metodología de Orientada a Objetos, no serán desarrolladas.

- ***Modelo Conceptual de datos.*** La figura 4.6. muestra el modelo conceptual de datos.

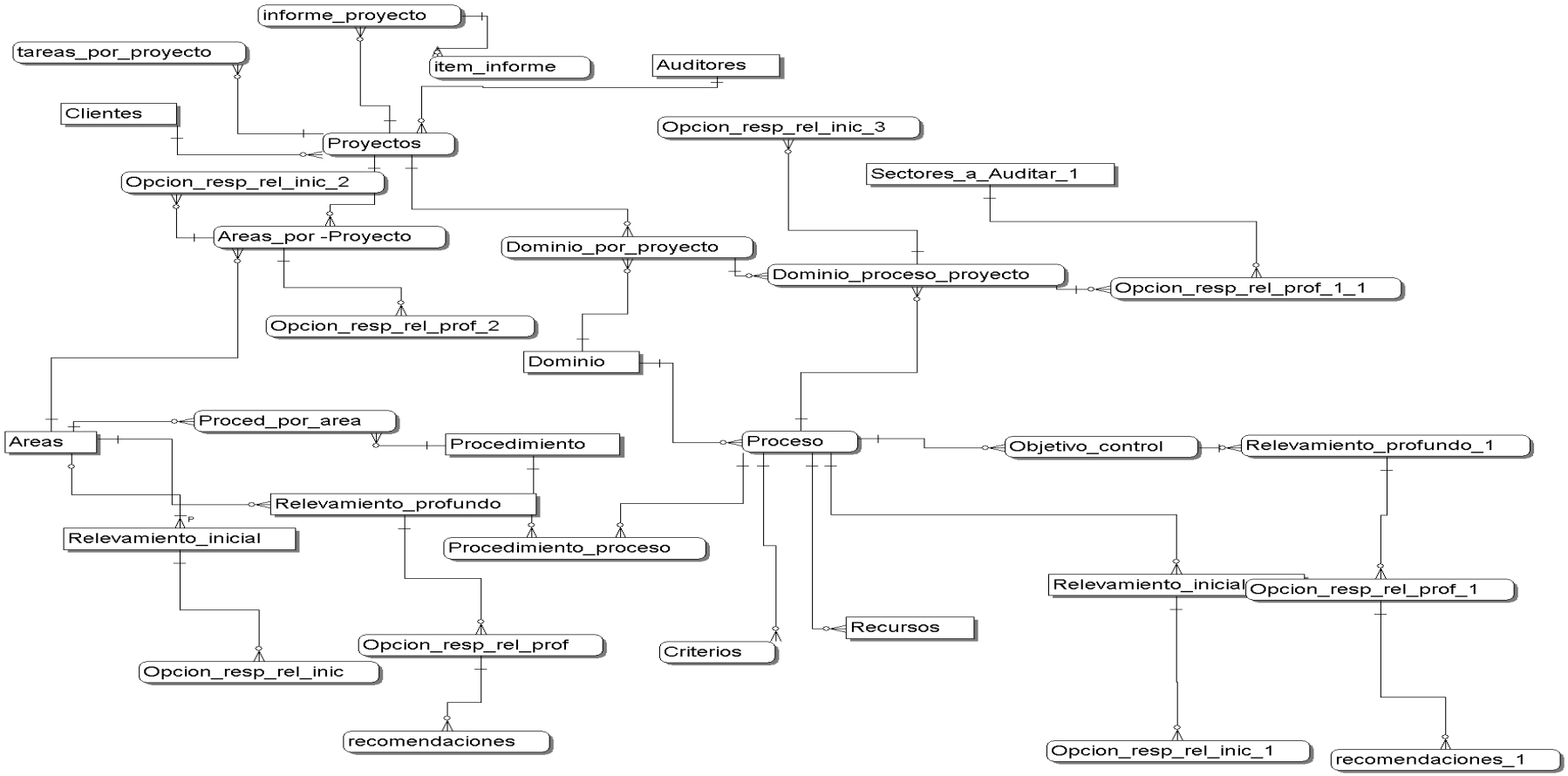


Figura 4.6. Modelo conceptual de datos

- ***Glosario de términos***

La tabla 4.8. muestra el glosario de términos relacionados con la auditoría de sistema:

Termino	Significado
COBIT	Control Objectives for Information and related Technology
AICPA	Instituto Americano de Contadores Públicos Certificado. (*American Institute of Certified PublicAccountants)*
CCEB	Criterios comunes para seguridad en tecnología de información. (*Common Criteria for Information Technology Security)*
CICA	Instituto Canadiense de Contadores. (*Canadian Institute of Chartered Accountants*)
CISA	Auditor Certificado de Sistemas de Información. (*Certified Information Systems Auditor*)
Control	Políticas, procedimientos, prácticas y estructuras organizacionales, diseñados para proporcionar una seguridad razonable de que los objetivos del negocio serán alcanzados y que eventos no deseados serán prevenidos o detectados y corregidos.
COSO	Comité de Organizaciones Patrocinadoras de la Comisión de Intercambio. "Tradeway" (*Committee of Sponsoring Organizations of the Tradeway Commission).*
DRI	Instituto Internacional de Recuperación de Desastres. (*Disaster Recovery Institute International*)
DTI	Departamento de Comercio e Industria del Reino Unido. (*Department of Trade and Industry of the United Kingdom)*
EDIFACT	Intercambio Electrónico de Datos para la Administración, el Comercio y la Industria (*Electronic Data Interchange for Administration, Comerse and Trade*)
EDPAF	Fundación de Auditores de Procesamiento Electrónico de Datos (*Electronic Data Processing Auditors Foundation*), ahora **ISACF**.
ESF	Foro Europeo de Seguridad (*European Security Forum*), cooperación de 70+ multinacionales europeas principalmente con el propósito de investigar problemas de seguridad y control comunes de TI.
GAO	Oficina General de Contabilidad de los EUA. (*U.S. General Accounting Office*)
I4	Instituto Internacional de Integridad de Información. (*International Information Integrity Institute*), asociación similar a ESF, con metas similares, pero con base principalmente en los Estados Unidos y dirigida por el Instituto de Investigaciones de Stanford (*Stanford Research Institute)*
IBAG	Grupo Consultivo de Negocios Infosec (*Infosec Business Advisory Group*), representantes de la industria que asesoran al Comité Infosec. Este Comité está compuesto por funcionarios de los gobiernos de la Comunidad Europea y asesora a la Comisión Europea sobre cuestiones de seguridad de TI.
IFAC	Federación Internacional de Contadores. (*International Federation of Accountants*)
IIA	Instituto de Auditores Internos. (*Institute of Internal Auditors*)
INFOSEC	Comité Consultivo para la Comisión Europea en Materia de Seguridad TI. (*Advisory Committee for IT Security Matters to the European Commission*)
ISACA	Asociación para la Auditoría y Control de Sistemas de Información. (*Information Systems audit. and Control Foundation)*

ISACF	Fundación para la Auditoría y Control de Sistemas de Información. (*Information Systems audit. and Control Foundation)*
ISO	Organización de Estándares Internacionales. (*International Standards Organisation*) (con oficinas en Génova, Suiza)
ISO9000	Estándares de manejo y aseguramiento de la calidad definidos por ISO.
ITIL	Biblioteca de Infraestructura de Tecnología de Información. (*Information Technology Infrastructure Library)*
ITSEC	Criterios de Evaluación de Seguridad de Tecnología de Información (*Information Technology Security Evaluation Criteria*). Combinación de los criterios de Francia, Alemania, Holanda y Reino Unido, soportadas consecuentemente por la Comisión Europea (ver también TCSEC, el equivalente en los Estados Unidos).
NBS	Departamento Nacional de Estándares de los Estados Unidos (*National Bureau of Standards of the U.S.)*
NIST	**(antes NBS)** Instituto Nacional de Estándares y Tecnología. (*National Institute of Standards and Technology*), con base en Washington D.C.
Objetivo de	Declaración del resultado deseado o propósito a ser alcanzado al implementar
Control de TI	procedimientos de control en una actividad particular de TI.
OECD	Organización para la Cooperación y el Desarrollo Económico. (*Organisation for Economic Cooperation and Development*)
OSF	Fundación de Software Público (*Open Software Foundation*)
PCIE	Consejo Presidencial de Integridad y Eficiencia. (*President´s Council on Integrity and Efficiency*)
TCSEC	Criterios de Evaluación de Sistemas Computarizados Confiables. (*Trusted Computer System Evaluation Criteria*), conocido también como "*The Orange Book*". Criterios de evaluación de seguridad para sistemas computarizados definidos originalmente por el Departamento de Defensa de los Estados Unidos. Ver también ITSEC, el equivalente europeo.
TickIT	Guía para la Construcción y Certificación de Sistemas de Administración de Calidad. (Guide to Software Quality Management System Construction and Certification)
COSO	*Committee of Sponsoring Organisations of the Treadway Commisssion InternalControl-Integrated Framework*, 1992

Tabla 4.8. Descripción tablas del modelo conceptual

4.2.2.1.2.Tarea ASI 1.2: Identificación del Entorno Tecnológico

- ***Catálogo de requisitos:***

  - Se deberá utilizar herramientas basadas en la filosofía Open Source.
  - Se deberá desarrollar en un entorno web seguro.

- ***Entorno tecnológico:***
  - Servidor web
  - Servidor de Internet
  - Servidor de base de datos y aplicación

- Sistema operativo Linux
- Lenguaje de programación Open Source
- Entorno de desarrollo Open Source

4.2.2.1.3.Tarea ASI 1.3: Especificación de Estándares y Normas

- ***Catálogo de normas:***

Son válidas las especificadas en EVS 3.1 Identificación de las Directrices Técnicas y de Gestión.

4.2.2.1.4.Tarea ASI 1.4: Identificación de los Usuarios Participantes y Finales

- ***Catálogo de usuarios***

Son válidos los que se describen en la tarea PSI 2.2. – Organización del PSI

- ***Plan de trabajo***

El plan de trabajo incluirá las tareas definidas para completar la etapa de

Análisis, siguiendo los lineamientos establecidos en de Métrica III.

- Actividad ASI 1: Definición del sistema.
- Actividad ASI 2: Establecimiento de requisitos.
- Actividad ASI 3: Identificación de subsistemas de análisis.
- Actividad ASI 6: Elaboración del modelo de datos.
- Actividad ASI 7: Elaboración del modelo de procesos.
- Actividad ASI 8: Definición de interfaces de usuario.
- Actividad ASI 9: Análisis de consistencia y especificación de requisitos.
- Actividad ASI 10: Especificación del plan de pruebas.
- Actividad ASI 11: Aprobación del análisis del sistema de información.

4.2.2.2. Actividad ASI 2: Establecimiento de requisitos

4.2.2.2.1. Tarea ASI 2.1: Obtención de Requisitos

- ***Catálogo de requisitos***

La tabla 4.9. muestra las entrevistas realizadas

Numero de sesión	Entrevistado	Tema
1	Dr. Carlos Ferarris	Definición del problema, metodología para la auditoría de sistemas, uso del ordenador
2	Dr. Carlos Ferarris	Uso de estándares en la auditoría, COBIT
3	Dr. Carlos Ferarris	Auditoría en organismos públicos y privados
4	Dr. Carlos Ferarris	Uso de software en el proceso de auditoría
1	Ing. Horacio Masachesi	Definición del problema, metodología para la auditoría de sistemas, uso del ordenador
2	Ing. Horacio Masachesi	Definición del alcance y objetivos de la auditoría
3	Ing. Horacio Masachesi	Estudio preliminar y su relación con el alcance de la auditoría
4	Ing. Horacio Masachesi	Determinación de recursos y planificación, su relación con las etapas anteriores
5	Ing. Horacio Masachesi	Desarrollo de la auditoría y su relación con las etapas anteriores
6	Ing. Horacio Masachesi	Informe final y su relación con las etapas anteriores.

Tabla 4.9: entrevistas

La entrevista inicial con cada uno de los especialistas fue no estructurada y el objetivo fue precisar el problema, el resto de las entrevistas fue semiestructurada. Como resultado de las entrevistas y del análisis de la documentación se relevaron preguntas relacionadas con el proceso de auditoría *(ver anexo 3, cuestionarios*) y se clasificaron estas preguntas (*ver anexo 4, check list)*

- *Requisitos funcionales*

- Definir el Alcance y Objetivos del proceso de auditoría.
- Desarrollar el estudio preliminar en función del alcance de la auditoría planteada.
- Definir los recursos necesarios para realizar la auditoría.
- Desarrollar una planificación acorde con el alcance de la auditoría, las características de la empresa a auditar y el personal asignado a la tarea.
- Desarrollar la auditoría considerando el alcance, las características de la empresa a auditar, los recursos asignados y la planificación realizada.
- Realizar el informe final de la auditoría considerando las recomendaciones que surgen a partir de las respuestas a los check list realizados durante la auditoría.

❖ *Requisitos de rendimiento*

- Se debe tener un tiempo de respuesta razonable. Estimándose que este tiempo de respuesta no debe ser mayor a 10 segundos.

❖ *Seguridad*

- Se requiere que sea posible definir usuarios y perfiles para cada uno de esos perfiles

❖ *Implantación*

- No se observan requisitos especiales para la implantación

❖ *Disponibilidad del sistema*

- Se requiere que se pueda disponer del sistema sin necesidad de realizar una instalación especial para operarlo.
- Se debe poder acceder desde ordenadores sin mucha capacidad de memoria y almacenamiento. Se estima que los clientes deben tener un procesador Pentium III o superior, un mínimo de memoria de 128 Mb y un disco rígido de 40 Gb.

4.2.2.2.2. Tarea ASI 2.2 Especificación de casos de uso.

Esta tarea es obligatoria en el caso de orientación a objetos, y opcional en el caso de análisis estructurado, como apoyo a la obtención de requisitos.

El objetivo de esta tarea es especificar cada caso de uso identificado en la tarea anterior, desarrollando el escenario.

- *Para completar los casos de uso, es preciso especificar información relativa a:*
- *Descripción del escenario, es decir, cómo un actor interactúa con el sistema, y cual es la respuesta obtenida.*
- *Precondiciones y poscondiciones.*
- *Identificación de interfaces de usuario.*
- *Condiciones de fallo que afectan al escenario, así como la respuesta del sistema (escenarios secundarios).*

En escenarios complejos, es posible utilizar como técnica de especificación los diagramas de transición de estados, así como la división en casos de uso más simples, actualizando el modelo de casos de uso.

Para la obtención de esta información es imprescindible la participación activa de los usuarios.

No corresponde desarrollar dado que no se implementa orientación a objetos.

4.2.2.2.3. *Tarea ASI 2.3: Análisis de Requisitos*

- ***Catalogo de requisitos***

No se han detectado inconsistencias ni ambigüedades, por lo tanto la especificación realizada en ASI 2.1, es válida.

4.2.2.2.4. *Tarea ASI 2.4: Validación de Requisitos*

- ***Catalogo de requisitos***

Se distribuyó a los usuarios del sistema el Catálogo de Requerimientos, con el objetivo que los estudien y validen, y de ser necesario hagan las recomendaciones que consideren. Al no detectarse nuevos requisitos, el Catálogo de requisitos sigue siendo válido.

Luego del análisis por parte de los usuarios de los mismos, no surgieron modificaciones , por se cierra la tarea completada con el acuerdo de los usuarios.

4.2.2.3. Actividad ASI 3: Identificación de Subsistemas de Análisis

4.2.2.3.1. Tarea ASI 3.1: Determinación de Subsistemas de Análisis

- ***Subsistemas***

El objetivo de esta actividad se relaciona con descomponer el sistema en subsistemas.

✓ Subsistema de **Configuración:** este módulo permite la carga de las tablas básicas, auditores, permite la carga inicial de una matriz de preguntas general, y parámetros del sistema. La figura 4.7 muestra la descomposición funcional de este subsistema.

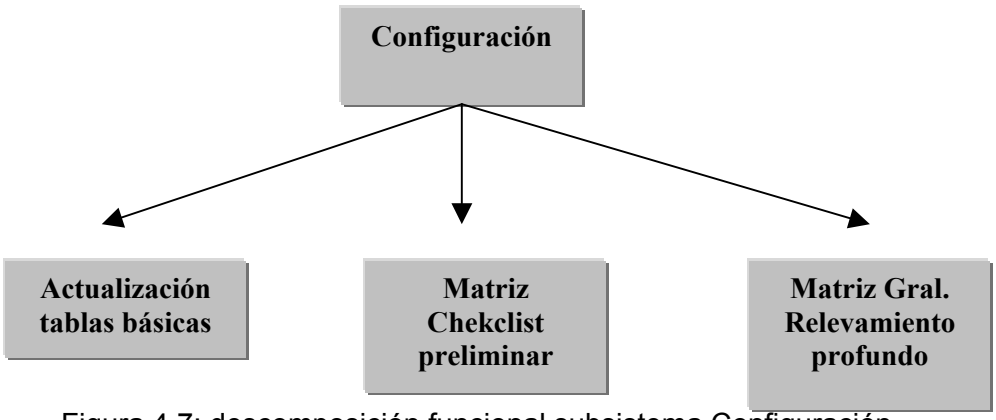


Figura 4.7: descomposición funcional subsistema Configuración

✓ Subsistema de **Inicio de la auditoría**: este módulo asiste al auditor en el proceso de determinación del alcance y objetivos, guiándolo a través de cuestionarios específicos, de acuerdo al tipo de organización que se trate, que permitan orientarlo metodológicamente en el proceso de definición del alcance y los objetivos generales y específicos. Este módulo permite el ingreso de los datos de la empresa , los auditores y los datos del proyecto.

La figura 4.8 muestra la descomposición funcional de este subsistema.

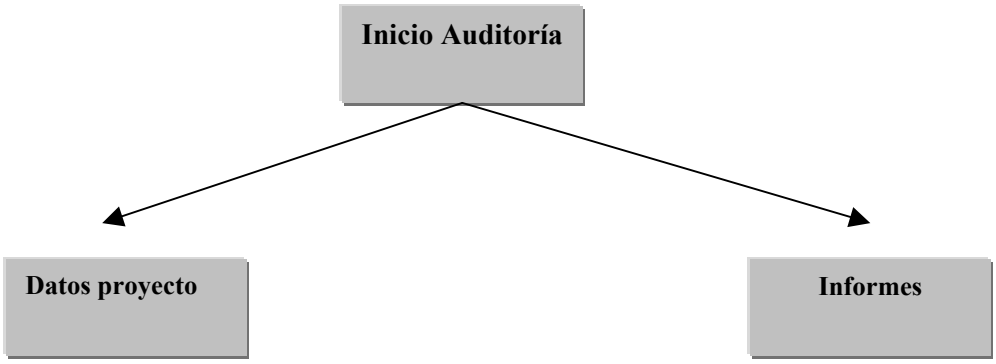


Figura 4.8 descomposición funcional subsistema Inicio de la auditoría

✓ Subsistema de **Estudio preliminar**: este módulo tiene la función de asistir al auditor en el estudio preliminar, en función de los limites del proyecto propone cuestionarios que permitan definir, la estructura interna del Área de Informática a auditar, las aplicaciones existentes, el personal relacionado con la tarea, el inventario y arquitectura del hardware y software, la documentación existente, las características de las telecomunicaciones, la cantidad y características de las bases de datos, etc.

La figura 4.9 muestra la descomposición funcional de este subsistema.

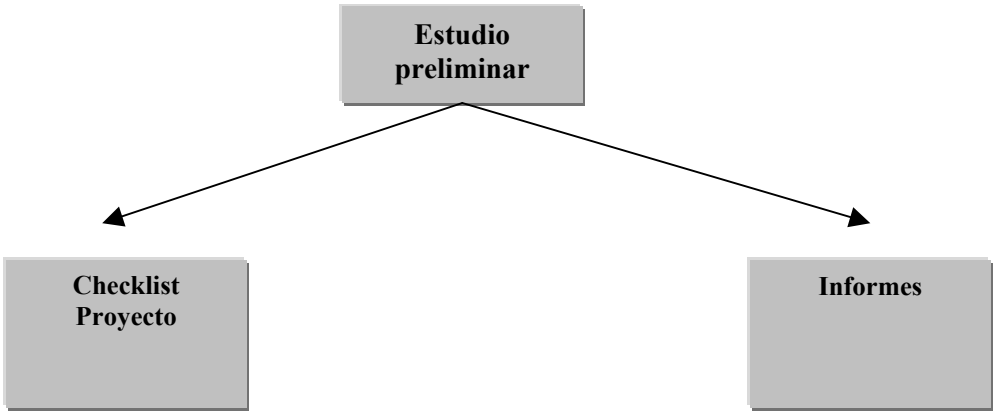


Figura 4.9. descomposición funcional subsistema Estudio preliminar

✓ Subsistema de **recursos**: El asistente en función de los objetivos, alcance y el estudio preliminar deberá sugerirle al auditor **los recursos** necesarios para realizar la tarea.

La figura 4.10 muestra la descomposición funcional de este subsistema.

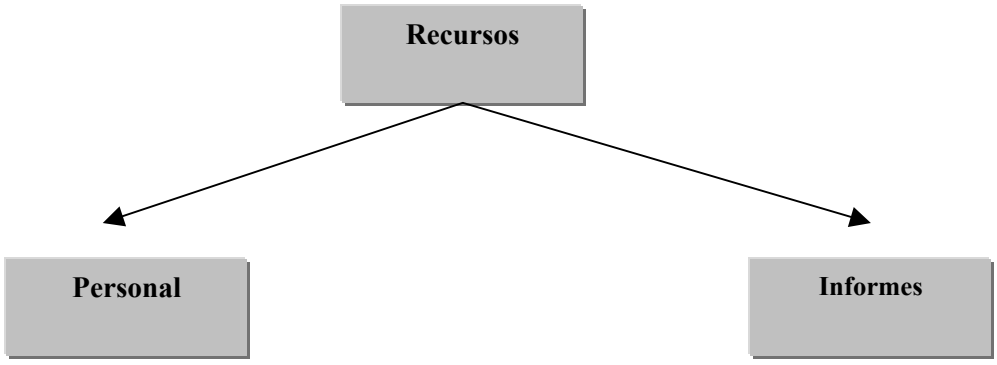


Figura 4.10 descomposición funcional subsistema Inicio de la auditoría

✓ Subsistema de **planificación**: Asiste al proceso de **planificación** adaptando la misma a la organización específica donde se intenta realizar la tarea, proponiendo de acuerdo a los pasos anteriormente desarrollados un plan de trabajo tentativo.

La figura 4.11 muestra la descomposición funcional de este subsistema.

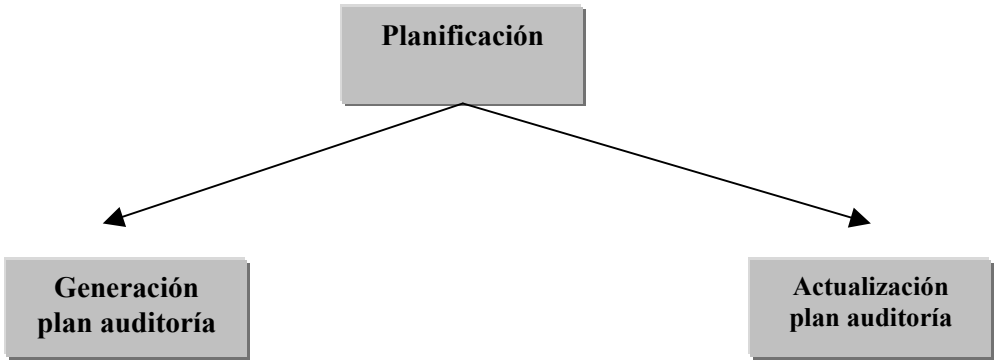


Figura 4.11 descomposición funcional subsistema Planificación

✓ Subsistema de **desarrollo**: Asiste en el desarrollo de la auditoría, sugiriendo distintos cuestionarios y checklist para cada una de las áreas a auditar (desarrollo, producción, redes, gestión, etc.), definiendo los objetivos de control de acuerdo a las características de la organización.

La figura 4.12 muestra la descomposición funcional de este subsistema.

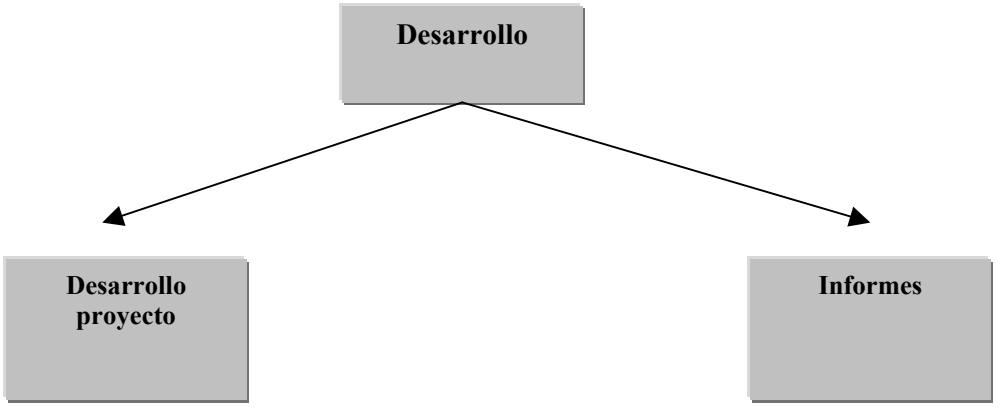


Figura 4.12 descomposición funcional subsistema Desarrollo

✓ Subsistema de **informe final**: El asistente deberá orientar al auditor en la elaboración del **informe final** considerando las tareas realizadas anteriormente.

La figura 4.13. muestra la descomposición funcional de este subsistema.

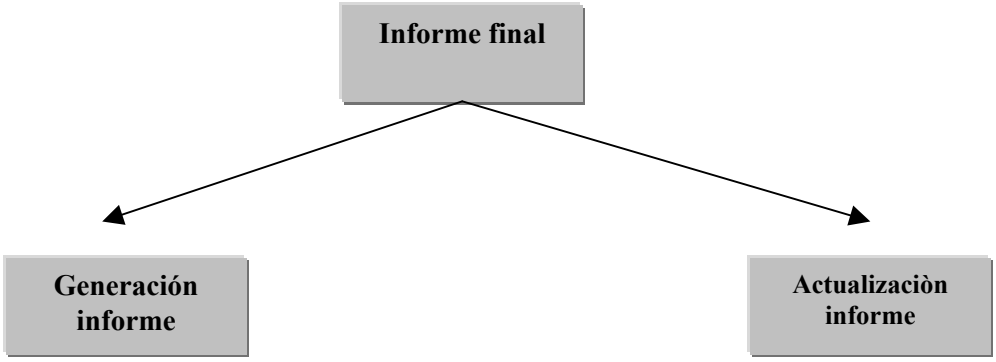


Figura 4.13. descomposición funcional subsistema Informe Final

4.2.2.3.2. Tarea ASI 3.2: Integración de Subsistemas de Análisis

- ***Modelo de procesos***

El modelo de procesos definido en ASI 3.1, donde se realiza la especificación de los subsistemas, es correcta, no hay duplicidad de elementos y hay precisión en el uso de los términos del glosario.

4.2.2.4. Actividad ASI 4: Análisis de los casos de uso:

El objetivo de esta actividad, que sólo se realiza en el caso de Análisis Orientado a Objetos, es identificar las clases cuyos objetos son necesarios para realizar un caso de uso y describir su comportamiento mediante la interacción dichos objetos.

Esta actividad se lleva a cabo para cada uno de los casos de uso contenidos en un subsistema de los definidos en la actividad Identificación de Subsistemas de Análisis (ASI 3). Las tareas de esta actividad no se realizan de forma secuencial sino en paralelo, con continuas realimentaciones entre ellas y con las realizadas en las actividades Establecimiento de Requisitos (ASI 2), Identificación de Subsistemas de Análisis (ASI 3), Análisis de Clases (ASI 5) y Definición de Interfaces de Usuario (ASI 8).

No corresponde dado que no se aplica orientación a objetos

4.2.2.5. Actividad ASI 5: Análisis de clases

El objetivo de esta actividad que sólo se realiza en el caso de Análisis Orientado a Objetos es describir cada una de las clases que ha surgido, identificando las responsabilidades que tienen asociadas, sus atributos, y las relaciones entre ellas. Para esto, se debe tener en cuenta la normativa establecida en la tarea Especificación de Estándares y Normas (ASI 1.3), de forma que el modelo de clases cumpla estos criterios, con el fin de evitar posibles inconsistencias en el diseño.

Teniendo en cuenta las clases identificadas en la actividad Análisis de los Casos de Uso (ASI 4), se elabora el modelo de clases para cada subsistema. A medida que avanza el análisis, dicho modelo se va completando con las clases que vayan apareciendo, tanto del estudio de los casos de uso, como de la interfaz de usuario necesaria para el sistema de información.

No se corresponde dado que no se aplica orientación a objetos

4.2.2.6. Actividad ASI 6: Elaboración del Modelo de Datos

4.2.2.6.1. Tarea ASI 6.1: Elaboración del Modelo Conceptual de Datos

- **Modelo conceptual de datos**

La figura 4.14 muestra el modelo conceptual de datos.

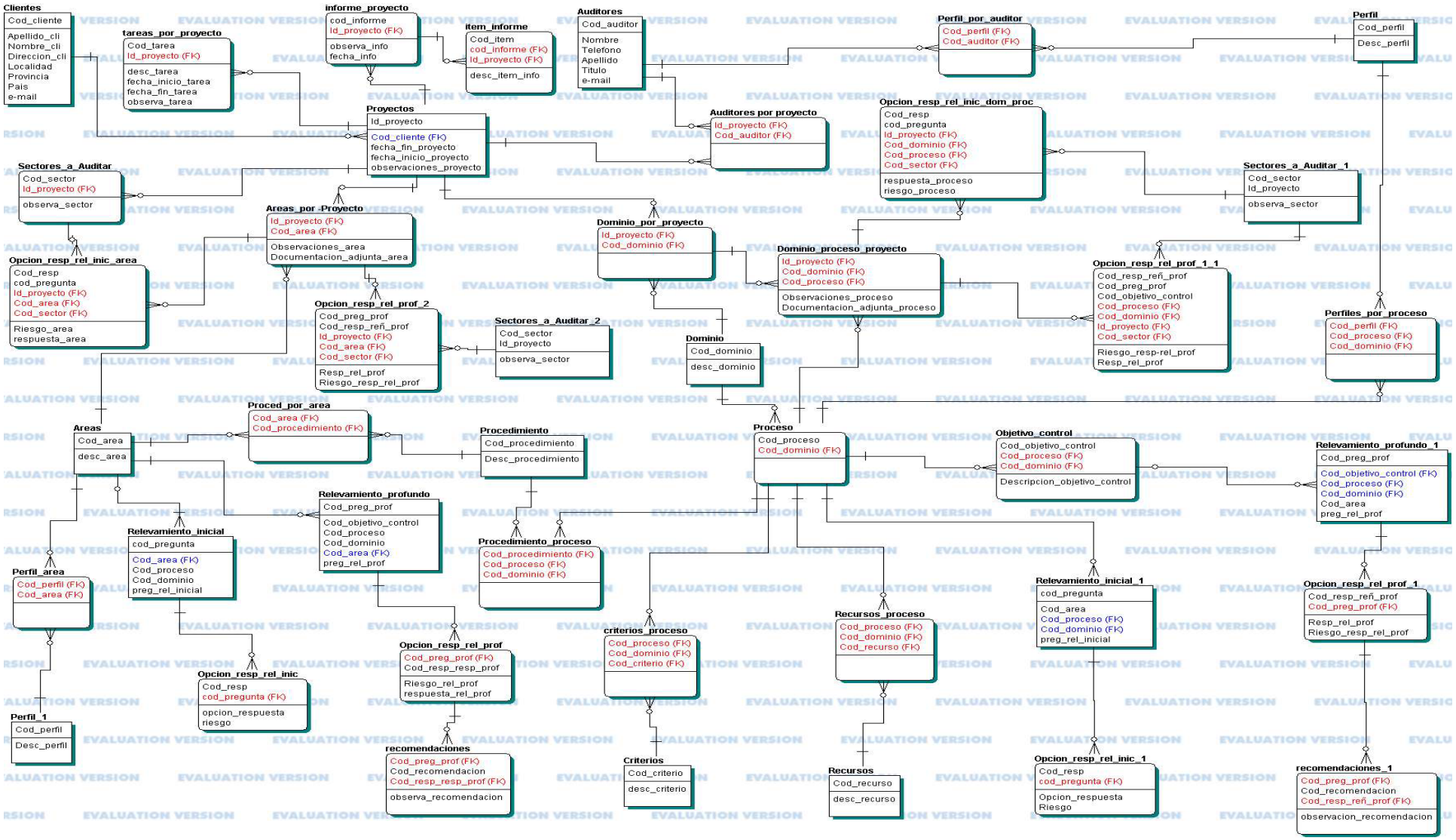

Clientes
Cod_cliente
Apellido_cli
Nombre_cli
Direccion_cli
Localidad
Provincia
Pais
e-mail
tareas_por_proyecto
Cod_tarea
Id_proyecto (FK)
desc_tarea
fecha_inicio_tarea
fecha_fin_tarea
observa_tarea
informe_proyecto
cod_informe
Id_proyecto (FK)
observa_info
fecha_info
item_informe
Cod_item
cod_informe (FK)
Id_proyecto (FK)
desc_item_info
Auditores
Cod_auditor
Nombre
Telefono
Apellido
Titulo
e-mail
Perfil_por_auditor
Cod_perfil (FK)
Cod_auditor (FK)
Perfil
Cod_perfil
Desc_perfil
Proyectos
Id_proyecto
Cod_cliente (FK)
fecha_fin_proyecto
fecha_inicio_proyecto
observaciones_proyecto
Auditores por proyecto
Id_proyecto (FK)
Cod_auditor (FK)
Opcion_resp_rel_inic_dom_proc
Cod_resp
cod_pregunta
Id_proyecto (FK)
Cod_dominio (FK)
Cod_proceso (FK)
Cod_sector (FK)
respuesta_proceso
riesgo_proceso
Sectores_a_Auditar
Cod_sector
Id_proyecto (FK)
observa_sector
Sectores_a_Auditar_1
Cod_sector
Id_proyecto
observa_sector
Areas_por_Proyecto
Id_proyecto (FK)
Cod_area (FK)
Observaciones_area
Documentacion_adjunta_area
Dominio_por_proyecto
Id_proyecto (FK)
Cod_dominio (FK)
Dominio_proceso_proyecto
Id_proyecto (FK)
Cod_dominio (FK)
Cod_proceso (FK)
Observaciones_proceso
Documentacion_adjunta_proceso
Opcion_resp_rel_prof_1_1
Cod_resp_reñ_prof
Cod_preg_prof
Cod_objetivo_control
Cod_proceso (FK)
Cod_dominio (FK)
Id_proyecto (FK)
Cod_sector (FK)
Riesgo_resp-rel_prof
Resp_rel_prof
Perfiles_por_proceso
Cod_perfil (FK)
Cod_proceso (FK)
Cod_dominio (FK)
Opcion_resp_rel_inic_area
Cod_resp
cod_pregunta
Id_proyecto (FK)
Cod_area (FK)
Cod_sector (FK)
Riesgo_area
respuesta_area
Opcion_resp_rel_prof_2
Cod_preg_prof
Cod_resp_reñ_prof
Id_proyecto (FK)
Cod_area (FK)
Cod_sector (FK)
Resp_rel_prof
Riesgo_resp_rel_prof
Sectores_a_Auditar_2
Cod_sector
Id_proyecto
observa_sector
Dominio
Cod_dominio
desc_dominio
Proced_por_area
Cod_area (FK)
Cod_procedimiento (FK)
Areas
Cod_area
desc_area
Procedimiento
Cod_procedimiento
Desc_procedimiento
Proceso
Cod_proceso
Cod_dominio (FK)
Objetivo_control
Cod_objetivo_control
Cod_proceso (FK)
Cod_dominio (FK)
Descripcion_objetivo_control
Relevamiento_profundo_1
Cod_preg_prof
Cod_objetivo_control (FK)
Cod_proceso (FK)
Cod_dominio (FK)
Cod_area
preg_rel_prof
Relevamiento_profundo
Cod_preg_prof
Cod_objetivo_control
Cod_proceso
Cod_dominio
Cod_area (FK)
preg_rel_prof
Relevamiento_inicial
cod_pregunta
Cod_area (FK)
Cod_proceso
Cod_dominio
preg_rel_inicial
Procedimiento_proceso
Cod_procedimiento (FK)
Cod_proceso (FK)
Cod_dominio (FK)
Perfil_area
Cod_perfil (FK)
Cod_area (FK)
Relevamiento_inicial_1
cod_pregunta
Cod_area
Cod_proceso (FK)
Cod_dominio (FK)
preg_rel_inicial
Opcion_resp_rel_prof_1
Cod_resp_reñ_prof
Cod_preg_prof (FK)
Resp_rel_prof
Riesgo_resp_rel_prof
Opcion_resp_rel_prof
Cod_preg_prof (FK)
Cod_resp_resp_prof
Riesgo_rel_prof
respuesta_rel_prof
criterios_proceso
Cod_proceso (FK)
Cod_dominio (FK)
Cod_criterio (FK)
Recursos_proceso
Cod_proceso (FK)
Cod_dominio (FK)
Cod_recurso (FK)
Opcion_resp_rel_inic
Cod_resp
cod_pregunta (FK)
opcion_respuesta
riesgo
Perfil_1
Cod_perfil
Desc_perfil
recomendaciones
Cod_preg_prof (FK)
Cod_recomendacion
Cod_resp_resp_prof (FK)
observa_recomendacion
Criterios
Cod_criterio
desc_criterio
Recursos
Cod_recurso
desc_recurso
Opcion_resp_rel_inic_1
Cod_resp
cod_pregunta (FK)
Opcion_respuesta
Riesgo
recomendaciones_1
Cod_preg_prof (FK)
Cod_recomendacion
Cod_resp_reñ_prof (FK)
observacion_recomendacion

Figura 4.14. Modelo conceptual de datos

4.2.2.6.2. Tarea ASI 6.2: Elaboración del Modelo Lógico de Datos

- ***Modelo lógico de datos***

La tabla 4.10 muestra las descripciones de entidades y atributos

Entidad	Descripción	Atributo	*Valor* / Descripción
1. Areas	Representa las áreas donde se desarrolla la auditoría de sistemas.	Cod_area	*Numérico* Código del área donde se desarrollara la auditoría
		desc_area	*Organización gestión y base jurídica* *Recursos Humanos* *Sistemas en desarrollo* *Operación y soporte* *Ambiente físico* *Hardware* *Software* *Seguridad lógica y física* *Parámetros de medición* Nombre del área donde se desarrollara la auditoría
2. Areas_por -Proyecto	Representa las áreas que abordará cada proyecto	Id_proyecto	(ver entidad PROYECTOS)
		Cod_area	(ver entidad AREAS)
		Cod_sector	(Ver entidad SECTORES_A_AUDITAR)

		Observaciones_area	*Alfanumérico* Observaciones del auditor relacionadas con la auditoría realizada en el área
		Documentacion_adjunta_area	Alfanumérico Documentación adjunta del área auditada
3. Auditores	Representa los auditores de sistemas	Cod_auditor	*Numérico* Código del auditor
		Nombre	*Alfanumérico* Nombre del auditor de sistema
		Apellido	*Alfanumérico* Apellido del auditor de sistemas
		Telefono	*Numérico* Teléfono del auditor de sistemas
		Titulo	*Alfanumérico* Titulo universitario del auditor de sistemas
		e-mail	*Alfanumérico* Correo electrónico del auditor de sistemas
4.Auditores por proyecto	Representa los auditores que intervienen en cada proyecto	Id_proyecto	(ver entidad PROYECTO)
		Cod_auditor	(ver entidad AUDITORES)
5. Clientes	Representa los clientes que son auditados	Cod_cliente	*Numérico* Código del cliente
		Apellido_cli	*Alfanumérico* Apellido del cliente
		Nombre_cli	*Alfanumérico* Nombre del cliente
		Direccion_cli	*Alfanumérico* Dirección del cliente
		Localidad	*Alfanumérico* Localidad del cliente
		Provincia	*Alfanumérico* Provincia del cliente

		Pais	*Alfanumérico*
			País del cliente
		e-mail	*Alfanumérico*
			Correo electrónico del cliente
6. Criterios	Representa los criterios comunes para seguridad en tecnología de información	Cod_criterio	*Numérico*
			Código del criterio
		desc_criterio	*Calidad* *Fiduciarios* *Seguridad*
			Criterios comunes relacionados con la tecnología de la información
7.criterios_proceso	Representa los criterios a considerar en cada proceso	Cod_proceso	(ver entidad PROCESO)
		Cod_dominio	(ver entidad DOMINIO)
		Cod_criterio	(ver entidad CRITERIOS)
8.Dominio	Representa las áreas donde se realiza una auditoría	Cod_dominio	*Numérico*
			Código del dominio donde se desarrollará la auditoría
		Des_dominio	***Planeación y organización*** ***Adquisición e implementación*** ***Entrega y soporte*** *Monitoreo*
			Nombre del dominio donde se desarrollará la auditoría
9.Dominio_por_proyecto	Representa los dominios que se abordan en un proyecto	Id_proyecto	(ver entidad PROYECTOS)
		Cod_dominio	(ver entidad DOMINIOS)
10.Dominio_proceso_proyecto	Representa los procesos dentro de un determinado dominio que se abordan en un proyecto	Id_proyecto	(ver entidad PROYECTOS)
		Cod_dominio	(ver entidad DOMINIOS)
		Cod_proceso	(ver entidad PROCESOS)
		Observaciones_proceso	*Alfanumérico*
			Observaciones del auditor relacionadas con la auditoría realizada en el dominio/proceso
		Documentacion_adjunta_proceso	*Alfanumérico*

			Documentación adjunta del dominio/proceso auditado
11.informe_proyecto	Representa el informe final de la auditoría.	cod_informe	*Numérico*
			Código del informe
		Id_proyecto	(ver entidad PROYECTOS)
		observa_info	*Alfanumérico*
			Observaciones del informe
		fecha_info	*Fecha*
			Fecha del informe
12.item_informe	Representa un item del informe final	Cod_item	*Numérico*
			Código del item
		cod_informe	*Numérico*
			Código del informe
		Id_proyecto	(ver entidad PROYECTOS)
		desc_item_info	Alfanumérico
			Descripción del item del informe
13.Objetivo_control	Representa una definición del resultado o propósito que se desea alcanzar implementando procedimientos de control en una actividad de TI particular	Cod_objetivo_control	*Numérico*
			Código objetivo de control
		Cod_proceso	(Ver entidad PROCESO)
		Cod_dominio	(Ver entidad DOMINIO)
		Descripcion_objetivo_control	*(ver tabla 16: relaciones)*
			Descripción del objetivo de control
14. Opcion_resp_rel_inic	Representa las opciones de respuesta a una determinada pregunta de la matriz de preguntas del relevamiento inicial	Cod_resp	*Numérico*
			Código de la respuesta
		cod_pregunta	(ver entidad RELEVAMIENTO_INICIAL)
		opcion_respuesta	*Alfanumérico*
			Opción de la respuesta
		riesgo	*1-2-3-4-5*
			Riesgo que implica la respuesta donde 1 es el menor riesgo
15Opcion_resp_rel_inic_area	Representa la respuesta dada en un sector determinado a una pregunta en un área especifica del relevamiento inicial.	Cod_resp	Ver entidad (OPCION_RESP_REL_INIC)
		cod_pregunta	(Ver entidad RELEVAMIENTO INICIAL)

		Id_proyecto	(Ver entidadPROYECTOS)
		Cod_area	(ver entidad AREAS)
		Cod_sector	(ver entidad SECTOR)
		Riesgo_area	*1 – 2- 3- 4 – 5*
			Riesgo
		Respuesta_AREA	*Alfanumérico*
			Observaciones
16.Opcion_resp_rel_inic_dom_proc	Representa la respuesta dada en un sector determinado a una pregunta en un dominio/proceso especifico del relevamiento inicial.	Cod_resp	Ver entidad (OPCION_RESP_REL_INIC)
		cod_pregunta	(Ver entidad RELEVAMIENTO INICIAL))
		Id_proyecto	(Ver entidadPROYECTOS)
		Cod_dominio	(ver entidad DOMINIO)
		Cod_proceso	(ver entidad PROCESO)
		Cod_sector	(ver entidad SECTOR)
		respuesta_proceso	*Alfanumérico*
			Observaciones
		riesgo_proceso	*1 – 2 – 3- 4 - 5*
			Riesgo
17.Opcion_resp_rel_prof	Representa las opciones de respuesta de una determinada pregunta del relevamiento profundo para una determinada pregunta de un área o dominio/proceso	Cod_preg_prof	(ver entidad RELEVAMIENTO PROFUNDO)
		Cod_resp_resp_prof	*Numérico*
			Código de alternativa de respuesta del relevamiento profundo
		Riesgo_rel_prof	*Alfanumérico*
			Riesgo que implica la respuesta
		respuesta_rel_prof	*1 – 2- 3 – 4 - 5*
18.Opcion_resp_rel_prof_area	Representa la respuesta dada en un sector determinado a una pregunta en un área especifica del relevamiento profundo.	Cod_preg_prof	(ver entidad RELEVAMIENTO PROFUNDO)
		Cod_resp_reñ_prof	(ver entidad OPCION_RESP_REL_PROF)
		Id_proyecto	(ver entidad PROYECTOS)
		Cod_area	(ver entidad AREAS)
		Resp_rel_prof	(ver entidad OPCION_RESP_REL_PROF)

		Cod_sector	(ver entidad SECTORES:A_AUDITAR)
		Riesgo_resp_rel_prof	*1 – 2 – 3 – 4- 5*
			Riesgo respuesta relevamiento profundo
		Resp_rel_prof	*Alfanumérico*
			Observación
19.Opcion_resp_rel_prof_dom_proc	Representa la respuesta dada en un sector determinado a una pregunta en un dominio/proceso especifica del relevamiento profundo.	Cod_resp_reñ_prof	(ver entidad OPCION_RESP_REL_PROF)
		Cod_preg_prof	(ver entidad RELEVAMIENTO PROFUNDO)
		Cod_objetivo_control	(ver entidad OBJETIVO_CONTROL)
		Cod_proceso	(ver entidad PROCESO)
		Cod_dominio	(ver entidad DOMINIO)
		Id_proyecto	(ver entidad PROYECTOS)
		Cod_sector	(ver entidad SECTORES:A_AUDITAR)
		Riesgo_resp-rel_prof	*1 – 2 -3 -4 –5*
			Riesgo respuesta relevamiento profundo
		Resp_rel_prof	*Alfanumérico*
			Observación
20.Perfil	Representa perfiles de auditores	Cod_perfil	*Numérico*
			Código del perfil del auditor
		Desc_perfil	*Alafanumérico*
			Descripción del perfil del auditor
21.Perfil_area	Representa los perfiles de auditores necesarios para realizar una auditoría en un área determinada	Cod_perfil	(ver entidad PERFIL)
		Cod_area	(ver entidad AREA)
22.Perfil_por_auditor	Representa los perfiles de cada auditor	Cod_perfil	(ver entidad PERFIL)
		Cod_auditor	(ver entidad AUDITORES)
23.Perfiles_por_proceso	Representa los perfiles necesarios para realizar un auditoría en un determinado proceso/dominio	Cod_perfil	(ver entidad PERFIL)
		Cod_proceso	(ver entidad PROCESO)
		Cod_dominio	(ver entidad DOMINIO)

24.Proced_por_area	Representa los procedimientos necesarios para realizar una auditoría en un determinado AREA	Cod_area	(ver entidad AREA)
		Cod_procedimiento	(Ver entidad PROCEDIMIENTOS)
25.Procedimientos	Representa las distintas acciones necesarias para realizar una auditoría por ejemplo entrevista, observación, revisión, etc.	Cod_procedimiento	*Numérico*
			Código de procedimiento
		Desc_procedimiento	*alfanumérico*
			Descripción del procedimiento
26.Procedimiento_proceso	Representa los procedimientos necesarios para realizar una auditoría en un determinado proceso	Cod_procedimiento	(Ver entidad PROCEDIMIENTOS)
		Cod_proceso	(ver entidad PROCESO)
		Cod_dominio	(ver entidad DOMINIO)
27.Proceso	Representa el Conjunto de actividades que se desarrollan en un determinado	Cod_proceso	*Numérico*
			Código del proceso
		Cod_dominio	(Ver entidad DOMINIO)
		Desc_proceso	*(Ver tabla 16: relaciones)*
			Descripción del proceso
28.Proyectos	Representa cada proyecto de auditoría de sistemas	Id_proyecto	*Numérico*
			Identificación del proyecto
		Cod_cliente	(ver entidad CLIENTES)
		fecha_fin_proyecto	*Fecha*
			Fecha de fin del proyecto
		fecha_inicio_proyecto	*Fecha*
			Fecha de inicio del proyecto
		observaciones_proyecto	Alfanumérico
			Observaciones relacionadas con el proyecto
29.Recomendaciones	Representa la recomendación genérica que corresponde realizar a la respuesta dada. Esta recomendación es utilizada en el informe final	Cod_preg_prof	(ver entidad OPCION_RESP_REL_PRO)
		Cod_recomendacion	*Numérico*
			Código de recomendación
		Cod_resp_resp_prof	(ver entidad OPCION_RESP_REL_PRO)
		observa_recomendacion	*alfanumérico*
			Recomendación
30.Recursos	Representa los recursos de la tecnología de	Cod_recurso	*Numérico*

	la información		Código del recurso
		Desc_recurso	*Gente* *Sistemas de aplicación* *Tecnología* *Instalaciones* *Datos*
			Descripción de los recursos
31.Recurso_proceso	Representa los recursos intervinientes en cada proceso	Cod_proceso	(ver entidad PROCESOS)
		Cod_dominio	(ver entidad DOMINIO)
		Cod_recurso	(ver entidad RECURSOS)
32. Relevamiento_inicial	Representa la matriz completa de preguntas que se pueden realizar en un relevamiento inicial para un determinado área o un dominio/proceso	cod_pregunta	*Numérico*
			Código de la pregunta
		Cod_area	(ver entidad AREAS)
		Cod_proceso	(ver entidad PROCESOS)
		Cod_dominio	(ver entidad DOMINIOS)
		preg_rel_inicial	alfanumérico
			Pregunta del relevamiento inicial
33.Relevamiento_profundo	Representa las preguntas a realizar en el relevamiento profundo en un área o dominio/proceso determinado	Cod_preg_prof	*numérico*
			Código de pregunta del relevamiento profundo
		Cod_objetivo_control	(ver entidad OBJETIVO_CONTROL)
		Cod_proceso	(Ver entidad PROCESO)
		Cod_dominio	(Ver entidad DOMINIO)
		Cod_area	(Ver entidad AREA)
		preg_rel_prof	*alfanumérico*
			Pregunta del relevamiento profundo
34.Sectores_a_Auditar	Representa los sectores de una empresa que se auditan, estos sectores podrán ser sucursales, centros de costos, etc.	Cod_sector	(ver entidad SECTORES)
		Id_proyecto	(ver entidad PROYECTOS)
		observa_sector	*alfanumérico*
			Observaciones relacionadas con el sector a auditor.
35.tareas_por_proyecto	Representa las actividades que se deben realizar en la auditoría, estas constituyen el	Cod_tarea	*numérico*
			Código de tarea

	plan de trabajo	Id_proyecto	(ver entidad PROYECTOS)
		desc_tarea	*alfanumèrico*
			Descripción de la tarea
		fecha_inicio_tarea	*fecha*
			Fecha inicio de la tarea
		fecha_fin_tarea	*fecha*
			Fecha fin de la tarea
		observa_tarea	*alfanumérico*
			observación

Tabla 4.10.: Descripciónes de entidades y atributos

4.2.2.6.3. Tarea ASI 6.3: Normalización del Modelo Lógico de Datos

- ***Modelo lógico de datos normalizado***

Considerando las recomendaciones de esta tarea se revisó el modelo de datos elaborado en tareas anteriores y se verifico que el modelo presentado ya cumple con la 3era Forma Normal.

4.2.2.6.4. Tarea ASI 6.4: Especificación de Necesidades de Migración de Datos y Carga Inicial.

Está tarea se realiza si es necesaria una migración de datos de otros sistemas, o una carga inicial de información.

Se especifican las necesidades de migración o carga inicial de los datos requeridos por el sistema. Como punto de partida, se toma el modelo lógico de datos normalizado, junto con las estructuras de datos del sistema o sistemas origen. Es preciso tener en cuenta aspectos tales como:

- ✓ *Planificación de la migración y carga inicial.*
- ✓ *Prioridad en las cargas.*
- ✓ *Requisitos de conversión de información: necesidades de depuración de información, importación de información complementaria, validaciones y controles, etc.*
- ✓ *Plan de pruebas específico.*
- ✓ *Necesidades especiales de equipamiento hardware y estimaciones de capacidad, en función de los volúmenes de las estructuras de datos origen.*
- ✓ *Necesidades especiales de utilidades software.*
- ✓ *Posibles modificaciones del sistema origen, que faciliten la ejecución o verificación de la migración o carga inicial.*

Como resultado de esta tarea se obtiene una primera especificación del plan de migración de datos y carga inicial del sistema, que se completará en el proceso Diseño del Sistema de Información (DSI).

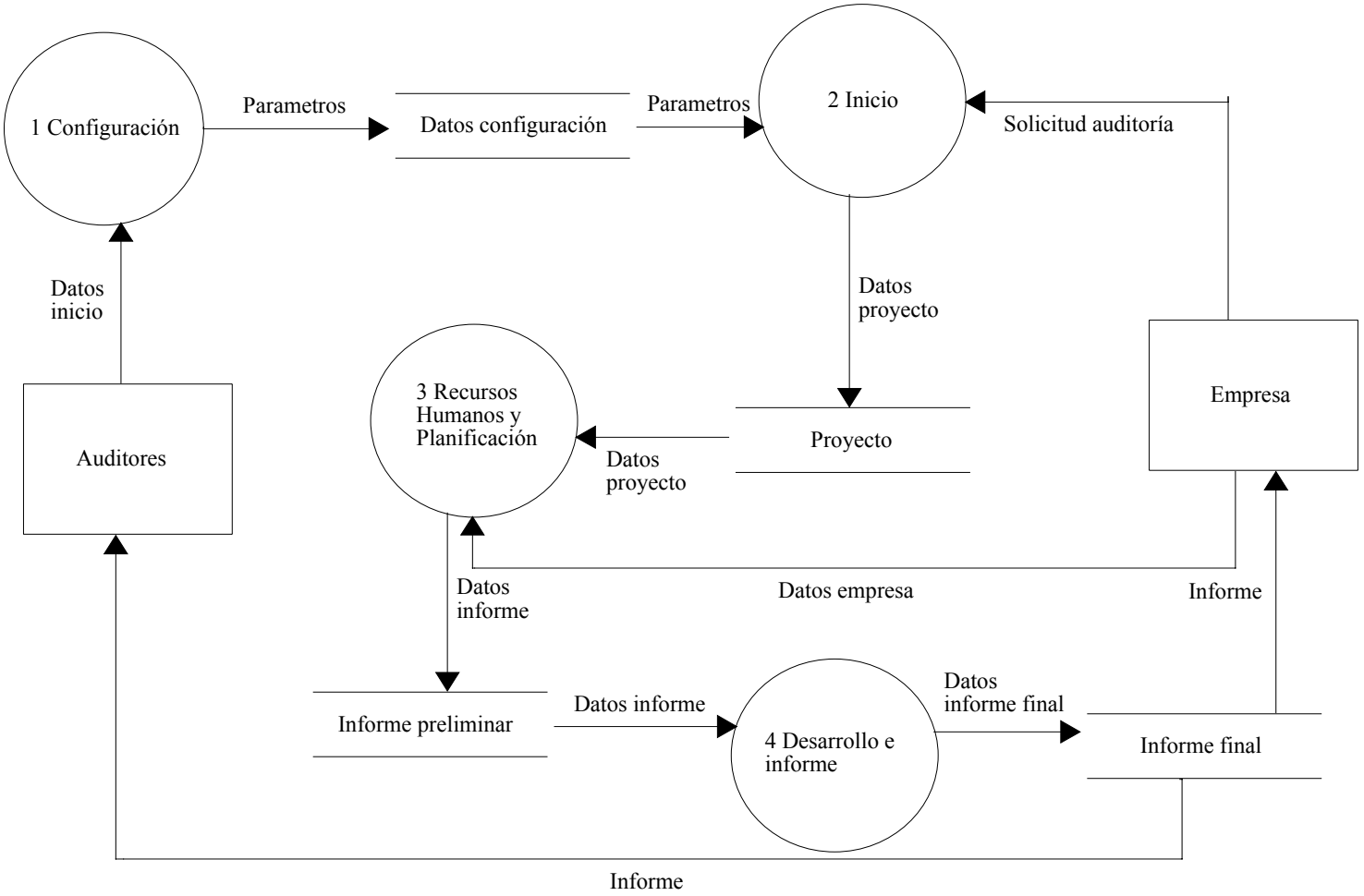
Esta tarea no se realiza, dado que no es necesario realizar una migración de datos.

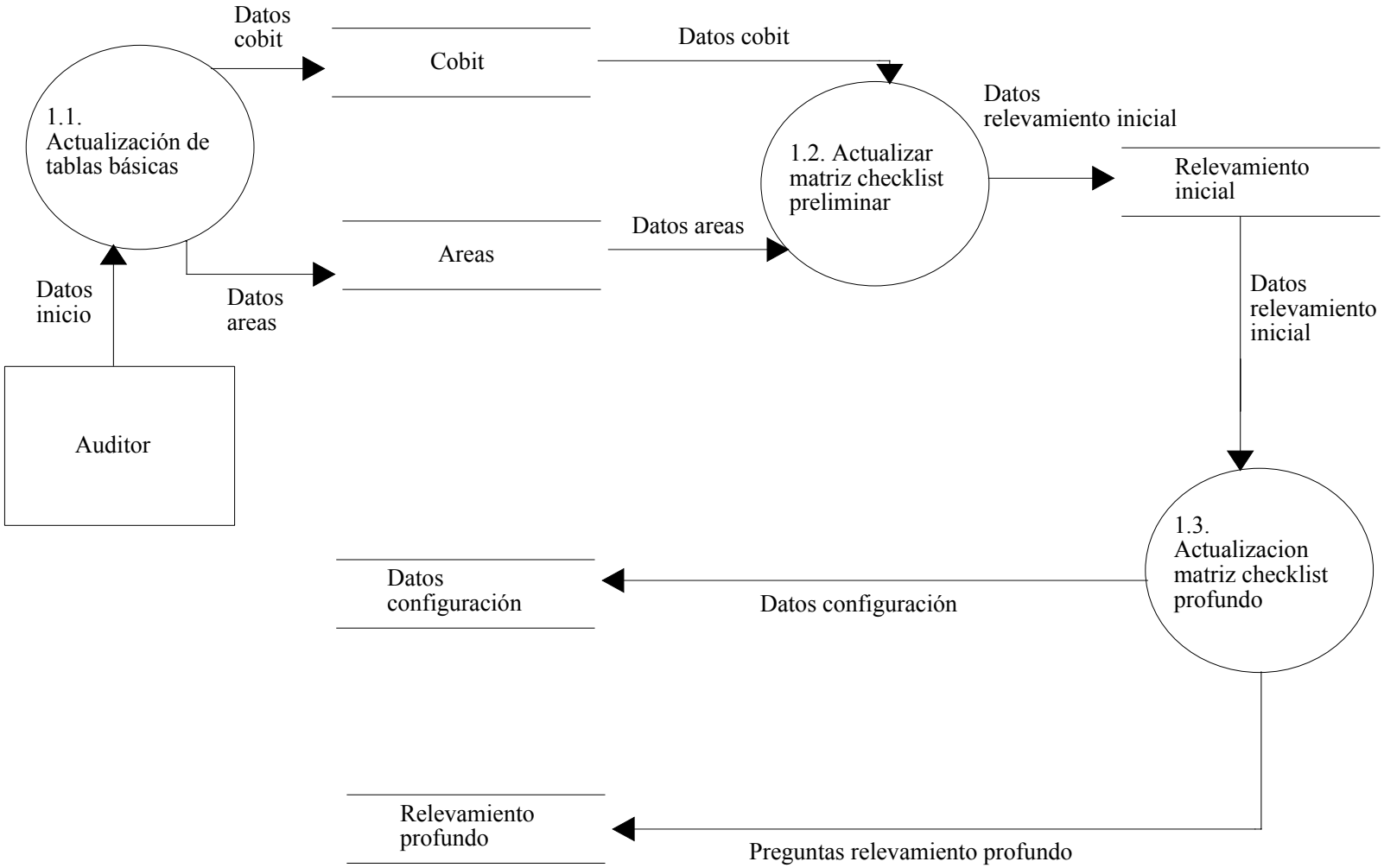
4.2.2.7. Actividad ASI 7: Elaboración del Modelo de Procesos

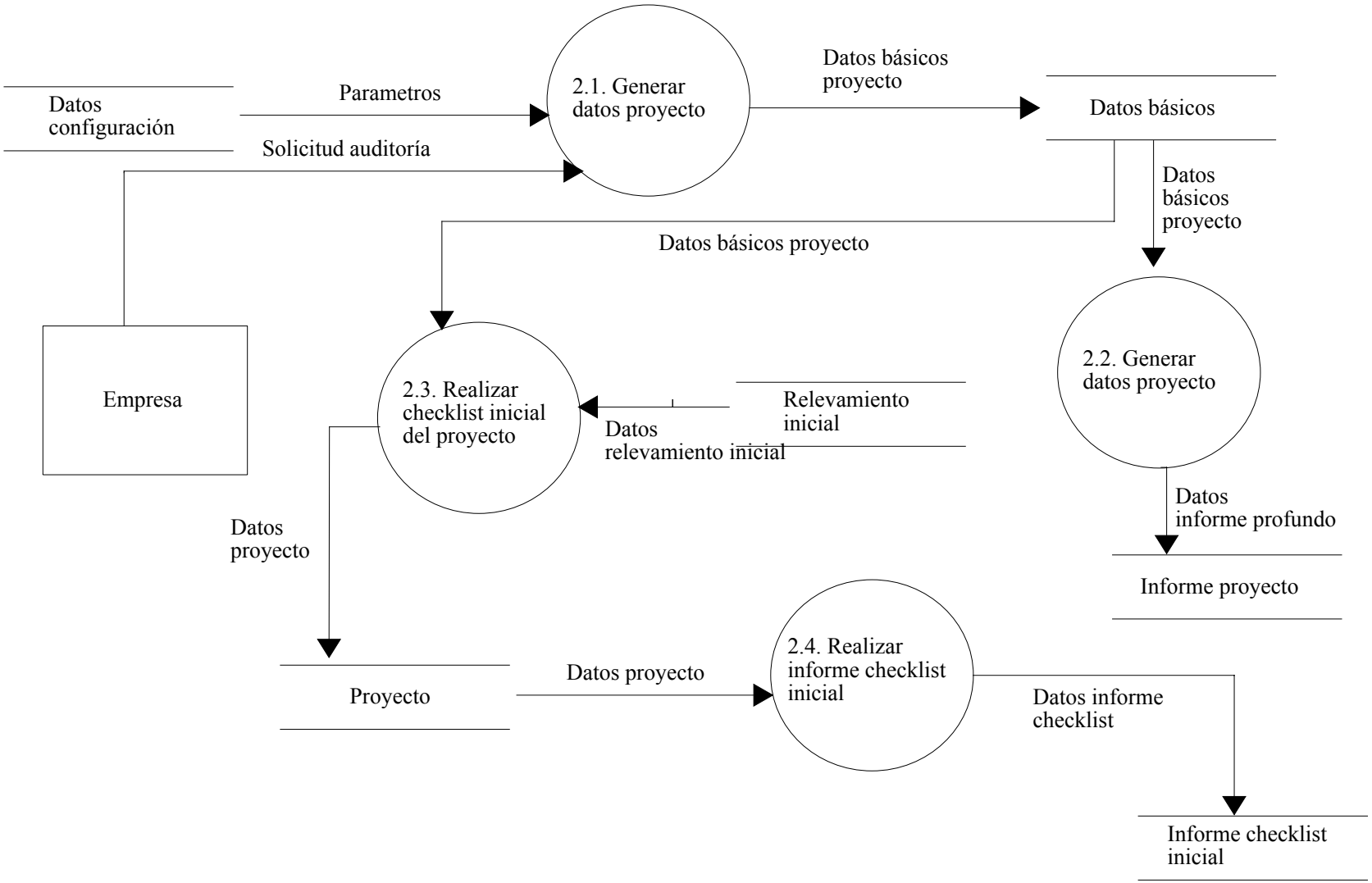
4.2.2.7.1. Tarea ASI 7.1: Obtención del Modelo de Procesos del Sistema

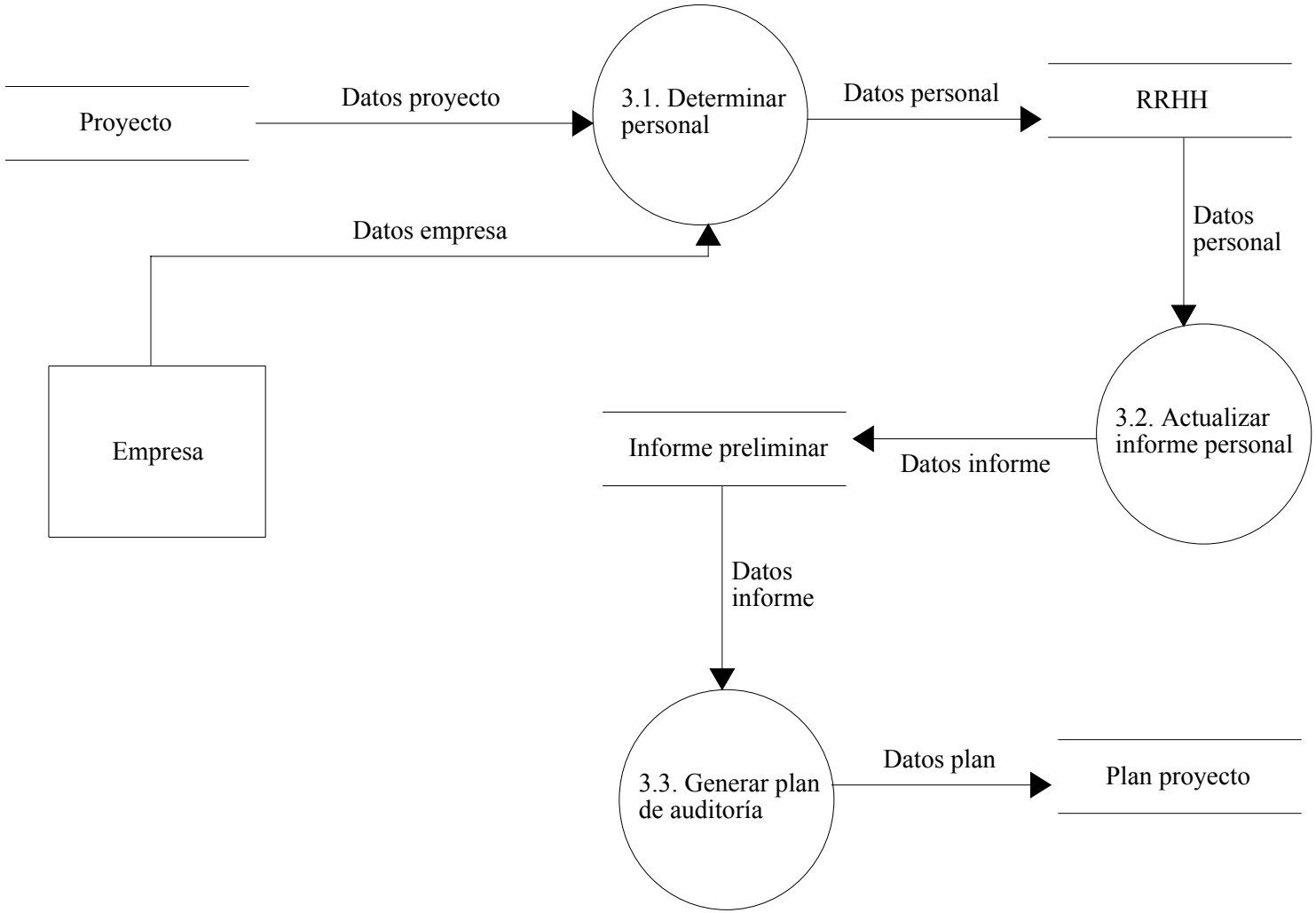
- ***Modelo de procesos***

La figura 4.15. muestra el modelo de procesos


1 Configuración
Parametros
Datos configuración
Parametros
2 Inicio
Solicitud auditoría
Datos inicio
Datos proyecto
Auditores
3 Recursos Humanos y Planificación
Proyecto
Empresa
Datos proyecto
Datos informe
Datos empresa
Informe
Informe preliminar
Datos informe
4 Desarrollo e informe
Datos informe final
Informe final
Informe


Datos cobit
Cobit
Datos cobit
1.1. Actualización de tablas básicas
1.2. Actualizar matriz checklist preliminar
Datos relevamiento inicial
Relevamiento inicial
Areas
Datos areas
Datos inicio
Datos areas
Datos relevamiento inicial
Auditor
1.3. Actualizacion matriz checklist profundo
Datos configuración
Datos configuración
Relevamiento profundo
Preguntas relevamiento profundo


Datos configuración
Parametros
2.1. Generar datos proyecto
Datos básicos proyecto
Datos básicos
Solicitud auditoría
Datos básicos proyecto
Datos básicos proyecto
Empresa
2.3. Realizar checklist inicial del proyecto
Relevamiento inicial
Datos relevamiento inicial
2.2. Generar datos proyecto
Datos informe profundo
Informe proyecto
Datos proyecto
Proyecto
Datos proyecto
2.4. Realizar informe checklist inicial
Datos informe checklist
Informe checklist inicial


Proyecto
Datos proyecto
3.1. Determinar personal
Datos personal
RRHH
Datos personal
Datos empresa
Empresa
3.2. Actualizar informe personal
Informe preliminar
Datos informe
Datos informe
3.3. Generar plan de auditoría
Datos plan
Plan proyecto

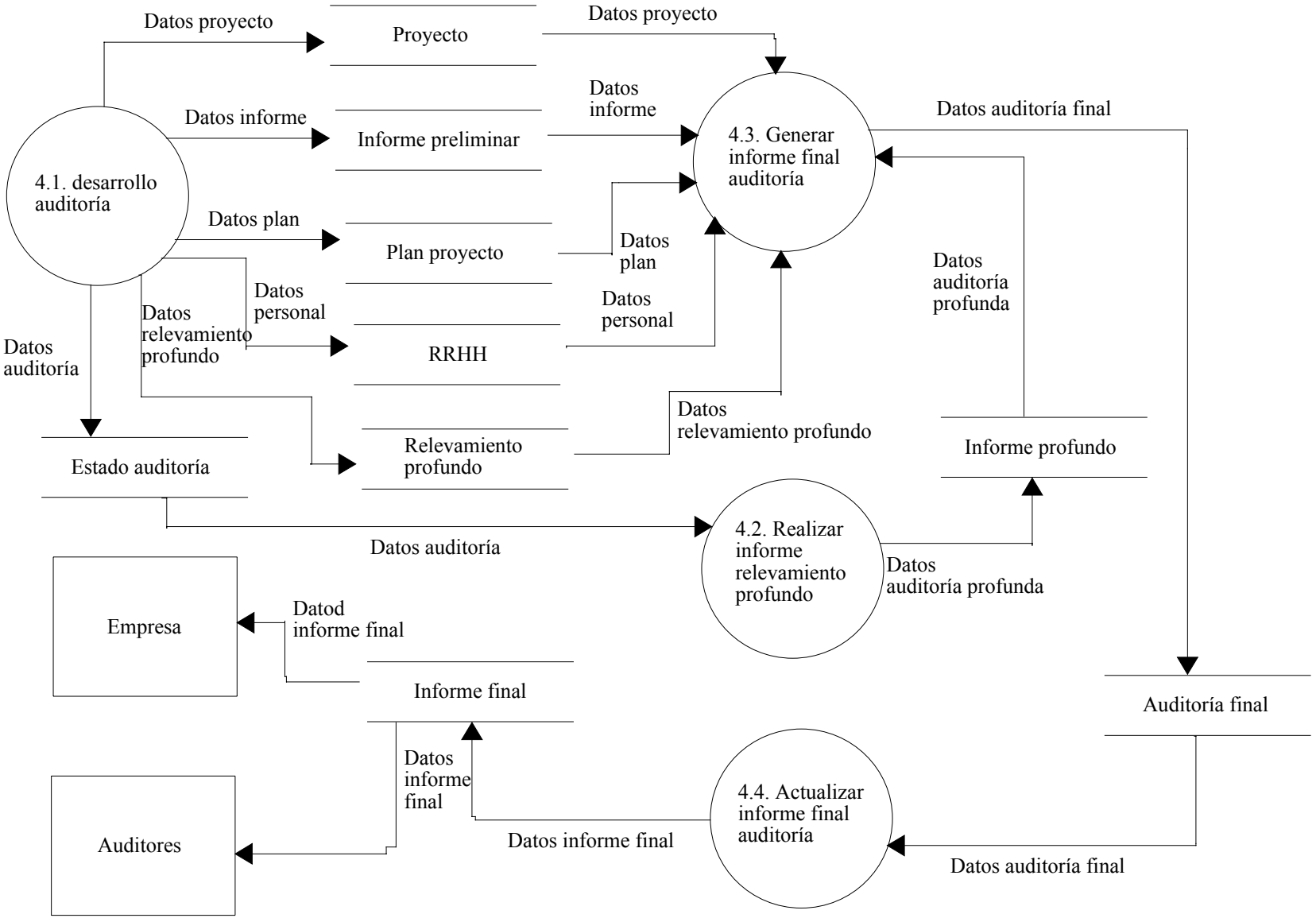

Datos proyecto
Proyecto
Datos proyecto
Datos informe
Informe preliminar
Datos informe
4.1. desarrollo auditoría
4.3. Generar informe final auditoría
Datos auditoría final
Datos plan
Plan proyecto
Datos plan
Datos personal
Datos relevamiento profundo
RRHH
Datos personal
Datos auditoría profunda
Datos auditoría
Datos relevamiento profundo
Relevamiento profundo
Informe profundo
Estado auditoría
Datos auditoría
4.2. Realizar informe relevamiento profundo
Datos auditoría profunda
Empresa
Datod informe final
Informe final
Auditoría final
Datos informe final
4.4. Actualizar informe final auditoría
Auditores
Datos informe final
Datos auditoría final

Figura 4.15 Modelo de procesos

En el modelo de procesos se especifican en forma detallada los procesos que implican el sistema y las funciones que resuelven como lo muestra la tabla 4.11.

Proceso 1.1	**Actualización tablas básicas**
Objetivo	Generar las tablas básicas necesarias para que el asistente opere
Entrada	Areas Dominios Procesos Objetivos de control Criterios de la información Recursos de la información Perfiles Procedimientos y técnicas
Descripción del proceso	Se podrán realizar ingresos, modificaciones, bajas y listados de las tablas básicas necesarias para el funcionamiento del sistema, se deberá mantener actualizadas las mismas de acuerdo a las recomendaciones dadas por COBIT, relacionándose las áreas y los dominios/procesos con el perfil de auditor necesario para realizar la tarea, y los procedimientos y técnicas necesarias en cada caso para realizar la auditoría, este proceso podrá ser realizado pro el usuario administrador
Salida	Tablas básicas actualizadas

Proceso 1.2.	**Actualizar Matriz Chekclist preliminar**
Objetivo	Generar y actualizar la matriz de preguntas del relevamiento preliminar.
Entrada	Preguntas relevamiento inicial Alternativas de respuesta relevamiento inicial
Descripción del proceso	Se deberán poder ingresar, modificar, eliminar y listar las preguntas y las distintas alternativas de respuestas para cada área o dominio/proceso de COBIT del relevamiento inicial.
Salida	Matriz de preguntas del relevamiento preliminar actualizada

Proceso 1.3	**Actualizar Matriz Gral. Relevamiento profundo**
Objetivo	Generar y actualizar la matriz de preguntas del relevamiento profundo
Entrada	Preguntas Respuestas Recomendaciones de acuerdo a cada respuesta
Descripción del proceso	Se deberán poder ingresar, modificar, eliminar y listar las preguntas, las distintas alternativas de respuestas para cada área o dominio/proceso/objetivo de control de COBIT del relevamiento profundo, se deberá actualizar las distintas

	recomendaciones de acuerdo a las respuestas dadas en el relevamiento profundo.
Salida	Matriz de preguntas, respuestas y recomendaciones del relevamiento profundo actualizadas.

Proceso 2.1	**Generar Datos proyecto**
Objetivo	Generar un nuevo proyecto incorporando los datos del mismo y los alcances de la auditoría
Entrada	Clientes Auditores Sectores Areas o procesos/dominios a auditar
Descripción del proceso	Se deberá poder ingresar, modificar y listar los datos relacionados con el cliente del proyecto, los auditores asignados, los sectores o sucursales de la empresa donde se realizará la tarea. Se deberá definir desde el punto de vista metodológico si se trabaja por áreas o de acuerdo a COBIT por dominios y procesos. Se deberá definir en el caso de trabajar por áreas o por dominios/procesos, cuales se abordará. Esto establecerá el alcance de la auditoría y guiará el resto de procesos del asistente al ser el filtro tanto para el relevamiento preliminar como para el profundo
Salida	Datos del proyecto actualizados

Proceso 2.2.	**Generar informe Proyecto**
Objetivo	Generar un reporte con los datos básicos del proyecto.
Entrada	Clientes Auditores Sectores Areas o procesos/dominios a auditar Proyecto
Descripción del proceso	En función de los datos del proyecto se generará un informe con una carátula de datos básicos y el alcance de la auditoría.
Salida	Reporte

Proceso 2.3.	**Realizar Checklist inicial Proyecto**
Objetivo	Realizar el estudio preliminar
Entrada	Preguntas relevamiento inicial Alternativas de respuesta relevamiento inicial Clientes Sectores Areas o procesos/dominios a auditar Proyecto

Descripción del proceso	Se deberá generar en forma automática una matriz de preguntas especifica para el proyecto, la misma se establecerá en función del alcance, es decir de las áreas o dominios/procesos que se establecieron para el proyecto, esta matriz será un subconjunto del la matriz general de preguntas del relevamiento preliminar. Se repetirá esta matriz de preguntas para cada sector a auditar. Se deberán poder ingresar las respuestas de cada pregunta, pudiendo modificarse las mismas.
Salida	Relevamiento inicial del proyecto actualizado

Proceso 2.4.	**Realizar informe Checklist inicial proyecto**
Objetivo	Generar un informe del relevamiento inicial
Entrada	Proyecto Relevamiento inicial del proyecto
Descripción del proceso	En función del relevamiento inicial del proyecto se genera un informe del mismo. Este reporte se podrá filtrar para un sector determinado o para todos.
Salida	Reporte

Proceso 3.1.	**Determinar personal**
Objetivo	Establecer el personal necesario para realizar la auditoría
Entrada	Proyecto Perfil Sectores Areas o procesos/dominios a auditar
Descripción del proceso	Generar en forma automática los perfiles del personal necesarios para realizar la auditoría. Para realizar este proceso se deberá considerar el alcance del la auditoría (áreas o dominios/procesos a auditar) y el perfil de auditor necesario para abordar la tarea. En función a esos perfiles el sistema deberá proponer del staff de auditores quienes están en condiciones de acuerdo de realizar la tarea. Se deberá poder actualizar los auditores del proyecto, incorporando o eliminando alguno de ellos.
Salida	Personal necesario para realizar la auditoría.

Proceso 3.2.	**Actualizar informe personal**
Objetivo	Generar un reporte del personal interviniente en el proyecto
Entrada	Proyecto Personal
Descripción del proceso	Generar un reporte con los datos del proyecto y el personal necesario para realizar la auditoría
Salida	Reporte

Proceso 3.3.	**Generar Plan de auditoría**

Objetivo	Generar la planificación de la auditoría del proyecto
Entrada	Proyecto Procedimientos y técnicas Sectores Areas o procesos/dominios a auditar
Descripción del proceso	Se deberá generar en forma automática un listado de tareas a realizar en la auditoría, este listado se obtiene a partir del alcance del proyecto y los procedimientos y técnicas que el asistente propone para cada área o dominio proceso a auditar. Se deberá poder en función de las tareas propuestas cargar y modificar el plan de la auditoría del proyecto. Se deberán poder agregar tareas y eliminar las mismas. Se deberá poder ingresar la fecha de inicio y fin de cada tarea. Se deberá poder consultar la planificación. Se deberá poder visualizar el estado de avance de la auditoría especificando posibles atrasos.
Salida	Plan de auditoría

Proceso 3.4.	**Actualización plan de auditoría**
Objetivo	Actualizar y gestionar el plan de auditoría
Entrada	Plan de auditoría
Descripción del proceso	Se deberá actualizar las tareas, especificando las realizadas, suspendidas y anuladas.
Salida	Plan de auditoría actualizado

Proceso 4.1.	**Desarrollar auditoría**
Objetivo	Realizar el estudio profundo
Entrada	Preguntas relevamiento profundo Alternativas de respuesta relevamiento profundo Clientes Sectores Areas o procesos/dominios a auditar Proyecto
Descripción del proceso	Se deberá generar en forma automática una matriz de preguntas para el relevamiento profundo especifica para el proyecto, la misma se establecerá en función del alcance, es decir de las áreas o dominios/procesos/objetivo de control que se establecieron para el proyecto, esta matriz será un subconjunto del la matriz general de preguntas del relevamiento profundo Se repetirá esta matriz de preguntas para cada sector a auditar. Se deberán poder ingresar las respuestas de cada pregunta, pudiendo modificarse las mismas.

	Se deberá poder ingresar documentación adjunta para cada pregunta. Se deberá poder ingresar observaciones para cada pregunta
Salida	Relevamiento profundo actualizado

Proceso 4.2.	**Realizar informe relevamiento profundo**
Objetivo	Generar un informe del relevamiento profundo
Entrada	Proyecto / Relevamiento profundo del proyecto
Descripción del proceso	En función del relevamiento profundo del proyecto se genera un informe del mismo. Este reporte se podrá filtrar para un sector determinado o para todos.
Salida	Reporte

Proceso 4.3.	**Generar informe final de auditoría**
Objetivo	Generar estructura del informe final del proyecto
Entrada	Proyecto Relevamiento inicial Relevamiento profundo Planificación Personal Recomendaciones
Descripción del proceso	Se deberá generar en forma automática en función del resultado del relevamiento profundo y de las recomendaciones estándares ingresadas para cada respuesta posible, las recomendaciones y propuestas a realizar.
Salida	Estructura básica del informe final

Proceso 4.4.	**Actualizar informe final de auditoría**
Objetivo	Realizar el informe final de la auditoría de un proyecto
Entrada	Proyecto Estructura básica del informe final
Descripción del proceso	Se deberá poder ingresar, eliminar, modificar ítems del informe final. Se deberá poder listar el informe final
Salida	Informe final

Tabla 4.11. descripción de procesos

4.2.2.7.2. Tarea ASI 7.2: Especificación de Interfaces con otros Sistemas

- ***Descripción de interfaz con otros sistemas***

El sistema no interactúa con otros sistemas, por lo tanto no corresponde desarrollar esta descripción.

4.2.2.8. Actividad ASI 8: Definición de Interfaces de Usuario

4.2.2.8.1. Tarea ASI 8.1: Especificación de Principios Generales de la Interfaz

- ***Especificación de Interfaz de Usuarios:***
  - ***Principios generales de la interfaz***
    - Todas las ventanas tendrán acceso a un menú de ayuda que se activará al presionar la tecla F10
    - Todas las pantallas se desarrollarán a partir de templates que permitirán identificar los datos generales, nombre del sistema y su logotipo, nombre del módulo, perfil de usuario.
    - Todos los mensajes de error se mostrarán a través de ventanas emergentes**.**
    - Todas las salidas impresas deberán incluir la fecha, el nombre del listado, el usuario que emitió el listado, el número de hoja.
    - En todas las eliminaciones deberá existir la confirmación de la misma por parte del usuario.
    - En todas las pantallas aparecerá el menú del usuario.
    - En todas las pantallas se posibilitará el cierre de la cesión.
    - En todas las pantallas la tecla de escape permitirá anular la operación que se esta realizando.

4.2.2.8.2. Tarea ASI 8.2: Identificación de Perfiles y Diálogos

- ***Especificación de Interfaz de Usuarios:***
  - ***Descomposición funcional en diálogos***

    No se podrá tener más de una pantalla abierta.

    El menú permanecerá fijo de acuerdo al perfil de cada usuario.

    Deberá existir una opción que permita volver a la pantalla anterior.

  - ***Catálogo de perfiles de usuario***

El sistema tiene dos niveles de seguridad:

- ✓ El acceso a las páginas Web
- ✓ El acceso a los datos almacenados en las Bases de Datos.

Por una cuestión de seguridad y simplicidad se solicitará el ingreso de una clave para el acceso a las páginas Web del servidor Apache y solo habrá un usuario para establecer la conexión a la base de datos

Perfiles de usuario: El sistema prevé tres perfiles de usuario, Administrador, supervisor y auditor:

- ✓ El perfil administrador, el módulo al que accede es el de Configuración, donde realiza la carga de los parámetros básicos del sistema, como por ejemplo la carga de la estructura de COBIT, la carga de la estructura de Areas, la carga de preguntas del relevamiento inicial y el profundo, la administración de usuarios.
- ✓ El perfil de supervisor permite el acceso a los módulos de Inicio, estudio preliminar, recursos, planificación, desarrollo e informe final. El perfil de jefe de proyecto se diferencia del de auditor ya que es la persona responsable de dar por iniciado un proyecto, administrará los recursos necesarios para cada proyecto y la planificación del mismo.
- ✓ El perfil del auditor permite el acceso a los módulos estudio preliminar, desarrollo e informes, a los módulos de Inicio, recursos y planificación accede solo a modo de consulta y no accede al módulo de configuración.

4.2.2.8.3. Tarea ASI 8.3: Especificación de Formatos Individuales de la Interfaz de Pantalla.

- ***Especificación de Interfaz de Usuarios:***
  - ***Formatos individuales de Interfaz de pantalla***
    - Las pantallas no podrán cambiar de tamaño, ni de ubicación.
    - El menú aparecerá con formato fijo a la izquierda de la pantalla.
  - ***Catalogo de controles y elementos de diseño de Interfaz de pantalla***
    - Los controles que se ocupen de listar, aparecerán activos cuando el usuario tenga la opción de listar.
    - Los controles que se ocupen de realizar modificaciones solo se activaran cuando el usuario pueda realizar una modificación.
    - Los controles que se ocupen de realizar un alta solo se activarán cuando el usuario pueda realizar un alta.

4.2.2.8.4. Tarea ASI 8.4: Especificación del Comportamiento Dinámico de la Interfaz

- ***Especificación de interfaz de usuario***
    - ***Modelo de navegación de interfaz de pantalla***

Para representar cada uno de los módulos se los identifica con los siguientes números:

- 1 = Configuración
- 2 = Inicio
- 3 = Estudio preliminar
- 4 = Recursos
- 5 = Planificación
- 6 = Desarrollo
- 7 = Informe Final

En la figura 4.16 se muestra el modelo navegacional del perfil Administrador:

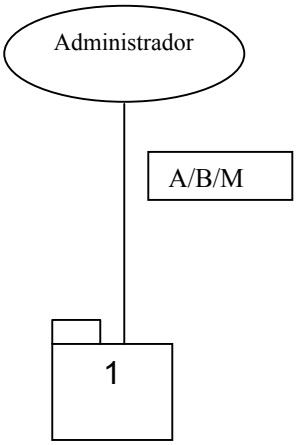


Figura 4.16.: Modelo Navegacional perfil Administrador

En la figura 4.17. se muestra el modelo navegacional del perfil supervisor:

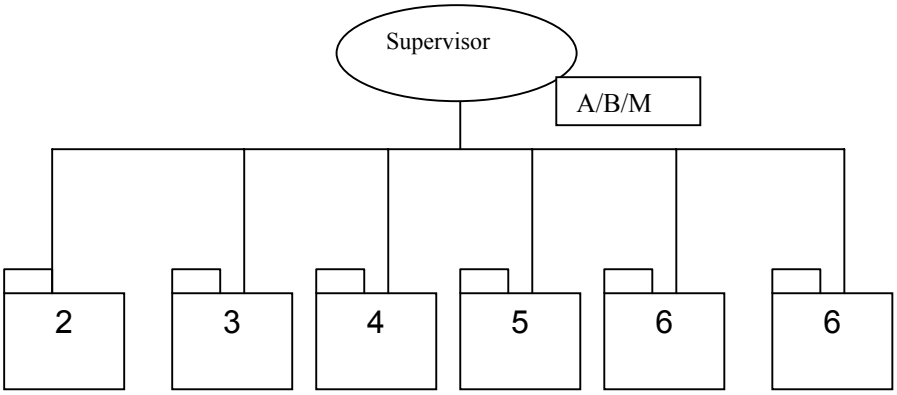


Figura 4.17. Modelo navegacional perfil Supervisor

La figura 4.18. muestra el diagrama navegacional del auditor

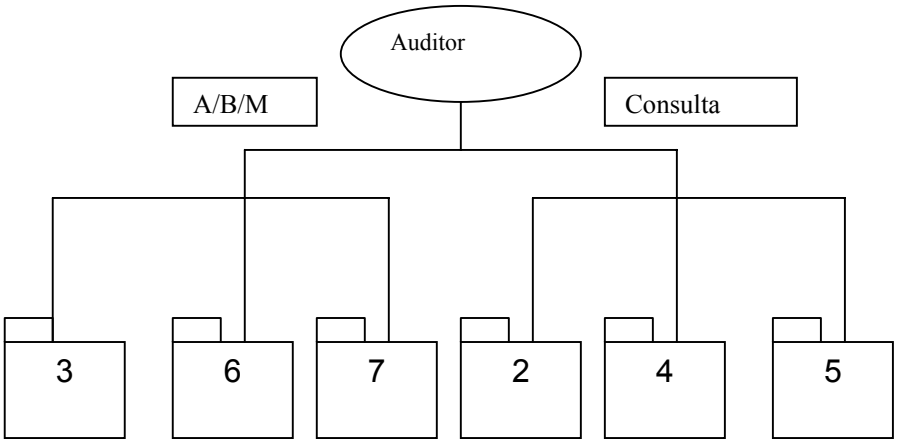


Figura 4.18. Modelo navegacional perfil Auditor

- ***Prototipo de interfaz interactiva***

La figura 4.19 muestra el prototipo de interfaz de ingreso al sistema:

Figura 4.19.: Prototipo Interfaz ingreso al sistema

La figura 4.20 muestra el prototipo de interfaz del perfil auditor

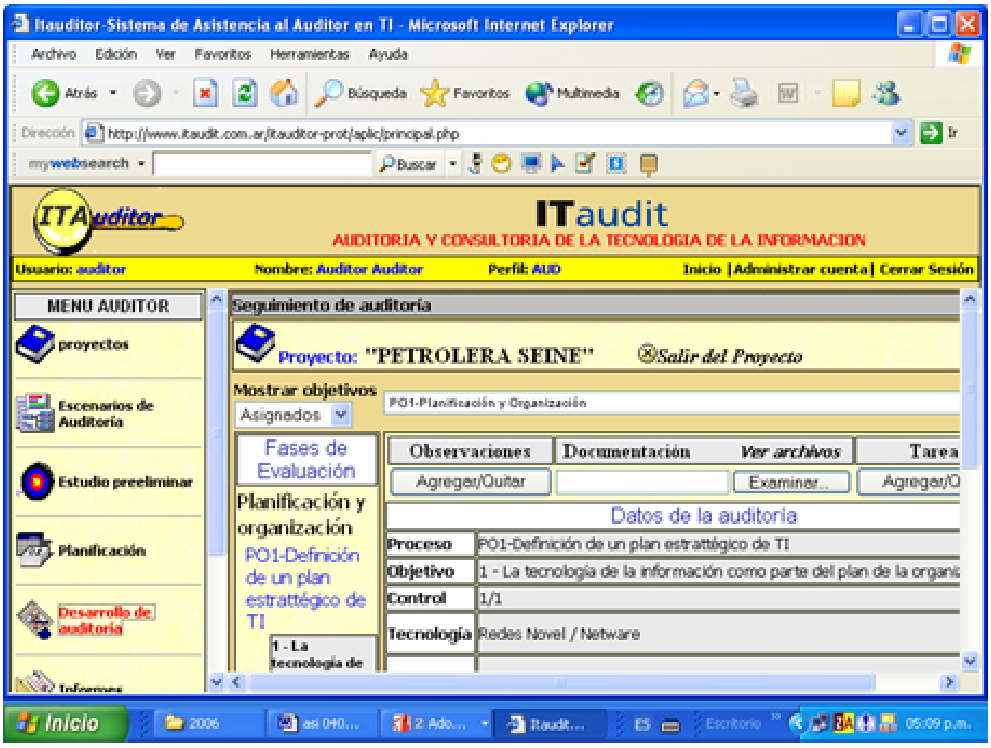


Figura 4.20. Prototipo interfaz Perfil auditor

La figura 4.21 muestra el prototipo de interfaz del perfil Supervisor:

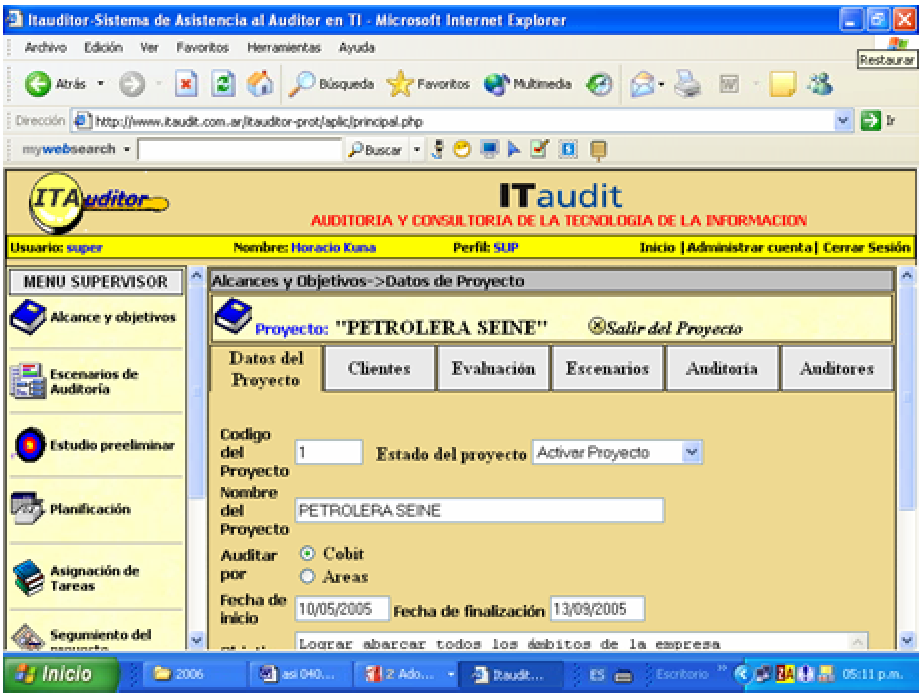


Figura 4.21: Prototipo de interfaz del perfil supervisor

La figura 4.22. muestra el prototipo de interfaz del perfil administrador:

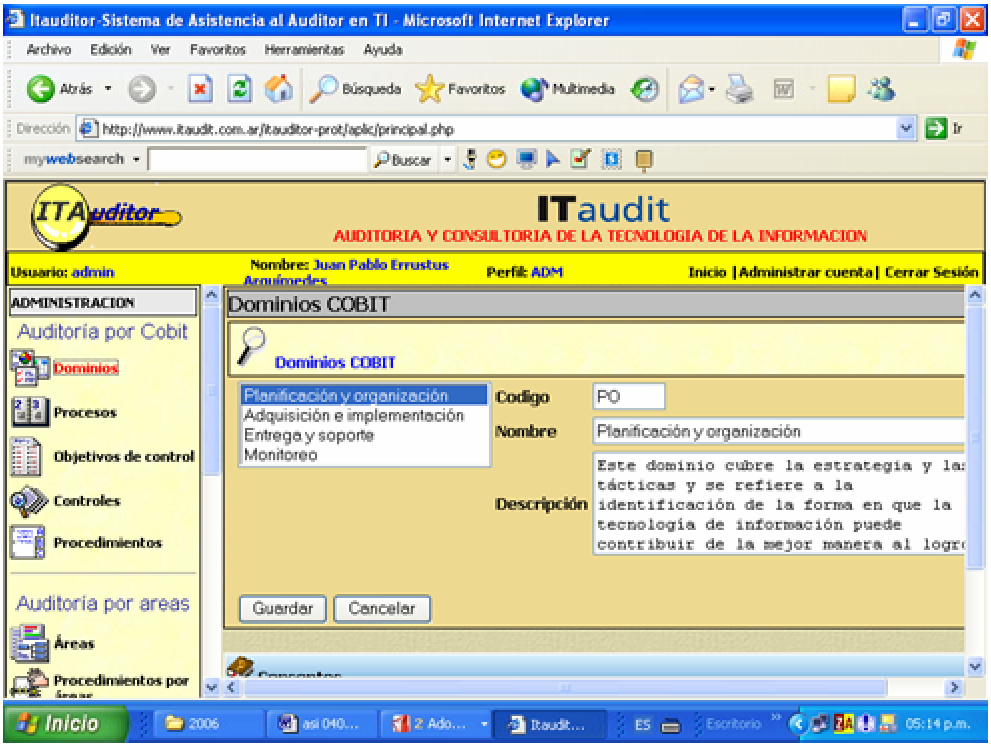


Figura 4.22.: Prototipo interfaz perfil administrador

En el *anexo 5 interfaces* se observan otros diseños de pantallas.

4.2.2.8.5.Tarea ASI 8.5: Especificación de Formatos de Impresión

- ***Especificación de la interfaz de usuario***
  - ***Formatos de impresión***

Los listados y reportes también tendrán templates de manera de separar el código HTML y el PHP. Al ser un desarrollo Web, el tamaño de la hoja y el tipo de impresión es administrado por el sistema operativo.

La cabecera tendrá los siguientes datos:

- Datos de la empresa que realiza la auditoría.
- Título del listado.
- Datos de la empresa Auditada

El detalle tendrá las siguientes características:

Distribuido en varias columnas, en el caso de tenerlas, con el título correspondiente en cada columna.

- Los número alineados por el punto decimal

- Títulos en negrita

El pie tendrá las siguientes características:

- Número de página y cantidad de páginas (X de Y), alineado a la izquierda
- Fecha y hora
- Usuario que emitió el informe

- ***Prototipo de interfaz de impresión***

La figura 4.23. muestra el prototipo de interfaz de impresión

Figura 4.23. Interfaz de impresión

4.2.2.9.Actividad ASI 9: Análisis de consistencia y especificación de requisitos

4.2.2.9.1.Tarea ASI 9.1: Verificación de los modelos

El uso de una herramienta CASE para el desarrollo del modelo de datos permitió realizar en forma automática los diferentes controles en el momento de

construir los modelo, tanto sea en lo relacionado con la consistencia del modelo, la definición de cada elemento, etc. Por lo tanto se da por cumplida esta tarea

4.2.2.9.2.Tarea ASI 9.2: Análisis de Consistencia entre métodos

Se da por cumplida esta tarea al utilizarse una herramienta CASE lo que permitió realizar controles de consistencia en el momento de la construcción de los modelos.

4.2.2.9.3.Tarea ASI 9.3: Validación de los Modelos

Esta tarea se realizó analizando y comparando los requisitos con los modelos realizados, se realizaron reuniones con los directores para validar el análisis realizado.

4.2.2.9.4.Tarea ASI 9.4: Elaboración de la Especificación de Requisitos de Software (ERS)

La Especificación de requisitos fue realizada en los siguientes documentos:

- ASI2.1 Obtención de requisitos
- ASI 6.2: Elaboración del Modelo Lógico de Datos
- ASI 7.1: Obtención del Modelo de Procesos del Sistema
- ASI 8.1: Especificación de Principios Generales de la Interfaz

Este conjunto de documentos componen la especificación de requisitos del sistema.

4.2.2.10. Actividad ASI 10: Especificación del plan de pruebas

4.2.2.10.1.Tarea ASI 10.1: Definición del Alcance de las Pruebas

- ***Plan de pruebas***
  - Especificación de los niveles de pruebas

Se realizarán pruebas de caja negra sobre cada uno de los módulos con el objetivo de comprobar los siguientes aspectos:

- Seguridad: Definición de usuarios, perfiles y accesos.
- Presentación: Relacionado con la apariencia del sistema y su concordancia con el diseño establecido.
- Consistencia de datos: Se controlará la consistencia entre cada uno de los datos que se ingresan.

- Funcionales: Se probarán cada una de las funciones del Prototipo desarrollado y su consistencia con los requisitos definidos en el Análisis. Se elaborará un documento con el resultado de estas pruebas.
- Carga de Datos: Para cada una de las funciones del sistema, se verificará que los datos sean correctamente cargados. Se elaborará un documento con el resultado de estas pruebas.
- Interfaz de Usuario: El usuario final emitirá opinión respecto de la navegación entre las diferentes páginas Web que componen la aplicación.

4.2.2.10.2.Tarea ASI 10.2: Definición de Requisitos del Entorno de Pruebas

- ***Plan de pruebas***
  - ***Definición de requisitos del entorno tecnológico***

    - Requisitos tecnológicos:

      Servidor Web con acceso a Internet. Pentium III o superior. El software instalado en este servidor deberá ser el Apache, Firebird, PHP y sistema operativo Linux

      Ordenador con acceso a acceso a Internet. Pentium III o superior. Deberá tener instalado un navegador tipo Mozila

    - Instalación de la aplicación

      Se deberá instalar la aplicación.

      Se deberá instalar la base de datos del sistema.

      Se deberá probar la instalación.

      Se deberá probar el acceso a Internet.

    - Realización de las pruebas

      Las pruebas se realizarán en el ordenador con acceso a Internet.

      Se documentarán todas las pruebas.

4.2.2.10.3.Tarea ASI 10.3: Definición de las Pruebas de Aceptación del Sistema

- ***Plan de pruebas***

Los criterios con los que el usuario validará el sistema son:

- ✓ Funcionalidad, el usuario validará que el sistema realice aquello para lo cual fue diseñado.
- ✓ Rendimiento, el usuario controlará que el rendimiento del sistema sea el adecuado.
- ✓ Seguridad, el usuario controlará que la seguridad del sistema cumpla con los requisitos no funcionales establecidos.

4.2.2.11.Actividad ASI 11: Aprobación del Análisis del sistema de información

4.2.2.11.1.Tarea ASI 11.1: Presentación y Aprobación del Análisis del Sistema de Información

- ***Aprobación del ASI***

Se realizó una reunión formal entre el tesista y los directores del proyecto donde se aprobó el Análisis del Sistema de Información

Capítulo 4

Solución

Sección 4.2.3. – Diseño del Sistema de Información

4.2.3. DISEÑO DEL SISTEMA DE INFORMACION

4.2.3.1. Actividad DSI 1: Definición de la Arquitectura del Sistema

4.2.3.1.1.Tarea DSI 1.1: Definición de Niveles de Arquitectura

- ***Diseño de la Arquitectura del Sistema***
    - ***Particionamiento Físico del Sistema de Información***

El Sistema IIAUDIT, es básicamente una aplicación Web dinámica y esta basado en la comunicación entre los siguientes elementos:

- ✓ Lenguaje de programación HTML.
- ✓ Lenguaje de programación PHP.
- ✓ La comunicación con un Web Server (Apache).
- ✓ Motor de base de datos relacional Firebird.

La aplicación se construye con los lenguajes HTML + PHP, donde el primero resuelve la interfaz con el usuario final y el segundo las reglas de negocios, y se accede al motor de base de datos Firebird donde están almacenados los datos

El servidor web Apache permite el acceso remoto a la aplicación, para esto tiene acceso al directorio donde se encuentran las páginas web del sistema.

La base de datos puede estar en el mismo servidor web o en otro equipo, siendo lo optimo contar con un servidor web y un servidor de base de datos, aunque también pueden estar en el mismo equipo físico.

Los datos que manejará el sistema no tienen un volumen que requiera en esta etapa tener dos servidores, en el caso que sea necesario para mejorar la performance se podrá instalar otro servidor para separar ambas funciones.

La figura 4.24. representa el diagrama de despliegue

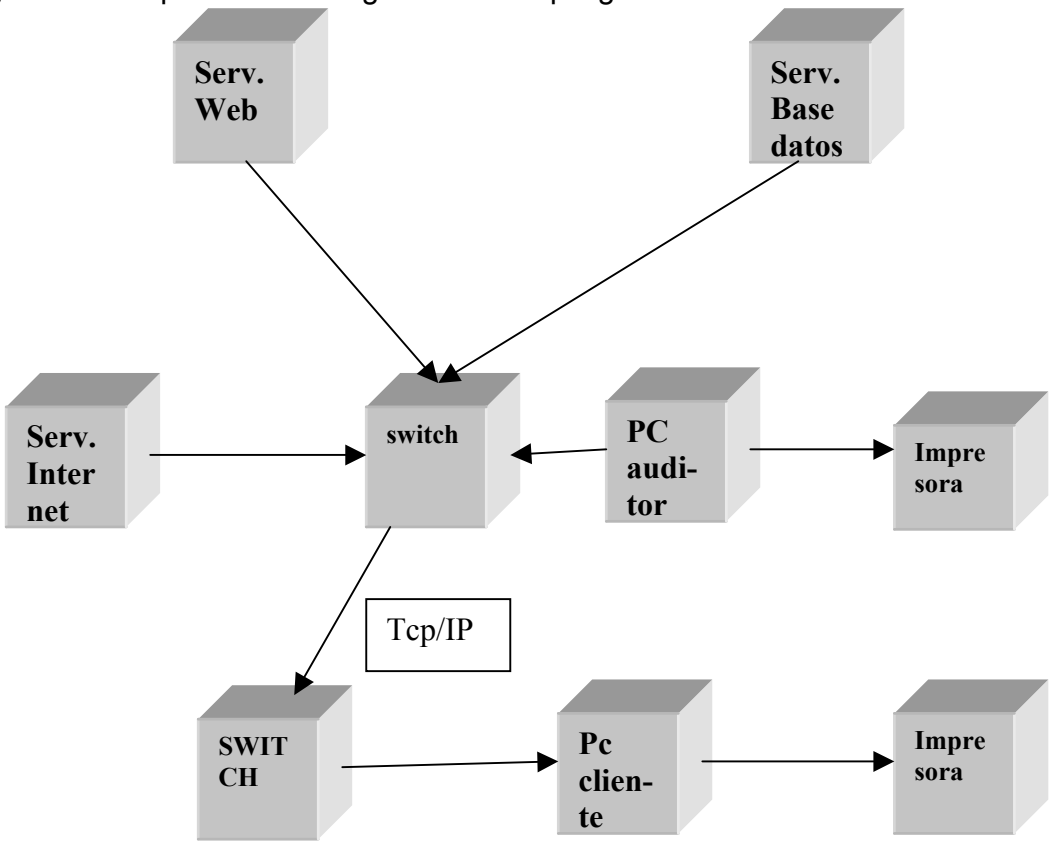


Figura 4.24.: Diagrama de despliegue

4.2.3.1.2. Tarea DSI 1.2: Identificación de Requisitos de Diseño y Construcción

- ***Catálogo de requisitos:***

No se han detectado nuevos requisitos a los ya detectados en la Tarea ASI 9.4: Elaboración de la Especificación de Requisitos Software (ERS), documentados en los siguientes documentos:

- ASI2.1 Obtención de requisitos
- ASI 6.2: Elaboración del Modelo Lógico de Datos
- ASI 7.1: Obtención del Modelo de Procesos del Sistema
- ASI 8.1: Especificación de Principios Generales de la Interfaz

4.2.3.1.3.Tarea DSI 1.3: Especificaciones de Excepción

- ***Catálogo de excepciones***

Se determinaron tres tipos de excepciones: comunicación, validación y permisos. Las excepciones de comunicación se relacionan con inconvenientes

que aparecen cuando no existe conexión entre los componentes principales del sistema; las excepciones de de validación se relacionan con aspecto que hacen a la aceptación de los datos a ingresar en el sistema; la excepciones de permisos tienen que ver la verificación que se hace a los usuarios que intentan ingresar al sistema.

Las tablas 4.12 a 4.19. representan las excepciones contempladas en la presente tesis:

Numero de Excepción	001-C
Tipo de excepción	Comunicación
Descripción de la excepción	El módulo intenta conectarse con la aplicación a través de la WEB
Condición	No se establece la conexión
Respuesta esperada	Mensaje de error: “No fue posible establecer la conexión”

Tabla 4.12.: Excepción 1 de Comunicación

Numero de Excepción	002-C
Tipo de excepción	Comunicación
Descripción de la excepción	El módulo intenta conectarse con la base de datos
Condición	No se establece la conexión
Respuesta esperada	Mensaje de error: “No fue posible establecer la conexión con la base de datos”

Tabla 4.13.: Excepción 2 de Comunicación

Numero de Excepción	003-C
Tipo de excepción	Comunicación
Descripción de la excepción	El módulo esta operando y se pierde la conexión con la aplicación
Condición	Se pierde la conexión con la aplicación
Respuesta esperada	Mensaje de error: “Se perdió la conexión”

Tabla 4.14.: Excepción 2 de Comunicación

Numero de Excepción	004-C
Tipo de excepción	Comunicación
Descripción de la excepción	El módulo esta operando y se pierde la conexión con la base de datos
Condición	No se establece la conexión con la base de datos
Respuesta esperada	Mensaje de error: “Se perdió la conexión con la base de datos”

Tabla 4.15.: Excepción 2 de Comunicación

Numero de Excepción	001-V
Tipo de excepción	Validación
Descripción de la excepción	Se intenta cargar un dato que se encuentra fuera de los rangos permitidos
Condición	Carga de datos
Respuesta esperada	Mensaje de error: “Valores fuera de rango”

Tabla 4.16.: Excepción 2 de Comunicación

Numero de Excepción	002-V
Tipo de excepción	Validación
Descripción de la excepción	Se intenta cargar un dato de distinto tipo al permitido
Condición	Carga de datos
Respuesta esperada	Mensaje de error: “Tipo de dato incorrecto”

Tabla 4.17.: Excepción 2 de Comunicación

Numero de Excepción	001-P
Tipo de excepción	Permiso
Descripción de la excepción	Se intenta ingresar al sistema con un usuario incorrecto
Condición	Ingreso al sistema
Respuesta esperada	Mensaje de error: “Usuario incorrecto”

Tabla 4.18.: Excepción 2 de Comunicación

Numero de Excepción	002-V
Tipo de excepción	Validación
Descripción de la excepción	Se intenta ingresar al sistema con una clave incorrecta
Condición	Ingreso al sistema
Respuesta esperada	Mensaje de error: “Clave incorrecta”

Tabla 4.19.: Excepción 2 de Comunicación

4.2.3.1.4.Tarea DSI 1.4: Especificación de Estándares y Normas de Diseño y Construcción

- ***Catálogo de normas***

No se detectan nuevos estándares y normas a las ya detectadas en el Análisis del Sistema de Información, por lo tanto se da por cumplida esta tarea.

4.2.3.1.5.Tarea DSI 1.5: Identificación de Subsistemas de Diseño

- ***Diseño de la Arquitectura del Sistema***
    - ***Descripción de los subsistemas de Diseño***

Se va a aplicar el three-tier framework, cuyos tres componentes principales son:

- ✓ La interfaz del usuario.
- ✓ Las reglas de negocios.
- ✓ Los datos.

El objetivo es facilitar el mantenimiento y reducir la complejidad aislando cada uno de los subsistemas de diseño.

Esta arquitectura permite ocultar las distintas capas, la interfaz de usuario (HTML) se comunica con la de reglas de negocios (PHP) y esta capa con la de datos.

Existen dos niveles de seguridad, uno relacionado con la aplicación y otro con la base de datos, las reglas de negocios gestionan la seguridad de la aplicación debiendo administrar distintos perfiles de usuarios, la capa de datos es responsable de administrar la seguridad de la base de datos, previéndose un único usuario con permisos para acceder a los datos almacenados.

4.2.3.1.6.Tarea DSI 1.6: Especificación del Entorno Tecnológico

- ***Entorno tecnológico del sistema***
  - ***Especificación del entorno tecnológico***

A continuación se especifican los distintos elementos de la infraestructura técnica que dan soporte al sistema ITAUDIT:

Entorno de Hardware

La tabla 4.20. muestra el entorno tecnológico del Hardware

Equipo	Nombre	Tarea	Ubicación
Pentium III o sup.	Servidor Web	Dar servicios Web	Auditor
Pentium III o sup.	Servidor Internet	Dar servicios de Internet	Auditor
Pentium III o sup.	Servidor Base de datos y aplicación	Base de datos y aplicación	Auditor
Pentium III o sup.	Pc auditor	Operar sistema	Auditor
Pentium III o sup.	PC cliente	Operar Sistema	Cliente

Tabla 4.20. Entorno tecnológico del Hardware

Entorno del software

La tabla 4.21. representa el entorno tecnológico del software

Nombre	Función	PC
Apache	Dar servicios Web	Servidor Web
Linux	Dar servicios de Internet	Servidor Internet
Firebird 1.5.4	Gestor de base de datos	Servidor Base de datos y aplicación
PHP	Lenguaje de programación	Servidor Base de datos y aplicación
Linux / Windows	Sistema operativo	Servidor Base de datos y aplicación
Linux / Windows	Sistema operativo	Pc auditor
Linux / Windows	Sistema operativo	Pc cliente

Tabla 4.21. Entorno tecnológico del Software

- ***Restricciones técnicas: por cada elemento de la infraestructura antes mencionada.***

No se detectan restricciones técnicas

- ***Estimación de planificación de capacidades***

  - ✓ Espacio en disco servidor web y de base de datos: 100 Mb
  - ✓ Al tratarse de una aplicación web son mínimos los requerimientos del cliente.
  - ✓ Memoria de servidor de base de datos y web: 512 Mb
  - ✓ Memoria cliente: 128 Mb
  - ✓ Ancho de banda del enlace en el cliente mínimo requerido: 512 Mb
  - ✓ Ancho de banda del enlace del servidor web mínimo requerido: 1 Gb

4.2.3.1.7.Tarea DSI 1.7: Especificación de Requisitos de Operación y Seguridad

- ***Procedimientos de seguridad y control de acceso***

Los aspectos relacionados con la seguridad ya se han desarrollado en la Tarea ASI 8.2: Identificación de Perfiles y Diálogos, al no aparecer nuevos aspectos relacionados con el tema, se considera aplicable dicho documento.

- ***Procedimientos de administración y operación***

En cuanto a la operación del sistema no existen horarios particulares para la operación. Las tareas de administración del sistema una vez puesto en producción son:

  - ✓ Administración de usuarios, carga y definición de perfiles, actualización de claves de ingreso.
  - ✓ Administración de la base de datos, actualización de la estructura de la misma.
  - ✓ Back-ups de la base de datos y de la aplicación.

4.2.3.2. Actividad DSI 2: Diseño de la Arquitectura de Soporte

4.2.3.2.1.Tarea DSI 2.1: Diseño de Subsistemas de Soporte

- ***Diseño detallado de los subsistemas de soporte***

Dado que se dispone en la instalación de servicios comunes que respondan satisfactoriamente a los requisitos planteados, esta tarea no se desarrolla.

4.2.3.2.2.Tarea DSI 2.2: Identificación de Mecanismos Genéricos de Diseño

- ***Mecanismos Genéricos de diseño y construcción.***

Se utilizan Templates para mantener una interfaz común en toda la aplicación. Esto ya fue descripto en las tareas ASI 8.1. a 8.5.

4.2.3.3. Actividad DSI 3: Diseño de casos de uso reales

Esta actividad, que se realiza solo en el caso de Diseño Orientado a Objetos, tiene como propósito especificar el comportamiento del sistema de información para un caso de uso, mediante objetos o subsistemas de diseño que interactúan, y determinar las operaciones de las clases e interfaces de los distintos subsistemas de diseño.

Para ello, una vez identificadas las clases participantes dentro de un caso de uso, es necesario completar los escenarios que se recogen del análisis, incluyendo las clases de diseño que correspondan y teniendo en cuenta las restricciones del entorno tecnológico, esto es, detalles relacionados con la implementación del sistema. Es necesario analizar los comportamientos de excepción para dichos escenarios. Algunos de ellos pueden haber sido identificados en el proceso de análisis, aunque no se resuelven hasta este momento. Dichas excepciones se añadirán al catálogo de excepciones para facilitar las pruebas.

Algunos de los escenarios detallados requerirán una nueva interfaz de usuario. Por este motivo es necesario diseñar el formato de cada una de las pantallas o impresos identificados.

Es importante validar que los subsistemas definidos en la tarea Identificación de Subsistemas de Diseño (DSI 1.5) tienen la mínima interfaz con otros subsistemas. Por este motivo, se elaboran los escenarios al nivel de subsistemas y, de esta forma, se delimitan las interfaces necesarias para cada uno de ellos, teniendo en cuenta toda la funcionalidad del sistema que recogen los casos de uso. Además, durante esta actividad pueden surgir requisitos de implementación, que se recogen en el catálogo de requisitos.

Las tareas de esta actividad se realizan en paralelo con las de Diseño de Clases (DSI 4).

No corresponde dado que no se aplica orientación a objetos

4.2.3.4.Actividad DSI 4: Diseño de clases

El propósito de esta actividad, que se realiza sólo en el caso de Diseño Orientado a Objetos, es transformar el modelo de clases lógico, que proviene del análisis, en un modelo de clases de diseño. Dicho modelo recoge la especificación detallada de cada una de las clases, es decir, sus atributos, operaciones, métodos, y el diseño preciso de las relaciones establecidas entre ellas, bien sean de agregación, asociación o jerarquía. Para llevar a cabo todos estos puntos, se tienen en cuenta las decisiones tomadas sobre el entorno tecnológico y el entorno de desarrollo elegido para la implementación.

Se identifican las clases de diseño, que denominamos clases adicionales, en función del estudio de los escenarios de los casos de uso, que se está realizando en paralelo en la actividad Diseño de Casos de Uso Reales (DSI 3), y aplicando los mecanismos genéricos de diseño que se consideren convenientes por el tipo de especificaciones tecnológicas y de desarrollo. Entre ellas se encuentran clases abstractas, que integran características comunes con el objetivo de especializarlas en clases derivadas. Se diseñan las clases de interfaz de usuario, que provienen del análisis. Como consecuencia del estudio de los escenarios secundarios que se está realizando, pueden aparecer nuevas clases de interfaz.

También hay que considerar que, por el diseño de las asociaciones y agregaciones, pueden aparecer nuevas clases, o desaparecer incluyendo sus atributos y métodos en otras, si se considera conveniente por temas de optimización.

La jerarquía entre las clases se va estableciendo a lo largo de esta actividad, a medida que se van identificando comportamientos comunes en las clases, aunque haya una tarea propia de diseño de la jerarquía.

Otro de los objetivos del diseño de las clases es identificar para cada clase, los atributos, las operaciones que cubren las responsabilidades que se identificaron en el análisis, y la especificación de los métodos que implementan esas operaciones, analizando los escenarios del Diseño de Casos de Uso Reales (DSI 3). Se determina la visibilidad de los atributos y operaciones de cada clase, con respecto a las otras clases del modelo.

Una vez que se ha elaborado el modelo de clases, se define la estructura física de los datos correspondiente a ese modelo, en la actividad Diseño Físico de Datos (DSI 6).

Además, en los casos en que sea necesaria una migración de datos de otros sistemas o una carga inicial de información, se realizará su especificación a partir del modelo de clases y las estructuras de datos de los sistemas origen.

Como resultado de todo lo anterior se actualiza el modelo de clases del análisis, una vez recogidas las decisiones de diseño.

No corresponde dado que no se aplica orientación a objetos

4.2.3.5. Actividad 5: Diseño de la Arquitectura de Módulos del Sistema

4.2.3.5.1.Tarea DSI 5.1: Diseño de Módulos del Sistema

- ***Diseño de la Arquitectura Modular del Sistema.***

Esta tarea fue desarrollada en ASI 3.1: Determinación de Subsistemas de Análisis, al no encontrarse nuevos elementos se da por cumplida.

4.2.3.5.2.Tarea DSI 5.2: Diseño de Comunicaciones entre Módulos

- ***Diseño de la arquitectura modular del sistema***

La tabla 4.22 representa la relación que existe entre cada uno de los módulos

origen	**Módulo destino**	**Relación**
Inicio / configuración	Estudio preliminar	En el módulo de inicio se especifica el tipo de auditoria a realizar, por áreas o Cobit, y el alcance de la auditoría (definiendo que áreas o procesos de COBIT se abordará) El estudio preliminar esta acotado al tipo de auditoria y el alcance especificado en el módulo de inicio. En el módulo de configuración se carga el check-list del estudio preliminar, cada pregunta se asocia a un área o Dominio/Proceso de Cobit
Estudio preliminar / Inicio	Recursos	En el inicio se determina el limite de la auditoría El estudio preliminar brinda información

		relacionada con las características de la empresa y el tamaño de la misma. Los recursos que el sistema debe establecer se relacionan con los resultados del estudio preliminar
Recursos / Inicio / estudio preliminar	Planificación	El inicio establece los límites de la auditoría y el tipo de auditoria a realizar. El estudio preliminar establece las características generales de la empresa a auditar La planificación debe surgir del tipo de auditoria a realizar (COBIT o Areas), el limite de la auditoría y la información obtenida en el estudio preliminar
Planificación / configuración	Desarrollo	La planificación establece las actividades a desarrollar de acuerdo a los limites de la auditoría, el tipo de auditoria y la información obtenida en el estudio preliminar En la configuración se ingresa el check list del desarrollo de la auditoría El desarrollo se hace considerando las preguntas ingresadas en el módulo de configuración y filtrando las mismas de acuerdo a lo establecido en la planificación
Desarrollo	Informe final	El desarrollo da como resultado un conjunto de riesgos y recomendaciones El informe final se elabora en función de los riesgos detectados en el desarrollo y las recomendaciones obtenidas.

Tabla 4.22. Relaciones entre módulos

4.2.3.5.3. Tarea DSI 5.3: Revisión de la Interfaz de Usuario

- ***Diseño de interfaz de usuario***

Se verificaron las especificaciones ya definidas y dado que no se consideraron nuevas, se considera validos los documentos obtenidos en las tareas ASI 8.1. a ASI 8.4.

4.2.3.6.Actividad DSI 6: Diseño Físico de Datos

4.2.3.6.1.Tarea DSI 6.1: Diseño del Modelo Físico de Datos

- ***Modelo físico de datos***

La tabla 4.23 muestra el modelo físico de datos

Tablas

Table Name	Table Type	Primary Keys	# Col
Areas	Independent	Cod_area,	2
Areas_por -Proyecto	Dependent	Id_proyecto,Cod_area,	4
Auditores	Independent	Cod_auditor,	6
Auditores por proyecto	Dependent	Id_proyecto,Cod_auditor	2
Clientes	Independent	Cod_cliente,	8
Criterios	Independent	Cod_criterio,	2
criterios_proceso	Dependent	Cod_proceso,Cod_dominio,Cod_criterio	3
Dominio	Independent	Cod_dominio,	2
Dominio_por_proyecto	Dependent	Id_proyecto,Cod_dominio	2
Dominio_proceso_proyecto	Dependent	Id_proyecto,Cod_dominio,Cod_proceso,	5
informe_proyecto	Dependent	cod_informe,Id_proyecto,	4
item_informe	Dependent	Cod_item,cod_informe,Id_proyecto,	4
Objetivo_control	Dependent	Cod_objetivo_control,Cod_proceso,Cod_dominio,	4
Opcion_resp_rel_inic	Dependent	Cod_resp,cod_pregunta,	4
Opcion_resp_rel_inic_1	Dependent	Cod_resp,cod_pregunta,	4
Opcion_resp_rel_inic_2	Dependent	Cod_resp,cod_pregunta,Id_proyecto,Cod_area,Cod_sector,	7
Opcion_resp_rel_inic_3	Dependent	Cod_resp,cod_pregunta,Id_proyecto,Cod_dominio,Cod_proceso,	7
Opcion_resp_rel_prof	Dependent	Cod_preg_prof,Cod_resp_resp_prof,	4
Opcion_resp_rel_prof_1	Dependent	Cod_resp_reñ_prof,Cod_preg_prof,Cod_objetivo_control,Cod_proceso,Cod_dominio,	7
Opcion_resp_rel_prof_1_1	Dependent	Cod_resp_reñ_prof,Cod_preg_prof,Cod_objetivo_control,Cod_proceso,Cod_dominio,Id_proyecto,Cod_sector,	9
Opcion_resp_rel_prof_2	Dependent	Cod_preg_prof,Cod_resp_reñ_prof,Id_proyecto,Cod_area,	6
Perfil	Independent	Cod_perfil,	2
Perfil_1	Independent	Cod_perfil,	2
Perfil_area	Dependent	Cod_perfil,Cod_area	2
Perfil_por_auditor	Dependent	Cod_perfil,Cod_auditor	2
Perfiles_por_proceso	Dependent	Cod_perfil,Cod_proceso,Cod_dominio	3
Proced_por_area	Dependent	Cod_area,Cod_procedimiento	2
Procedimiento	Independent	Cod_procedimiento,	2
Procedimiento_proceso	Dependent	Cod_procedimiento,Cod_proceso,Co	3

		d_dominio	
Proceso	Dependent	Cod_proceso,Cod_dominio	2
Proyectos	Independent	Id_proyecto,	5
recomendaciones	Dependent	Cod_preg_prof,Cod_recomendacion, Cod_resp_resp_prof,	4
recomendaciones_1	Dependent	Cod_preg_prof,Cod_recomendacion, Cod_resp_reñ_prof,Cod_objetivo_control,Cod_proceso,Cod_dominio,	7
Recursos	Independent	Cod_recurso,	2
Recursos_proceso	Dependent	Cod_proceso,Cod_dominio,Cod_recurso	3
Relevamiento_inicial	Independent	cod_pregunta,	3
Relevamiento_inicial_1	Independent	cod_pregunta,	5
Relevamiento_profundo	Independent	Cod_preg_prof,	3
Relevamiento_profundo_1	Dependent	Cod_preg_prof,Cod_objetivo_control, Cod_proceso,Cod_dominio,	6
Sectores_a_Auditar	Dependent	Cod_sector,Id_proyecto,	3
Sectores_a_Auditar_1	Independent	Cod_sector,Id_proyecto,	3
tareas_por_proyecto	Dependent	Cod_tareaId_proyecto	6

Areas

Table Name	Areas
Owner Name	
Primary Keys	Cod_area

Columns

Column Name	Domain	Datatype	Null	Definition
Cod_area		INTEGER	N	
desc_area		VARCHAR(40)	Y	

Areas_por -Proyecto

Table Name	Areas_por –Proyecto
Owner Name	
Primary Keys	Id_proyecto,Cod_area

Columns

Column Name	Domain	Datatype	Null	Definition
Id_proyecto		INTEGER	N	
Cod_area		INTEGER	N	
Observaciones_area		CHAR(10)	Y	
Documentacion_adjunta_area		CHAR(10)	Y	

Auditores

Table Name	Auditores
Owner Name	
Primary Keys	Cod_auditor

Columns

Column Name	Domain	Datatype	Null	Definition
Cod_auditor		INTEGER	N	
Nombre		VARCHAR(40	Y	

		)		
Telefono		CHAR(10)	Y	
Apellido		VARCHAR(40)	Y	
Titulo		CHAR(10)	Y	
e-mail		CHAR(10)	Y	

Auditores por proyecto

Table Name	Auditores por proyecto
Owner Name	
Primary Keys	Id_proyecto,Cod_auditor

Columns

Column Name	Domain	Datatype	Null	Definition
Id_proyecto		INTEGER	N	
Cod_auditor		INTEGER	N	

Clientes

Table Name	Clientes
Owner Name	
Primary Keys	Cod_cliente

Columns

Column Name	Domain	Datatype	Null	Definition
Cod_cliente		INTEGER	N	
Apellido_cli		CHAR(10)	Y	
Nombre_cli		CHAR(10)	Y	
Direccion_cli		CHAR(10)	Y	
Localidad		CHAR(10)	Y	
Provincia		CHAR(10)	Y	
Pais		CHAR(10)	Y	
e-mail		CHAR(10)	Y	

Criterios

Table Name	Criterios
Owner Name	
Primary Keys	Cod_criterio

Columns

Column Name	Domain	Datatype	Null	Definition
Cod_criterio		INTEGER	N	
desc_criterio		CHAR(10)	Y	

criterios_proceso

Table Name	criterios_proceso
Owner Name	
Primary Keys	Cod_proceso,Cod_dominio,Cod_criterio

Columns

Column Name	Domain	Datatype	Null	Definition
Cod_proceso		CHAR(10)	N	
Cod_dominio		INTEGER	N	
Cod_criterio		INTEGER	N	

Dominio

Table Name	Dominio
Owner Name	
Primary Keys	Cod_dominio

Columns

Column Name	Domain	Datatype	Null	Definition
Cod_dominio		INTEGER	N	
desc_dominio		CHAR(10)	Y	

Dominio_por_proyecto

Table Name	Dominio_por_proyecto
Owner Name	
Primary Keys	Id_proyecto,Cod_dominio

Columns

Column Name	Domain	Datatype	Null	Definition
Id_proyecto		INTEGER	N	
Cod_dominio		INTEGER	N	

Dominio_proceso_proyecto

Table Name	Dominio_proceso_proyecto
Owner Name	
Primary Keys	Id_proyecto,Cod_dominio,Cod_proceso

Columns

Column Name	Domain	Datatype	Null	Definition
Id_proyecto		INTEGER	N	
Cod_dominio		INTEGER	N	
Cod_proceso		CHAR(10)	N	
Observaciones_proceso		CHAR(10)	Y	
Documentacion_adjunta_proceso		CHAR(10)	Y	

informe_proyecto

Table Name	informe_proyecto
Owner Name	
Primary Keys	cod_informe,Id_proyecto

Columns

Column Name	Domain	Datatype	Null	Definition
cod_informe		CHAR(10)	N	
Id_proyecto		INTEGER	N	
observa_info		CHAR(10)	Y	
fecha_info		CHAR(10)	Y	

item_informe

Table Name	item_informe
Owner Name	
Primary Keys	Cod_item,cod_informe,Id_proyecto

Columns

Column Name	Domain	Datatype	Null	Definition
Cod_item		CHAR(10)	N	
cod_informe		CHAR(10)	N	
Id_proyecto		INTEGER	N	
desc_item_info		CHAR(10)	Y	

Objetivo_control

Table Name	Objetivo_control
Owner Name	
Primary Keys	Cod_objetivo_control,Cod_proceso,Cod_dominio

Columns

Column Name	Domain	Datatype	Null	Definition
Cod_objetivo_control		INTEGER	N	
Cod_proceso		CHAR(10)	N	
Cod_dominio		INTEGER	N	
Descripcion_objetivo_control		CHAR(10)	Y	

Opcion_resp_rel_inic

Table Name	Opcion_resp_rel_inic
Owner Name	
Primary Keys	Cod_resp,cod_pregunta

Columns

Column Name	Domain	Datatype	Null	Definition
Cod_resp		INTEGER	N	
cod_pregunta		INTEGER	N	
opcion_respuesta		CHAR(10)	Y	
riesgo		CHAR(10)	Y	

Opcion_resp_rel_inic_1

Table Name	Opcion_resp_rel_inic_1
Owner Name	

Primary Keys	Cod_resp,cod_pregunta

Columns

Column Name	Domain	Datatype	Null	Definition
Cod_resp		INTEGER	N	
cod_pregunta		INTEGER	N	
Opcion_respuesta		CHAR(10)	Y	
Riesgo		CHAR(10)	Y	

Opcion_resp_rel_inic_2

Table Name	Opcion_resp_rel_inic_2
Owner Name	
Primary Keys	Cod_resp,cod_pregunta,Id_proyecto,Cod_area,Cod_sector

Columns

Column Name	Domain	Datatype	Null	Definition
Cod_resp		INTEGER	N	
cod_pregunta		INTEGER	N	
Id_proyecto		INTEGER	N	
Cod_area		INTEGER	N	
Cod_sector		INTEGER	N	
Riesgo_area		CHAR(10)	Y	
respuesta_area		CHAR(10)	Y	

Opcion_resp_rel_inic_3

Table Name	Opcion_resp_rel_inic_3
Owner Name	
Primary Keys	Cod_resp,cod_pregunta,Id_proyecto,Cod_dominio,Cod_proceso

Columns

Column Name	Domain	Datatype	Null	Definition
Cod_resp		INTEGER	N	
cod_pregunta		INTEGER	N	
Id_proyecto		INTEGER	N	
Cod_dominio		INTEGER	N	
Cod_proceso		CHAR(10)	N	
respuesta_proceso		CHAR(10)	Y	
riesgo_proceso		CHAR(10)	Y	

Opcion_resp_rel_prof

Table Name	Opcion_resp_rel_prof
Owner Name	
Primary Keys	Cod_preg_prof,Cod_resp_resp_prof

Columns

Column Name	Domain	Datatype	Null	Definition
Cod_preg_prof		INTEGER	N	

Cod_resp_resp_prof		INTEGER	N	
Riesgo_rel_prof		CHAR(10)	Y	
respuesta_rel_prof		CHAR(10)	Y	

Opcion_resp_rel_prof_1

Table Name	Opcion_resp_rel_prof_1
Owner Name	
Primary Keys	Cod_resp_reñ_prof,Cod_preg_prof,Cod_objetivo_control,Cod_proceso,Cod_dominio

Columns

Column Name	Domain	Datatype	Null	Definition
Cod_resp_reñ_prof		INTEGER	N	
Cod_preg_prof		INTEGER	N	
Cod_objetivo_control		INTEGER	N	
Cod_proceso		CHAR(10)	N	
Cod_dominio		INTEGER	N	
Resp_rel_prof		CHAR(10)	Y	
Riesgo_resp_rel_prof		CHAR(10)	Y	

Opcion_resp_rel_prof_1_1

Table Name	Opcion_resp_rel_prof_1_1
Owner Name	
Primary Keys	Cod_resp_reñ_prof,Cod_preg_prof,Cod_objetivo_control,Cod_proceso,Cod_dominio,Id_proyecto,Cod_sector

Columns

Column Name	Domain	Datatype	Null	Definition
Cod_resp_reñ_prof		INTEGER	N	
Cod_preg_prof		INTEGER	N	
Cod_objetivo_control		INTEGER	N	
Cod_proceso		CHAR(10)	N	
Cod_dominio		INTEGER	N	
Id_proyecto		INTEGER	N	
Cod_sector		INTEGER	N	
Riesgo_resp-rel_prof		CHAR(10)	Y	
Resp_rel_prof		CHAR(10)	Y	

Opcion_resp_rel_prof_2

Table Name	Opcion_resp_rel_prof_2
Owner Name	
Primary Keys	Cod_preg_prof,Cod_resp_reñ_prof,Id_proyecto,Cod_area

Columns

Column Name	Domain	Datatype	Null	Definition
Cod_preg_prof		INTEGER	N	
Cod_resp_reñ_prof		INTEGER	N	
Id_proyecto		INTEGER	N	
Cod_area		INTEGER	N	
Resp_rel_prof		CHAR(10)	Y	
Riesgo_resp_rel_prof		CHAR(10)	Y	

Perfil

Table Name	Perfil
Owner Name	
Primary Keys	Cod_perfil

Columns

Column Name	Domain	Datatype	Null	Definition
Cod_perfil		INTEGER	N	
Desc_perfil		CHAR(10)	Y	

Perfil_1

Table Name	Perfil_1
Owner Name	
Primary Keys	Cod_perfil

Columns

Column Name	Domain	Datatype	Null	Definition
Cod_perfil		INTEGER	N	
Desc_perfil		CHAR(10)	Y	

Perfil_area

Table Name	Perfil_area
Owner Name	
Primary Keys	Cod_perfil,Cod_area

Columns

Column Name	Domain	Datatype	Null	Definition
Cod_perfil		INTEGER	N	
Cod_area		INTEGER	N	

Perfil_por_auditor

Table Name	Perfil_por_auditor
Owner Name	
Primary Keys	Cod_perfil,Cod_auditor

Columns

Column Name	Domain	Datatype	Null	Definition
Cod_perfil		INTEGER	N	
Cod_auditor		INTEGER	N	

Perfiles_por_proceso

Table Name	Perfiles_por_proceso
Owner Name	
Primary Keys	Cod_perfil,Cod_proceso,Cod_dominio

Columns

Column Name	Domain	Datatype	Null	Definition
Cod_perfil		INTEGER	N	
Cod_proceso		CHAR(10)	N	
Cod_dominio		INTEGER	N	

Proced_por_area

Table Name	Proced_por_area
Owner Name	
Primary Keys	Cod_area,Cod_procedimiento

Columns

Column Name	Domain	Datatype	Null	Definition
Cod_area		INTEGER	N	
Cod_procedimiento		INTEGER	N	

Procedimiento

Table Name	Procedimiento
Owner Name	
Primary Keys	Cod_procedimiento

Columns

Column Name	Domain	Datatype	Null	Definition
Cod_procedimiento		INTEGER	N	
Desc_procedimiento		CHAR(10)	Y	

Procedimiento_proceso

Table Name	Procedimiento_proceso
Owner Name	
Primary Keys	Cod_procedimiento,Cod_proceso,Cod_dominio

Columns

Column Name	Domain	Datatype	Null	Definition
Cod_procedimient		INTEGER	N	

o				
Cod_proceso		CHAR(10)	N	
Cod_dominio		INTEGER	N	

Proceso

Table Name	Proceso
Owner Name	
Primary Keys	Cod_proceso,Cod_dominio

Columns

Column Name	Domain	Datatype	Null	Definition
Cod_proceso		CHAR(10)	N	
Cod_dominio		INTEGER	N	

Proyectos

Table Name	Proyectos
Owner Name	
Primary Keys	Id_proyecto

Columns

Column Name	Domain	Datatype	Null	Definition
Id_proyecto		INTEGER	N	
Cod_cliente		INTEGER	N	
fecha_fin_proyecto		CHAR(10)	Y	
fecha_inicio_proyecto		CHAR(10)	Y	
observaciones_proyecto		CHAR(10)	Y	

recomendaciones

Table Name	recomendaciones
Owner Name	
Primary Keys	Cod_preg_prof,Cod_recomendacion,Cod_resp_resp_prof

Columns

Column Name	Domain	Datatype	Null	Definition
Cod_preg_prof		INTEGER	N	
Cod_recomendacion		INTEGER	N	
Cod_resp_resp_prof		INTEGER	N	
observa_recomendacion		CHAR(10)	Y	

recomendaciones_1

Table Name	recomendaciones_1
Owner Name	
Primary Keys	Cod_preg_prof,Cod_recomendacion,Cod_resp_reñ_prof,Cod_objetivo_control,Cod_proceso,Cod_dominio

Columns

Column Name	Domain	Datatype	Null	Definition
Cod_preg_prof		INTEGER	N	
Cod_recomendacion		INTEGER	N	
Cod_resp_reñ_prof		INTEGER	N	
Cod_objetivo_control		INTEGER	N	
Cod_proceso		CHAR(10)	N	
Cod_dominio		INTEGER	N	
observacion_recomendacion		CHAR(10)	Y	

Recursos

Table Name	Recursos
Owner Name	
Primary Keys	Cod_recurso

Columns

Column Name	Domain	Datatype	Null	Definition
Cod_recurso		INTEGER	N	
desc_recurso		CHAR(10)	Y	

Recursos_proceso

Table Name	Recursos_proceso
Owner Name	
Primary Keys	Cod_proceso,Cod_dominio,Cod_recurso

Columns

Column Name	Domain	Datatype	Null	Definition
Cod_proceso		CHAR(10)	N	
Cod_dominio		INTEGER	N	
Cod_recurso		INTEGER	N	

Relevamiento_inicial

Table Name	Relevamiento_inicial
Owner Name	
Primary Keys	cod_pregunta

Columns

Column Name	Domain	Datatype	Null	Definition
cod_pregunta		INTEGER	N	
Cod_area		INTEGER	Y	
preg_rel_inicial		CHAR(10)	Y	

Relevamiento_inicial_1

Table Name	Relevamiento_inicial_1
Owner Name	
Primary Keys	cod_pregunta

Columns

Column Name	Domain	Datatype	Null	Definition
cod_pregunta		INTEGER	N	
Cod_area		INTEGER	Y	
Cod_proceso		CHAR(10)	N	
Cod_dominio		INTEGER	N	
preg_rel_inicial		CHAR(10)	Y	

Relevamiento_profundo

Table Name	Relevamiento_profundo
Owner Name	
Primary Keys	Cod_preg_prof

Columns

Column Name	Domain	Datatype	Null	Definition
Cod_preg_prof		INTEGER	N	
Cod_area		INTEGER	N	
preg_rel_prof		CHAR(10)	Y	

Relevamiento_profundo_1

Table Name	Relevamiento_profundo_1
Owner Name	
Primary Keys	Cod_preg_prof,Cod_objetivo_control,Cod_proceso,Cod_dominio

Columns

Column Name	Domain	Datatype	Null	Definition
Cod_preg_prof		INTEGER	N	
Cod_objetivo_control		INTEGER	N	
Cod_proceso		CHAR(10)	N	
Cod_dominio		INTEGER	N	
Cod_area		INTEGER	N	
preg_rel_prof		CHAR(10)	Y	

Sectores_a_Auditar

Table Name	Sectores_a_Auditar
Owner Name	
Primary Keys	Cod_sector,Id_proyecto

Columns

Column Name	Domain	Datatype	Null	Definition
Cod_sector		INTEGER	N	
Id_proyecto		INTEGER	N	
observa_sector		CHAR(10)	Y	

Sectores_a_Auditar_1

Table Name	Sectores_a_Auditar_1
Owner Name	
Primary Keys	Cod_sector,Id_proyecto

Columns

Column Name	Domain	Datatype	Null	Definition
Cod_sector		INTEGER	N	
Id_proyecto		INTEGER	N	
observa_sector		CHAR(10)	Y	

tareas_por_proyecto

Table Name	tareas_por_proyecto
Owner Name	
Primary Keys	Cod_tarea,Id_proyecto

Columns

Column Name	Domain	Datatype	Null	Definition
Cod_tarea		CHAR(10)	N	
Id_proyecto		INTEGER	N	
desc_tarea		CHAR(10)	Y	
fecha_inicio_tarea		CHAR(10)	Y	
fecha_fin_tarea		CHAR(10)	Y	
observa_tarea		CHAR(10)	Y	

Tabla 4.23. Modelo físico de datos

4.2.3.6.2.Tarea DSI 6.2: Especificación de Caminos de Acceso a los Datos

El objetivo de esta tarea es determinar los caminos de acceso a los datos persistentes del sistema, utilizados por los principales módulos / clases de acuerdo al modelo físico de datos, con el fin de optimizar el rendimiento de los gestores de datos o sistemas de ficheros y el consumo de recursos, así como disminuir los tiempos de respuesta.

Se recomienda realizar esta tarea para aquellos módulos/clases que reúnan, entre otras, alguna de las siguientes características:

- *Tratamiento crítico.*
- *Concurrencia.*
- *Accesos complejos a datos.*

Para el inicio de esta tarea, se toma como referencia el Diseño Detallado de los Subsistemas de Soporte (DSI 2.1) y el Diseño de la Arquitectura Modular (DSI 5) o Diseño de Clases (DSI 4) de los subsistemas específicos, productos que se están generando en paralelo a esta actividad.

Para cada módulo / clase se identifican las tablas o ficheros y el tipo de acceso realizado, así como el orden que debe seguirse para la obtención de los datos. Asimismo, se efectúa una estimación del número de accesos que deben realizarse teniendo en cuenta, a su vez, la frecuencia y la prioridad del acceso.

La información obtenida sirve para identificar accesos excesivamente costosos o redundantes que pueden comprometer el rendimiento final del sistema y que, por lo tanto, exigen la optimización del modelo físico de datos, mediante la creación de nuevos accesos, posibles desnormalizaciones o particiones del modelo físico de datos.

Al no requerir este desarrollo, tratamiento crítico, concurrencia o accesos complejos a datos, esta tarea no se desarrolla.

4.2.3.6.3.Tarea DSI 6.3: Optimización del Modelo Físico de Datos

En esta tarea se optimiza el diseño físico de datos, con el objetivo de mejorar el tiempo de respuesta en el acceso a datos persistentes, hacer una adecuada utilización de los recursos del sistema y, en consecuencia, garantizar que el diseño satisface las necesidades de tratamiento establecidas para el sistema de información en cuanto a que se ajusta a los requisitos de rendimiento exigidos.

A partir de la especificación de la secuencia de accesos de aquellos módulos / clases identificados como críticos, obtenida en la tarea anterior, se detectan las posibles mejoras con el fin de conseguir los niveles de rendimiento establecidos y, por lo tanto, una mayor eficiencia del sistema. Como resultado, puede ser necesaria una desnormalización controlada que se aplica para reducir o simplificar el número de accesos a los sistemas de almacenamiento de datos.

La desnormalización puede obligar a:

Introducir elementos redundantes (campos, campos derivados, etc.).

Definir nuevos caminos de acceso.

Redefinir relaciones.

Dividir o unir tablas.

En la revisión de la estructura física de datos se deben tener en cuenta criterios relacionados con:

Módulos / clases identificados como críticos.

Estimación de volúmenes.

Frecuencia y tipo de acceso.

Estimaciones de crecimiento por periodo.

Requisitos relativos al rendimiento, seguridad, confidencialidad y disponibilidad, entre otros, considerados relevantes.

Es importante que la desnormalización se lleve a cabo de una forma controlada, para evitar anomalías en el tratamiento de los datos.

Dado que no se desarrollo la tarea DSI 6.2., esta tarea no corresponde realizarla.

4.2.3.6.4.Tarea DSI 6.4: Especificación de la Distribución de Datos

En esta tarea se determina el modelo de distribución de datos, teniendo en cuenta los requisitos de diseño establecidos. Se establece la ubicación de los gestores de bases de datos o sistemas de ficheros, así como de los distintos elementos de la estructura física de datos, en los nodos correspondientes, de acuerdo al particionamiento físico del sistema de información especificado en la actividad Diseño de la Arquitectura del Sistema (DSI 1).

El resultado de esta actividad es la especificación de los modelos físicos particulares de cada nodo, esquemas físicos de datos, así como su asignación a los nodos.

Al no existir procesamiento distribuido, esta tarea no se desarrolla.

4.2.3.7. Actividad DSI 7: Verificación y aceptación de la Arquitectura del Sistema

4.2.3.7.1.Tarea DSI 7.1: Verificación de la Especificación de Diseño

Se realizó esta tarea con el objetivo de controlar la calidad del diseño del Sistema, las tareas de Análisis y Diseño fueron realizadas con una herramienta CASE que realiza en forma automática controles de consistencia. Para hacer esta tarea se utilizaron los siguientes documentos:

- Catálogo de Requisitos, tarea DSI 1.2.
- Catálogo de Normas, tarea DSI 1.4
- Diseño de la Arquitectura del Sistema, tarea DSI 1.5
- Entorno Tecnológico del Sistema, tarea DSI 1.6
- Diseño Detallado de Subsistemas de Soporte, tarea DSI 2.1
- Diseño de la Arquitectura Modular, tarea DSI 5.2
- Diseño de Interfaz de Usuario, tarea DSI 5.3
- Modelo Físico de Datos, tarea DSI 6.1

Se controló la calidad de estos documentos de diseño y cuando se encontró algún error se realizaron las correcciones que permitieron mejorar la calidad del diseño.

4.2.3.7.2.Tarea DSI 7.2: Análisis de Consistencia de las Especificaciones de Diseño

- ***Verificación del diseño***

La tabla 4.24. representa las verificaciones realizadas:

Análisis	***Descripción***	
Arquitectura del Sistema / Subsistemas	Cada subsistema de diseño está asociado al menos con un nodo del particionamiento físico del sistema de información.	Verificado ok
Arquitectura del Sistema / Modelo Físico de Datos:	➢ Todos los elementos definidos en el Modelo Físico de Datos Optimizado se incorporan, al menos, en un esquema físico de datos. ➢ Cada esquema del Modelo Físico de Datos está asociado con un nodo del particionamiento físico del sistema de información	Verificado ok
Arquitectura del Sistema / Entorno Tecnológico del Sistema de Información:	➢ Cada nodo del particionamiento del sistema de información está soportado por el entorno tecnológico. ➢ Se da soporte a todas las necesidades de comunicaciones entre nodos.	Verificado ok
Arquitectura del Sistema / Diseño Detallado de Subsistemas:	➢ Cada módulo o clase del diseño detallado pertenece al menos a un subsistema. ➢ La interfaz del subsistema está proporcionada por interfaces de módulos o clases internas	Verificado ok

	al subsistema. ➢ La especificación de dependencias mediante el estudio de las interfaces entre subsistemas, ya que la existencia de interfaz implica el establecimiento de una dependencia.	
Catálogo de Excepciones / Diseño Detallado de Subsistemas: .	➢ Cada excepción del catálogo es tratada en el diseño de detalle del sistema de información, según los criterios establecidos en la creación del catálogo.	Verificado ok
Diseño Detallado de Subsistemas / Modelo Físico de Datos:	➢ Los elementos del modelo físico de datos corresponden con los elementos utilizados por los módulos del diseño detallado, tanto de los subsistemas específicos como de los de soporte.	Verificado ok
Diseño Detallado de Subsistemas / Interfaz de Usuario:	➢ Los datos o formatos de mensajes necesarios en el diseño de la interfaz de usuario corresponden con los datos o formatos de mensajes de los correspondientes módulos. ➢ Para cada evento / acción solicitado por el usuario existe un módulo que le da respuesta.	Verificado ok

Tabla 4.24. Verificaciones de diseño

4.2.3.7.3.Tarea DSI 7.3: Aceptación de la Arquitectura del Sistema

- ***Aceptación técnica del diseño***

Se realizó una reunión entre el Tesista y los Directores y se aceptó formalmente el diseño realizado.

4.2.3.8. Actividad DSI 8: Generación de especificaciones de construcción

4.2.3.8.1.Tarea DSI 8.1: Especificación del Entorno de Construcción

- ***Especificaciones de construcción del sistema de información***
  - ***Especificaciones del entorno de construcción***

La tabla 4.25. muestra el entorno tecnológico del Hardware, se debe considerar que varias tareas pueden ser desarrolladas por el mismo ordenador, por ejemplo desarrollo y base de datos, servidor web y servidor de Internet, etc.

Equipo	Nombre	Tarea
Pentium III o sup.	Servidor Web	Dar servicios Web
Pentium III o sup.	Servidor Internet	Dar servicios de Internet
Pentium III o sup.	Servidor Base de datos y aplicación	Base de datos y aplicación
Pentium III o sup.	Pc desarrollo	Desarrollar el sistema

Tabla 4.25. Entorno hardware de construcción

La tabla 4.26. Muestra el software necesario para construir el sistema

Nombre	función	PC
Apache	Dar servicios Web	Servidor Web
Linux	Dar servicios de Internet	Servidor Internet
Firebird 1.5.4	Gestor de base de datos	Servidor Base de datos y aplicación
Editor de páginas web (Microsoft Front Página).	Diseñar las páginas web	PC Desarrollo
IBEXPERT	Diseño y administración Base de datos	Servidor Base de datos y aplicación

		y aplicación
PHP	Lenguaje de programación	Servidor Base de datos y aplicación
Linux / Windows	Sistema operativo	Servidor Base de datos y aplicación
Linux / Windows	Sistema operativo	Pc desarrollo

Tabla 4.26. Software necesario para el desarrollo

- Restricciones técnicas del entorno.

No existen restricciones técnicas.

- Planificación de capacidades previstas, o la información que estime oportuno el departamento de sistemas para efectuar dicha planificación.

De acuerdo a las características de la aplicación se estima que el tamaño de la base de datos futura no será mayor a 200 Mb de espacio en disco.

- Requisitos de operación y seguridad del entorno de construcción.

La seguridad se debe configurar en los siguientes niveles:

Acceso Físico: La lugar donde se desarrollará el sistema deberá tener adecuados niveles de seguridad en cuanto al acceso físico de las personas que ingresan a la misma.

Horario de operación: No existirán limitaciones de horario.

Acceso al servidor: Todos los servidores serán administrados por el Maestrando, se creará una única clave de administrador.

Administración de usuarios que accederán a la aplicación: El Maestrando creará claves de usuario para el testeo de la aplicación de acuerdo a las necesidades

Firewalls: Para proteger la aplicación, la base de datos y el entorno de desarrollo se instalará un firewall o cortafuegos, a los efectos de proteger esta información.

Backups: Se realizarán copias de seguridad diarias de todos los fuentes y de las bases de datos en forma diaria.

4.2.3.8.2. Tarea DSI 8.2: Definición de Componentes y Subsistemas de Construcción

- ***Especificaciones de construcción de sistema de información***
    - ***Descripción de subsistemas de construcción y dependencias***

Los subsistemas de construcción son:

- la interfaz del usuario.
- Las reglas de negocios.
- Los datos.

    - ***Descripción de componentes***

- Páginas PHP: Al tener acceso a la base de datos se trata de páginas dinámicas y son el Kernel de la aplicación
- Páginas web de presentación de la aplicación: Al no acceder a la base de datos son páginas estáticas, y su función es la de se la interfase de interacción con el usuario de manera de poder navegar por la aplicación.

    - ***Plan de integración del sistema de Información***

Dadas las características de la aplicación a desarrollar esta tarea no se desarrolla.

4.2.3.8.3.Tarea DSI 8.3: Elaboración de Especificaciones de Construcción

Se realiza una especificación detallada de cada componente, en pseudo código o lenguaje natural, completando la información que se considere necesaria según el entorno tecnológico.

Asimismo, se determinan y especifican todos los elementos o parámetros complementarios a la propia definición de componentes que, en función del entorno tecnológico, completan las especificaciones de construcción. Como ejemplos, es posible citar las tablas de definición de programas y transacciones en monitores de teleproceso, etc.

La especificación detallada de componentes fue desarrollada de manera pormenorizada en la tarea ASI 7.1. Obtención del Modelo de Procesos del sistema, al no encontrarse nuevos elementos se considera válido el documento elaborado en la esta tarea.

4.2.3.8.4.Tarea DSI 8.4: Elaboración de Especificaciones del Modelo Físico de Datos

En la Tarea DSI 6.1: Diseño del Modelo Físico de Datos, se detalló la estructura física del las bases de datos del sistema a desarrollar, este documento generado es el que se utilizará como especificación para la construcción.

4.2.3.9. Actividad DSI 9: Diseño de la migración y carga inicial de datos

Esta actividad sólo se lleva a cabo cuando es necesaria una carga inicial de información, o una migración de datos de otros sistemas, cuyo alcance y estrategia a seguir se habrá establecido previamente.

Para ello, se toma como referencia el plan de migración y carga inicial de datos, que recoge las estructuras físicas de datos del sistema o sistemas origen implicadas en la conversión, la prioridad en las cargas y secuencia a seguir, las necesidades previas de depuración de la información, así como los requisitos necesarios para garantizar la correcta implementación de los procedimientos de migración sin comprometer el funcionamiento de los sistemas actuales.

A partir de dicho plan, y de acuerdo a la estructura física de los datos del nuevo sistema, obtenida en la actividad Diseño Físico de Datos (DSI 6), y a las características de la arquitectura y del entorno tecnológico propuesto en la actividad Definición de la Arquitectura del Sistema (DSI 1), se procede a definir y diseñar en detalle los procedimientos y procesos necesarios para realizar la migración.

Se completa el plan de pruebas específico establecido en el plan de migración y carga inicial, detallando las pruebas a realizar, los criterios de aceptación o rechazo de la prueba y los responsables de la organización, realización y evaluación de resultados.

Asimismo, se determinan las necesidades adicionales de infraestructura, tanto para la implementación de los procesos como para la realización de las pruebas.

Como resultado de esta actividad, se actualiza el plan de migración y carga inicial de datos con la información siguiente:

- *Especificación del entorno de migración.*
- *Definición de procedimientos de migración.*
- *Diseño detallado de módulos.*
- *Especificación técnica de las pruebas.*
- *Planificación de la migración y carga inicial.*

Es importante considerar que una carga inicial de información no tiene el mismo alcance y complejidad que una migración de datos, de modo que las tareas de esta actividad se deben llevar a cabo en mayor o menor medida en función de las características de los datos a cargar.

Dadas las características del sistema a desarrollar no se realiza migración de datos por lo tanto esta actividad no se desarrolla.

4.2.3.10.Actividad DSI 10: Especificación técnica del plan de pruebas.

4.2.3.10.1.Tarea 10.1: Especificación del Entorno de Pruebas

- ***Plan de pruebas***
  - ***Especificación del entorno de pruebas***

El entorno de pruebas es el mismo que el especificado en la tarea DSI 8.1: Especificación del Entorno de Construcción.

4.2.3.10.2.Tarea DSI 10.2: Especificación Técnica de Niveles de Prueba

- ***Plan de pruebas***
  - ***Especificación Técnica de Niveles de Prueba***

Esta tarea se da por cumplida al considerarse que los documentos generados en la Tarea ASI 10.1: Definición del Alcance de las Pruebas y en el la Tarea ASI 10.3: Definición de las Pruebas de Aceptación del Sistema, cubren la Especificación técnica de los niveles de prueba.

4.2.3.10.3.Tarea DSI 10.3: Revisión de la Planificación de Pruebas

En la Tarea ASI 10.2: Definición de Requisitos del Entorno de Pruebas, se especifica el orden, nivel y tipo de pruebas y los recursos necesarios para ejecutar las mismas.

- ***Plan de pruebas***
  - ***Planificación de las pruebas***

En cuanto al cronograma de tiempos, esta tarea se desarrollará en la etapa de Construcción del sistema de información.

4.2.3.11.Actividad DSI 11: Establecimiento de requisitos de implementación

En esta actividad se completa el catálogo de requisitos con aquéllos relacionados con la documentación que el usuario requiere para operar con el nuevo sistema, y los relativos a la propia implantación del sistema en el entorno de operación.

La incorporación de estos requisitos permite ir preparando, en los procesos de Construcción del Sistema de Información (CSI) e Implantación y Aceptación del Sistema (IAS), los medios y recursos necesarios para que los usuarios, tanto finales como de operación, sean capaces de utilizar el nueva sistema de forma satisfactoria.

Esta actividad no se desarrolla al no detectarse requisitos de implementación

4.2.3.12. Actividad DSI 12: Aprobación del diseño del sistema de información

4.2.3.12.1.Tarea DSI 12.1: Presentación y Aprobación del Diseño del Sistema de Información

- ***Aprobación del Diseño del Sistema de Información***

Se realizó una reunión entre el Maestrando y los directores del proyecto y se aprobó formalmente el Diseño del Sistema de Información.

Capítulo 4

Solución

Sección 4.2.4. – Construcción del Sistema de Información

4.2.4.Construcción del Sistema de Información

4.2.4.1.Actividad CSI 1: Preparación del entorno de generación y construcción.

4.2.4.1.1.Tarea CSI 1.1: Implantación de la Base de Datos Física o Ficheros

- ***Base de datos física***

De acuerdo a lo especificado en la Tarea DSI 8.1: Especificación del Entorno de Construcción, se crea la base de datos, para esto se:

- Armado de la red: Se instaló una red entre dos equipos utilizando un cable cruzado, un servidor (Pentium III, 256 Mb RAM, HD 40 Gb) y un cliente (Pentium IV, 256 Mb Ram HD 80 Gb).
- Instalación del gestor de base de datos: en la PC del Cliente se instala y configura con una única clave de administrador la base de datos de acuerdo a las características definidas en la Tarea DSI 8.1 (Especificación del Entorno de Construcción)
  - Creación de la base de datos: A partir del diseño de la base de datos realizado en la tarea DSI 6.1: Diseño del Modelo Físico de Datos, se generó en forma automática con la herramienta CASE el script de creación de la base de datos, que se fue ejecutado en la base de datos.

4.2.4.1.2.Tarea CSI 1.2: Preparación del Entorno de Construcción

- ***Entorno de Construcción***

La tabla 4.27 muestra el entorno de construcción del sistema:

Herramienta	Características	Nivel arquitectónico	Uso
Ace FTP 3	Software para subir/Descargar archivos desde/hacia el servidor Freeware		Desarrollo y soporte
Case Studio	Herramienta case		Modelamiento y semántica de datos
Embarcadero ERStudio	Herramienta case		Modelamiento y semántica de datos
Firebird 2	Motor de Base de Datos Relacionales y transaccionales Open Source	Datos	Almacenará la información del sistema a desarrollar
IBEXPERT	Herramienta Front End para administrar Bases de Datos y ejecutar scrips del Motor Firebird	Datos	Desarrollo y soporte

Internet Explorer	Navegador Web	Interfaz de usuario	Interacción Usuario/ Aplicación
Javascript y Jscript	Lenguaje para entorno web que se ejecuta del lado del cliente , embebido en los navegadores web	Reglas de negocios	Leguaje para la validación de ingreso de datos del lado del cliente.(Navegador Web)
Linux	Sistema operativo basado en Unís		SO para servidor donde correrá la aplicación a desarrollar
Macromedia Dreamweaver	Herramienta para el desarrollo de interfaces y código de lenguajes de entorno web.	Interfaz de usuario	Para diseño de las interfaces de la aplicación (HTML CSS, XML, XSL)y Codificación del la lógica de la aplicación
Mozilla Firefox	Navegador web	Interfaz de usuario	Interacción Usuario/ Aplicación
Mysql	Motor de Base de Datos	Datos	Almacenará Información de la Pagina Oficial de la Empresa ITAudit
MySql Administrator	Herramienta Front-End para administrar bases de datos Mysql	Datos	Desarrollo y soporte
MySql Control Center	Herramienta Front End para administrar bases de datos Mysql	Datos	Desarrollo y soporte
Mysql Query	Herramienta Front End para correr scripts de bases de datos Mysql	Datos	Desarrollo y soporte

PHP	PHP (acrónimo de "PHP: Hypertext Preprocessor") es un lenguaje de "código abierto" interpretado, de alto nivel, embebido en páginas HTML y ejecutado en el servidor.	Reglas de negocios	Lenguaje con el que se codificará la aplicación, y Web Services SOAP
PhpMyAdmin 2.6.1	Herramienta front end de entorno Web para el motor de base de datos Mysql	Datos	Desarrollo y soporte
PuTTY	Herramienta front end para acceder a servidores Unix /Linux		Para acceder a servidor Linux desde Windows
Umbrello	Herramienta Case para modelamiento para UML. Genera documentación y código		Modelamiento de Datos y Análisis de Dominio de la aplicación
Visio 2003	Software para Graficar		Modelamiento de Semántica, datos y dominio de la aplicación
Visual Paradigm for UML	Herramienta Case para modelamiento para UML. Genera documentación y código		Modelamiento de Datos y Análisis de Dominio de la aplicación
Windows	Sistema operativo Multitarea		SO para ejecutar herramientas y aplicaciones

4.27. Entorno de construcción

4.2.4.2. Actividad CSI 2: Generación del código de los componentes y procedimientos

4.2.4.2.1.Tarea CSI 2.1: Generación del Código de Componentes

- ***Código fuente de los componentes***

El código se genera de acuerdo a las definiciones del documento generado en la tarea tarea ASI 7.1. Obtención del Modelo de Procesos del sistema, dónde se especifica la funcionalidad que de e tener cada uno de los módulos.

También se tuvieron en cuenta las recomendaciones relacionadas con standards y normas especificadas en los siguientes tareas:

- ✓ Tarea ASI 8.1: Especificación de Principios Generales de la Interfaz
- ✓ Tarea ASI 8.2: Identificación de Perfiles y Diálogos
- ✓ Tarea ASI 8.3: Especificación de Formatos Individuales de la Interfaz de Pantalla
- ✓ Tarea ASI 8.4: Especificación del Comportamiento Dinámico de la Interfaz
- ✓ Tarea ASI 8.5: Especificación de Formatos de Impresión

Se siguieron las especificaciones de diseño que se realizaron en las tareas:

- ✓ Tarea DSI 8.3: Elaboración de Especificaciones de Construcción.
- ✓ Tarea DSI 8.4: Elaboración de Especificaciones del Modelo Físico de Datos.
- ✓ Tarea DSI 6.1: Diseño del Modelo Físico de Datos.
- ✓ Tarea DSI 5.2: Diseño de Comunicaciones entre Módulos

Dado que los lenguajes de programación son interpretados (HTML y PHP), no es necesario realizar compilaciones y enlaces a bibliotecas.

4.2.4.2.2.Tarea CSI 2.2: Generación del Código de los Procedimientos de Operación y Seguridad

- ***Producto software***
  - ***Procedimientos de operación y administración del sistema***

Los procedimientos de operación fueron implementados de acuerdo al documento generado en la tarea DSI 1.7: Especificación de Requisitos de Operación y Seguridad.

  - ***Procedimientos de seguridad y control de acceso***

Los procedimientos de seguridad fueron implementados de acuerdo al documento generado en la tarea DSI 1.7: Especificación de Requisitos de Operación y Seguridad.

4.2.4.3. Actividad CSI 3: Ejecución de las pruebas unitarias.

4.2.4.3.1.Tarea CSI 3.1: Preparación del Entorno de las Pruebas Unitarias

- ***Entorno de pruebas unitarias***

Para la realización de las pruebas unitarias se replicó con la misma configuración del entorno de desarrollo expuesto en la tarea CSI 1.2: Preparación del Entorno de Construcción.

En esta actividad se realizan las pruebas de cada componente del sistema y como se integra con el resto de los componentes, asegurando el correcto funcionamiento a través de las interfaces entre módulos. En algunos casos para poder realizar estas pruebas es necesario la creación de componentes auxiliares. Para reducir la generación de componentes auxiliares se utiliza una estrategia de integración incremental.

El testing implica un proceso de depuración del sistema hasta lograr que cada caso de prueba tenga un resultado “correcto” esto implica que no se observaron errores en la prueba. Existe otro estado que es “errores” que implica un proceso de corrección de algún tipo al no coincidir la salida esperada con la salida obtenida.

La estrategia elegida de prueba fue la de caja negra.

Los perfiles involucrados en la prueba son:

- Tesista: Responsable del diseño, y evaluación de las pruebas
- Testeador: Se recurrió a un asistente para realizar las pruebas
- Director de la tesis: responsable de evaluar el proceso y realizar la prueba de aceptación.

4.2.4.3.2.Tarea CSI 3.2: Realización y Evaluación de las Pruebas Unitarias

- ***Resultado y evaluación de las pruebas unitarias***

La tabla 4.28 muestra el resultado de las pruebas de integración y unitarias.

Num.Caso DE PRUEBA	_____	_____	_____	
1	Carga de dominios	Ingreso del dominio “Adquisición o implementación””	Alta realizada. Autonumeración del código a partir del ultimo alta dado.	Correcto
2	Modificación de dominios	Modificación del dominio “Adquisición o implementación” por “Adquisición e implementación”	Modificación realizada. No debe permitir modificar el código.	Correcto
3	Listado de dominios	Listador dominios	Listado de dominios	Correcto
4	Eliminar Dominio	Eliminar dominio “Adquisición e implementación”	El sistema debe mostrar el registro y presentar un mensaje que diga “esta seguro que quiere eliminar” al contestar que si se elimina el registro	Correcto
5	Carga de procesos	Ingreso del proceso “adquirir y mantener la arquitectura tecnológica”	Alta realizada. Autonumeración del código a partir del ultimo alta dado.	Correcto
6	Actualización de procesos	Actualizar el código de proceso ”1”	El módulo debe enviar un mensaje que diga “no es posible modificar el código de Proceso”	Correcto
7	Búsqueda de procesos	Buscar el proceso “aaaaaaa”	El módulo envía un mensaje de error “no existe ese proceso	
8	Eliminar un proceso	Eliminar el proceso “adquirir y mantener la arquitectura tecnológica”	El sistema debe mostrar el registro y presentar un mensaje que diga “esta seguro que quiere eliminar” al contestar que si se elimina el registro	Correcto

9	Carga de áreas	Ingreso del área “hardware”	Alta realizada. Autonumeración del código a partir del ultimo alta dado.	Correcto
10	Actualización de áreas	Actualizar el área “hardware” por el área “ “	El módulo debe enviar un mensaje de error “el área	Correcto
11	Listar áreas	Listar todas las áreas	Listado de áreas	Correcto
12	Eliminar un área	Eliminar el área “hardware”	El sistema debe mostrar el registro y presentar un mensaje que diga “esta seguro que quiere eliminar” al contestar que si se elimina el registro	Correcto
13	Carga de objetivos de control	Ingreso del objetivo de control “Plan de la tecnología de la Información a largo plazo”	Alta realizada. Autonumeración del código a partir del ultimo alta dado.	Correcto
14	Actualización objetivos de control	Actualización del objetivo de control “Plan de la tecnología de la Información a largo plazo” por “Plan de tecnología”	Cambio realizado	Correcto
15	Listar objetivos de control	Listar todos los objetivos de control	Listado de los objetivos de control	Correcto
16	Eliminar objetivo de control	Eliminar el objetivo de control “Plan de la tecnología de la Información a largo plazo”	El sistema debe mostrar el registro y presentar un mensaje que diga “esta seguro que quiere eliminar” al contestar que si se elimina el registro	Correcto
17	Carga de perfiles	Ingreso del perfil “especialista en hardware”	Alta realizada. Autonumeración del código a partir del ultimo alta dado.	Correcto

18	Actualización de perfiles	Modificar el perfil “especialista en hardware” por "123456789012345 678901234567890123456789012 345678901234567890123456789 012345678901234567890123456 789012345678901234567890123 456789012345678901234567890 123”	El módulo debe emitir un error que diga “la longitud máxima de la descripción del perfil es de 150 caracteres” y no debe permitir modificar	Correcto
19	Eliminar perfiles	Eliminar el perfil “especialista en hardware”	El sistema debe mostrar el registro y presentar un mensaje que diga “esta seguro que quiere eliminar” al contestar que si se elimina el registro	Correcto
19	Listar perfiles	Listar todos los perfiles	El módulo debe emitir un mensaje de error “no hay perfiles para listar”	Correcto
20	Carga de procedimientos	Dar de alta el procedimiento “revisión de documentación”	Alta realizada. Autonumeración del código a partir del ultimo alta dado.	Correcto
21	Actualización de procedimientos	Modificar el procedimiento “revisión de documentación” por el procedimiento “Revisión de documentación”	Modificación realizada	Correcto
22	Buscar procedimiento	Buscar el procedimiento “1”	Visualizar el procedimiento “Revisión de documentación”	Correcto
23	Eliminar procedimientos	Eliminar el procedimiento “Revisión de documentación”	El sistema debe mostrar el registro y presentar un mensaje que diga “esta seguro que quiere eliminar” al contestar que si se elimina el registro	Correcto
24	Carga de Personas	Ingreso de la persona: Nombre: Juan Dirección : Larrea 32	El módulo debe enviar un mensaje de error “falta ingresar apellido”	Correcto

25	Carga de Personas	Ingreso de la persona: Nombre: Juan Apellido: Perez Dirección : Larrea 32	Alta realizada. Autonumeración del código a partir del ultimo alta dado	Correcto
26	Actualización de datos personales	Modificar “Larrea 32” por “Larrea332”	Modificación realizada	Correcto
27	Buscar datos personales	Buscar el código de persona “1”	Mostrar la persona: Nombre: Juan Apellido: Perez Dirección : Larrea 32	Correcto
28	Elimina datos personales	Eliminar la persona con código “1”	El módulo debe mostrar la persona Nombre: Juan Apellido: Perez Dirección : Larrea 32 y presentar un mensaje que diga “esta seguro que quiere eliminar” al contestar que si se elimina el registro	Correcto
29	Agregar auditor	Dar de alta el auditor con código “1” y titulo “licenciado en sistemas”	Alta realizada. Autonumeración del código a partir del ultimo alta dado	Correcto
30	Actualizar auditor	Modificar el titulo del auditor “1” “licenciado en sistemas” por “Ingeniero en Sistemas”	Modificación realizada	Correcto
31	Listar Auditores	Listar todos los auditores	Listado de auditores	Correcto
32	Dar de baja un auditor	Eliminar el auditor “1”	El sistema debe mostrar el registro y presentar un mensaje que diga “esta seguro que quiere eliminar” al contestar que si se elimina el registro	Correcto

33	Agregar Cliente	Dar de alta el auditor con código “1” y el cargo “gerente”	Alta realizada. Autonumeración del código a partir del ultimo alta dado	Correcto
34	Actualizar Cliente	Modificar el cargo del cliente “1” “gerente” por “Gerente”	Modificación realizada	Correcto
35	Listar Cliente	Listar todos los clientes	Listado de clientes	Correcto
36	Dar de baja un Cliente	Eliminar el auditor “1”	El sistema debe mostrar el registro y presentar un mensaje que diga “esta seguro que quiere eliminar” al contestar que si se elimina el registro	Correcto
37	Carga de recursos	Alta del recurso “tecnología”	Alta realizada. Autonumeración del código a partir del ultimo alta dado.	correcto
38	Modificación de un recurso	Modificar el recurso “tecnología” por “Tecnología”	Modificacion realizada	Correcto
39	Listar Recursos	Listar todos los recursos	Listado de recursos	Correcto
40	Eliminar recursos	Eliminar el recurso “Tecnología”	El sistema debe mostrar el registro y presentar un mensaje que diga “esta seguro que quiere eliminar” al contestar que si se elimina el registro	Correcto
41	Carga de recursos	Alta del país “argentina”	Alta realizada. Autonumeración del código a partir del ultimo alta dado.	correcto
42	Modificación de un pais	Modificar el recurso “argentina” por “Argentina”	Modificacion realizada	Correcto
43	Listar Paises	Listar todos los paises	Listado de recursos	Correcto
44	Eliminar paises	Eliminar el pais “Argentina”	El sistema debe mostrar el registro y presentar un mensaje que diga “esta seguro que quiere eliminar” al contestar que si se elimina el registro	Correcto

45	Carga de una provincia	Alta de la Provincia “Misiones”	Alta realizada. Autonumeración del código a partir del ultimo alta dado.	correcto
46	Modificación de una provincia	Modificar la provincia “Misiones” por “Corrientes”	Modificación realizada	Correcto
47	Listar Provincias	Listar todos las Provincias	Listado de provincias	Correcto
48	Eliminar Provincias	Eliminar la Provincia “Corrientes”	El sistema debe mostrar el registro y presentar un mensaje que diga “esta seguro que quiere eliminar” al contestar que si se elimina el registro	Correcto
49	Carga de una Localidad	Alta de la Localidad “Posadas”	Alta realizada. Autonumeración del código a partir del ultimo alta dado.	correcto
50	Modificación de una Localidad	Modificar la Localidad “Posadas” por “Corrientes”	Modificación realizada	Correcto
51	Listar Localidades	Listar todos las Localidades	Listado de Localidades	Correcto
52	Eliminar Localidad	Eliminar la Localidad “Corrientes”	El sistema debe mostrar el registro y presentar un mensaje que diga “esta seguro que quiere eliminar” al contestar que si se elimina el registro	Correcto
53	Carga de una Tareas	Alta de la Tareas: Desc_tarea: “Revisión plan de contingencias” Fecha_inic_tarea: 01/01/2005 Fecha_fin_tarea: 30/01/2005 Observ_tarea: “solicitar copia del plan”	Alta realizada. Autonumeración del código a partir del ultimo alta dado.	correcto

54	Modificación de una tarea	Modificar en la tarea "1" Fecha_fin_tarea: 30/01/2005 Por Fecha_fin_tarea: 30/01/2004	El módulo debe enviar un mensaje de error "la fecha de fin de tarea no puede ser menor que la fecha de inicio" y no se realiza la modificación	Correcto
55	Listar tareas	Listar todos las Tareas	Listado de tareas	Correcto
56	Eliminar tareas	Eliminar la tarea "Revisión plan de contingencias"	El sistema debe mostrar el registro y presentar un mensaje que diga "esta seguro que quiere eliminar" al contestar que si se elimina el registro	Correcto
57	Carga de un Proyecto	Alta de un Proyecto: Nombre_proyecto: "Universidad XXX" Fecha_inic_proy: 01/01/2005 Fecha_fin_proy: 30/01/2005	Alta realizada. Autonumeración del código a partir del ultimo alta dado.	correcto
58	Modificación de un Proyecto	Modificar en el Proyecto "1" Fecha_fin_tarea: 30/01/2005 Por Fecha_fin_tarea: 32/01/2004	El módulo debe enviar un mensaje de error "fecha de fin de proyecto errónea" y no se realiza la modificación	Correcto
59	Listar Proyectos	Listar todos los Proyectos	Listado de Proyectos	Correcto
60	Eliminar Proyectos	Eliminar el Proyecto "Universidad XXX"	El sistema debe mostrar el registro y presentar un mensaje que diga "esta seguro que quiere eliminar" al contestar que si se elimina el registro	Correcto
61	Carga de un Informe	Alta de un Informe: Observ_informe: "Informe auditoría Universidad XXX" fecha_informe: 01/01/2005	Alta realizada. Autonumeración del código a partir del ultimo alta dado.	correcto

62	Modificación de un Informe	Modificar el Informe “1” Fecha_fin_tarea: 30/01/2005 Por Fecha_fin_tarea: 30/03/2005	Modificación realizada	Correcto
63	Listar Informes	Listar informe “1”	Listado de Informe	Correcto
64	Eliminar Informes	Eliminar el informe “1”	El sistema debe mostrar el registro y presentar un mensaje que diga “esta seguro que quiere eliminar” al contestar que si se elimina el registro	Correcto
65	Carga de un Item de un informe	Alta de un Ítem de un informe: Desc_item_informe: “Personal participante de la auditoría	Alta realizada. Autonumeración del código a partir del ultimo alta dado.	correcto
66	Modificación de un ítem de Informe	Modificar el Informe “1” Desc_item_informe: “Personal participante de la auditoría Por Desc_item_informe: “Personal participante de la auditoría: “	Modificación realizada	Correcto
67	Listar items Informes	Listar ítem informe “1”	Listado de Ítem informe	Correcto
68	Eliminar ítem informes	Eliminar el ítem informe “1”	El sistema debe mostrar el registro y presentar un mensaje que diga “esta seguro que quiere eliminar” al contestar que si se elimina el registro	Correcto
69	Carga de preguntas del relevamiento inicial	Dar de alta la pregunta “Se cuenta con manuales técnicos del hardware instalado”	Alta realizada	Correcto

70	Modificación de una pregunta del relevamiento inicial	Modificar la pregunta "1" Pregunta_relev_inicial: "Se cuenta con manuales técnicos del hardware instalado" Por Pregunta_relev_inicial: "Se cuenta con manuales técnicos del hardware instalado en la empresa"	Modificación realizada	Correcto
71	Listar pregunta del relevamiento inicial	Listar pregunta del relevamiento inicial "1"	Listado de pregunta del relevamiento inicial	Correcto
72	Eliminar ítem informes	Eliminar la pregunta del relevamiento inicial "1"	El sistema debe mostrar el registro y presentar un mensaje que diga "esta seguro que quiere eliminar" al contestar que si se elimina el registro	Correcto
73	Carga de opciones de respuesta del relevamiento inicial	Dar de alta opción de respuesta del relevamiento inicial : Opcion_respuesta: "si" Riesgo: "5"	Alta realizada	Correcto
74	Modificación de una opción de respuesta del relevamiento inicial	Modificar de la opción "1" Riesgo: "5" Por Riesgo: "4"	Modificación realizada	Correcto
75	Listar opciones de respuestas del relevamiento inicial	Listar opciones de respuesta del relevamiento inicial "1"	Listado de opciones de respuesta del relevamiento inicial	Correcto

76	Eliminar opción de respuesta	Eliminar la opción respuesta del relevamiento inicial “1”	El sistema debe mostrar el registro y presentar un mensaje que diga “esta seguro que quiere eliminar” al contestar que si se elimina el registro	Correcto
77	Carga de preguntas del relevamiento profundo	Alta de la pregunta “los manuales del hardware están actualizados”	Alta realizada	Correcto
78	Modificación de una pregunta del relevamiento profundo	Modificar la pregunta: “los manuales del hardware están actualizados” por “Los manuales del hardware están actualizados”	Modificación realizada	Correcto
79	Listar preguntas del relevamiento profundo	Listar preguntas del relevamiento profundo	Listado de preguntas del relevamiento profundo	Correcto
80	Eliminar preguntas del relevamiento profundo	Eliminar la pregunta del relevamiento profundo “1”	El sistema debe mostrar el registro y presentar un mensaje que diga “esta seguro que quiere eliminar” al contestar que si se elimina el registro	Correcto
81	Carga de opciones de respuesta del relevamiento profundo	Dar de alta opción de respuesta del relevamiento profundo : Opcion_respuesta: “si” Riesgo: “5”	Alta realizada	Correcto

82	Modificación de una opcion de respuesta del relevamiento profundo	Modificar de la opción "1" Riesgo: "5" Por Riesgo: "4"	Modificación realizada	Correcto
83	Listar opciones de respuestas del relevamiento profundo	Listar opciones de respuesta del relevamiento profundo "1"	Listado de opciones de respuesta del relevamiento profundo	Correcto
84	Eliminar opción de respuesta del relevamiento profundo	Eliminar la opcion respuesta del relevamiento profundo "1"	El sistema debe mostrar el registro y presentar un mensaje que diga "esta seguro que quiere eliminar" al contestar que si se elimina el registro	Correcto
85	Asignar auditor a una tarea dentro de un proyecto	Asignar a un auditor una tarea dentro de un proyecto. cod_tarea="1" cod_auditor="25" id_proyecto=1	Alta realizada	Correcto
86	Eliminar a un auditor de una tarea dentro de un proyecto	Eliminar a un auditor una tarea dentro de un proyecto cod_tarea="1" cod_auditor="25" id_proyecto=1	El sistema debe mostrar el registro y presentar un mensaje que diga "esta seguro que quiere eliminar" al contestar que si se elimina el registro	Correcto
87	Asignar un dominio dentro de un proceso dentro de un proyecto	Dar de alta: Cod_dominio="1" Cod_proceso="2" Id_proyecto="1" Documentación_adjunta="c:\auditoría \manual sistema facturación.doc	Alta realizada	Correcto

88	Eliminar un dominio dentro de un proceso dentro de un proyecto	Eliminar: Cod_dominio=”1” Cod_proceso=”2” Id_proyecto=”1” Documentación_adjunta=”c:\auditoría \manual sistema facturación.doc	El sistema debe mostrar el registro y presentar un mensaje que diga “esta seguro que quiere eliminar” al contestar que si se elimina el registro	correcto

Tabla 4.28. pruebas unitarias

4.2.4.4. Actividad CSI 4: Ejecución de las pruebas de integración

4.2.4.4.1.Tarea CSI 4.1: Preparación del Entorno de las Pruebas de Integración

- **Entorno de pruebas de integración**

Para la realización de las pruebas de integración se replicó con la misma configuración el entorno de desarrollo expuesto en la tarea CSI 1.2: Preparación del Entorno de Construcción.

4.2.4.4.2.Tarea CSI 4.2: Realización de las Pruebas de Integración

- ***Resultado de las pruebas de integración:*** La tabla 4.29 representa el resultado de estas pruebas

Num.Caso DE PRUEBA	_____	_____	_____	
1	Integración Configuración Inicio	Ingreso al subsistema de Inicio con los perfiles definidos en la configuración	Se ingresa al subsistema de inicio con los perfiles definidos.	Correcto
2	Integración Configuración / Estudio preliminar	Ingreso al subsistema de lEstudio preliminar con los perfiles definidos en la configuración	Se ingresa al subsistema de Estudio preliminar con los perfiles definidos.	Correcto
3	Integración Configuración / Recursos	Ingreso al subsistema de Recursos con los perfiles definidos en la configuración	Se ingresa al subsistema de Recursos con los perfiles definidos.	Correcto
4	Integración Configuración / Planificación	Ingreso al subsistema de Planificación con los perfiles definidos en la configuración	Se ingresa al subsistema de Planificación con los perfiles definidos.	Correcto
5	Integración Configuración / Desarrollo	Ingreso al subsistema de Desarrollo con los perfiles definidos en la configuración"	Se ingresa al subsistema de desarrollo con los perfiles definidos.	Correcto
6	Integración Configuración / Informe final	Ingreso al subsistema de Informe Final con los perfiles definidos en la configuración	Se ingresa al subsistema de Informe final con los perfiles definidos.	Correcto
7	Inicio estudio preliminar	Ingreso de datos del proyecto en el módulo de estudio preliminar	Datos del proyecto ingresados en el subsistema de inicio	Correcto
8	Inicio / Estudio preliminar	Check list del estudio preliminar	Check list del estudio inicial en función de las caracteristicas definidas en el subsistema de inicio	Correcto
9	Estudio recursos / planificación	Distribución de tareas por persona en subsistema de planificación	Personal en planificación de acuerdo a los recursos definidos en el subsistema de recursos	Correcto

10	Inicio / desarrollo	Check list del desarrollo	Check list del desarrollo en función de las caracteristicas definidas en el subsistema de inicio	Correcto
11	Desarrollo informe final	Informe final	Recomendaciones del informe final relacionadas con las respuestas del cheklist del desarrollo	Correcto

Tabla 4.29 Resultado de las pruebas de integración

4.2.4.4.3.Tarea CSI 4.3: Evaluación del Resultado de las Pruebas de Integración

- ***Evaluación del resultado de las pruebas de integración***

Se realizaron varios ciclos de pruebas unitarias y de integración con el objetivo de verificar y validar la integración de cada módulo del sistema, esto posibilito la depuración de errores que permite observar que los resultados esperados son los obtenidos.

4.2.4.5.Actividad CSI 5: Ejecución de las pruebas del sistema

4.2.4.5.1.Tarea CSI 5.1: Preparación del Entorno de las Pruebas del Sistema

- ***Entorno de pruebas del sistema***

El entorno de pruebas del sistema es el mismo especificado en la tarea CSI 3.1: Preparación del Entorno de las Pruebas Unitarias.

4.2.4.5.2.Tarea CSI 5.2: Realización de las Pruebas del Sistema

- ***Resultado de las pruebas del sistema***

El objetivo de las pruebas del sistema es encontrar defectos al sistema completo simulando un entorno de producción, se realizan:

❖ Pruebas funcionales: cuyo objetivo es garantizar que se realizan en forma correcta las funciones definidas en la etapa de definición de requerimientos.

❖ Pruebas de rendimiento, el objetivo de este tipo de pruebas es asegurar que el tiempo de respuesta es el esperado.

❖ Pruebas de facilidad de uso: se trata de comprobar que la operación del sistema tiene esta cualidad.

Perfiles involucrados:

Tesista: Responsable del diseño de todas las pruebas, y de la ejecución y evaluación de las mismas.

UsuarioAuditor: Responsable de la ejecución y evaluación de las pruebas de facilidad de uso.

Director de la tesis: Responsable de controlar que las pruebas se efectúen correctamente.

La tabla 4.30. muestra los resultados de los casos de prueba del sistema

Entrada	Resultado
Prueba del proceso 1: Actualización de tablas básicas Area=Hardware Dominio=Adquisición e implementación	Tablas actualizadas

Proceso=Adquirir y mantener la arquitectura tecnológica Objetivo de control= Mantenimiento Preventivo para Hardware. Criterios de información= Efectividad Recursos= Tecnología Perfiles=especialista en hardware Procedimientos=Evaluación documentación	
Prueba del proceso 2: Actualizar matriz checklist preliminar Pregunta= Existen manuales del hardware instalado Opción de respuesta = Si / No Riesgo respuesta no=3 Area=Hardware Dominio=Adquisición e implementación Proceso=Adquirir y mantener la arquitectura tecnologica	Matriz checklist actualizada
Prueba del procedimiento 3 : Actualizar matriz del relevamiento profundo Pregunta= Los manuales del hardware están actualizados Opción de respuesta = Si / No Recomendación respuesta "no"= Solicitar al proveedor los manuales actualizados del hardware Riesgo respuesta no=3 Area=Hardware Dominio=Adquisición e implementación Proceso=Adquirir y mantener la arquitectura tecnológica	Matriz checklist actualizada
Prueba del procedimiento 4 Generar datos del proyecto Cliente= Juan Perez Auditor=Horacio Kuna Sector=casa central Area=Hardware Fecha inicio 15/06/2005 Fecha finalización 15/08/2005	Datos del proyecto generados
Prueba del procedimiento 5 Generar informe proyecto Cliente= Juan Perez Auditor=Horacio Kuna Sector=casa central Area=Hardware Fecha inicio 15/06/2005 Fecha finalización 15/08/2005	Reporte generado
Prueba del procedimiento 6 Realizar Checklist inicial Proyecto Cliente= Juan Perez Auditor=Horacio Kuna Sector=casa central Area=Hardware Pregunta= Existen manuales del hardware instalado Opción de respuesta = No	Matriz generada. Respuestas cargadas
Prueba proceso 7 Realizar informe Checklist inicial proyecto Cliente= Juan Perez Auditor=Horacio Kuna	Informe del relevamiento inicial producido

Sector=casa central Area=Hardware Fecha inicio 15/06/2005 Fecha finalización 15/08/2005	
Prueba proceso 8 Determinar personal Cliente= Juan Perez Auditor=Horacio Kuna Sector=casa central Area=Hardware Fecha inicio 15/06/2005 Fecha finalización 15/08/2005	Determinación de personal realizada
Prueba procedimiento 9 Actualizar informe personal Cliente= Juan Perez Auditor=Horacio Kuna Sector=casa central Area=Hardware Fecha inicio 15/06/2005 Fecha finalización 15/08/2005	Reporte generado
Prueba procedimiento 10 Generar Plan de auditoría Cliente= Juan Perez Auditor=Horacio Kuna Sector=casa central Area=Hardware Fecha inicio 15/06/2005 Fecha finalización 15/08/2005 Procedimiento= Evaluación documentación	Listado de tareas generado
Prueba procedimeinto11 Actualizar plan de auditoría Cliente= Juan Perez Auditor=Horacio Kuna Sector=casa central Area=Hardware Fecha inicio 15/06/2005 Fecha finalización 15/08/2005 Tarea= Evaluación documentación Estado de la tarea = realizada	Plan de auditoría actualizado
Prueba del proceso 12 Desarrollo de la auditoría Cliente= Juan Perez Auditor=Horacio Kuna Sector=casa central Area=Hardware Pregunta= Los manuales del hardware están actualizados Opción de respuesta = No	Checklist generado. Respuestas cargadas
Prueba del proceso 13 Realizar informe relevamiento profundo Cliente= Juan Perez Auditor=Horacio Kuna Sector=casa central Area=Hardware Pregunta= Los manuales del hardware están actualizados	Reporte generado

Opción de respuesta = No	
Prueba del proceso 14 Generar Informe final de auditoría Cliente= Juan Perez Auditor=Horacio Kuna Sector=casa central Area=Hardware Fecha inicio 15/06/2005 Fecha finalización 15/08/2005 Tarea= Evaluación documentación Estado de la tarea = realizada Pregunta= Los manuales del hardware están actualizados Opción de respuesta = No Pregunta= Existen manuales del hardware instalado Opción de respuesta = No	Informe generado
Prueba del proceso 15 Actualizar informe final de auditoría Cliente= Juan Perez Auditor=Horacio Kuna Sector=casa central Area=Hardware Fecha inicio 15/06/2005 Fecha finalización 15/08/2005 Tarea= Evaluación documentación Estado de la tarea = realizada Pregunta= Los manuales del hardware están actualizados Opción de respuesta = No Pregunta= Existen manuales del hardware instalado Opción de respuesta = No Tarea= el cliente debe emitir opinión sobre el informe de auditoría	Informe final actualizado

Tabla 4.30. pruebas del sistema

4.2.4.5.3.Tarea CSI 5.3: Evaluación del Resultado de las Pruebas del Sistema

- ***Evaluación del resultado de las pruebas del sistema.***

Se realizaron varios ciclos del sistema con el objetivo de verificar y validar el sistema, esto posibilito la depuración de errores que permite observar que los resultados esperados son los obtenidos.

4.2.4.6. Actividad CSI 6: Elaboración de los manuales de usuario

4.2.4.6.1.Tarea CSI 6.1: Elaboración de los Manuales de Usuario

El objetivo de esta tarea es elaborar la documentación de usuario, tanto usuario final como de explotación, de acuerdo a los requisitos establecidos en la tarea Especificación de Requisitos de Documentación de Usuario (DSI 11.1), y recogidos en el catálogo de requisitos.

Los requisitos de documentación especifican aspectos relativos a los tipos de documentos a elaborar y estándares a seguir en la generación de los mismos, y para cada uno de ellos:

- *Formato y soporte en el que se desarrollarán*
- *Estructura*
- *Distribución y mantenimiento de la documentación y número de copias a editar.*

Esta tarea no se realiza ya que se trata de un prototipo, el manual de usuario se elaborará en próximas versiones del sistema.

4.2.4.7.Actividad CSI 7: Definición de la formación de usuarios finales.

4.2.4.7.1.Tarea CSI 7.1: Definición del Esquema de Formación

- ***Especificación de la Formación a Usuarios Finales***
  - ***Esquema de formación***

Dado que se trata de un sistema que no se implementará en una empresa en particular esta tarea no se desarrolla.

4.2.4.7.2.Tarea CSI 7.2: Especificación de los Recursos y Entornos de Formación

El objetivo de esta tarea es detallar los recursos necesarios para llevar a cabo la formación, relativos a los materiales de formación, equipos físicos y lógicos, aulas, etc.

También se determinan las características que debe reunir el entorno para realizar la formación, en cuanto a la necesidad de hacer cargas iniciales o migración de datos, activar los procedimientos de seguridad y control de acceso específicos etc.

Dado que se trata de un sistema que no se implementará en una empresa en particular esta tarea no se desarrolla.

4.2.4.8.Actividad CSI 8: Construcción de los componentes y procedimientos de migración y carga inicial de datos.

El objetivo de esta actividad es la codificación y prueba de los componentes y procedimientos de migración y carga inicial de datos, a partir de las especificaciones recogidas en el plan de migración y carga inicial de datos obtenido en el proceso Diseño del Sistema de Información.

Previamente a la generación del código, se prepara la infraestructura tecnológica necesaria para realizar la codificación y las pruebas de los distintos componentes y procedimientos asociados, de acuerdo a las características del

entorno de migración especificado en el plan de migración y carga inicial de datos.

Finalmente, se llevan a cabo las verificaciones establecidas en la especificación técnica del plan de pruebas propio de la migración.

4.2.4.8.1.Tarea CSI 8.1: Preparación del Entorno de Migración y Carga Inicial de Datos

Se dispone el entorno en el que se van a construir los componentes y procedimientos de migración y carga inicial de datos, considerando las bibliotecas o librerías a utilizar, herramientas o utilidades específicas para la conversión, y compiladores, entre otros, cuya necesidad se habrá establecido en la tarea Especificación del Entorno de Migración (DSI 9.1).

Asimismo, se determinan los datos necesarios para realizar las pruebas de los componentes y procedimientos asociados y se configura el entorno de acuerdo a dichas necesidades.

- ***Entorno de migración***

Dadas las características del sistema esta tarea no se desarrolla al no tener que migrarse datos

4.2.4.8.2.Tarea CSI 8.2: Generación del Código de los Componentes y Procedimientos de Migración y Carga Inicial de Datos

El objetivo de esta tarea es la generación del código correspondiente a los procedimientos y componentes necesarios para llevar a cabo la migración, definidos en el plan de migración y carga inicial de datos obtenido en las tareas Diseño de Procedimientos de Migración y Carga Inicial (DSI 9.2) y Diseño Detallado de Componentes de Migración y Carga Inicial (DSI 9.3).

Para generar el código fuente se tienen en cuenta los estándares de nomenclatura y codificación utilizados por la organización y recogidos en el catálogo de normas para este tipo de componentes.

- ***Código fuente de los componentes de migración.***

Dado que se trata de un sistema que no se implementará en una empresa en particular esta tarea no se desarrolla.

- ***Procedimientos de migración.***

Dado que se trata de un sistema que no se implementará en una empresa en particular esta tarea no se desarrolla.

4.2.4.8.3.Tarea CSI 8.3: Realización y Evaluación de las Pruebas de Migración y Carga Inicial de Datos

El objetivo de esta tarea es efectuar las pruebas de los distintos componentes y procedimientos de migración y evaluar su resultado. Esta evaluación recoge el grado de cumplimiento de las mismas, y consiste en:

- ✓ *Comparar los resultados obtenidos con los esperados*
- ✓ *Identificar el origen de cada problema detectado para poder remitirlo a quien proceda, determinar la envergadura de las modificaciones y qué acciones deben llevarse a cabo para resolverlo de forma satisfactoria.*
- ✓ *Indicar si el plan de pruebas debe volver a realizarse total o parcialmente, y si será necesario contemplar nuevos casos de prueba no considerados anteriormente.*

- ***Resultados de las pruebas de migración***

Dado que se trata de un sistema que no se implementará en una empresa en particular esta tarea no se desarrolla.

- ***Evaluación de los resultados de las pruebas de migración***

Dado que se trata de un sistema que no se implementará en una empresa en particular esta tarea no se desarrolla.

4.2.4.9.Actividad CSI 9: Aprobación del sistema de Información

4.2.4.9.1.Tarea CSI 9.1: Presentación y Aprobación del Sistema de Información

- ***Sistema de información***
- ***Aprobación del Sistema de Información***

En esta tarea se recopilaron todos los productos del sistema de información y fueron presentados formalmente a los directores de la Tesis y se dio por aprobada la fase de Construcción del Sistema de Información

Capítulo 4

Solución

Sección 4.2.5. – Implementación y aceptación del sistema

4.2.5. Implantación y aceptación del Sistema

4.2.5.1.Actividad IAS 1: Establecimiento del plan de Implementación

- ***Plan de implementación y equipo de implementación***

ITAUDIT es un prototipo desarrollado como trabajo de tesis, que requerirá ser implantado

4.2.5.2.Actividad IAS 2: Formación necesaria para la implantación

- ***Plan de formación***

ITAUDIT es un prototipo desarrollado como trabajo de tesis, por lo tanto el plan de formación del equipo de implantación y de los usuarios finales, quedan fuera del alcance de este trabajo

4.2.5.3. Actividad IAS 3: Incorporación del sistema al entorno de operación

En esta actividad se realizan todas las tareas necesarias para la incorporación del sistema al entorno de operación en el que se van a llevar a cabo las pruebas de implantación y aceptación del sistema.

Mientras que las pruebas unitarias, de integración y del sistema se pueden ejecutar en un entorno distinto de aquél en el que finalmente se implantará, las pruebas de implantación y aceptación del sistema deben ejecutarse en el entorno real de operación. El propósito es comprobar que el sistema satisface todos los requisitos especificados por el usuario en las mismas condiciones que cuando se inicie la producción.

Por tanto, como paso previo a la realización de dichas pruebas y de acuerdo al plan de implantación establecido, se verifica que los recursos necesarios están disponibles para que se pueda realizar, adecuadamente, la instalación de todos los componentes que integran el sistema, así como la creación y puesta a punto de las bases de datos en el entorno de operación. Asimismo, se establecen los procedimientos de explotación y uso de las bases de datos de acuerdo a la normativa existente en dicho entorno.

- ***Instalación***

ITAUDIT es un prototipo desarrollado como trabajo de tesis, no será incorporado a ningún entorno de operación.

4.2.5.4. Actividad IAS 4: Carga de datos al entorno de operaciones

Teniendo en cuenta que los sistemas de información que forman parte del sistema a implantar pueden mejorar, ampliar o sustituir a otros ya existentes en la organización, puede ser necesaria una carga inicial y/o una migración de datos cuyo alcance dependerá de las características y cobertura de cada

sistema de información implicado. Por tanto, la necesidad de una migración de datos puede venir determinada desde el proceso Estudio de Viabilidad del Sistema (EVS), en la actividad Selección de la Solución (EVS 6). Allí se habrá establecido la estrategia a seguir en la sustitución, evaluando las opciones del enfoque de desarrollo e instalación más apropiados para llevarlo a cabo.

En cualquier caso, en la actividad Diseño de la Migración y Carga Inicial de Datos (DSI 9) se habrán definido y planificado los procesos y procedimientos necesarios para llevar a cabo la migración, realizándose su codificación en la actividad Construcción de los Componentes y Procedimientos de Migración y Carga Inicial de Datos (CSI 8).

- ***Migración y carga inicial de datos***

ITAUDIT es un prototipo desarrollado como trabajo de tesis, que no viene a sustituir un software ya existente, por lo tanto no requiere migración ni carga inicial de datos.

4.2.5.5.Actividad IAS 5: Pruebas de Implantación del Sistema

La finalidad de las pruebas de implantación es doble:

- *Comprobar el funcionamiento correcto del mismo en el entorno de operación.*
- *Permitir que el usuario determine, desde el punto de vista de operación, la aceptación del sistema instalado en su entorno real, según el cumplimiento de los requisitos especificados.*

Para ello, el responsable de implantación revisa el plan de pruebas de implantación y los criterios de aceptación del sistema, previamente elaborados. Las pruebas las realizan los técnicos de sistemas y de operación, que forman parte del grupo de usuarios técnicos que ha recibido la formación necesaria para llevarlas a cabo.

Una vez ejecutadas estas pruebas, el equipo de usuarios técnicos informa de las incidencias detectadas al responsable de implantación, el cual analiza la información y toma las medidas correctoras que considere necesarias para que el sistema dé respuesta a las especificaciones previstas, momento en el que el equipo de operación lo da por probado.

- ***Pruebas de implantación***

ITAUDIT es un prototipo desarrollado como trabajo de tesis, las pruebas e implantación quedan fuera del alcance de este trabajo

4.2.5.6. Actividad IAS 6: Pruebas de aceptación del Sistema

4.2.5.6.1.Tarea IAS 6.1: Preparación de las Pruebas de Aceptación

- ***Plan de pruebas***

Dado que se trata de un proyecto de tesis de Maestría, para realizar esta prueba se coordina con los directores de la misma para realizar esta prueba, la misma se desarrollará en el mismo ambiente donde se realizaron las pruebas del sistema.

4.2.5.6.2.Tarea IAS 6.2: Realización de las Pruebas de Aceptación

- ***Resultado de las pruebas de aceptación***

Los directores de la tesis realizaron las pruebas de aceptación del sistema resultando las mismas satisfactorias.

4.2.5.6.3.Tarea IAS 6.3: Evaluación del Resultado de las Pruebas de Aceptación

- ***Evaluación del resultado de las pruebas de aceptación***

Se evalúan como positivas las pruebas de aceptación, como resultado adicional los directores aportan elementos para realizar futuras líneas de investigación relacionadas con el proyecto.

4.2.5.7.Actividad IAS 7: Preparación del Mantenimiento del Sistema

El objetivo de esta actividad es permitir que el equipo que va a asumir el mantenimiento del sistema esté familiarizado con él antes de que el sistema pase a producción. Para conseguir este objetivo, se ha considerado al responsable de mantenimiento como parte integrante del equipo de implantación. Por lo tanto, se habrá tenido en cuenta su perfil al elaborar el esquema de formación correspondiente.

Una vez que el responsable de mantenimiento ha recibido la formación necesaria y adquirido una visión global del sistema que se va a implantar, se le entregan los productos que serán objeto del mantenimiento. De esta manera, obtiene de una forma gradual un conocimiento profundo del funcionamiento y facilidades que incorpora el sistema, que van a permitirle acometer los cambios solicitados por los usuarios con mayor facilidad y eficiencia. Se reduce, en consecuencia, el esfuerzo invertido en el mantenimiento.

Es importante resaltar que la existencia de una configuración del software permite reducir el esfuerzo requerido y mejora la calidad general del software a mantener, aunque no garantiza un mantenimiento libre de problemas. Una pobre configuración del software puede tener un impacto negativo sobre su facilidad de mantenimiento.

- ***Plan de mantenimiento***

ITAUDIT es un prototipo desarrollado como trabajo de tesis, por lo cual el plan de mantenimiento queda fuera del alcance del presente trabajo.

4.2.5.8. Actividad IAS 8: Establecimiento del acuerdo de nivel de servicio

Antes de la aprobación definitiva del sistema por parte del Comité de Dirección es conveniente:

- *Determinar los servicios que requiere el mismo.*
- *Especificar los niveles de servicio con los que se va a valorar la calidad de ese prestación.*
- *Definir qué compromisos se adquieren con la entrega del sistema.*

Para ello, en primer lugar, se negocia entre los máximos responsables del usuario y de operación qué servicios y de qué tipo se van a prestar. Una vez acordados, se detallan los niveles de servicio definiendo sus propiedades funcionales y de calidad. Se establece cuáles de ellas son cuantificables y qué indicadores se van a aplicar. Es importante señalar que los niveles de servicio son específicos para cada uno de los subsistemas que componen el sistema de información, y dependen del entorno de operación y de la localización geográfica en que se implante un sistema de información concreto, pudiendo haber servicios básicos para todo el sistema o específicos para un subsistema de información concreto.

Por último, se establece formalmente el acuerdo de nivel de servicio, considerando los recursos necesarios, plazos de restablecimiento del servicio, coste y mecanismos de regulación que están asociados a cada servicio especificado anteriormente.

Según el ámbito y el alcance de los tipos de servicio que se vayan a prestar, se determinar los productos del ciclo de vida del software necesarios para poder establecer el acuerdo de nivel de servicio.

- ***Especificación de tipos de servicio***

ITAUDIT es un prototipo desarrollado como trabajo de tesis que no será implantado, por lo tanto se es necesarios realizar una especificación de tipos de servicio

4.2.5.9. Actividad 9: Presentación y aprobación del sistema

4.2.5.9.1.Tarea IAS 9.1: Convocatoria de la Presentación del Sistema

- ***Plan de presentación del sistema***

Para realizar esta tarea se compila toda la documentación del sistema y se preparan dos carpetas para cada uno de los Directores del proyecto. Se

establece el lugar y hora donde se entregará la documentación y se mostrará la última versión del prototipo.

4.2.5.9.2.Tarea IAS 9.2: Aprobación del Sistema

- ***Aprobación del sistema***

Después de la presentación los directores del proyecto aprueban formalmente la tesis.

4.2.5.10.Actividad IAS 10: Paso a Producción

Esta actividad tiene como objetivo establecer el punto de inicio en que el sistema pasa a producción, se traspasa la responsabilidad al equipo de mantenimiento y se empiezan a dar los servicios establecidos en el acuerdo de nivel de servicio, una vez que el Comité de Dirección ha aprobado el sistema.

Para ello es necesario que, después de haber realizado las pruebas de implantación y de aceptación del sistema, se disponga del entorno de producción perfectamente instalado en cuanto a hardware y software de base, componentes del nuevo sistema y procedimientos manuales y automáticos.

En función del entorno en el que se hayan llevado a cabo las pruebas de implantación y aceptación del sistema, habrá que instalar los componentes del sistema total o parcialmente. También se tendrá en cuenta la necesidad de migrar todos los datos o una parte de ellos.

Una vez que el sistema ya está en producción, se le notifica al responsable de mantenimiento, al responsable de operación y al Comité de Dirección.

- ***Sistema en producción***

ITAUDIT es un prototipo desarrollado como trabajo de tesis, que no está previsto pasar a producción.

Capítulo 4

Solución

Sección 4.3. – Mantenimiento del Sistema de Información

4.3.PROCESO DE MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

El objetivo de este proceso es la obtención de una nueva versión de un sistema de información desarrollado con MÉTRICA Versión 3 ó Versión 2, a partir de las peticiones de mantenimiento que los usuarios realizan con motivo de un problema detectado en el sistema, o por la necesidad de una mejora del mismo.

En este proceso se realiza el registro de las peticiones de mantenimiento recibidas, con el fin de llevar el control de las mismas y de proporcionar, si fuera necesario, datos estadísticos de peticiones recibidas o atendidas en un determinado periodo, sistemas que se han visto afectados por los cambios, en qué medida y el tiempo empleado en la resolución de dichos cambios. Es recomendable, por lo tanto, llevar un catálogo de peticiones de mantenimiento sobre los sistemas de información, en el que se registren una serie de datos que nos permitan disponer de la información antes mencionada.

En el momento en el que se registra la petición, se procede a diagnosticar de qué tipo de mantenimiento se trata. Atendiendo a los fines, podemos establecer los siguientes tipos de mantenimiento:

- *Correctivo: son aquellos cambios precisos para corregir errores del producto software.*
- *Evolutivo: son las incorporaciones, modificaciones y eliminaciones necesarias en un producto software para cubrir la expansión o cambio en las necesidades del usuario.*
- *Adaptativo: son las modificaciones que afectan a los entornos en los que el sistema opera, por ejemplo, cambios de configuración del hardware, software de base, gestores de base de datos, comunicaciones, etc.*
- *Perfectivo: son las acciones llevadas a cabo para mejorar la calidad interna de los sistemas en cualquiera de sus aspectos: reestructuración del código, definición más clara del sistema y optimización del rendimiento y eficiencia.*

Estos dos últimos tipos quedan fuera del ámbito de MÉTRICA Versión 3 ya que requieren actividades y perfiles distintos de los del proceso de desarrollo.

Una vez registrada la petición e identificado el tipo de mantenimiento y su origen, se determina de quién es la responsabilidad de atender la petición. En el supuesto de que la petición sea remitida, se registra en el catálogo de peticiones de mantenimiento y continua el proceso. La petición puede ser denegada. En este caso, se notifica al usuario y acaba el proceso.

Posteriormente, según se trate de un mantenimiento correctivo o evolutivo, se verifica y reproduce el problema, o se estudia la viabilidad del cambio propuesto por el usuario. En ambos casos se estudia el alcance de la modificación. Hay que analizar las alternativas de solución identificando, según el tipo de mantenimiento de que se trate, cuál es la más adecuada. El plazo y urgencia de la solución a la petición se establece de acuerdo con el estudio anterior.

La definición de la solución incluye el estudio del impacto de la solución propuesta para la petición en los sistemas de información afectados. Mediante el análisis de dicho estudio, la persona encargada del Proceso de Mantenimiento valora el esfuerzo y coste necesario para la implementación de la modificación.

Las tareas de los procesos de desarrollo que va a ser necesario realizar son determinadas en función de los componentes del sistema actual afectados por la modificación. Estas tareas pertenecen a actividades de los procesos Análisis, Diseño, Construcción e Implantación.

Por último, y antes de la aceptación del usuario, es preciso establecer un plan de pruebas de regresión que asegure la integridad del sistema de información afectado.

La mejor forma de mantener el coste de mantenimiento bajo control es una gestión del Proceso de Mantenimiento efectiva y comprometida. Por lo tanto, es necesario registrar de forma disciplinada los cambios realizados en los sistemas de información y en su documentación. Esto repercutirá directamente en la mayor calidad de los sistemas resultantes.

4.3.1.ACTIVIDAD MSI 1: REGISTRO DE LA PETICIÓN

El objetivo de esta actividad es establecer un sistema estandarizado de registro de información para las peticiones de mantenimiento, con el fin de controlar y canalizar los cambios propuestos por un usuario o cliente, mejorando el flujo de trabajo de la organización y proporcionando una gestión efectiva del mantenimiento.

Es importante asignar responsabilidades para evitar la realización de cambios que beneficien a un usuario, pero que produzcan un impacto negativo sobre otros muchos. Por tanto, es necesario que todas las peticiones de mantenimiento sean presentadas de una forma estandarizada, que permita su clasificación y facilite la identificación del tipo de mantenimiento requerido.

Una vez que la petición ha sido registrada, que ha determinado el tipo de mantenimiento y los sistemas de información a los que inicialmente puede afectar, se comprueba su viabilidad, de acuerdo a las prestaciones de mantenimiento establecidas para dichos sistemas de información.

4.3.1.1.Tarea MSI 1.1: Registro de la Petición

Esta tarea tiene como objetivo registrar las peticiones que los usuarios solicitan con motivo de la detección de un problema o por la necesidad de una mejora. Se crea un catálogo que constituye un medio para la comunicación entre el usuario o cliente y el responsable de mantenimiento. Este catálogo servirá de base para abordar, en tareas posteriores, el análisis de la petición, realizar la modificación solicitada y proporcionar datos estadísticos sobre peticiones recibidas o atendidas.

La información que debe incluir dicho registro se determina de acuerdo a las normas o estándares existentes en la organización para la recepción de peticiones de mantenimiento. En el caso de un error se debe incluir una completa descripción de las circunstancias que llevaron al fallo, adjuntando datos de entrada, listados, o cualquier otro material de soporte que se considere oportuno. Para peticiones de mejora se debe remitir una especificación de los requisitos a contemplar.

En cualquier caso, será imprescindible recoger la identificación, origen y tipo de petición, asignarle una prioridad inicial e incorporar una descripción, lo más precisa posible, que facilite su posterior análisis.

Dadas las características del proyecto de Tesis, donde el producto a desarrollar es un prototipo que no se implementará en ninguna empresa u organismo, esta tarea no se realiza.

4.3.1.2.Tarea MSI 1.2: Asignación de la Petición

En esta tarea se determina el tipo de mantenimiento requerido por la petición catalogada, teniendo en cuenta toda la información que se ha registrado en la tarea anterior. Hay que identificar también los sistemas de información inicialmente afectados por petición.

A continuación, se comprueba que el servicio de mantenimiento, definido en el plan de mantenimiento para el sistema de información, cubre el tipo de mantenimiento que requiere la petición. Sobre la base de estos criterios, se acepta o rechaza la petición y se notifica a quién corresponda.

Si la petición es aceptada, se determina de quién es la responsabilidad de atender la solicitud para proceder a su estudio posterior.

Dadas las características del proyecto de Tesis, donde el producto a desarrollar es un prototipo que no se implementará en ninguna empresa u organismo, esta tarea no se realiza.

4.3.2.ACTIVIDAD MSI 2: ANÁLISIS DE LA PETICIÓN

En esta actividad se lleva a cabo el diagnóstico y análisis del cambio para dar respuesta a las peticiones de mantenimiento que han sido aceptadas en la actividad anterior.

Se analiza el alcance de la petición en lo referente a los sistemas de información afectados, valorando hasta que punto pueden ser modificados en función del ciclo de vida estimado para los mismos y determinando la necesidad de desviar la petición hacia el proceso Estudio de Viabilidad del Sistema (EVS) o Análisis del Sistema de Información (ASI), en función del impacto sobre los sistemas de información afectados.

El enfoque de este estudio varía según el tipo de mantenimiento, teniendo en cuenta que en el caso de un mantenimiento correctivo que implique un error crítico debe abordarse el cambio de forma inmediata sin profundizar en el origen del mismo. No obstante, una vez reanudado el servicio, es imprescindible analizar el problema y determinar cuál es la solución definitiva.

Dadas las características del proyecto de Tesis, donde el producto a desarrollar es un prototipo que no se implementará en ninguna empresa u organismo, esta tarea no se realiza.

4.3.2.1.Tarea MSI 2.1: Verificación y Estudio de la Petición

Antes de iniciar el estudio de la petición, se verifica que la información registrada es correcta. Para determinar su validez:

> *Si se trata de un mantenimiento correctivo, se debe reproducir el problema.*
>
> *En el caso de un mantenimiento evolutivo, hay que comprobar que la petición es razonable o factible.*

Una vez examinada la petición comienza su estudio, que será diferente en función del tipo de mantenimiento establecido:

Si se trata de una petición de mantenimiento correctivo, y según el acuerdo de nivel de servicio establecido para los sistemas de información afectados, se evalúa hasta qué punto es crítico el problema. Así es posible determinar si la solución es a corto plazo, es decir, urgente o inmediata, o si es a medio o a largo plazo:

Si el problema es crítico, su análisis y solución comienza inmediatamente con el fin de reanudar rápidamente el nivel de servicio. Sin embargo, este modo de actuación no elimina la necesidad de una revisión posterior del problema para valorar los posibles efectos secundarios, establecer una solución definitiva y actualizar todos los productos implicados.

Si no es crítico, la petición se clasifica para proceder en la tarea siguiente a determinar cuál es la solución más adecuada.

En el caso de un mantenimiento evolutivo se delimita su alcance determinando si se trata de una modificación a los sistemas de información inicialmente afectados o de una incorporación para cubrir nuevas funcionalidades no contempladas hasta el momento en dichos sistemas de información.

Dadas las características del proyecto de Tesis, donde el producto a desarrollar es un prototipo que no se implementará en ninguna empresa u organismo, esta tarea no se realiza.

4.3.2.2.Tarea MSI 2.2: Estudio de la Propuesta de Solución

A partir del catálogo de peticiones, y para cada una de ellas, se estima su alcance valorando la prioridad inicialmente asignada, de acuerdo a los requisitos planteados. A continuación, se analiza la relación entre peticiones. Se decide cuáles pueden abordarse de forma conjunta asignando, si procede, una prioridad global a los grupos identificados y determinando en qué secuencia deben implementarse los cambios.

Asimismo, es necesario concretar los requisitos solicitados para cada petición y analizar con más detalle los sistemas de información implicados, valorando las características de mantenimiento de los mismos y la cantidad de cambios sufridos desde su puesta en producción.

También se debe comprobar la existencia de otras peticiones en curso que afecten a los mismos sistemas de información, evaluando la repercusión que puede tener la realización de la petición de mantenimiento sobre estos cambios o desarrollos y analizar su convivencia. Además, se analiza el impacto que la

modificación puede provocar en el entorno tecnológico y en los niveles de servicio inicialmente acordados para cada uno de los sistemas de información, valorando hasta que punto pueden verse comprometidos.

En el caso de una petición de mantenimiento evolutivo, se estudia cómo atenderla teniendo en cuenta la política de versiones vigente en ese momento. Si se trata de una incorporación o eliminación, se determina la necesidad de llevar a cabo algunas actividades del proceso Análisis del Sistema de Información de modo previo a la identificación de los elementos afectados. Igualmente, se puede tomar la decisión de abordar el proceso Estudio de Viabilidad del Sistema atendiendo a los requisitos a cubrir, al alcance de la modificación, a las implicaciones en el entorno tecnológico, y al ciclo de vida estimado para los sistemas de información afectados, así como a la existencia de opciones de mercado más idóneas.

En el caso de peticiones de mantenimiento correctivo que hayan precisado de una solución de emergencia, no se darán por cerradas hasta que, o bien se compruebe que con dicha solución el sistema no se ha visto comprometido ni tampoco otros sistemas relacionados con él, o bien que después de haber aplicado una solución a corto/medio plazo y realizadas las pruebas pertinentes, el sistema conserva su integridad y operatividad. Por tanto, una vez que se ha reanudado el servicio, hay que realizar las restantes actividades para detectar el origen del problema y asegurar que los cambios introducidos no generan otros de mayor envergadura o comprometen el correcto funcionamiento de otros sistemas de información relacionados.

En cualquiera de las situaciones anteriores, se hace una estimación preliminar del esfuerzo requerido mediante los indicadores establecidos en el acuerdo de nivel de servicio para cada sistema de información, según la tecnología aplicada, naturaleza y tamaño del sistema de información y los tipos de lenguajes utilizados, bases de datos, etc.

Por último, si se considera necesario, hay que proponer alternativas de solución para dar respuesta de forma satisfactoria a los requisitos planteados o problemas detectados, determinando una fecha límite de implantación y un coste aproximado en función de la estimación realizada anteriormente. Se elige, junto con el usuario, la solución más adecuada, y se obtiene la aprobación o rechazo de la petición. En caso de rechazo, la petición se da por cerrada en el catálogo.

Dadas las características del proyecto de Tesis, donde el producto a desarrollar es un prototipo que no se implementará en ninguna empresa u organismo, esta tarea no se realiza.

4.3.3.ACTIVIDAD MSI 3: PREPARACIÓN DE LA IMPLEMENTACIÓN DE LA MODIFICACIÓN

Una vez finalizado el estudio previo de la petición y aprobada su implementación, se pasa a identificar de forma detallada cada uno de los elementos afectados por el cambio mediante el análisis de impacto. Este análisis tiene como objetivo determinar qué parte del sistema de información se ve afectada, y en qué medida, dejando claramente definido y documentado qué componentes hay que modificar, tanto de software como de hardware.

Con el resultado de este análisis se dispone de los datos cuantitativos sobre los que aplicar los indicadores establecidos. Esto permitirá fijar un plan de acción, valorando la necesidad de realizar un reajuste de dichos indicadores, con el fin de cumplir el plazo máximo de entrega.

Una vez aceptado el plan de acción, se activan los correspondientes procesos de desarrollo para llevar a cabo la implementación de la solución. Al mismo tiempo, se especifican las pruebas de regresión con el fin de evitar el efecto onda en el sistema, una vez realizados los cambios.

4.3.3.1.Tarea MSI 3.1: Identificación de Elementos Afectados

Se realiza un análisis detallado del impacto de la petición, con el fin de conocer el alcance real de la modificación en función del número, características y relaciones existentes entre los elementos afectados. De esta manera se puede establecer una secuencia y planificación correcta del desarrollo de los cambios, valorando los recursos necesarios para llevarlo a cabo. En el caso de un mantenimiento evolutivo que implique una incorporación o eliminación, el alcance real de la modificación se determina después de realizar el proceso Análisis del Sistema de Información, según se indicó en la actividad anterior.

Por tanto, a partir del resultado del estudio obtenido en la actividad anterior, se identifica cada sistema de información afectado creando argumentos de búsqueda para determinar qué elementos y en qué medida están implicados en el proceso de cambio.

En este análisis quedarán reflejados, de la forma que se considere más conveniente, los elementos de la infraestructura tecnológica (hardware, software de base, comunicaciones, etc.) y los elementos asociados a los productos software implicados en cada petición (modelos, pantallas, informes, módulos, programas fuentes, programas objetos, JCL´s, archivos de datos, manuales de usuario, manuales de explotación...), así como las referencias

cruzadas. La asociación de elementos a cada petición, permitirá el control de la gestión del cambio sobre un mismo elemento.

Dadas las características del proyecto de Tesis, donde el producto a desarrollar es un prototipo que no se implementará en ninguna empresa u organismo, esta tarea no se realiza.

4.3.3.2.Tarea MSI 3.2: Establecimiento del Plan de Acción

Se identifican las actividades y tareas de los procesos de desarrollo Estudio de Viabilidad del Sistema, Análisis del Sistema de Información, Diseño del Sistema de Información, Construcción del Sistema de Información e Implantación y Aceptación del Sistema que es preciso realizar, en función de las características, complejidad y alcance de la petición estudiada, así como del plan de mantenimiento establecido para los sistemas de información implicados.

Una vez delimitado el alcance del plan de acción, se aplican los indicadores establecidos para el conjunto de componentes afectados, realizando los reajustes que oportunos. Se establece un plan de trabajo en el que se determina el coste asociado, los plazos estimados para su implementación con las fechas de comienzo y fin, y la composición del equipo de trabajo inicial necesario, teniendo en cuenta el alcance de la modificación, el nivel de esfuerzo requerido y el plan de trabajo establecido.

Finalmente, se definen puntos de control que permiten hacer un seguimiento del plan de trabajo durante la implementación de la modificación, determinando con qué frecuencia y en que situaciones se llevará a cabo.

Una vez aprobado el plan de acción y asignados los recursos, se lleva a cabo su inicio.

Dadas las características del proyecto de Tesis, donde el producto a desarrollar es un prototipo que no se implementará en ninguna empresa u organismo, esta tarea no se realiza.

4.3.3.3.Tarea MSI 3.3: Especificación del Plan de Pruebas de Regresión

Las pruebas de regresión tratan de eliminar el llamado efecto onda, es decir, que los cambios provocados por una petición no introduzcan un comportamiento no deseado o errores adicionales en otros componentes no modificados. Por tanto, es necesario comprobar que los cambios que se lleven a cabo en los componentes afectados, no produzcan estos efectos sobre el mismo u otros componentes.

Con este objetivo se deben especificar los casos de prueba en función de las relaciones existentes entre los distintos componentes identificados en la tarea Identificación de Elementos Afectados (MSI 3.1). De esta forma, los casos de prueba aseguran que la nueva versión satisface las necesidades planteadas al considerar, a su vez, los sistemas de información que no han sido modificados pero están directamente relacionados con ellos y, en consecuencia, pueden verse afectados.

Dadas las características del proyecto de Tesis, donde el producto a desarrollar es un prototipo que no se implementará en ninguna empresa u organismo, esta tarea no se realiza.

4.3.4.ACTIVIDAD MSI 4: SEGUIMIENTO Y EVALUACIÓN DE LOS CAMBIOS HASTA LA ACEPTACIÓN

Se realiza el seguimiento de los cambios que se están llevando a cabo en los procesos de desarrollo, de acuerdo a los puntos de control del ciclo de vida del cambio establecidos en el plan de acción. Durante este seguimiento, se comprueba que sólo se han modificado los elementos que se ven afectados por el cambio y que se han realizado las pruebas correspondientes, especialmente las pruebas de integración y del sistema. Del resultado obtenido se hace una evaluación del cambio para la posterior aprobación.

Una vez finalizado el cambio en desarrollo, se realizan las pruebas de regresión que especificadas en la actividad anterior, comprobando que ningún sistema no modificado, pero con posibilidades de verse afectado, ha variado su comportamiento habitual. Se informa si ha habido incidencias con el fin de que se resuelvan del modo más conveniente. Se evalúan las pruebas.

La aprobación de la petición se realiza al finalizar las pruebas de regresión, y después de comprobar que todo lo que ha sido modificado o puede verse afectado por el cambio, funciona correctamente

Con el cierre de la petición se podrán incluir en el catálogo, si se considera oportuno, parte de la información obtenida durante el proceso de mantenimiento que pueda facilitar posteriores análisis.

4.3.4.1.Tarea MSI 4.1: Seguimiento de los Cambios

Se hace el seguimiento del plan de acción de acuerdo a los puntos de control establecidos en la actividad anterior.

Se realiza el seguimiento de los cambios necesarios en los componentes de cada sistema de información afectado, así como en los productos asociados, siguiendo las actividades correspondientes a los procesos de Análisis, Diseño, Construcción e Implantación identificadas en la actividad anterior.

Asimismo, se lleva a cabo el control de la planificación establecida, que abarca los siguientes aspectos:

- *Realizar la traza de los cambios que la petición ha provocado a lo largo de los procesos de desarrollo implicados.*
- *Verificar que se han realizado satisfactoriamente las pruebas unitarias, de integración y del sistema que se consideraron necesarias para los componentes a modificar.*
- *Comprobar que sólo se ha modificado lo establecido y, en caso contrario, justificar el motivo.*
- *Asegurar que se han actualizado los productos correspondientes.*
- *Llevar el control de los distintos desarrollos existentes en paralelo sobre un mismo componente, con el fin de coordinar las modificaciones incluidas en cada uno de ellos, y asegurar que en el paso a producción se implantan correctamente.*

Dadas las características del proyecto de Tesis, donde el producto a desarrollar es un prototipo que no se implementará en ninguna empresa u organismo, esta tarea no se realiza.

4.3.4.2.Tarea MSI 4.2: Realización de las Pruebas de Regresión

Una vez finalizadas las actividades correspondientes al proceso de construcción, se realizan las pruebas de regresión definidas en la actividad anterior con el objeto de asegurar que ningún sistema de información implicado en el cambio ve comprometido su funcionamiento normal.

En el caso de detectarse problemas, se elabora un informe que recoge las incidencias y se remite a quién proceda para que tome las medidas correctivas que considere oportunas.

Finalmente, una vez que el comportamiento es correcto, se documenta el resultado global de la evaluación de las pruebas que incluye la aprobación por parte del responsable de mantenimiento.

Dadas las características del proyecto de Tesis, donde el producto a desarrollar es un prototipo que no se implementará en ninguna empresa u organismo, esta tarea no se realiza.

4.3.4.3.Tarea MSI 4.3: Aprobación y Cierre de la Petición

Se aprueba formalmente la finalización de la petición de mantenimiento de acuerdo a los resultados obtenidos en la tarea anterior. Se actualiza el catálogo de peticiones registrando el cierre de la petición tratada.

Asimismo, para llevar un control del coste y al mismo tiempo evaluar la facilidad de mantenimiento, es conveniente registrar datos cuantitativos relativos al tiempo empleado en el análisis de la petición, en el estudio del impacto, resolución del cambio, recursos empleados, etc. El registro de este tipo de información proporciona una base cuantitativa sobre la que tomar decisiones relativas a la eficacia de las técnicas y procedimientos de mantenimiento.

Dadas las características del proyecto de Tesis, donde el producto a desarrollar es un prototipo que no se implementará en ninguna empresa u organismo, esta tarea no se realiza.

Capítulo 4

Solución

Sección 4.4. – Interfaz de gestión del proyecto

4.4. Actividades relacionadas con la con la Gestión del proyecto

4.4.1.Actividades de inicio del proyecto

4.4.1.1.Actividad GPI 1: Estimación del Esfuerzo

4.4.1.1.1.Tarea GPI 1.1: Identificación de Elementos a Desarrollar

- ***Definición general del proyecto***
  - ***Catálogo de funciones***

Las funciones que cumple el sistema ITAUDIT se reflejan en los siguientes módulos:

- ✓ Alcances y objetivos

  a) A través de un check list inicial permitirá establecer inicialmente el alcance de la auditoría. Este cuestionario determinará las características de la empresa, sus funciones, áreas, dependencias, etc. El alcance estará determinado por las áreas que se auditarán y establecerá el límite de auditoría.

  Se almacenará en una tabla los datos básicos del proyecto las áreas a auditar.

  Se almacenará en una tabla las características de la empresa a auditar.

  Se almacenará en una tabla las áreas a auditar.

  Se emitirá un reporte con el alcance del proyecto.

  b) A través de un cuestionario se determinarán los objetivos del proyecto, en este punto se determinará por ejemplo si se analizarán los puntos de control de COBIT.

  Se almacenará en una tabla los objetivos de la auditoría.

  Se emitirá un informe con los objetivos del proyecto.

- ✓ Estudio preliminar

  a) A través de cuestionarios se realizará un relevamiento inicial de todo lo relacionado a las áreas de Tecnología de la Información que se encuentran dentro de la tarea delimitada en el punto a), donde se establecerá pro ejemplo la estructura interna del Área de Informática a auditar, las aplicaciones existentes, el personal relacionado con la tarea, el inventario y arquitectura del hardware y software, la documentación existente, etc.

Se almacenará en una tabla el resultado del relevamiento inicial.

Se emitirá un informe con el estudio preliminar.

✓ Recursos Humanos

a) El asistente en función de los objetivos, alcance y el estudio preliminar deberá sugerirle al auditor **los recursos** necesarios para realizar la tarea.

Se almacenará en una tabla los recursos necesarios para el proyecto.

Se emitirá un informe con los recursos humanos necesarios.

✓ Planificación

a) El sistema brindará un entorno gráfico para que el equipo de trabajo realice la planificación de la auditoría.

Se guardará en una tabla la planificación.

Se emitirá un informe con la planificación

✓ Desarrollo

a) el sistema de acuerdo al limite y los objetivos sugerirá los distintos cuestionarios y check list necesarios para realizar la auditoría, de acuerdo a los objetivos establecidos se seguirán o no los objetivos de control de COBIT.

Se almacenará en una tabla el resultado de esta tarea.

Se emitirá un informe con el resultado del desarrollo de la auditoría.

✓ Informe final

a) El asistente brindará un entorno gráfico para la realización del informe final. En algunos casos sugerirá algunas conclusiones en función del desarrollo de la auditoría.

Se almacenará en una tabla el resultado de esta tarea.

Se emitirá un informe con el resultado del informe final de la auditoría.

- Catálogo de entidades

A1) Módulo alcance y objetivos

- Tabla de auditoría (M)
- Tabla modelo de definición de proyecto (M)

- Tabla modelo de definición de características de la empresa (A)
- Tabla modelo de alcance (A)
- Tabla modelo de objetivos (B)
- 4 mensajes de error (B)
- Tabla de definición del proyecto (M)
- Tabla de definición de características de la empresa (A)
- Tabla de alcance (A)
- Tabla de objetivos (B)

(6 ILF) X 7 (complejidad baja) = 42 FP

(3 ILF) X 10 (complejidad media) = 30 FP

(4 ILF) X 15 (complejidad alta) = 60 FP

A2) Módulo Relevamiento Inicial

- Tabla modelo de relevamiento inicial (A)
- Tabla de relevamiento inicial (A)
- Mensaje de error (B)
- Tabla de Auditoría (M)

(1 ILF) X 7 (complejidad baja) = 7 FP

(1 ILF) X 10 (complejidad media) = 10 FP

(2 ILF) X 15 (complejidad alta) = 30 FP

A3) Módulo Recursos Humanos

- Tabla modelo de RRHH (A)
- Tabla de RRHHl (A)
- Mensaje de error (B)
- Tabla de Auditoría (M)

(1 ILF) X 7 (complejidad baja) = 7 FP

(1 ILF) X 10 (complejidad media) = 10 FP

(2 ILF) X 15 (complejidad alta) = 30 FP

A4) Módulo planificación

- Tabla modelo de Plan (A)
- Tabla de Plan (A)

- Mensaje de error (B)
- Tabla de Auditoría (M)

(1 ILF) X 7 (complejidad baja) = 7 FP

(1 ILF) X 10 (complejidad media) = 10 FP

(2 ILF) X 15 (complejidad alta) = 30 FP

A5) Módulo Desarrollo de la Auditoría

- Tabla modelo de desarrollo de la auditoría COBIT (A)
- Tabla de desarrollo de la auditoría COBIT (A)
- Tabla modelo de desarrollo de la auditoría no COBIT (A)
- Tabla de desarrollo de la auditoría no COBIT (A)
- 4 Mensaje de error (B)
- Tabla de Auditoría (M)

(4 ILF) X 7 (complejidad baja) = 28 FP

(1 ILF) X 10 (complejidad media) = 10 FP

(4 ILF) X 15 (complejidad alta) = 60 FP

A6) Módulo Informe

- Tabla modelo de Informe (A)
- Tabla de Informe (A)
- Mensaje de error (B)
- Tabla de Auditoría (M)

(1 ILF) X 7 (complejidad baja) = 7 FP

(1 ILF) X 10 (complejidad media) = 10 FP

(2 ILF) X 15 (complejidad alta) = 30 FP

La tabla 4.31 muestra los totales ILF

Módulo	Complejidad Baja	Complejidad Media	Complejidad Alta	Totales
Alcance y objetivos	42	30	60	132
Relevamiento Inicial	7	10	30	47
Recursos Humanos	7	10	30	47
Planificación	7	10	30	47
Desarrollo	28	10	60	98

Informe	7	10	30	47
Total ILF				418

Tabla 4.31: Totales ILF

c1) Módulo alcance y objetivos

- A/B/M Tabla modelo de definición de proyecto (3M)
- A/B/M Tabla modelo de definición de características de la empresa(3A)
- A/B/M Tabla modelo de alcance (3A)
- A/B/M Tabla modelo de objetivos (3B)
- A/B/M Tabla de definición del proyecto (3M)
- A/B/M Tabla de definición de características de la empresa (3A)
- A/B/M Tabla de alcance (3A)
- A/B/M Tabla de objetivos (3B)

(6 EI) X 3 (complejidad baja) = 18 FP

(3 EI) X 4 (complejidad media) = 12 FP

(12 EI) X 6 (complejidad alta) = 72 FP

c2) Módulo Relevamiento Inicial

- A/B/M Tabla modelo de relevamiento inicial (3A)
- A/B/M Tabla de relevamiento inicial (3A)

(6 EI) X 6 (complejidad alta) = 36 FP

c3) Módulo Recursos Humanos

- A/B/M Tabla modelo de RRHH (3A)
- A/B/M Tabla de RRHHl (3A)

(6 EI) X 6 (complejidad alta) = 36 FP

c4) Módulo planificación

- A/B/M Tabla modelo de Plan (3A)
- A/B/M Tabla de Plan (3A)

(6 EI) X 6 (complejidad alta) = 36 FP

c5) Módulo Desarrollo de la Auditoría

- A/B/M Tabla modelo de desarrollo de la auditoría COBIT (3A)
- A/B/M Tabla de desarrollo de la auditoría COBIT (3A)

- A/B/M Tabla modelo de desarrollo de la auditoría no COBIT (3A)
- A/B/M Tabla de desarrollo de la auditoría no COBIT (3A)

(12 EI) X 6 (complejidad alta) = 72 FP

c6) Módulo Informe

- A/B/M Tabla modelo de Informe (3A)
- A/B/M Tabla de Informe (3A)

(6 EI) X 6 (complejidad alta) = 36 FP

La tabla 4.32 muestra los totales de EI

Módulo	Complejidad Baja	Complejidad Media	Complejidad Alta	Totales
Alcance y objetivos	18	12	72	102
Relevamiento Inicial	0	0	36	36
Recursos Humanos	0	0	36	36
Planificación	0	0	36	36
Desarrollo	0	0	72	72
Informe	0	0	36	36
Total EI				318

Tabla 32 : EI

D) salidas (EO)

Son datos o información de control que salen de los límites de la aplicación.

d1) Módulo alcance y objetivos

- Informe de datos del proyecto (B)
- Informe de características de la empresa (B)
- Informe de alcance (B)
- Informe objetivos (B)

(4 EO) X 4 (complejidad baja) = 16 FP

d2) Módulo Relevamiento Inicial

- Informe de relevamiento inicial (B)

(1 EO) X 4 (complejidad baja) = 4 FP

d3) Módulo Recursos Humanos

- Informe de RRHH (B)

(1 EO) X 4 (complejidad baja) = 4 FP

d4) Módulo planificación

- Informe modelo de Plan (B)

(1 EO) X 4 (complejidad baja) = 4 FP

d5) Módulo Desarrollo de la Auditoría

- Informe de desarrollo de la auditoría no COBIT (B)
- Informe de desarrollo de la auditoría no COBIT (M)

(1 EO) X 4 (complejidad baja) = 4 FP

(1 EO) X 5 (complejidad media) = 5 FP

d6) Módulo Informe

- Informe final (M)

(1 EO) X 5 (complejidad media) = 5 FP

La tabla 4.33 muestra los totales de EO

Módulo	Complejidad Baja	Complejidad Media	Complejidad Alta	Totales
Alcance y objetivos	16	0	0	16
Relevamiento Inicial	4	0	0	4
Recursos Humanos	4	0	0	4
Planificación	4	0	0	4
Desarrollo	4	5	0	9
Informe	0	5	0	5
Total EO				42

Tabla 4.33: EO

E) Consultas (EI)

Son requisitos de información que se realizan a la aplicación en una combinación única de entrada y salida.

e1) Módulo alcance y objetivos

- Búsqueda de proyectos (B)
- Búsqueda de empresas (B)
- Búsqueda de alcances (B)
- Búsqueda de objetivos (B)
- Menú (B)

- Ayuda (B)

(6 EI) X 3 (complejidad baja) = 18 FP

e2) Módulo Relevamiento Inicial

- Búsqueda de relevamiento inicial (B)
- Menú (B)
- Ayuda (B)

(3 EI) X 3 (complejidad baja) = 9 FP

e3) Módulo Recursos Humanos

- Búsqueda de RRHH (B)
- Menú (B)
- Ayuda (B)

(3 EI) X 3 (complejidad baja) = 9 FP

e4) Módulo planificación

- Búsqueda de planificación (B)
- Menú (B)
- Ayuda (B)

(3 EI) X 3 (complejidad baja) = 9 FP

e5) Módulo Desarrollo de la Auditoría

- Búsqueda de desarrollo de la auditoría (B)
- Menú (B)
- Ayuda (B)

(3 EI) X 3 (complejidad baja) = 9 FP

e6) Módulo Informe

- Búsqueda Informe final (M)
- Menú (B)
- Ayuda (B)

(3 EI) X 3 (complejidad baja) = 9 FP

La tabla 4.34 muestra los totales de EI

Módulo	Complejidad Baja	Complejidad Media	Complejidad Alta	Totales
alcance y objetivos	18	0	0	18
Relevamiento Inicial	9	0	0	9

Recursos Humanos	9	0	0	9
Planificación	9	0	0	9
Desarrollo	9	0	0	9
Informe	9	0	0	9
Total EI				63

Tabla 4.34: Totales EI

4.4.1.1.2. Tarea GPI 1.2: Cálculo del Esfuerzo

- ***Definición general del proyecto***
  - ***Esfuerzo estimado***

  ✓ ***Puntos de Función sin ajustar***

  La tabla 4.35 muestra los puntos de función sin ajustar:

Parámetros	**Cantidad**			**Peso**			**Total**			
	B	M	A	B	M	A	B	M	A	T
ILF	14	8	16	7	10	15	98	80	240	418
FLE	0	0	0	0	0	0	0	0	0	0
EI	6	3	48	3	4	6	18	12	288	318
EO	8	2	0	4	5	0	32	10	0	42
Consultas	21	0	0	3	0	0	63	0	0	0
FP= ***841***										

Tabla 4.35. Puntos de función sin ajustar

✓ ***Calculo de Puntos de Función Ajustado***

Con el objetivo de ajustar los puntos de función se cuantifican las siguientes características del sistema que se muestran en la tabla 4.36:

Característica	**Valor**
Comunicaciones	0
Func. distrib.	0
Rendimiento	2
Configuraciones	0
Frec. Transac	2
Entrada datos	1
Eric. Usuario	0
Actualización	4
Proc. Complejos	4

Reutilización	0
Fac. Instalac	0
Fac. Operación	2
Inst. Diversa	0
Fac. Cambios	5
TDI	20
AF(TDI x 0.01) + 0.91	**1.11**

Tabla 4.36 Gestión: características desarrollo

Nota: Se utiliza el coeficiente 0.91 para ajustar según lo establecido por Horowitz E.

CALCULO DE PUNTOS DE FUNCION AJUSTADOS

FPA = 841 X 1.11

FPA= 934

- ✓ ***Cálculo de factor de ajuste***

La tabla 4.37 muestra el factor de ajuste de esfuerzo

Factor	Base	Incremento	EAF
RELY	NOM	0	
DATA	NOM	0	
DOCU	NOM	0	
CPLX	NOM	0	
RUSE	NOM	0	
TIME	NOM	0	
STOR	NOM	0	
PVOL	NOM	0	
PCAP	VHI	0	
ACAP	VHI	0	
PCON	VHI	0	
APEX	VHI	0	
LTEX	VHI	0	
PLEX	VHI	00	
TOOL	NOM	75%	
SITE	NOM	75%	
USR	NOM	0	
			0.22

Tabla 4.37. EAF

- ➢ **Datos generales del proyecto**

Modelo de Desarrollo: Preliminar (Early Design).

Factor de Escala: Según tabla 4.38

Categoría	Valor
Procedentedness	3.72
Development Flexibility	3.04
Architecture / risk resolution	4.24
Team cohesión	3.29
Process Maturity	4.68

Tabla 4.38. Factores de escala

- **Estimación de esfuerzo**

Para poder establecer el tiempo y costo del desarrollo se aplicará el modelo de COCOMO II, se utilizará el software USC COCOMO II (1999) de la Universidad de Carolina del Sur (USA) [Horowitz, 1999]

- ✓ **RESULTADOS FINALES**

Empleando esta herramienta de software da como resultado lo que muestra la figura 4.25

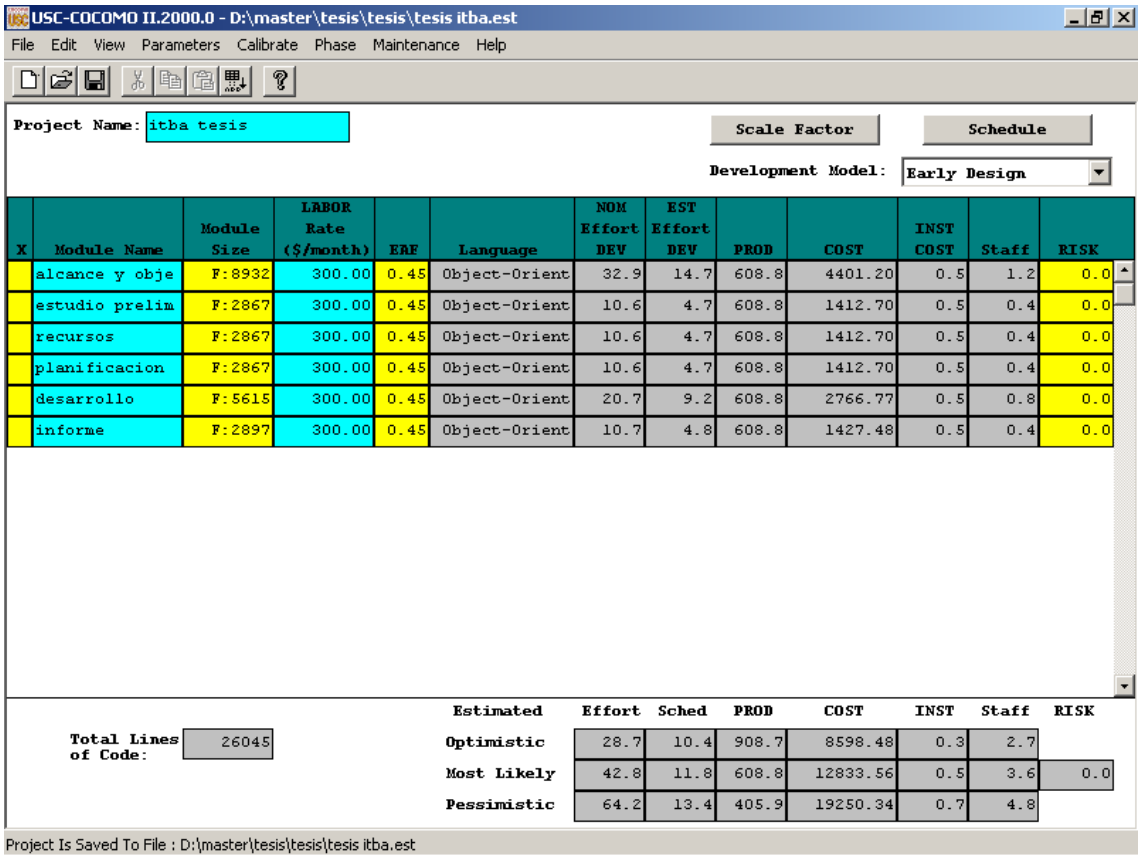


Figura 4.25: Esfuerzo

- **Tamaño estimado del sistema en Líneas de código: 26045**
- **Esfuerzo estimado Optimista: 29 meses / hombre**
- **Esfuerzo estimado mas probable: 43 meses / hombre**
- **Esfuerzo estimado pesimista 64 meses / hombre**
- **Costo Optimista: 8.598**
- **Costo mas probable: 12.833**
- **Costo pesimista: 19.250**
- **Equipo probable: 3.6 personas**
- **Meses probables: 11.8 meses**

4.4.1.2. GPI 2 - Actividades relacionadas con la planificación

4.4.1.2.1.Tarea GPI 2.1: Selección de la Estrategia de Desarrollo

- ***Planificación general del proyecto***

La estrategia de desarrollo más adecuada para este proyecto, es el prototipo o también denominado construcción evolutiva en EUROMÉTODO, dado que ITAUDIT es un prototipo funcional que se será sometido a evaluaciones y revisiones para añadir nuevas funcionalidades y mejoras para cubrir mayor cantidad de requisitos.

4.4.1.2.2.Tarea GPI 2.2: Selección de la Estructura de Actividades, Tareas y Productos

- ***Planificación general del proyecto***

La tabla 4.39 representa la planificación general del proyecto:

Proceso	*Actividad*	*Tarea*
PROCESO DE PLANIFICACIÓN DE SISTEMAS DE INFORMACIÓN	*ACTIVIDAD PSI 1: INICIO DEL PLAN DE SISTEMAS DE INFORMACIÓN*	*Tarea PSI 1.1: Análisis de la Necesidad del PSI*
		Tarea PSI 1.2: Identificación del Alcance del PSI
		Tarea PSI 1.3: Determinación de Responsables
	ACTIVIDAD PSI 2: DEFINICIÓN Y ORGANIZACIÓN DEL PSI	*Tarea PSI 2.1: Especificación del Ámbito y Alcance*
		Tarea PSI 2.2: Organización del PSI
		Tarea PSI 2.3: Definición del Plan de Trabajo
		Tarea PSI 2.4: Comunicación del Plan de Trabajo
	ACTIVIDAD PSI 3: ESTUDIO DE LA INFORMACIÓN RELEVANTE	*Tarea PSI 3.1: Selección y Análisis de Antecedentes*
		Tarea PSI 3.2: Valoración de Antecedentes
	ACTIVIDAD PSI 4: IDENTIFICACIÓN DE REQUISITOS	*Tarea PSI 4.1: Estudio de los Procesos del PSI*
		Tarea PSI 4.2: Análisis de las Necesidades de Información
		Tarea PSI 4.3: Catalogación de Requisitos
	ACTIVIDAD PSI 5: ESTUDIO DE LOS SISTEMAS DE INFORMACIÓN ACTUALES	*Tarea PSI 5.1: Alcance y Objetivos del Estudio de los Sistemas de Información Actuales*
		Tarea PSI 5.2: Análisis de los Sistemas de Información Actuales
		Tarea PSI 5.3: Valoración de los Sistemas de Información Actuales
	ACTIVIDAD PSI 6: DISEÑO DEL MODELO DE SISTEMAS DE INFORMACIÓN	*Tarea PSI 6.1: Diagnóstico de la Situación Actual*
		Tarea PSI 6.2: Definición del Modelo de Sistemas de Información
		Tarea PSI 7.1: Identificación de las Necesidades de Infraestructura Tecnológica
		Tarea PSI 7.2: Selección de la Arquitectura Tecnológica
	ACTIVIDAD PSI 8: DEFINICIÓN DEL PLAN DE ACCIÓN	*Tarea PSI 8.1: Definición de Proyectos a Realizar*
		Tarea PSI 8.2: Elaboración del Plan de Mantenimiento del PSI
	ACTIVIDAD PSI 9: REVISIÓN Y	*Tarea PSI 9.1: Convocatoria de la Presentación*

	APROBACIÓN DEL PSI	
		Tarea PSI 9.2: Evaluación y Mejora de la Propuesta
		Tarea PSI 9.3: Aprobación del PSI
ESTUDIO DE VIABILIDAD DEL SISTEMA	*ACTIVIDAD EVS 1: ESTABLECIMIENTO DEL ALCANCE DEL SISTEMA*	*Tarea EVS 1.1: Estudio de la Solicitud*
		Tarea EVS 1.2: Identificación del Alcance del Sistema
		Tarea EVS 1.3: Especificación del Alcance del Sistema
	ACTIVIDAD EVS 2: ESTUDIO DE LA SITUACIÓN ACTUAL	*Tarea EVS 2.1: Valoración del Estudio de la Situación Actual*
		Tarea EVS 2.2: Identificación de los Usuarios Participantes en el Estudio de la situación Actual
		Tarea EVS 2.3: Descripción de los Sistemas de Información Existentes
		Tarea EVS 2.4: Realización del Diagnóstico de la situación actual
	ACTIVIDAD EVS 3: DEFINICIÓN DE REQUISITOS DEL SISTEMA	*Tarea EVS 3.1: Identificación de las Directrices Técnicas y de Gestión*
		Tarea EVS 3.2: Identificación de Requisitos
		Tarea EVS 3.3: Catalogación de Requisitos
	ACTIVIDAD EVS 4: ESTUDIO DE ALTERNATIVAS DE SOLUCIÓN	*Tarea EVS 4.1: Preselección de Alternativas de Solución*
		Tarea EVS 4.2: Descripción de Alternativas de Solución
	ACTIVIDAD EVS 5: VALORACIÓN DE LAS ALTERNATIVAS	*Tarea EVS 5.1: Estudio de la Inversión*
		Tarea EVS 5.2: Estudio de Riesgos
		Tarea EVS 5.3: Planificación de Alternativas
	ACTIVIDAD EVS 6: SELECCIÓN DE LA SOLUCIÓN	*Tarea EVS 6.1: Convocatoria de la Presentación*
		Tarea EVS 6.2: Evaluación de las Alternativas de Selección
		Tarea EVS 6.3: Aprobación de la Solución
ANÁLISIS DEL SISTEMA DE INFORMACIÓN	*ACTIVIDAD ASI 1: DEFINICIÓN DEL SISTEMA*	*Tarea ASI 1.1: Determinación del Alcance del Sistema*
		Tarea ASI 1.2: Identificación del Entorno Tecnológico
		Tarea ASI 1.3: Especificación de Estándares y Normas
		Tarea ASI 1.4: Identificación de los Usuarios Participantes y Finales

	ACTIVIDAD ASI 2: ESTABLECIMIENTO DE REQUISITOS	*Tarea ASI 2.1: Obtención de Requisitos*
		Tarea ASI 2.2: Especificación de Casos de Uso
		Tarea ASI 2.3: Análisis de Requisitos
		Tarea ASI 2.4: Validación de Requisitos
	ACTIVIDAD ASI 3: IDENTIFICACIÓN DE SUBSISTEMAS DE ANÁLISIS	*Tarea ASI 3.1: Determinación de Subsistemas de Análisis*
		Tarea ASI 3.2: Integración de Subsistemas de Análisis
	ACTIVIDAD ASI 6: ELABORACIÓN DEL MODELO DE DATOS	*Tarea ASI 6.1: Elaboración del Modelo Conceptual de Datos*
		Tarea ASI 6.2: Elaboración del Modelo lógico de Datos
		Tarea ASI 6.3: Normalización del Modelo lógico de Datos
		Tarea ASI 6.4: Especificación de Necesidades de Migración de Datos y Carga Inicial
	ACTIVIDAD ASI 7: ELABORACIÓN DEL MODELO DE PROCESOS	*Tarea ASI 7.1: Obtención del Modelo de Procesos del Sistema*
		Tarea ASI 7.2: Especificación de Interfaces con otros Sistemas
	ACTIVIDAD ASI 8: DEFINICIÓN DE INTERFACES DE USUARIO	*Tarea ASI 8.1: Especificación de Principios Generales de la Interfaz*
		Tarea ASI 8.2: Identificación de Perfiles y Diálogos
		Tarea ASI 8.3: Especificación de Formatos Individuales de la Interfaz de Pantalla
		Tarea ASI 8.4: Especificación del Comportamiento Dinámico de la Interfaz
		Tarea ASI 8.5: Especificación de Formatos de Impresión
	ACTIVIDAD ASI 9: ANÁLISIS DE CONSISTENCIA Y ESPECIFICACIÓN DE REQUISITOS	*Tarea ASI 9.1: Verificación de los modelos*
		Tarea ASI 9.2: Análisis de Consistencia entre métodos
		Tarea ASI 9.3: Validación de los Modelos
		Tarea ASI 9.4: Elaboración de la Especificación de Requisitos de Software (ERS)
	ACTIVIDAD ASI 10: ESPECIFICACIÓN DEL PLAN DE	*Tarea ASI 10.1: Definición del Alcance de las Pruebas*

	PRUEBAS	
		Tarea ASI 10.2: Definición de Requisitos del Entorno de Pruebas
		Tarea ASI 10.3: Definición de las Pruebas de Aceptación del Sistema
	ACTIVIDAD ASI 11: APROBACIÓN DEL ANÁLISIS DEL SISTEMA DE INFORMACIÓN	*Tarea ASI 11.1: Presentación y Aprobación del Análisis del Sistema de Información*
DISEÑO DEL SISTEMA DE INFORMACIÓN	*ACTIVIDAD DSI 1: DEFINICIÓN DE LA ARQUITECTURA DEL SISTEMA*	*Tarea DSI 1.1: Definición de Niveles de Arquitectura*
		Tarea DSI 1.2: Identificación de Requisitos de Diseño y Construcción
		Tarea DSI 1.3: Especificaciones de Excepción
		Tarea DSI 1.4: Especificación de Estándares y Normas de Diseño y Construcción
		Tarea DSI 1.5: Identificación de Subsistemas de Diseño
		Tarea DSI 1.6: Especificación del Entorno Tecnológico
		Tarea DSI 1.7: Especificación de Requisitos de Operación y Seguridad
	ACTIVIDAD DSI 2: DISEÑO DE LA ARQUITECTURA DE SOPORTE	*Tarea DSI 2.1: Diseño de Subsistemas de Soporte*
		Tarea DSI 2.2: Identificación de Mecanismos Genéricos de Diseño
	ACTIVIDAD DSI 5: DISEÑO DE LA ARQUITECTURA DE MÓDULOS DEL SISTEMA	*Tarea DSI 5.1: Diseño de Módulos del Sistema*
		Tarea DSI 5.2: Diseño de Comunicaciones entre Módulos
		Tarea DSI 5.3: Revisión de la Interfaz de Usuario
	ACTIVIDAD DSI 6: DISEÑO FÍSICO DE DATOS	*Tarea DSI 6.1: Diseño del Modelo Físico de Datos*
		Tarea DSI 6.2: Especificación de Caminos de Acceso a los Datos
		Tarea DSI 6.3: Optimización del Modelo Físico de Datos
		Tarea DSI 6.4: Especificación de la Distribución de Datos
	ACTIVIDAD DSI 7: VERIFICACIÓN Y ACEPTACIÓN DE LA ARQUITECTURA DEL SISTEMA	*Tarea DSI 7.1: Verificación de la Especificación de Diseño*
		Tarea DSI 7.2: Análisis de Consistencia de las Especificaciones de Diseño

		Tarea DSI 7.3: Aceptación de la Arquitectura del Sistema
	ACTIVIDAD DSI 8: GENERACIÓN DE ESPECIFICACIONES DE CONSTRUCCIÓN	*Tarea DSI 8.1: Especificación del Entorno de Construcción*
		Tarea DSI 8.2: Definición de Componentes y Subsistemas de Construcción
		Tarea DSI 8.3: Elaboración de Especificaciones de Construcción
		Tarea DSI 8.4: Elaboración de Especificaciones del Modelo Físico de Datos
	ACTIVIDAD DSI 9: DISEÑO DE LA MIGRACIÓN Y CARGA INICIAL DE DATOS	*Tarea DSI 9.1: Especificación del Entorno de Migración*
		Tarea DSI 9.2: Diseño de Procedimientos de Migración y Carga Inicial
		Tarea DSI 9.3: Diseño Detallado de Componentes de Migración y Carga Inicial
		Tarea DSI 9.4: Revisión de la Planificación de la Migración
	ACTIVIDAD DSI 10: ESPECIFICACIÓN TÉCNICA DEL PLAN DE PRUEBAS	*Tarea DSI 10.1: Especificación del Entorno de Pruebas*
		Tarea DSI 10.2: Especificación Técnica de Niveles de Prueba
		Tarea DSI 10.3: Revisión de la Planificación de Pruebas
	ACTIVIDAD DSI 11: ESTABLECIMIENTO DE REQUISITOS DE IMPLEMENTACIÓN	*Tarea DSI 11.1: Especificación de Requisitos de Documentación de Usuario*
		Tarea DSI 11.2: Especificación de Requisitos de Implementación
	ACTIVIDAD DSI 12: APROBACIÓN DEL DISEÑO DEL SISTEMA DE INFORMACIÓN	*Tarea DSI 12.1: Presentación y Aprobación del Diseño del Sistema de Información*
CONSTRUCCIÓN DEL SISTEMA DE INFORMACIÓN	*ACTIVIDAD CSI 1: PREPARACIÓN DEL ENTORNO DE GENERACIÓN Y CONSTRUCCIÓN*	*Tarea CSI 1.1: Implantación de la Base de Datos Física o Ficheros*
		Tarea CSI 1.2: Preparación del Entorno de Construcción
	ACTIVIDAD CSI 2: GENERACIÓN DEL CÓDIGO DE LOS COMPONENTES Y PROCEDIMIENTOS	*Tarea CSI 2.1: Generación del Código de Componentes*
		Tarea CSI 2.2: Generación del

		Código de los Procedimientos de Operación y Seguridad
	ACTIVIDAD CSI 3: EJECUCIÓN DE LAS PRUEBAS UNITARIAS	*Tarea CSI 3.1: Preparación del Entorno de las Pruebas Unitarias*
		Tarea CSI 3.2: Realización y Evaluación de las Pruebas Unitarias
	ACTIVIDAD CSI 4: EJECUCIÓN DE LAS PRUEBAS DE INTEGRACIÓN	*Tarea CSI 4.1: Preparación del Entorno de las Pruebas de Integración*
		Tarea CSI 4.2: Realización de las Pruebas de Integración
		Tarea CSI 4.3: Evaluación del Resultado de las Pruebas de Integración
	ACTIVIDAD CSI 5: EJECUCIÓN DE LAS PRUEBAS DEL SISTEMA	*Tarea CSI 5.1: Preparación del Entorno de las Pruebas del Sistema*
		Tarea CSI 5.2: Realización de las Pruebas del Sistema
		Tarea CSI 5.3: Evaluación del Resultado de las Pruebas del Sistema
	ACTIVIDAD CSI 7: DEFINICIÓN DE LA FORMACIÓN DE USUARIOS FINALES	*Tarea CSI 7.1: Definición del Esquema de Formación*
		Tarea CSI 7.2: Especificación de los Recursos y Entornos de Formación
	ACTIVIDAD CSI 8: CONSTRUCCIÓN DE LOS COMPONENTES Y PROCEDIMIENTOS DE MIGRACIÓN Y CARGA INICIAL DE DATOS	*Tarea CSI 8.1: Preparación del Entorno de Migración y Carga Inicial de Datos*
		Tarea CSI 8.2: Generación del Código de los Componentes y Procedimientos de Migración y Carga Inicial de Datos
		Tarea CSI 8.3: Realización y Evaluación de las Pruebas de Migración y Carga Inicial de Datos
	ACTIVIDAD CSI 9: APROBACIÓN DEL SISTEMA DE INFORMACIÓN	*Tarea CSI 9.1: Presentación y Aprobación del Sistema de Información*
IMPLANTACIÓN Y ACEPTACIÓN DEL SISTEMA	*ACTIVIDAD IAS 6: PRUEBAS DE ACEPTACIÓN DEL SISTEMA*	*Tarea IAS 6.1: Preparación de las Pruebas de Aceptación*
		Tarea IAS 6.2: Realización de las Pruebas de Aceptación
		Tarea IAS 6.3: Evaluación del Resultado de las Pruebas de Aceptación
	ACTIVIDAD IAS 9: PRESENTACIÓN Y APROBACIÓN DEL	*Tarea IAS 9.1: Convocatoria de la Presentación del Sistema*

	SISTEMA	
		Tarea IAS 9.2: Aprobación del Sistema

Tabla 4.39. Planificación General del proyecto

- ***Catálogo de productos a generar***
  - Planificación del Sistema de Información
  - Estudio de viabilidad del sistema
  - Análisis del Sistema
  - Diseño del sistema
  - Base de datos y sistema
  - Aceptación del sistema

4.4.1.2.3.Tarea GPI 2.3: Establecimiento del Calendario de Hitos y Entregas

- ***Planificación general del proyecto***
  - ***Hitos del proyecto***

La tabla 4.40 muestra los hitos del proyecto

Proceso	***Actividad***	***fecha***
PROCESO DE PLANIFICACIÓN DE SISTEMAS DE INFORMACIÓN	*ACTIVIDAD PSI 1: INICIO DEL PLAN DE SISTEMAS DE INFORMACIÓN*	*25/04/05*
	ACTIVIDAD PSI 2: DEFINICIÓN Y ORGANIZACIÓN DEL PSI	*27/04/05*
	ACTIVIDAD PSI 3: ESTUDIO DE LA INFORMACIÓN RELEVANTE	*29/05/05*
	ACTIVIDAD PSI 4: IDENTIFICACIÓN DE REQUISITOS	*1/06/05*
	ACTIVIDAD PSI 5: ESTUDIO DE LOS SISTEMAS DE INFORMACIÓN ACTUALES	*03/06/05*
	ACTIVIDAD PSI 6: DISEÑO DEL MODELO DE SISTEMAS DE INFORMACIÓN	*05/06/05*
	ACTIVIDAD PSI 8: DEFINICIÓN DEL PLAN DE ACCIÓN	*07/06/05*
	ACTIVIDAD PSI 9: REVISIÓN Y APROBACIÓN DEL PSI	*10/05/05*
ESTUDIO DE VIABILIDAD DEL SISTEMA	*ACTIVIDAD EVS 1: ESTABLECIMIENTO DEL ALCANCE DEL SISTEMA*	*11/05/05*
	ACTIVIDAD EVS 2: ESTUDIO DE LA SITUACIÓN ACTUAL	*13/05/05*
	ACTIVIDAD EVS 3: DEFINICIÓN DE REQUISITOS DEL SISTEMA	*19/05/05*
	ACTIVIDAD EVS 4: ESTUDIO DE	*22/05/05*

	ALTERNATIVAS DE SOLUCIÓN	
	ACTIVIDAD EVS 5: VALORACIÓN DE LAS ALTERNATIVAS	*25/05/05*
	ACTIVIDAD EVS 6: SELECCIÓN DE LA SOLUCIÓN	*27/05/05*
ANÁLISIS DEL SISTEMA DE INFORMACIÓN	*ACTIVIDAD ASI 1: DEFINICIÓN DEL SISTEMA*	*30/05/05*
	ACTIVIDAD ASI 2: ESTABLECIMIENTO DE REQUISITOS	*1506/05*
	ACTIVIDAD ASI 3: IDENTIFICACIÓN DE SUBSISTEMAS DE ANÁLISIS	*29/06/05*
	ACTIVIDAD ASI 6: ELABORACIÓN DEL MODELO DE DATOS	*14/07/05*
	ACTIVIDAD ASI 7: ELABORACIÓN DEL MODELO DE PROCESOS	*28/07/05*
	ACTIVIDAD ASI 8: DEFINICIÓN DE INTERFACES DE USUARIO	*07/08/05*
	ACTIVIDAD ASI 9: ANÁLISIS DE CONSISTENCIA Y ESPECIFICACIÓN DE REQUISITOS	*14/08/08*
	ACTIVIDAD ASI 10: ESPECIFICACIÓN DEL PLAN DE PRUEBAS	*25/08/05*
	ACTIVIDAD ASI 11: APROBACIÓN DEL ANÁLISIS DEL SISTEMA DE INFORMACIÓN	*06/09/05*
DISEÑO DEL SISTEMA DE INFORMACIÓN	*ACTIVIDAD DSI 1: DEFINICIÓN DE LA ARQUITECTURA DEL SISTEMA*	*07/09/05*
	ACTIVIDAD DSI 2: DISEÑO DE LA ARQUITECTURA DE SOPORTE	*21/09/05*
	ACTIVIDAD DSI 5: DISEÑO DE LA ARQUITECTURA DE MÓDULOS DEL SISTEMA	*07/10/05*
	ACTIVIDAD DSI 6: DISEÑO FÍSICO DE DATOS	*21/10/05*
	ACTIVIDAD DSI 7: VERIFICACIÓN Y ACEPTACIÓN DE LA ARQUITECTURA DEL SISTEMA	*07/10/05*
	ACTIVIDAD DSI 8: GENERACIÓN DE ESPECIFICACIONES DE CONSTRUCCIÓN	*21/10/05*
	ACTIVIDAD DSI 9: DISEÑO DE LA MIGRACIÓN Y CARGA INICIAL DE DATOS	*1/11/05*
	ACTIVIDAD DSI 10: ESPECIFICACIÓN TÉCNICA DEL PLAN DE PRUEBAS	*6/11/05*
	ACTIVIDAD DSI 11: ESTABLECIMIENTO DE REQUISITOS DE IMPLEMENTACIÓN	*15/11/05*
	ACTIVIDAD DSI 12: APROBACIÓN DEL DISEÑO DEL SISTEMA DE INFORMACIÓN	*21/11/05*
CONSTRUCCIÓN DEL SISTEMA DE INFORMACIÓN	*ACTIVIDAD CSI 1: PREPARACIÓN DEL ENTORNO DE GENERACIÓN Y CONSTRUCCIÓN*	*22/11/05*
	ACTIVIDAD CSI 2: GENERACIÓN DEL CÓDIGO DE LOS COMPONENTES Y PROCEDIMIENTOS	*10/12/05*
	ACTIVIDAD CSI 3: EJECUCIÓN DE LAS PRUEBAS UNITARIAS	*30/12/05*
	ACTIVIDAD CSI 4: EJECUCIÓN DE LAS	*20/01/06*

	PRUEBAS DE INTEGRACIÓN	
	ACTIVIDAD CSI 5: EJECUCIÓN DE LAS PRUEBAS DEL SISTEMA	*10/02/06*
	ACTIVIDAD CSI 7: DEFINICIÓN DE LA FORMACIÓN DE USUARIOS FINALES	*28/02/06*
	ACTIVIDAD CSI 8: CONSTRUCCIÓN DE LOS COMPONENTES Y PROCEDIMIENTOS DE MIGRACIÓN Y CARGA INICIAL DE DATOS	*20/03/06*
	ACTIVIDAD CSI 9: APROBACIÓN DEL SISTEMA DE INFORMACIÓN	*10/04/06*
IMPLANTACIÓN Y ACEPTACIÓN DEL SISTEMA	*ACTIVIDAD IAS 6: PRUEBAS DE ACEPTACIÓN DEL SISTEMA*	*11/04/06*
	ACTIVIDAD IAS 9: PRESENTACIÓN Y APROBACIÓN DEL SISTEMA	*25/05/06*

Tabla 4.40 Hitos del proyecto

- ***Productos a entregar***

La tabla 4.41 representa los productos a entregar:

Producto	Fecha
Planificación del Sistema de Información	10/05/05
Estudio de viabilidad del sistema	27/05/05
Análisis del Sistema	06/09/05
Diseño del sistema	21/11/05
Base de datos y sistema	10/04/06
Aceptación del sistema	25/05/06

Tabla 4.41. Productos a entregar

4.4.1.2.4.Tarea GPI 2.4: Planificación Detallada de Actividades y Recursos Necesarios

El objetivo de esta tarea es la programación global del proyecto, planificando en el tiempo las actividades y tareas, y realizando la asignación de recursos necesaria en función de los distintos perfiles implicados. La planificación

detallada de actividades y tareas, recursos y plazos, permite concretar con exactitud el plan de costes del proyecto.

Para la programación de tiempos y esfuerzos se utilizan técnicas de planificación basadas en datos de gestión de proyectos similares realizados en la instalación o de referencias externas.

Los recursos del proyecto se especifican mediante la Estructura de Descomposición de Trabajo y la planificación de actividades y tareas del método PERT y el Diagrama de Gantt, que se complementa con la Asignación de recursos, Histograma de recursos, Patrón de límites o la Planificación de actividades y recursos.

Dado que este proyecto es desarrollado por una sola persona como trabajo de tesis, no se considera necesario una organización de los recursos ni planificación detallada.

4.4.1.2.5.Tarea GPI 2.5: Presentación y Aceptación de la Planificación General del Proyecto

- ***Planificación general del proyecto (aceptada)***

  La planificación general del proyecto es aceptada en el marco del desarrollo de trabajo de tesis de Master en Ingeniería del Software

En función del esfuerzo estimado en el punto anterior se establece la siguiente planificación considerando que se estima en 11,8 meses como la alternativa más probable de duración del proyecto, el plan de actividades se expresa en días, considerando un total del proyecto de 284 días (11,8 meses x 24 días por mes). La tabla 4.42 muestra la planificación de actividades.

Tarea	***Descripción***	***Tiempo estimado en días***
PSI	Plan De Sistemas de Información	***12***
EVS	Estudio de viabilidad del sistema	**13**
ASI	Análisis del sistema de Información	**72**
DSI	Diseño del sistema de Información	**54**
CSI	Construcción del sistema de Información	**100**
IAS	Implantación y aceptación del sistema	**33**
MSI	Mantenimiento del sistema de información	***No se aplica***
Gestión del proyecto		**Esta actividad se**

	incluye en cada una de las fases de Métrica v3
Seguridad	**Esta actividad se incluye en cada una de las fases de Métrica v3**
Gestión de Configuración	**Esta actividad se incluye en cada una de las fases de Métrica v3**
Aseguramiento de la calidad	**Esta actividad se incluye en cada una de las fases de Métrica v3**
TOTAL	**284 días**

Tabla 4.42: Actividades

ACTIVIDADES DE SEGUIMIENTO Y CONTROL

ITAUDIT es el resultado de un trabajo de tesis, que es desarrollado por una sola persona; por tal motivo no se considera necesario realizar actividades de seguimiento y control, mas que las que realiza el director de tesis.

Capítulo 4

Solución

Sección 4.5. – Interfaz de seguridad

4.5.PLANIFICACIÓN DEL SISTEMA DE INFORMACIÓN

En la actualidad, la mayoría de las organizaciones suelen disponer, en mayor o menor grado, de una política de seguridad. Esta política constituirá el punto de partida de la interfaz de seguridad, completándola o adaptándola en aquellos aspectos que así lo requieran. Si la organización no dispone de ella será necesario realizar un esfuerzo suplementario dirigido a la identificación de los objetivos de seguridad ya que su determinación no es una tarea trivial.

La planificación influirá en las decisiones adoptadas en el proceso de Planificación de Sistemas de Información al igual que otros aspectos tales como la calidad, ya que debe ser un parámetro mas a contemplar en el análisis y evaluación de soluciones.

- ***Plan de seguridad en Sistemas de Información***

  Dado que ITAUDIT no se desarrolla dentro del ámbito de ninguna organización, no se identifican objetivos de seguridad en la planificación de sistemas de información

4.5.1. ESTUDIO DE VIABILIDAD DEL SISTEMA

La primera actividad de la interfaz de seguridad que debe abordarse en el proceso de Estudio de Viabilidad del Sistema es el estudio de la seguridad requerida en este proceso, seleccionando a continuación a los miembros del equipo de seguridad para los procesos de Estudio de Viabilidad, Análisis, Diseño, Construcción e Implantación del Sistema de Información. Se trata de una tarea de vital importancia para las siguientes actividades de seguridad, tanto las relativas a la seguridad del sistema de información, como para las concernientes a la seguridad del proceso de desarrollo. Es importante que tanto el Responsable de Seguridad como el equipo de seguridad se basen en la política de seguridad de la organización y en la seguridad para el plan de acción (PSI-SEG 3.1). Si no se ha realizado el proceso Planificación del Sistema de Información y las actividades de la Interfaz de Seguridad correspondiente al mismo, se partirá de la política de seguridad de la Organización y el nivel de riesgo aceptable.

- ***Plan de seguridad requerida para el proceso Estudio de Viabilidad***

  Dado que ITAUDIT no se desarrolla dentro del ámbito de ninguna organización, no se identifican objetivos de seguridad para el proceso de estudio de viabilidad del sistema de información

4.5.2.ANÁLISIS DEL SISTEMA DE INFORMACIÓN

En las actividades de la interfaz de seguridad que se realizan durante el proceso de Análisis del Sistema de Información se hace referencia a lo que se denomina "función de seguridad" y "mecanismo de seguridad". El entendimiento de ambos conceptos es fundamental para comprender su papel dentro del trabajo de desarrollo de un sistema de información:

- *Una función de seguridad se define como "un servicio que garantiza la seguridad del sistema de información"*
- *Un mecanismo de seguridad se define como " la lógica o el algoritmo que implementa una función de seguridad, ya sea en hardware o en software"*

Las funciones y mecanismos adicionales de seguridad definidos en las actividades de interfaz se implementarán en el sistema a través de Métrica III, al igual que los demás requisitos de seguridad.

- ***Plan de seguridad requerida para el proceso de análisis del sistema de información***

Dado que ITAUDIT es un prototipo que se desarrolla como trabajo de tesis, no es necesario determinar niveles de seguridad dentro del marco de los procesos de análisis sistemas de información.

4.5.3.DISEÑO DEL SISTEMA DE INFORMACIÓN

- ***Seguridad requerida en el proceso de diseño de Sistemas de Información***

– El sistema se desarrollará en un entorno Web, por lo tanto se prevén todas las políticas de seguridad relacionadas con este entorno, firewall, seguridad del sistema operativo, etc. Se analizará la alternativa de crear un sitio seguro.
– Perfiles de usuario: El sistema prevé tres perfiles de usuario, Administrador, auditor señor, auditor junior. El perfil administrador, accede a todo el sistema incluyendo el módulo de administración que asigna roles de usuarios y permite la carga de checklist. El perfil de auditor Señor accede a todos los módulos menos el de administración. El perfil de auditor junior, accede a todos los módulos menos el de administrador, pero solo en modo consulta.
– Base de datos: El desarrollo se realizará utilizando la base de datos FireBird que posee control de transacciones, que evita la perdida de datos en caso de cortes de luz. La base de datos incorpora logs de transacciones que brindan pistas de auditoría.

– Backup: se establece una política de resguardo diario incremental y backup total en forma semanal. Se establece la realización de un backup semanal que se almacenará en un lugar distinto al que se encuentra el servidor de la aplicación.

4.5.4.CONSTRUCCIÓN DEL SISTEMA DE INFORMACIÓN

Dada la gran cantidad de productos generados en este proceso y según las características del proyecto, el entorno de construcción debe ser sometido a controles de seguridad que eviten filtraciones indeseables de datos relativos al sistema de información. Además se verifica el resultado de las pruebas de las funciones y mecanismos adicionales de seguridad.

Se completa la definición de la Formación a Usuarios Finales (CSI 7) con un plan de formación específico en seguridad dirigido a los distintos usuarios del sistema y en el que se contemplan diferentes niveles de perfil.

- ***Seguridad requerida en el proceso de construcción de Sistemas de Información***

Dado que ITAUDIT es un trabajo de desarrollo para una tesis, no requiere al momento de la construcción, estrictas medidas de seguridad, dado que es desarrollado por una sola persona, (tesista)

4.5.5.IMPLANTACIÓN Y ACEPTACIÓN DEL SISTEMA

En este proceso se define de forma detallada la seguridad para la implementación del sistema una vez construido, especificando tanto las actividades relacionadas con la seguridad intrínseca del propio sistema, como las que velan por la seguridad del proceso. El equipo de seguridad tiene como objetivo reforzar los procedimientos de seguridad y control de acceso previstos en Métrica III en el proceso de Implantación y Aceptación del Sistema (IAS 3).

Tiene especial importancia el asegurar que se cubren los requisitos de seguridad, a través de las pruebas de implantación, comprobando las funciones y mecanismos adicionales. Dichos requisitos se deberán tener en cuenta al establecer el acuerdo de nivel de servicio para el sistema antes de su puesta en producción.

- ***Seguridad requerida en el proceso de implantación de Sistemas de Información***

Dado que ITAUDIT no se implantará en un entorno en particular, esta tarea no es necesario desarrollarla.

Capítulo 4

Solución

Sección 4.6. – Interfaz de Gestión de Configuración

4.6.1.ESTUDIO DE VIABILIDAD DEL SISTEMA

4.6.1.1.ACTIVIDAD EVS-GC 1: DEFINICIÓN DE LOS REQUISITOS DE GESTIÓN DE CONFIGURACIÓN

4.6.1.1.1Tarea EVS-GC 1.1: Definición de los Requisitos de Gestión de Configuración

- ***Requisitos de gestión de configuración***

A lo largo de un proyecto de desarrollo e implementación de un proyecto software, los productos de software evolucionan y cambian. La Gestión de Configuración del Software es una disciplina encargada del control de la evolución de los productos de software.
Gestión de Configuración es el proceso de identificar y definir los elementos que se crean a lo largo del desarrollo, controlando el cambio de estos elementos a lo largo de su ciclo de vida, registrando y reportando el estado de los elementos y las solicitudes de cambio, y verificando que los elementos estén completos, que mantengan su integridad y que sean los correctos. Esto implica realizar las siguientes actividades:

- **Identificación de los elementos de configuración:** Es necesita definir un esquema que permita la identificación de los elementos desarrollados, esto implica identificar el tipo de componente y su estructura.
- **Control:** Cada elemento de configuración identificado sufre cambios, es necesario asegurar que el software sea consistente a través de la creación de una línea base del producto.
- **Estado:** Se debe registrar y reportar el estado de los componentes y solicitudes de cambio.
- **Auditoría y revisión:** Se debe validar que el producto este completo y se así mantener la consistencia entre los componentes, asegurando que estén en un estado apropiado a través de todo el ciclo de vida del producto y que el mismo sea una colección bien definida de componentes.

❖ **Elementos de configuración del Software**

Los elementos de configuración son los productos que se generan a lo largo del proceso software, que se desea gestionar, la lista de elementos de configuración es la que muestra la tabla 4.43:

Fase	**Elemento de configuración del Software**	**Tipo de elemento**
EVS	**Requisitos preliminares del sistema**	Documento
	Estimación de esfuerzo	Documento
	Plan de gestión de configuración	Documento
	Análisis de riesgo	Documento
	Planificación	Documento
ASI	**Requisitos del sistema**	Documento
	Modelo conceptual de datos	Diagrama
	Modelo de procesos	Diagrama
	Interfaz de usuario	Programa
	Plan de pruebas	Documento
DSI	**Arquitectura del sistema**	Diagrama
	Diseño físico de los datos	Documento
CSI	**Código fuente**	Programa
	Manual de usuarios	Documento
IAS	**Pruebas**	Documento

Tabla 4.43: Elementos de configuración

Estados de los elementos de configuración:

- **En edición**: El Elemento se encuentra en desarrollo.
- **Finalizado**: El Elemento se encuentra en etapa de aprobación por Director de la Tesis.
- **Aprobado**: EL Elemento se encuentra terminado y aprobado por el Director de la Tesis.

❖ **Líneas base del proyecto**

Los hitos que se definen son los que representa la figura 4.44

Línea Base	**Descripción**
Funcional	Incluye las actividades que comprenden las fases de EVS y ARS de Métrica V3

Diseño	Incluye las actividades que comprenden las fases de DSI de Métrica V3
Producto	Incluye las actividades que comprenden las fases de CSI de Métrica V3
Operativa	Incluye las actividades que comprenden las fases de IAS de Métrica V3

Tabla 4.44: líneas base

❖ **ECS por línea base**

La tabla 4.45 muestra los elementos de configuración

Fase	Línea Base	Elemento de configuración del Software	Tipo de elemento
EVS	Funcional	**Requisitos preliminares del sistema**	Documento
		Estimación de esfuerzo	Documento
		Plan de gestión de configuración	Documento
		Análisis de riesgo	Documento
		Planificación	Documento
ASI		**Requisitos del sistema**	Documento
		Modelo conceptual de datos	Diagrama
		Modelo de procesos	Diagrama
		Interfaz de usuario	Programa
		Plan de pruebas	Documento
DSI	Diseño	**Arquitectura del sistema**	Diagrama
		Diseño físico de los datos	Documento
CSI	Producto	**Código fuente**	Programa
		Manual de usuarios	Documento
IAS	Operativo	**Pruebas**	Documento

Tabla 4.45 elementos de configuración

4.6.1.2.ACTIVIDAD EVS-GC 2: ESTABLECIMIENTO DEL PLAN DE GESTIÓN DE CONFIGURACIÓN

4.6.1.2.1.Tarea EVS-GC 2.1: Definición del Plan de Gestión de la Configuración

- ***Plan de gestión de configuración para el sistema de información***

El plan que se aplica al presente desarrollo cubre todas las necesidades de configuración del sistema de información y se adecua al estándar.

4.6.1.2.2.Tarea EVS-GC 2.2: Especificación del Entorno Tecnológico para la Gestión de Configuración

- ***Plan de gestión de configuración para el sistema de información***
  - ***Entorno tecnológico***

    No se utilizará ningún entorno tecnológico en la mecanización de los procesos y controles del plan de gestión de configuración, este proceso se realiza en forma manual.

4.6.2.ANÁLISIS, DISEÑO, CONSTRUCCIÓN E IMPLANTACIÓN Y ACEPTACIÓN DEL SISTEMA DE INFORMACIÓN

4.6.2.1.ACTIVIDAD GC 1: IDENTIFICACCIÓN Y REGISTRO DE PRODUCTOS

4.6.2.1.1.Tarea GC 1.1: Identificación y Registro de los Productos de los Procesos en el Sistema de Gestión de Configuración

- ***Registro de los productos creados***

Cada elemento de configuración se identificará de la siguiente manera:

- Numero de registro
- Nombre del proyecto
- Código del elemento
- Nombre del elemento de configuración
- Fase
- Línea Base
- Tipo de elemento (documento, programa, documento)
- Numero de versión
- Estado (elaboración, terminado. Aprobado)

- Fecha
- Ordenador (Nombre del ordenador donde se almacena el registro)
- Carpeta (carpeta dentro del ordenador donde se almacena el registro)

Se registraran los elementos de configuración con el siguiente formulario que se muestra en la figura 4.26:

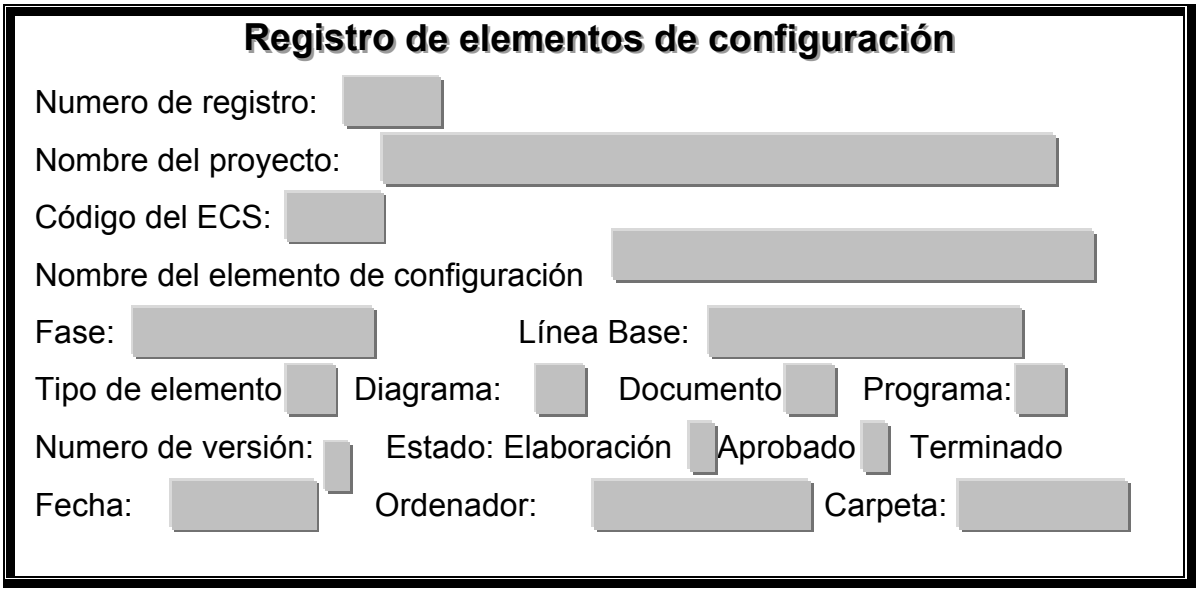


Figura 4.26. Registro de elementos de configuración

4.6.2.2.ACTIVIDAD GC 2: IDENTIFICACIÓN Y REGISTRO DEL PRODUCTO GLOBAL

4.6.2.2.1.Tarea GC 2.1: Registro en el Sistema de Gestión de la Configuración del Producto Global de Proceso

- ***Registro del producto global***

La figura 4.27 muestra el registro global del producto:

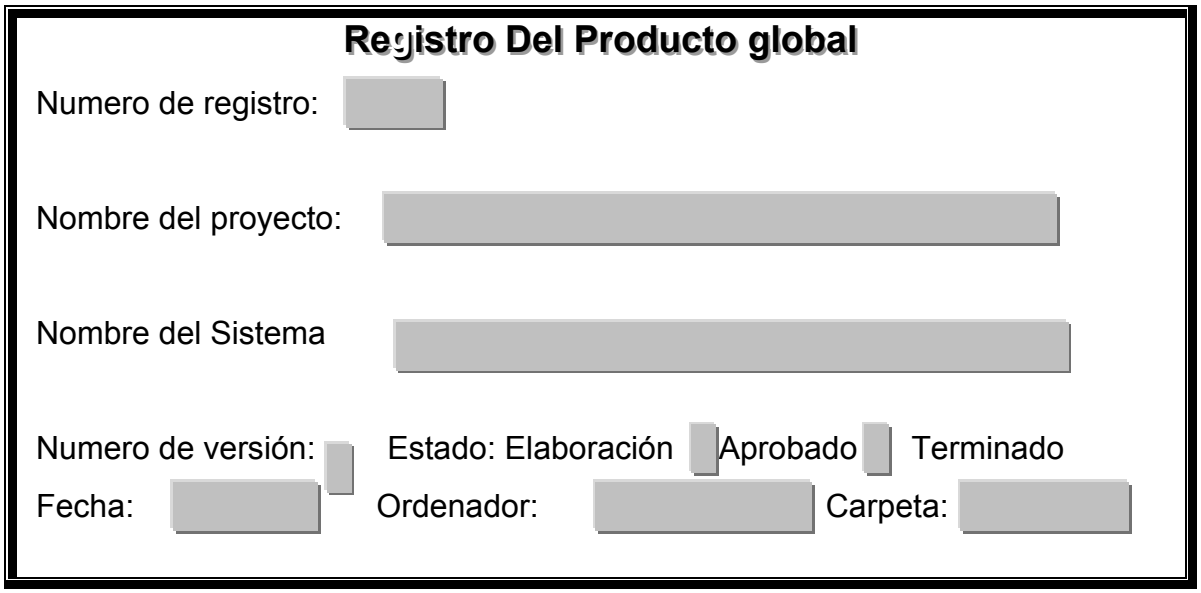


Figura 4.27 Registro del producto global

4.6.3.MANTENIMIENTO DEL SISTEMA DE INFORMACIÓN

4.6.3.1.ACTIVIDAD MSI-GC 1: REGISTRO DEL CAMBIO EN EL SISTEMA DE GESTIÓN DE LA CONFIGURACIÓN

4.6.3.1.1.Tarea MSI-GC 1.1: Registro del Cambio en el Sistema de Gestión de la Configuración

- ***Registro del cambio***

Se establece el siguiente ciclo de vida para la modificación de un elemento de configuración:

Los procesos de control que se realizarán para mantener la integridad de los productos, son los siguientes:

a) Solicitar el cambio

b) Catalogar el cambio (Elemento de configuración+numero de solicitud+urgencia)

c) Analizar el cambio

d) Evaluación del cambio (Impacto sobre otros ECS y Líneas base, Costo, tiempo estimado, esfuerzo técnico)

e) Aprobar o rechazar el cambio

f) Realización del cambio

g) Prueba del cambio

h) Instalación del cambio

i) Aprobación del cambio

Para gestionar los cambios de los elementos de configuración se utilizará el siguiente formulario (Figura 4.28) , se debe considerar que este formulario se utilizará cuando el proyecto se encuentra en una línea base distinta a la del elemento a modificar:

Formulario de solicitud de cambio

Nombre del Proyecto Número de Solicitud:

Fecha: Código de la solicitud:

Solicitante:

Cambio solicitado:

Evaluación del cambio: Impacto

Costo del cambio: Tiempo estimado:

Aprobado/Rechazado: Fecha:

Fecha inicio del cambio: Responsable del cambio:

Fecha inicio de la prueba: Responsable prueba:

Fecha Instalación cambio: Responsable instalación:

Fecha de aprobación: Firma:

Figura 4.28. formulario de solicitud de cambios

4.6.3.1.2.Tarea MSI-GC 1.2: Registro de la Nueva Versión de los Productos Afectados por el Cambio en el Sistema de Gestión de la Configuración

- ***Registro de la nueva versión de los productos afectados por el cambio***

La figura 4.29 muestra el registro de nuevas versiones de elementos de configuración:

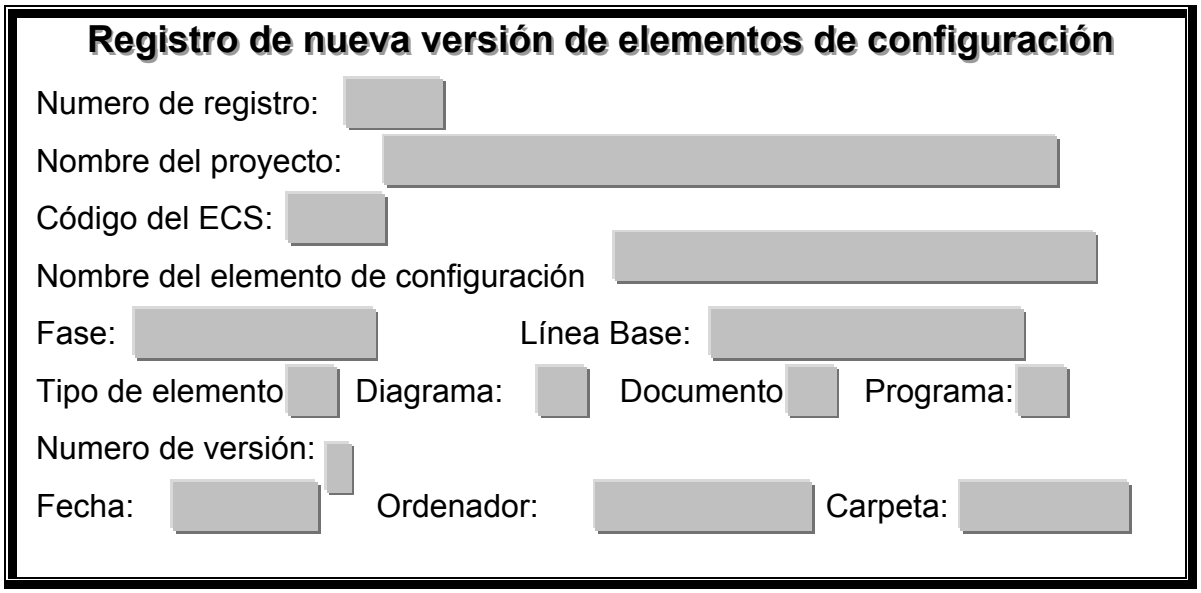


Figura 4.29. Registro de nuevas versiones de elementos de configuración

4.6.3.1.3.Tarea MSI-GC 1.3: Registro de la Nueva Versión de los Sistemas de Información en el Sistema de Gestión de la Configuración

- ***Registro de la nueva versión de los sistemas de información***

La figura 4.30 muestra el registro de nuevas versiones del sistema de información:

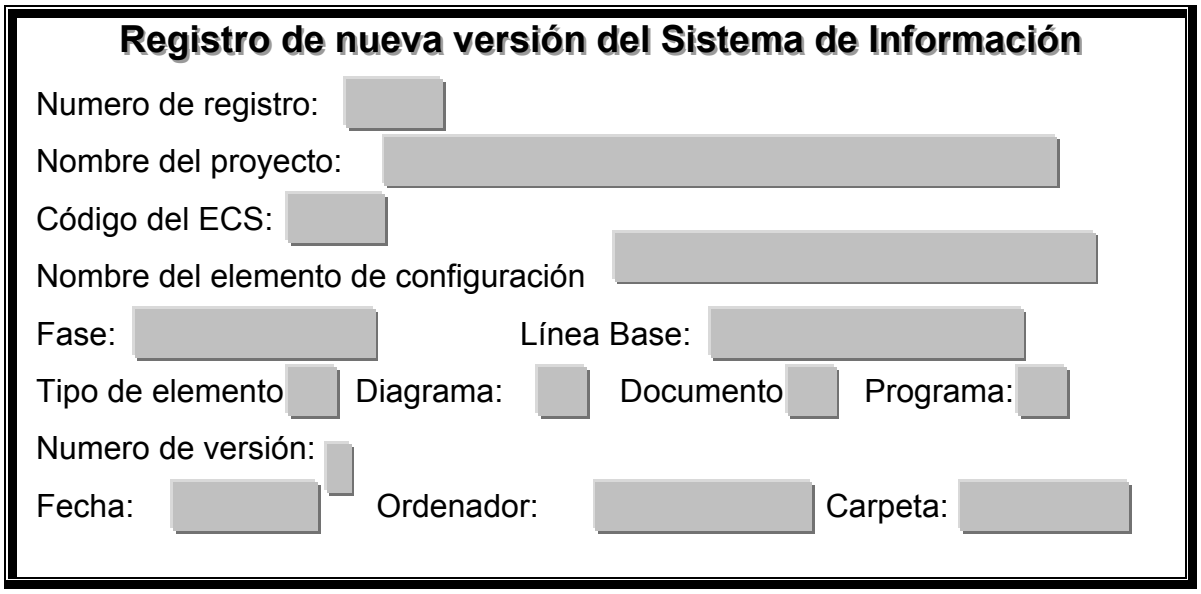


Figura 4.30. Registro de nuevas versiones del sistema de información

Capítulo 4

Solución

Sección 4.7. – Interfaz de aseguramiento de calidad

4.7.ASEGURAMIENTO DE LA CALIDAD

4.7.1.ESTUDIO DE VIABILIDAD DEL SISTEMA

En este proceso el grupo de aseguramiento de calidad inicia el estudio de los sistemas de información definidos en cada alternativa de solución propuesta, con el fin de identificar las condiciones en que se va a desarrollar y/o implantar, así como las características que deben reunir en cuanto a operación, mantenibilidad y portabilidad, para satisfacer las necesidades del cliente y los requisitos específicos.

La necesidad de establecer un plan específico de aseguramiento de calidad y el grado de intensidad con el que se aplican las actuaciones de calidad, vendrá determinada en función de este estudio y de los riesgos analizados por el equipo de desarrollo.

Una vez tomada la decisión de llevar a cabo un plan de aseguramiento de calidad en las alternativas propuestas, se define el contenido de dicho plan, de acuerdo a los estándares de calidad, si existen en la organización, sino se recomienda acudir a los estándares UNE-EN-ISO 9001:2000 Sistemas de Gestión de la Calidad – Requisitos y UNE-EN-ISO 9001:2000 Sistemas de Gestión de Calidad – Fundamentos y vocabulario. El plan de aseguramiento de calidad debe cubrir todas las necesidades establecidas de modo que, aquellas normas impuestas por los usuarios o clientes que difieran de las existentes en el sistema de calidad, deben quedar también reflejadas en el plan.

No se realizan actividades vinculadas al aseguramiento de la calidad en el proceso de estudio de viabilidad del sistema de información

4.7.2.ANÁLISIS DEL SISTEMA DE INFORMACIÓN

4.7.2.1.ACTIVIDAD ASI-CAL 1: ESPECIFICACIÓN INICIAL DEL PLAN DE ASEGURAMIENTO DE CALIDAD

4.7.2.1.1.Tarea ASI-CAL 1.1: Definición del Plan de Aseguramiento de Calidad para el Sistema de Información

- ***Plan de aseguramiento de la calidad, aspectos generales***

La calidad incluye todos aquellos aspectos o características de un producto o actividad que son de una importancia sustancial en relación a la satisfacción de los requisitos establecidos.

Se debe diferenciar la calidad del proceso y la calidad del producto entendiendo que es fundamental para garantizar un producto de calidad es tener un proceso de calidad.

❖ **Propiedades de calidad del producto.**

- Corrección: El sistema debe cumplir con sus especificaciones y satisfacer los objetivos de los usuarios.
- Fiabilidad: El sistema debe funcionar sin errores.
- Facilidad de uso: El sistema debe ser fácil de aprender y su operación no debe tener inconvenientes, incluso para personas no expertas en la auditoría de sistemas.
- Integridad: Se debe controlar el acceso ilegal al sistema y la base de datos.
- Flexibilidad: El sistema debe ser fácil de modificar, considerando que los productos del sistema deben poder mejorarse en función de las experiencias realizadas en cada proyecto.

4.7.2.2.ACTIVIDAD ASI-CAL 2: ESPECIFICACIÓN DETALLADA DEL PLAN DE ASEGURAMIENTO DE CALIDAD

4.7.2.2.1.Tarea ASI-CAL 2.1: Contenido del Plan de Aseguramiento de Calidad para el Sistema de Información

- ***Plan de aseguramiento de la calidad***

La figura 4.31 muestra las actividades de control de calidad

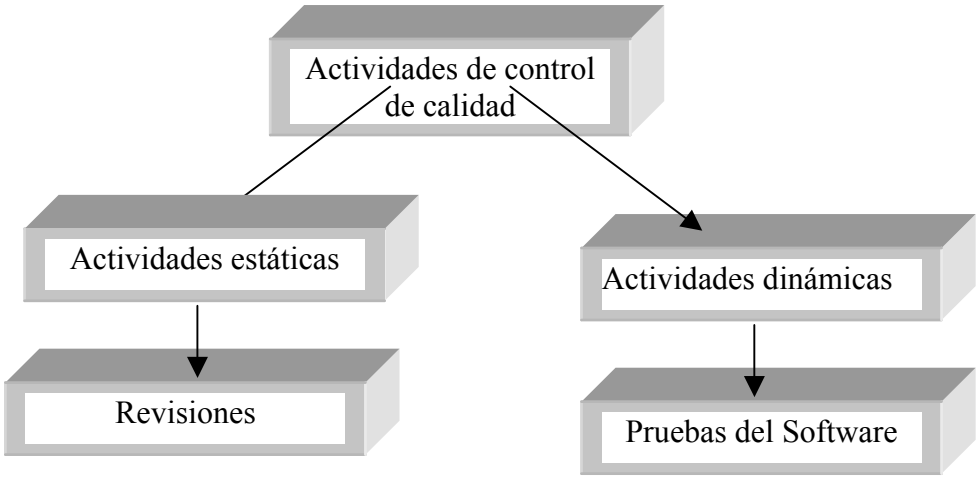


Figura 4.31 Actividades de control de calidad

❖ **Revisiones.**

Se trata de una reunión formal donde se presenta, el estado actual del proyecto al director de la tesis con el objetivo de detectar el correcto desarrollo de cada fase de la metodología, se realizaran las siguientes revisiones representadas en la tabla 4.46:

	REVISIONES
ASI	Análisis del sistema de Información
DSI	Diseño del sistema de Información
CSI	Construcción del sistema de Información
IAS	Implantación y aceptación del sistema

Tabla 4.46 detalle revisiones

La tabla 4.47 muestra los objetivos de control de cada revisión:

Revisión	Objetivos de control
Análisis del sistema de Información	• Los Requisitos del sistema • El Modelo conceptual de datos Modelo de procesos • La interfaz de usuario • El plan de pruebas
Diseño del sistema de información	• La arquitectura que se definió para el sistema • El diseño físico de los datos
Construcción del sistema de información	• El código fuente • Los manuales
Implementación y aceptación del sistema	• Pruebas

Tabla 4.47 Objetivos de control de las revisiones

4.7.2.3.ACTIVIDAD ASI-CAL 3: REVISIÓN DEL ANÁLISIS DE CONSISTENCIA

4.7.2.3.1.Tarea ASI-CAL 3.1: Revisión del Análisis de Consistencia

- ***Revisión de requisitos***

Los requisitos fueron revisados por el tesista y los directores de la tesis, arribándose a la conclusión que los mismos son precisos, completos y consistentes.

4.7.2.3.2.Tarea ASI-CAL 3.2: Revisión de la Consistencia entre Productos

- ***Revisión de la consistencia entre productos***

Se realiza una reunión de revisión entre el tesista y los directores de la tesis y se comprueba la consistencia entre productos.

4.7.2.4.ACTIVIDAD ASI-CAL 4: REVISIÓN DEL PLAN DE PRUEBAS

4.7.2.4.1.Tarea ASI-CAL 4.1: Revisión del Plan de Pruebas

- ***Revisión del plan de pruebas.***

El plan de pruebas fue revisado y aprobado.

4.7.2.5.ACTIVIDAD ASI-CAL 5: REGISTRO DE LA APROBACIÓN DEL ANÁLISIS DE SISTEMA

4.7.2.5.1.Tarea ASI-CAL 5.1: Registro de la Aprobación del Análisis de Sistema

- ***Registro de la aprobación del análisis del sistema de información.***

Se realiza una reunión entre los directores de la tesis y el tesista y se registra la aprobación del Análisis del Sistema de Información.

4.7.3.DISEÑO DEL SISTEMA DE INFORMACIÓN

4.7.3.1.ACTIVIDAD DSI-CAL 1: REVISIÓN DE LA VERIFICACIÓN DE LA ARQUITECTURA DEL SISTEMA

4.7.3.1.1.Tarea DSI-CAL 1.1: Revisión de la Consistencia entre Productos del Diseño

- ***Revisión de la arquitectura del sistema***

Se realiza una reunión formal entre el tesista y los directores y se comprueba que la arquitectura del sistema responde a los requisitos especificados en el diseño.

4.7.3.1.2.Tarea DSI-CAL 1.2: Registro de la aceptación de la Arquitectura del Sistema

- **Registro de la aceptación de la arquitectura del sistema**

Se registra formalmente la aceptación de la arquitectura del sistema.

4.7.3.2.ACTIVIDAD DSI-CAL 2: REVISIÓN DE LA ESPECIFICACIÓN TÉCNICA DEL PLAN DE PRUEBAS

4.7.3.2.1.Tarea dsi-CAL 2.1: Revisión del Diseño de las Pruebas Unitarias, de Integración y del sistema

- ***Revisión del diseño de pruebas***

Se denomina prueba al proceso de ejecutar el sistema con el objetivo de detectar errores, existen los siguientes tipos de prueba:

- *Prueba Modular:* Consiste en probar cada módulo en forma independiente
- *Prueba de Integración:* A medida que los diferentes módulos se integran en el sistema se realiza este tipo de prueba, el objetivo es comprobar que las interfaces entre los distintos módulos son correctas, esta integración se realizará utilizando la estrategia *big-bang*, o sea integrar y probar todo al mismo tiempo.
- *Prueba del sistema*: Esta prueba se realiza cuando se han integrado todos los módulos y se trata de comprobar que se han cumplido todos los requisitos.
- *Prueba de aceptación:* Una vez finalizado el sistema se espera que el director de la tesis apruebe el desarrollo.

En relación a la metodología a utilizar para las pruebas será la siguiente:

- *Métodos de caja negra:* Donde el sistema se ve como una caja negra y no se considera su estructura interna, se realizarán análisis de valores de frontera. Y adivinación de errores.

Para la realización de las pruebas se utilizará el siguiente formulario que se muestra en la figura 4.32

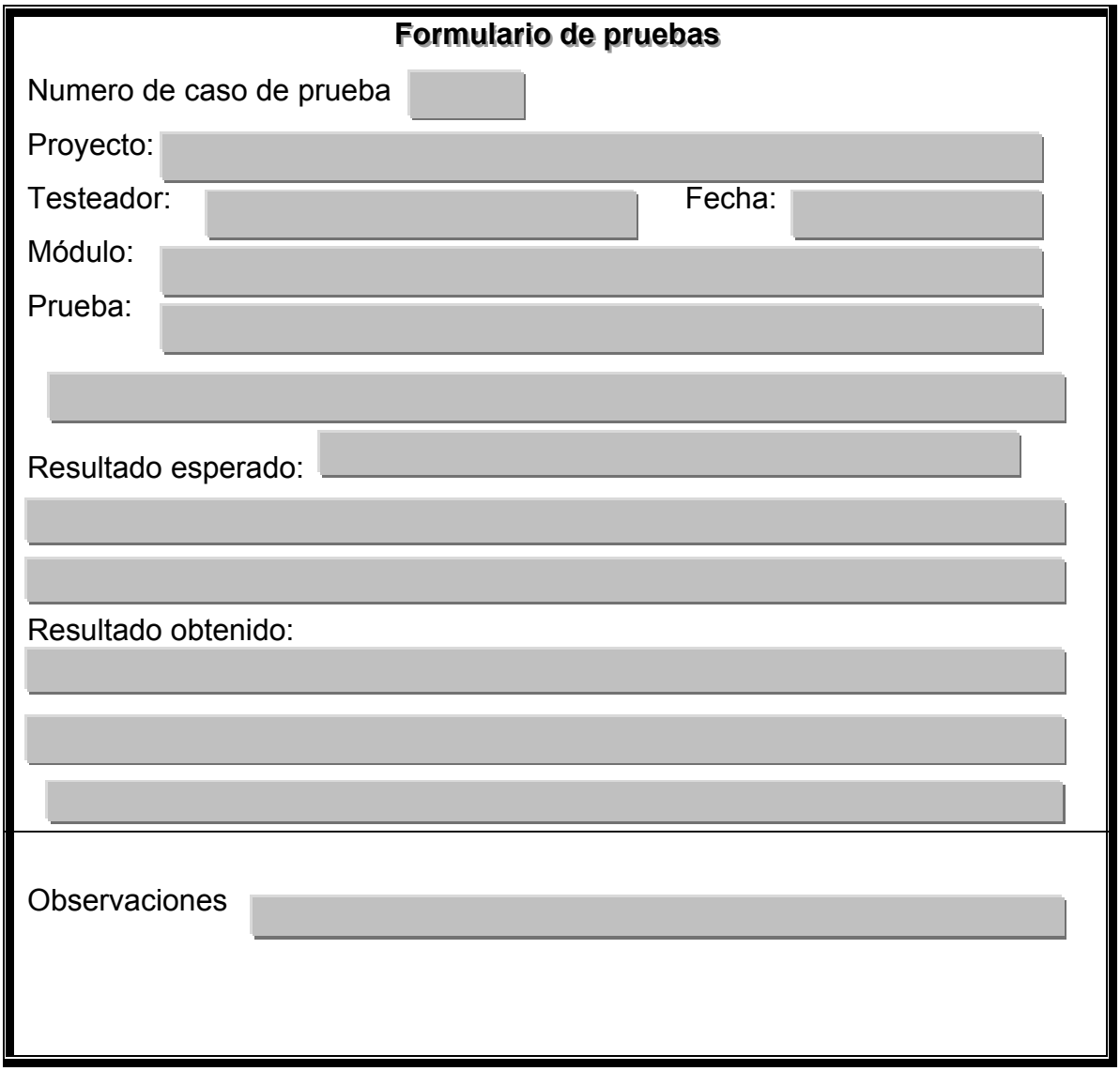


Figura 4.32. Formulario de pruebas

4.7.3.2.2.Tarea dsi-CAL 2.2: Revisión del Plan de Pruebas

- ***Revisión del plan de pruebas***

Se revisa y aprueba el plan de pruebas

4.7.3.3.ACTIVIDAD DSI-CAL 3: REVISIÓN DE LOS REQUISITOS DE IMPLANTACIÓN

4.7.3.3.1.Tarea DSI-CAL 3.1: Revisión de los Requisitos de Documentación de Usuario

Se comprueba que se han identificado los requisitos necesarios relativos a la documentación que se va a entregar a los usuarios y a operación.

- ***Revisión de los requisitos de documentación del Usuario***

Esta tarea no se realiza al no estar prevista en esta tesis la entrega de documentación al usuario final.

4.7.3.3.2.Tarea DSICAL 3.2: Revisión de los Requisitos de Implantación

Se comprueba que se han identificado y detallado los requisitos necesarios para la implantación del sistema relacionados con la instalación, formación e infraestructura.

- ***Revisión de los requisitos de implantación***

Esta tarea no se realiza al no preverse en esta tesis la implantación del sistema.

4.7.3.4.ACTIVIDAD DSI-CAL 4: REGISTRO DE LA APROBACIÓN DEL DISEÑO DEL SISTEMA DE INFORMACIÓN

4.7.3.4.1.Tarea DSI-CAL 4.1: Registro de la Aprobación del Diseño del Sistema de Información

- *Registro de la Aprobación del Diseño del Sistema de Información*

Se realiza una reunión formal entre los directores y el tesista y se aprueba formalmente el Diseño del Sistema de Información

4.7.4.CONSTRUCCIÓN DEL SISTEMA DE INFORMACIÓN

4.7.4.1.ACTIVIDAD CSI-CAL 1: REVISIÓN DEL CÓDIGO DE COMPONENTES Y PROCEDIMIENTOS

4.7.4.1.1.Tarea CSI-CAL 1.1: Revisión de Normas de Construcción

- ***Revisión del catálogo de componentes y procedimientos***

Se revisa y aprueba el catálogo de componentes y procedimientos

4.7.4.2.ACTIVIDAD CSI-CAL 2: REVISIÓN DE LAS PRUEBAS UNITARIAS, DE INTEGRACIÓN Y DEL SISTEMA

4.7.4.2.1.Tarea CSI-CAL 2.1: Revisión de la Realización de las Pruebas Unitarias

- ***Revisión de la realización de pruebas unitarias***

Se revisan y aprueban formalmente la realización de las pruebas unitarias.

4.7.4.2.2.Tarea CSI-CAL 2.2: Revisión de la Realización de las Pruebas de Integración

- ***Revisión de la Realización de las Pruebas de Integración***

Se revisan y aprueban formalmente la realización de las pruebas de integración.

4.7.4.2.3.Tarea CSI-CAL 2.3: Revisión de la Realización de las Pruebas del Sistema

- ***Revisión de la Realización de las Pruebas del Sistema***

Se revisan y aprueban formalmente la realización de las pruebas del sistema.

4.7.4.3.ACTIVIDAD CSI-CAL 3: REVISIÓN DE LOS MANUALES DE USUARIO

4.7.4.3.1.Tarea CSI-CAL 3.1: Revisión de los Manuales de Usuario

Se comprueba que los manuales de operaciones y de usuario se han descrito en forma clara y concisa y se ajustan a los criterios y normativas establecidos.

- ***Revisión de los Manuales de Usuario***

Esta tarea no se realiza al no preverse la elaboración de manuales de usuario

4.7.4.4.ACTIVIDAD CSI-CAL 4: REVISIÓN DE LA FORMACIÓN A USUARIOS FINALES

4.7.4.4.1.Tarea CSI-CAL 4.1: Revisión de la Formación a Usuarios Finales

Se revisa que se han definido los esquemas de formación a los usuarios finales del sistema de información y que se han identificado los distintos perfiles de usuario en función de sus capacidades, habilidades, experiencia y responsabilidades, así como los recursos necesarios para llevarlo a cabo.

- ***Revisión de la Formación a Usuarios Finales***

Esta tarea no se realiza al no preverse la formación de usuarios finales

4.7.4.5.ACTIVIDAD CSI-CAL 5: REGISTRO DE LA APROBACIÓN DEL SISTEMA DE INFORMACIÓN

4.7.4.5.1.Tarea CSI-CAL 5.1: Registro de la Aprobación del Sistema de Información

- ***Registro de la Aprobación del Sistema de Información***

Se realiza una reunión formal entre los directores y el tesista y se aprueba el Sistema de información construido.

4.7.5.IMPLANTACIÓN Y ACEPTACIÓN DEL SISTEMA

El grupo de aseguramiento de calidad en este proceso es responsable de revisar la existencia de un plan de implantación que se habrá elaborado conforme a la estrategia de implantación que se habrá elaborado conforme a la estrategia de implantación determinada en el Proceso de Estudio de Viabilidad de Sistema (EVS) y teniendo en cuenta los requisitos de implantación establecidos en el Proceso de Diseño del Sistema de Información (DSI)

También deben comprobar que se han realizado las pruebas de implantación y de aceptación según el plan de pruebas establecido en Métrica III y la normativa acordada en el plan de aseguramiento de calidad. Revisan la totalidad de las verificaciones y casos de prueba de implementación y aceptación que se hayan especificado para el sistema y las incidencias producidas, con el fin de determinar si puede verse afectada alguna propiedad de calidad. En cualquier caso, se registra la aprobación de las pruebas de implantación y aceptación por parte de operaciones y del usuario respectivamente.

En cuanto al mantenimiento, el grupo de aseguramiento de calidad debe asegurarse que se le entrega el producto software al responsable de mantenimiento, con las propiedades adecuadas par que pueda asumir el servicio de mantenimiento, una vez que el sistema se encuentre en producción.

4.7.5.1.ACTIVIDAD IAS-CAL 1: REVISIÓN DEL PLAN DE IMPLANTACIÓN DEL SISTEMA

4.7.5.1.1.Tarea IAS-CAL 1.1: Revisión del Plan de Implantación del Sistema

Se revisa que se ha elaborado un plan de implantación de acuerdo a la estrategia de implantación establecida en el Proceso de Estudio de la

Viabilidad del Sistema (EVS) y conforme a los requisitos de implantación establecidos.

Asimismo, se comprueba que se ha establecido un plan de trabajo para la implantación que permita determinar las actividades a realizar por el grupo de aseguramiento de calidad durante el proceso de implantación.

- ***Revisión del Plan de Implantación del Sistema***

Queda fuera del alcance del proyecto la implantación del sistema, por lo tanto esta tarea no se realiza.

4.7.5.2.ACTIVIDAD IAS-CAL 2: REVISIÓN DE LAS PRUEBAS DE IMPLANTACIÓN DEL SISTEMA

4.7.5.2.1.Tarea CSI-CAL 2.1: Revisión de la Realización de las Pruebas de Implantación del Sistema

Se comprueba la realización de las pruebas de implantación. Se lleva a cabo la revisión de las verificaciones y casos de prueba que se hayan determinado para cada sistema de información implicado en la implantación del sistema, tal como se especificó en los criterios de revisión de los respectivos planes de aseguramiento de calidad.

Para todo esto, se tendrá en cuenta la normativa establecida para la documentación de los resultado de dichas pruebas.

En caso de existir casos de prueba adicionales, incorporado como consecuencia de las medidas correctores tomadas para solventar los errores detectados, el grupo de aseguramiento de calidad revisará que se han resuelto de forma correcta.

Igualmente se revisaran las inconsistencias no resueltas con el fin de valorar hasta que punto se ven comprometidas las propiedades de calidad establecida inicialmente.

- ***Revisión de la Realización de las Pruebas de Implantación del Sistema***

Queda fuera del alcance del proyecto la implantación del sistema, por lo tanto esta tarea no se realiza.

4.7.5.2.2..Tarea CSI-CAL 2.2: Registro de la Aprobación de las Pruebas de Implantación del Sistema

Se registra la aprobación o rechazo de las pruebas de implantación por parte del responsable de operación.

- ***Registro de la Aprobación de las Pruebas de Implantación del Sistema***

Queda fuera del alcance del proyecto la implantación del sistema, por lo tanto esta tarea no se realiza.

4.7.5.3.Actividad IAS-CAL 3: Revisión de las Pruebas de Aceptación del Sistema

4.7.5.3.1.Tarea IAS-CAL 3.1: Revisión de la Realización de las Pruebas de Aceptación del Sistema

- ***Revisión de la Realización de las Pruebas de Aceptación del Sistema***

Se realiza una revisión formal de las pruebas de aceptación del sistema

4.7.5.3.2.Tarea IAS-CAL 3.2: Registro de la Aprobación de las Pruebas de aceptación del sistema

- ***Registro de la Aprobación de las Pruebas de Implantación del Sistema***

Se realiza una reunión entre el tesista y los directores y se acepta formalmente el sistema

4.7.5.4.ACTIVIDAD IAS-CAL 4: REVISIÓN DEL PLAN DE MANTENIMIENTO DEL SISTEMA

4.7.5.4.1.Tarea IAS-CAL 4.1: Revisión del Plan de Mantenimiento del Sistema

Se comprueba que los productos entregados al responsable de mantenimiento son los acordados y este asume el mantenimiento del sistema de información.

Asimismo, se comprueba que se ha formalizado un plan de mantenimiento del sistema de información, entre el cliente/usuario y responsable de mantenimiento.

Si se considera conveniente, se estudiará la necesidad de llevar a cabo un seguimiento y control de calidad del sistema de información, una vez que se encuentren en el entorno de producción.

- ***Revisión del Plan de Mantenimiento del Sistema***

Esta fuera del alcance de esta tesis el mantenimiento del sistema, por lo tanto esta tarea no se realiza.

4.7.5.5.ACTIVIDAD IAS-CAL 5: REGISTRO DE LA APROBACIÓN DE LA IMPLANTACIÓN DEL SISTEMA

4.7.5.5.1.Tarea CSI-CAL 5.1: Registro de la aprobación de la Implantación del sistema

Se registra la aprobación de la implantación del sistema y se comprueba que el dossier de aseguramiento de calidad forme parte del producto software.

- ***Registro de la aprobación de la Implantación del sistema***

Esta fuera del alcance de esta tesis la implantación del sistema, por lo tanto esta tarea no se realiza.

4.7.6.MANTENIMIENTO DEL SISTEMA DE INFORMACIÓN

El proceso de implantación y aceptación del sistema se habrá determinado la necesidad de llevar a cabo un seguimiento y control de la calidad en los sistemas de información, una vez se encuentren en el entorno de producción.

El grupo de aseguramiento de calidad intervendrá durante el mantenimiento, efectuando revisiones de seguimiento periódicas, mas o menos frecuentes según los casos, que sirven para constatar que el mantenimiento establecido para el sistema de información se realiza de forma correcta.

En algún caso, según las implicaciones del caso, puede ser necesario revisar puntualmente:

- *El contenido del plan de pruebas de regresión*
- *La ejecución de las pruebas de regresión según la normativa acordada en el plan de aseguramiento de calidad*
- *Las verificaciones y casos de prueba que se hayan incluido en el plan de pruebas para los cambios producidos por una petición*
- *Las incidencias detectadas con el fin de determinar si puede verse afectada alguna propiedad de calidad*

En caso de revisar la ejecución de las pruebas de regresión, se registrará la aprobación de las pruebas por el responsable de mantenimiento.

4.7.6.1.ACTIVIDAD MSI-CAL 1: REVISIÓN DEL MANTENIMIENTO DEL SISTEMA DE INFORMACIÓN

4.7.6.1.1.Tarea MSI-CAL 1.1: Revisión del Mantenimiento

Se verifican las peticiones incluidas en el catalogo de peticiones se corresponda con la previstas en la revisión del plan de mantenimiento del dossier de aseguramiento de la calidad que se obtiene en la tarea IAS-CAL 4.1.

Se realiza una revisión periódica del catálogo de requisitos comprobando que se mantiene actualizado. Asimismo, se revisa que el usuario acepta o rechaza la solución propuesta para dar respuesta a su petición y que aprueba formalmente el cierre de la petición.

Esta tarea de la interfaz de aseguramiento de calidad se aplica a todas las actividades del proceso de mantenimiento de sistemas de información.

- ***Revisión del Mantenimiento***

ITAUDIT es un prototipo desarrollado como trabajo de tesis, por lo cual el plan de mantenimiento queda fuera del alcance del presente trabajo.

4.7.6.2.ACTIVIDAD MSI-CAL 2: REVISIÓN DEL PLAN DE PRUEBAS DE REGRESIÓN

4.7.6.2.1.Tarea MSI-CAL 2.1: Comprobación de la Existencia del Plan de Pruebas de Regresión

Se revisa que se ha establecido un plan de pruebas de regresión de acuerdo a los criterios en el plan de aseguramiento de calidad para la elaboración del plan de pruebas desde el punto de vista de aseguramiento de la calidad, con el objetivo de determinar que métodos se van a aplicar para la ejecución de las pruebas, cuales van a ser los criterios de aceptación, como se van a realizar las actividades de verificación y como se van a emitir los resultados.

Se revisa la existencia de una normativa para la gestión de los resultados de las pruebas.

- ***Comprobación de la Existencia del Plan de Pruebas de Regresión***

ITAUDIT es un prototipo desarrollado como trabajo de tesis y no se implementará en una empresa en particular, por lo cual las pruebas de regresión quedan fuera del alcance del presente trabajo.

4.7.6.3.ACTIVIDAD MSI-CAL 3: REVISIÓN DE LA REALIZACIÓN DE LAS PRUEBAS DE REGRESIÓN

4.7.6.3.1.Tarea MSI-CAL 3.1: Revisión de la realización de la Pruebas de Regresión

Se comprueba la realización de las pruebas de regresión y se lleva a cabo la revisión de las verificaciones y casos de prueba que se hayan determinado para la correcta implantación del sistema.

Para todo esto, se tendrá en cuenta la normativa establecida para la documentación de los resultado de dichas pruebas.

En caso de existir casos de prueba adicionales, incorporado como consecuencia de las medidas correctores tomadas para solventar los errores detectados, el grupo de aseguramiento de calidad revisará que se han resuelto de forma correcta.

Igualmente se revisaran las inconsistencias no resueltas con el fin de valorar hasta que punto se ven comprometidas las propiedades de calidad establecida inicialmente.

Se registra la aprobación por parte del responsable de mantenimiento.

- ***Comprobación de la Existencia del Plan de Pruebas de Regresión***

ITAUDIT es un prototipo desarrollado como trabajo de tesis y no se implementará en una empresa en particular, por lo cual las pruebas de regresión quedan fuera del alcance del presente trabajo.

Capítulo 5

Experimentación

5.1 Objetivos

El objetivo de este capítulo es realizar una prueba del prototipo desarrollado en un ambiente real, con el propósito de demostrar que el mismo es un asistente eficiente para el auditor de sistemas para el desarrollo de su tarea.

5.2. Características de la experimentación realizada.

Se realizó la experimentación en INYM (Instituto Nacional de la Yerba Mate) este es un organismo que tiene como función el control de todo lo relacionado con la producción de yerba mate en todo el ámbito Nacional, cuenta con un directorio con representantes de los productores, los gobiernos provinciales y el gobierno Nacional.

Se realizó una reunión con el directorio donde se establecieron los objetivos y limites de la auditoría, se definió que la misma se desarrollaría solo sobre el área de “Organización gestión y base jurídica” de todo lo relacionado con la Tecnología de la Información.

Se decidió realizar la auditoría por Areas y no por COBIT, y dado que se trata de un prototipo se decidió la carga de un set reducido de preguntas en la herramienta, de modo de poder comprobar el funcionamiento del mismo.

El servidor con la aplicación se encontraba en la Universidad Nacional de Misiones y se accedió al prototipo desde un ordenador del INYM destinado a tal fin, se utilizó el navegador Mozilla.

En el sistema se encuentran cargadas las preguntas del relevamiento inicial y el check-list a utilizar en el desarrollo de la auditoría, tarea realizada previamente a la experimentación.

El sistema prevé tres perfiles:

- ✓ Administrador: Responsable de la configuración del sistema, este perfil no interviene en esta experimentación al haberse realizado previamente esta carga.
- ✓ Supervisor: responsable de iniciar un proyecto, planificar, determinar recursos y realizar el informe final. El supervisor es el responsable de cada proyecto de auditoría y debe cumplir los roles relacionados con esta tarea. En esta experimentación solo intervendrá una persona que asumirá dos perfiles, el de supervisor y el de auditor.

- ✓ Auditor: Es el responsable de realizar la auditoría, tanto el relevamiento inicial como el profundo, en este caso ese perfil es asumido por la misma persona que cumple el rol de supervisor.

5.3. Realización de la experimentación

El acceso al sistema se realiza desde un navegador web, la URL es: http://itaudit.com.ar/itauditor , se configuró el navegador Mozilla estableciendo como pagina de inicio la dirección antes mencionada en una computadora ubicada dentro del área administrativa del INYM, donde se realizará la auditoría.

5.3.1. Módulo de inicio

Ingreso al Sistema: El primer paso es iniciar un nuevo proyecto, para realizar esta acción se debe acceder al sistema con perfil de "supervisor", dado que es el mencionado perfil quien realiza esta tarea.

El "User ID" es "SUPERVISOR" y la "Password" es "SUPER" que deben ser ingresados en la pantalla de acceso que se ve en la figura 5.1, se debe elegir el botón "Ingresar" que se encuentra debajo de la password.

Figura 5.1. Ingreso al sistema

Una vez que se ingresa al sistema, se abre una pantalla, como la que aparece en la figura 5.2. En esta se pueden observar la lista de proyectos que fueron finalizados o que están en proceso de auditoria. En la parte izquierda de la pantalla está el menú de opciones disponibles para el perfil de supervisor.

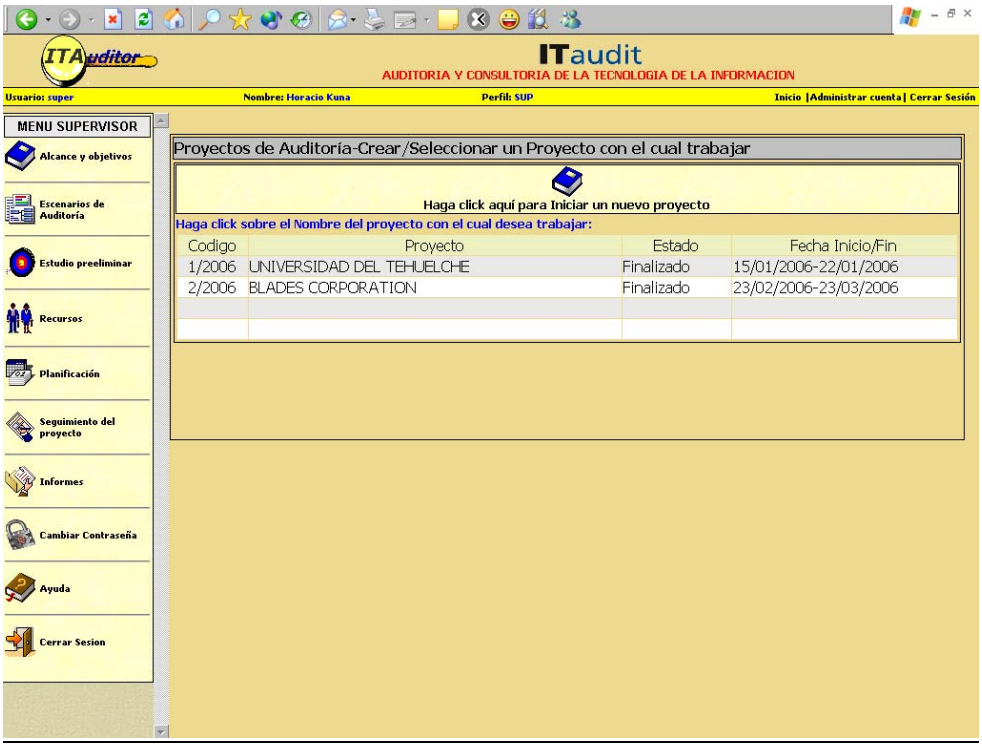


Figura 5.2. Proyectos existentes

Para ingresar un nuevo proyecto se debe seleccionar del menú supervisor, el botón “Alcance y objetivos”. Con esta acción se abre una pantalla como la que aparece en la figura 5.3. la misma tiene cinco solapas en la parte superior.

El inicio de un proyecto implica el ingreso de distinta información que se realiza dentro de la opción de menú “Alcance y Objetivos” en las distintas solapas, la primera de la izquierda dice “Datos del proyecto”, que es lo primero que se debe cargar en el sistema, los datos a ingresar son:

- Estado del proyecto: de un combo desplegable puede seleccionar entre Activar proyecto, Finalizado y Suspendido. Para el inicio del proyecto se debe elegir la primer opción.
- Nombre del proyecto: que identifique la organización sobre la cual se aplica el proyecto. Se debe ingresar “AUDITORIA DEL INYM”.
- Auditar por: donde se debe indicar entre las opciones Cobit o Áreas, según corresponda. Se debe elegir la opción “Área”.
- Fecha de inicio y Fecha de finalización del proyecto. La fecha de inicio será el 29/05/06 y la de finalización será 13/06/05.
- Objetivos: se debe ingresar el objetivo de la auditoria.
- Alcance: se debe ingresar el alcance de la misma.

Una vez ingresados estos datos, se deben guardar. Los proyectos pueden guardarse, cancelar el ingreso de algún proyecto o pueden darse de baja. En la parte inferior se encuentran los botones “Guardar”, “Dar de Baja Proyecto” y “Cancelar”. Después de ingresar los datos se debe elegir la opción “Guardar”

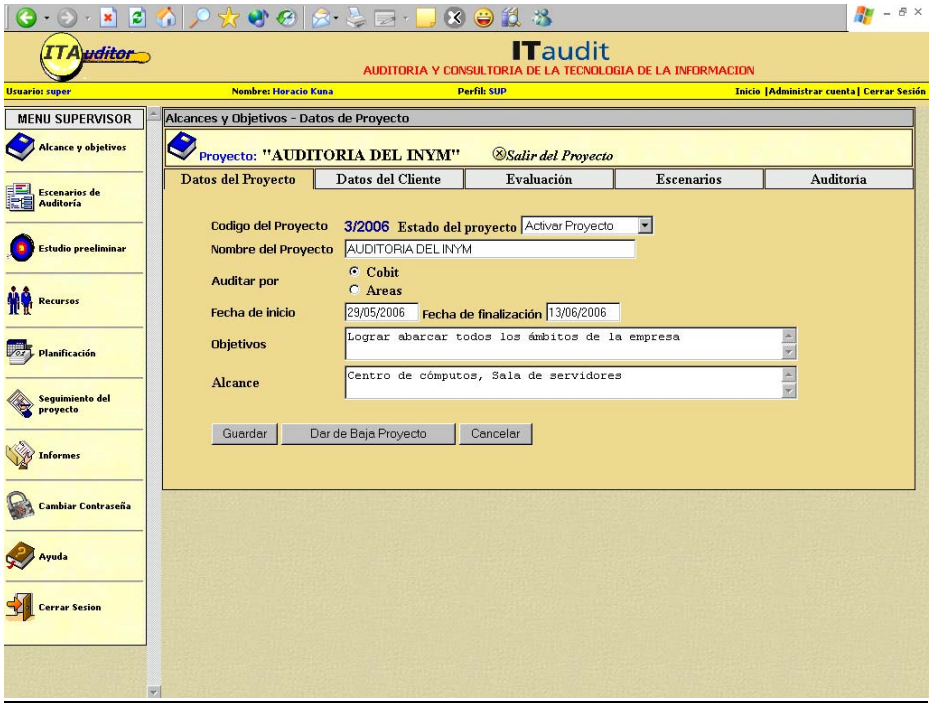


Figura 5.3. Inicio de un proyecto

El segundo paso es la carga de los datos del contacto principal en el INYM, esto se realiza ingresando en la segunda solapa desde la izquierda “Datos del cliente”, en la figura 5.4 se visualizan los datos que deben ingresarse:

- Nombre: Identifica el nombre del contacto principal de la empresa u organismo donde se realizará la auditoría, se debe ingresar “Pedro Enrique”.
- Apellido: Identifica el apellido del contacto principal donde se realizará la auditoría, se debe ingresar “Estigarribia Barrientos”.
- País: de un combo desplegable se debe elegir el país donde se ubica la empresa u organismo, se debe elegir “Argentina”.
- Provincia: Identifica la provincia donde se ubica la empresa u organismo que será auditado, se debe ingresar “Misiones”.
- Localidad: Identifica la ciudad donde se ubica la empresa u organismo que será auditado, se debe ingresar “Posadas”.

- Dirección: Identifica la dirección donde se ubica la empresa u organismo que será auditado, se debe ingresar “De los Elliotis 1987”
- Cargo: Identifica el cargo del contacto de la empresa donde se realizará la auditoría, se debe ingresar “ Gerente”
- Nombre de la empresa: Identifica la empresa u organismo donde se realizará la auditoría, se debe ingresar “INYM”.
- Teléfono: Identifica el numero telefónico del contacto donde se realizará la auditoría, se debe ingresar “03752-465857”
- Correo Electrónico: Identifica la dirección de correo electrónico del contacto principal, se debe ingresar “gonzalez@yahoo.es “

Una vez ingresados estos datos, se deben guardar. Los datos del cliente se pueden guardar, o cancelar el ingreso. En la parte inferior se encuentran los botones “Guardar”, y “Cancelar”. Después de ingresar los datos se debe elegir la opción “Guardar”.

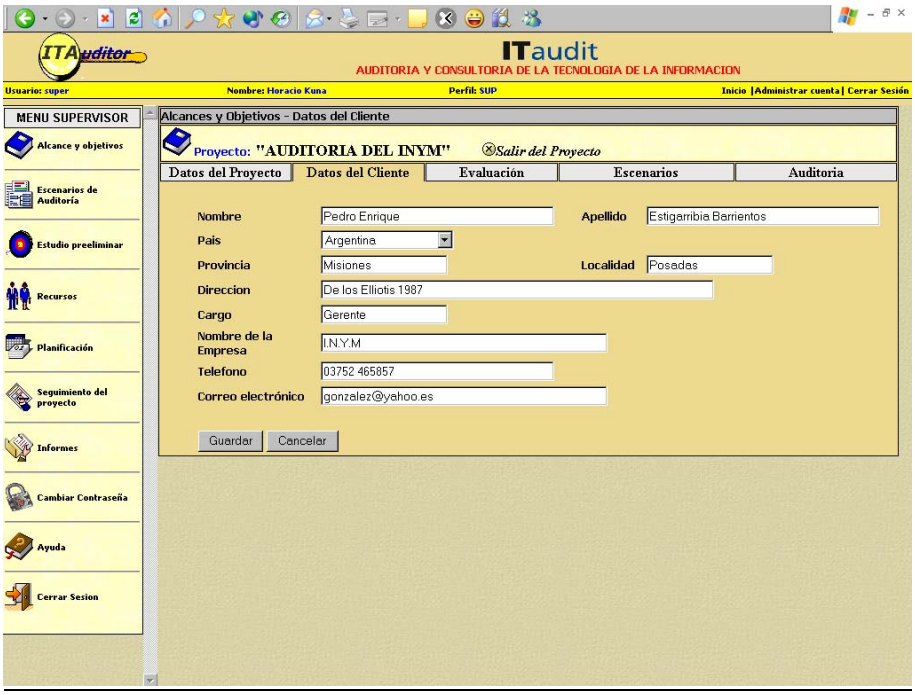


Figura 5.4. Datos del cliente

El tercer paso es la carga de los límites de la tarea, como se estableció en la reunión inicial desarrollada con los representantes del INYM, la misma se realizará por Áreas, estipulándose para este etapa abordar solo el área de “Organización, gestión y base jurídica”, la solapa de la derecha que dice

"Auditoría" dentro del menú principal ubicado a la izquierda de la pantalla "*Alcance y Objetivos"* permite realizar esta carga, el supervisor debe marcar el o las áreas donde se realizará la auditoría, como se observa en la figura 5.5. aparecen en la pantalla las siguientes áreas posibles de ser auditadas:

- Auditoría de la Gestión Informática
- Auditoría de la seguridad General
- Organización Gestión y base jurídica
- Auditoría de la producción
- Auditoría de las aplicaciones operativas
- Auditoría de los proyectos en desarrollo
- Auditoría del mantenimiento de aplicaciones
- Auditoría de la calidad del software

A la derecha de cada área existe una caja donde es posible marcar con el Mouse las elegidas para la auditoría, en el caso de esta experimentación se debe marcar "Organización Gestión y base jurídica".

Una vez marcadas las áreas a auditar, se deben guardar. Es posible guardar, o cancelar el ingreso . En la parte inferior se encuentran los botones "Guardar", y "Cancelar". Después de marcar las áreas se debe elegir la opción "Guardar".

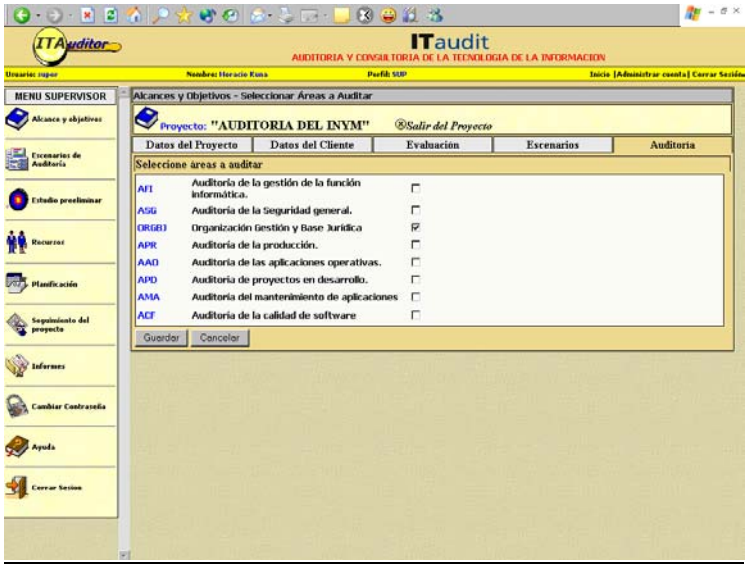


Figura 5.5. Areas a auditar

El último paso que se realiza al iniciar un proyecto es listar un reporte con los datos de la auditoría a realizar, para realizar esta acción se ingresa dentro del menú del supervisor ubicado a la izquierda de la pantalla a la opción *"Informes",* en la figura 5.6. se muestra la pantalla que aparece al ingresar a esta opción del menú, la misma tiene las siguientes categorías:

- Escenarios
- Papeles de trabajo
- Evaluaciones
- Proyectos

Cada una de estas categorías tiene distintas opciones a las que se acceden a través de un combo desplegable, se debe elegir dentro de la categoría “Proyectos” la opción “Datos del Proyectos”, una vez determinado el tipo de reporte a generar se debe elegir el nivel de detalle que debe tener el mismo, las alternativas son:

- Informe resumido
- Informe detallado

A través de un combo desplegable se debe elegir la opción “informe detallado”.

Una vez elegido el reporte a generar y el nivel de detalle existen dos alternativas, cancelar o generar el informe, en la parte inferior se encuentra el botón “Cancelar” y a la derecha de la categoría de reporte a realizar el botón “Generar Informe”, después de determinar el reporte se debe elegir la opción “generar Informe”

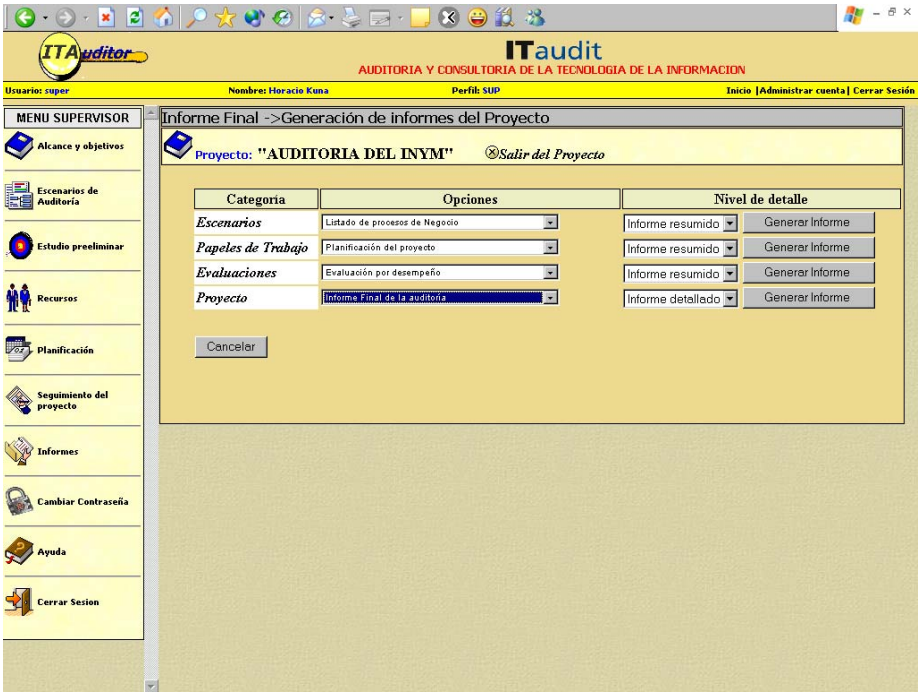


Figura 5.6. Informes

La figura 5.7 muestra el informe generado donde se encuentran todos los datos ingresados al iniciar un proyecto:

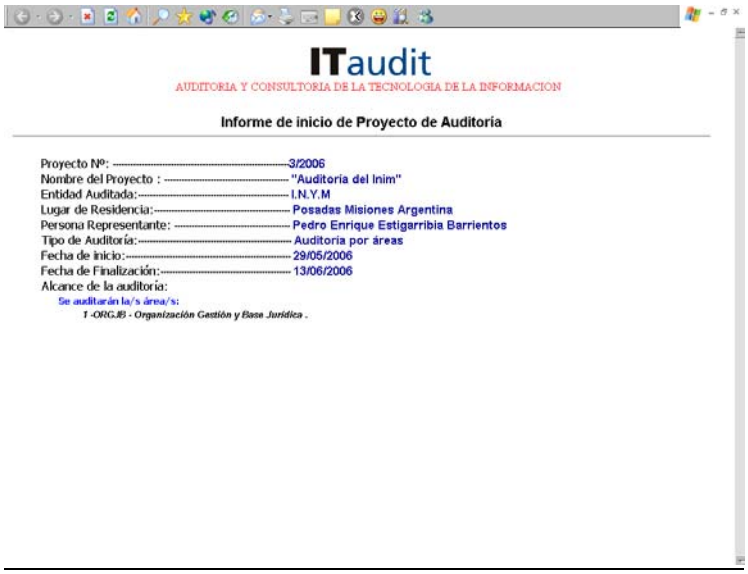


Figura 5.7 Informe Alcance y Objetivos

5.3.2. Módulo de estudio preliminar

Dado que es otro perfil de usuario el que realiza el estudio preliminar, se debe salir del sistema, ya que se accedió al mismo con perfil de Supervisor para iniciar el proyecto, y volver a ingresar con el perfil de Auditor que es el perfil que realiza el estudio preliminar. Para realizar esta acción en la parte superior derecha de la pantalla, como se observa en la figura 5.6., se encuentra la opción de "*Cerrar Cesión*", al elegir esta alternativa aparece la pantalla de ingreso al sistema como se observa en la figura 5.1.

El "User ID" es "AUDITOR" y la "Password" es "AUDIT" que deben ser ingresados en la pantalla de acceso, se debe elegir el botón "Ingresar" que se encuentra debajo de la password.

Para realizar el estudio preliminar se debe seleccionar del menú principal del Auditor, que se encuentra en la parte izquierda de la pantalla, el botón *"Estudio Preliminar*". Con esta acción se abre una pantalla como la que aparece en la figura 5.8.

El estudio preliminar implica el ingreso de distinta información, los datos a ingresar son:

- Persona entrevistada: Identifica la persona que se esta entrevistando para responder las preguntas del estudio preliminar, se debe ingresar "Ingeniero Raimundo Paranaibo".

- Cargo: Identifica el cargo de la persona que se esta entrevistando para responder las preguntas del estudio preliminar, se debe ingresar “Gerente General”.

Una vez ingresados estos datos, se deben responder las preguntas del relevamiento inicial. En el caso de la experimentación que se esta realizando aparece la pregunta:

- “La empresa cuenta con un área de Sistemas?”

Debajo de la pregunta aparecen dos check-box con las opciones “Si” y “No”, se debe elegir el primero.

Los preguntas del relevamiento preliminar pueden guardarse o cancelar el ingreso. En la parte inferior se encuentran los botones “Guardar Cuestionario” y “Cancelar”. Después de ingresar los datos se debe elegir la opción “Guardar Cuestionario”

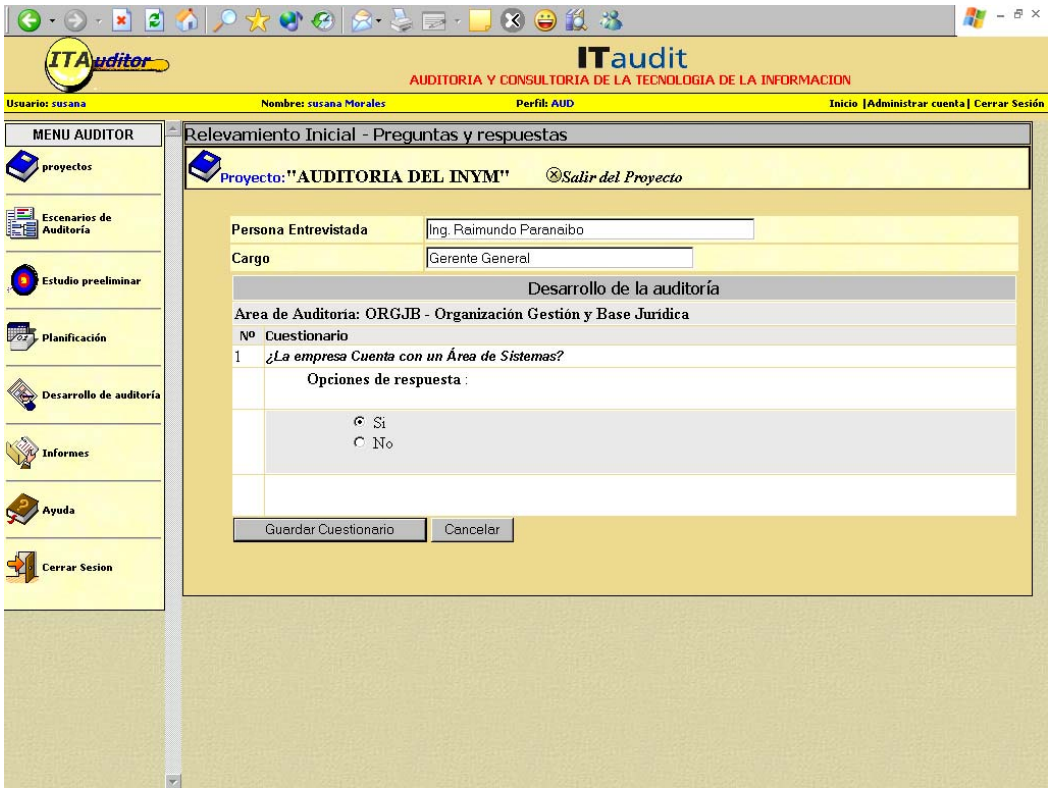


Figura 5.8. Preguntas estudio preliminar

Dado que la respuesta fue que existe un área de sistemas, en el desarrollo de la auditoría deberán responderse cuatro preguntas ingresadas con anterioridad al desarrollo de la auditoría en el módulo de configuración, ya que todas ellas están relacionadas con la respuesta “SI”.

El siguiente paso que se realiza en el estudio preliminar es listar un reporte con los resultados de este estudio, para ejecutar esta acción se ingresa dentro del menú del Auditor ubicado a la izquierda de la pantalla a la opción *"Informes",* en la figura 5.6. se muestra la pantalla que aparece al ingresar a este punto del menú, la misma tiene las siguientes categorías:

- Escenarios
- Papeles de trabajo
- Evaluaciones
- Proyectos

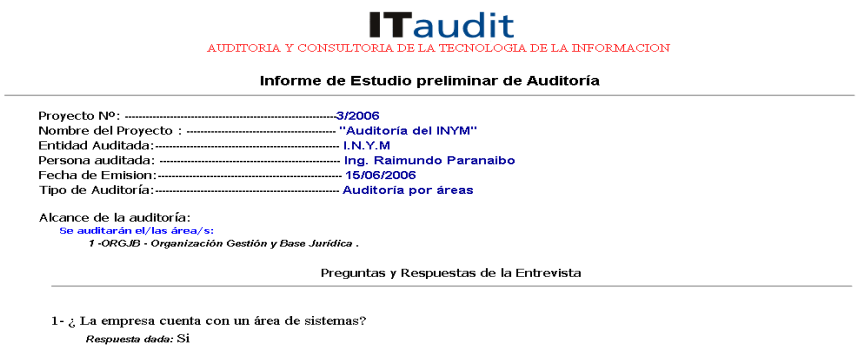
Se debe elegir dentro de la categoría "Proyectos" la opción "Informe preliminar", una vez determinado el tipo de reporte a generar se debe elegir el nivel de detalle que debe tener el mismo, las alternativas son:

- Informe resumido
- Informe detallado

A través de un combo desplegable se debe elegir la opción "informe detallado".

Una vez elegido el reporte a generar y el nivel de detalle existen dos alternativas, cancelar o generar el informe, en la parte inferior se encuentra el botón "Cancelar" y a la derecha de la categoría de reporte a realizar el botón "Generar Informe", después de determinar el reporte se debe elegir la opción "generar Informe"

En la figura 5.9. se visualiza el informe emitido.


ITaudit

AUDITORIA Y CONSULTORIA DE LA TECNOLOGIA DE LA INFORMACION

Informe de Estudio preliminar de Auditoría

Proyecto Nº: ---------- 3/2006
Nombre del Proyecto : ---------- "Auditoría del INYM"
Entidad Auditada: ---------- I.N.Y.M
Persona auditada: ---------- Ing. Raimundo Paranaibo
Fecha de Emision: ---------- 15/06/2006
Tipo de Auditoría: ---------- Auditoría por áreas

Alcance de la auditoría:
Se auditarán el/las área/s:
1 -ORGJB - Organización Gestión y Base Jurídica .

Preguntas y Respuestas de la Entrevista

1- ¿ La empresa cuenta con un área de sistemas?
Respuesta dada: Si

Figura 5.9. Reporte relevamiento preliminar

5.3.3. Módulo de recursos

Dado que es otro perfil de usuario el que determina los recursos humanos que intervendrán en la auditoría, se debe salir del sistema, ya que se accedió al mismo con perfil de Auditor para realizar el estudio preliminar, y volver a ingresar con el perfil de Supervisor que es el perfil que establece los recursos. Para realizar esta acción en la parte superior derecha de la pantalla, como se observa en la figura 5.8., se encuentra la opción de "*Cerrar Cesión*", al elegir esta alternativa aparece la pantalla de ingreso al sistema como se observa en la figura 5.1.

El "User ID" es "SUPERVISOR" y la "Password" es "SUPER" que deben ser ingresados en la pantalla de acceso, se debe elegir el botón "Ingresar" que se encuentra debajo de la password.

Al Ingresar al sistema, en el menú principal ubicado a la izquierda de la pantalla se debe ingresar a la opción *"Recursos"* , en esta pantalla como se ve en la figura 5.10. aparecen en la parte superior derecha tres botones:

- Ver todos: Muestra todos los auditores disponibles
- Sugerir equipo: este botón se encuentra a la derecha de la opción "Ver Todos" y sugiere un equipo de auditores en relación con el alcance del proyecto.
- Sugerir auditor: Sugiere un auditor relacionado a un tema específico.

Debajo del botón "Sugerir Auditor" se encuentra un combo desplegable con los distintos temas específicos que se pueden abordar en una auditoría. Para esta experimentación se debe elegir el tema "Especialista en gestión de Area de TI" y presionar el botón "Sugerir Auditor". Como resultado de esta acción aparece en la parte izquierda de la pantalla debajo del titulo "Auditores Disponibles" los profesionales que se especializan en el tema elegido, a la derecha de este cuadro aparece otro con el titulo "Auditores asignados al proyecto", entre ambos hay cuatro botones:

- ">": Pasa un auditor del cuadro "Auditores disponibles" a "Auditores asignados al proyecto"
- "<": Pasa un auditor del cuadro "Auditores asignados al proyecto" a "Auditores disponibles"
- ">>": Pasa todos los auditores del cuatro "Auditores disponibles" a "Auditores asignados al proyecto"
- "<<": Pasa todos los auditores del cuatro "Auditores asignados al proyecto" a "Auditores disponibles"

Después de presionar el botón “Sugerir Auditor” aparece “Horacio Kuna” en el cuadro “Auditor Disponible” y se lo debe pasar presionando el botón “>” al cuadro “Auditores asignados al proyecto” como se observa en la figura 5.10.

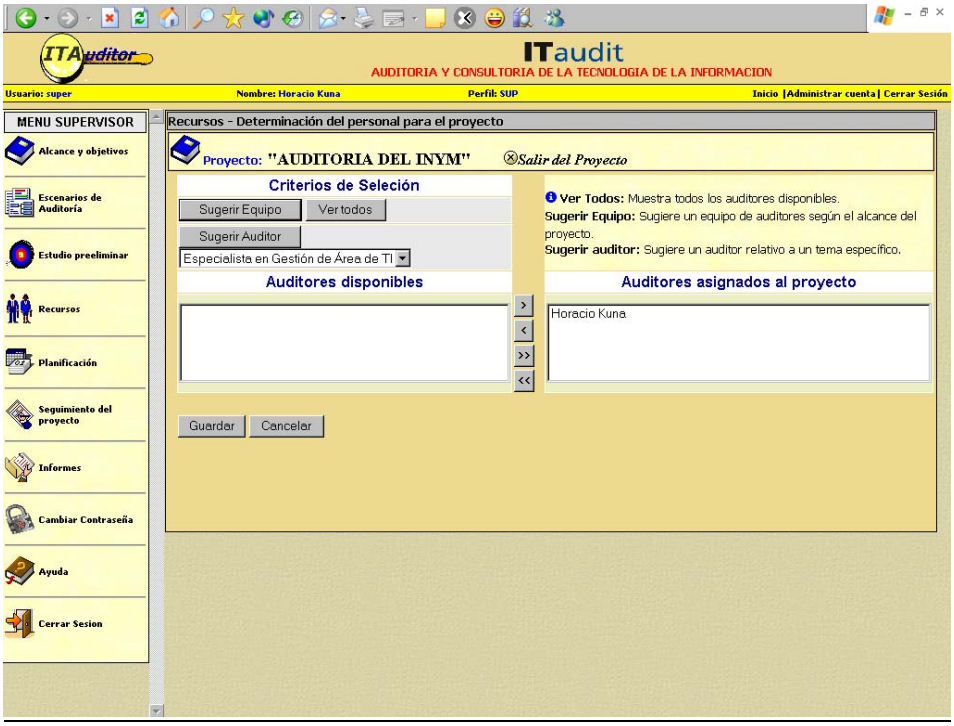


Figura 5.10. Recursos

5.3.4. Módulo de planificación

Sin salir del sistema ya que el supervisor es quien realiza el plan de trabajo, se debe ingresar dentro del menú principal, ubicado a la izquierda de la pantalla, a la opción *“Planificación”*, al ingresar a este punto del menú aparece una pantalla, como se ve en la figura 5.11, que tiene los datos generales de la auditoría que se esta realizando: el nombre del proyecto, las fechas de inicio y finalización y el tipo de auditoría . Debajo de estos datos se encuentran dos botones “Generar plan de trabajo” y Cancelar”, se debe elegir el primero de ellos.

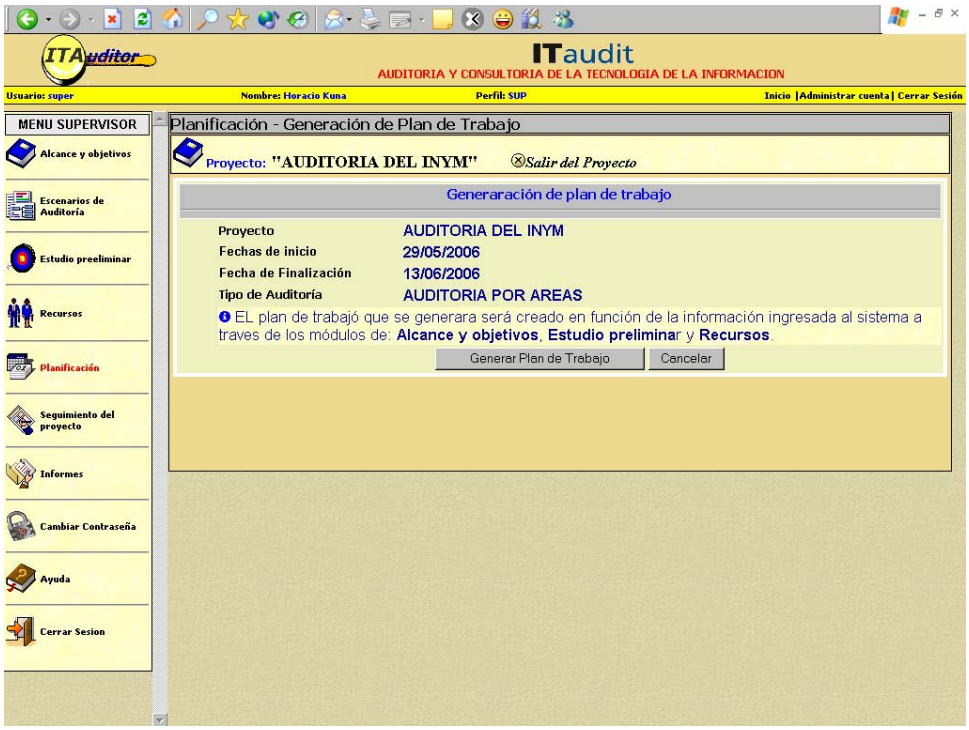


Figura 5.11. generación plan de trabajo

Como resultado de este proceso aparece una pantalla que tiene en la parte izquierda el plan de trabajo y en la parte derecha permite la carga de actividades.

El plan de trabajo implica el ingreso de distinta información que se realiza en la parte derecha de la pantalla como se observa en la figura 5.12, los datos a ingresar son:

- Ubicar la tarea: de un combo desplegable puede seleccionar entre “Antes de” y después de”.
- Tarea: Muestra en nombre de la tarea en el caso de realizar una modificación.
- Orden tarea: Se debe ingresar el número de la tarea cuando se incorpora una nueva.
- Descripción tarea: se debe ingresar la descripción de una tarea en el caso de realizar un alta o modificación.
- Objetivos: se debe ingresar el objetivo de la tarea.
- Fecha de inicio: se debe ingresar la fecha de inicio de la tarea.
- Fecha de finalización: se debe ingresar la fecha de finalización de la tarea.
- Asignar a: a través de un combo desplegable se elige el auditor al que se le asigna la tarea.
- Porcentaje: se debe ingresar el porcentaje de avance de la tarea.

- Adjuntar archivo: en este punto se pueden seleccionar archivos relacionados con cada tarea, podrán ser de cualquier formato, por ejemplo documentos escaneados, reglamentaciones, documentos de trabajo, etc., se los elige a través del botón “Examinar” que se encuentra a la derecha.

Una vez ingresados estos datos, se deben guardar. Las tareas pueden guardarse, cancelar el ingreso de alguna de ellas o pueden darse de baja, los archivos que se adjuntan a una tarea pueden agregarse a la misma. En el inferior de la parte derecha de la pantalla que permite la carga de tareas, se encuentran los botones “Guardar” para guardar una tarea, “Eliminar” para eliminar una tarea, “Cancelar” para cancelar una tarea y “Agregar” para agregar un archivo a una tarea. Después de ingresar los datos se debe elegir la opción “Guardar”.

Cuando se guarda una tarea la misma aparece en la parte izquierda de la pantalla, con algunos datos básicos como el nombre, la fecha de inicio y fin y el auditor asignado. Junto a cada tarea aparecen dos íconos, el primero permite modificar una tarea y el segundo eliminarla.

El resultado de esta carga es el que se ve en la figura 5.12.

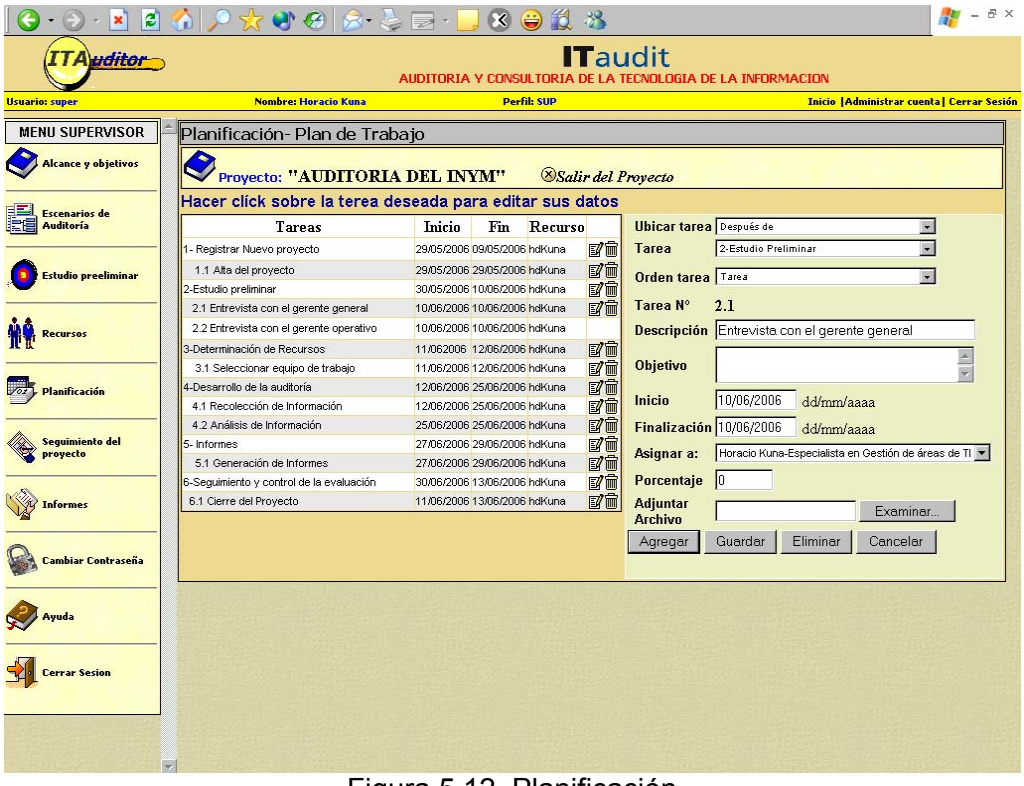


Figura 5.12. Planificación

5.3.5. Módulo de desarrollo

Dado que es otro perfil de usuario el que realiza la auditoría, se debe salir del sistema, ya que se accedió al mismo con perfil de Supervisor para realizar determinar los recursos humanos y planificar, y volver a ingresar con el perfil de Auditor que es el perfil que desarrolla la auditoría. Para realizar esta acción en la parte superior derecha de la pantalla, como se observa en la figura 5.12., se encuentra la opción de "*Cerrar Cesión*", al elegir esta alternativa aparece la pantalla de ingreso al sistema como se observa en la figura 5.1.

El "User ID" es "AUDITOR" y la "Password" es "AUDIT" que deben ser ingresados en la pantalla de acceso, se debe elegir el botón "Ingresar" que se encuentra debajo de la password.

Al Ingresar al sistema, en el menú principal ubicado a la izquierda de la pantalla se debe ingresar a la opción *"Desarrollo de la Auditoría"* , en esta pantalla como se ve en la figura 5.13. aparecen todas las preguntas del desarrollo de la auditoría, y un check-box para cada alternativa de respuesta. Se ingresan al sistema las respuestas al check-list que el sistema presenta, el auditor debe marcar las opciones de respuesta que da el auditado.

Una vez ingresados las respuestas, se deben guardar. Las respuestas pueden guardarse o cancelar el ingreso de ellas. En el inferior de la pantalla se encuentran los botones "Guardar cuestionario" y "Cancelar" . Después de ingresar los datos se debe elegir la opción "Guardar Cuestionario".

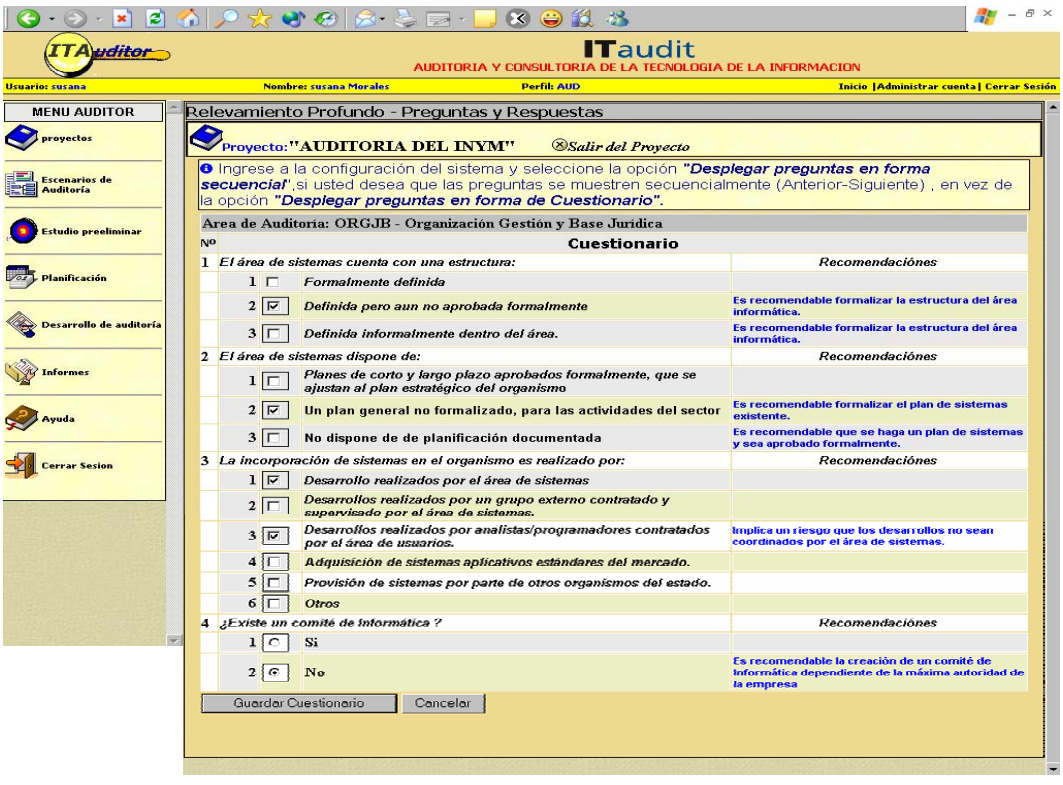
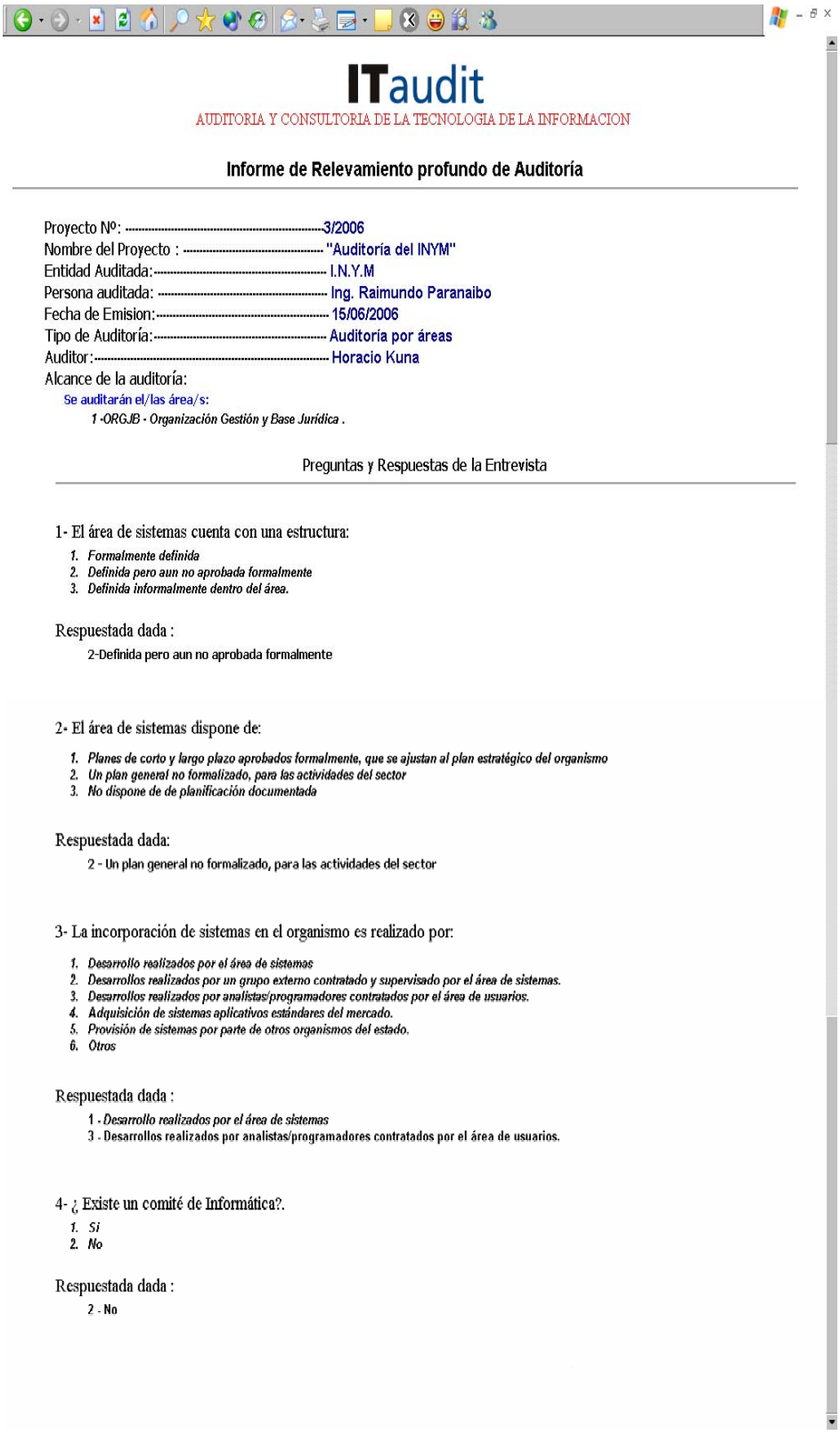


Figura 5.13 desarrollo de la auditoría

Como resultado del desarrollo de la auditoría se emite un reporte con las preguntas y respuestas, para realizar esta tarea el auditor debe ingresar a la opción del menú principal "*Informes*" y se emite un reporte que se muestra en la figura 5.14:



ITaudit

AUDITORIA Y CONSULTORIA DE LA TECNOLOGIA DE LA INFORMACION

Informe de Relevamiento profundo de Auditoría

Proyecto Nº: ---------- 3/2006
Nombre del Proyecto : ---------- "Auditoría del INYM"
Entidad Auditada: ---------- I.N.Y.M
Persona auditada: ---------- Ing. Raimundo Paranaibo
Fecha de Emision: ---------- 15/06/2006
Tipo de Auditoría: ---------- Auditoría por áreas
Auditor: ---------- Horacio Kuna
Alcance de la auditoría:
Se auditarán el/las área/s:
1 -ORGJB - Organización Gestión y Base Jurídica .

Preguntas y Respuestas de la Entrevista

1- El área de sistemas cuenta con una estructura:

1. *Formalmente definida*
2. *Definida pero aun no aprobada formalmente*
3. *Definida informalmente dentro del área.*

Respuestada dada :
2-Definida pero aun no aprobada formalmente

2- El área de sistemas dispone de:

1. *Planes de corto y largo plazo aprobados formalmente, que se ajustan al plan estratégico del organismo*
2. *Un plan general no formalizado, para las actividades del sector*
3. *No dispone de de planificación documentada*

Respuestada dada:
2 - Un plan general no formalizado, para las actividades del sector

3- La incorporación de sistemas en el organismo es realizado por:

1. *Desarrollo realizados por el área de sistemas*
2. *Desarrollos realizados por un grupo externo contratado y supervisado por el área de sistemas.*
3. *Desarrollos realizados por analistas/programadores contratados por el área de usuarios.*
4. *Adquisición de sistemas aplicativos estándares del mercado.*
5. *Provisión de sistemas por parte de otros organismos del estado.*
6. *Otros*

Respuestada dada :
1 - *Desarrollo realizados por el área de sistemas*
3 - Desarrollos realizados por analistas/programadores contratados por el área de usuarios.

4- ¿ Existe un comité de Informática?.

1. *Si*
2. *No*

Respuestada dada :
2 - No

Figura 5.14.:Informe relevamiento profundo

5.3.6. Módulo de informe final

Dado que es otro perfil de usuario el que realiza el informe final, se debe salir del sistema, ya que se accedió al mismo con perfil de Auditor para realizar el desarrollo de la auditoría, y volver a ingresar con el perfil de Supervisor que es el perfil que emite el informe final. Para realizar esta acción en la parte superior derecha de la pantalla, como se observa en la figura 5.13., se encuentra la opción de "*Cerrar Cesión*", al elegir esta alternativa aparece la pantalla de ingreso al sistema como se observa en la figura 5.1.

El "User ID" es "SUPERVISOR" y la "Password" es "SUPER" que deben ser ingresados en la pantalla de acceso, se debe elegir el botón "Ingresar" que se encuentra debajo de la password.

Para realizar el informe final se ingresa dentro del menú del Auditor ubicado a la izquierda de la pantalla a la opción *"Informes",* en la figura 5.6. se muestra la pantalla que aparece al ingresar a este punto del menú, la misma tiene las siguientes categorías:

- Escenarios
- Papeles de trabajo
- Evaluaciones
- Proyectos

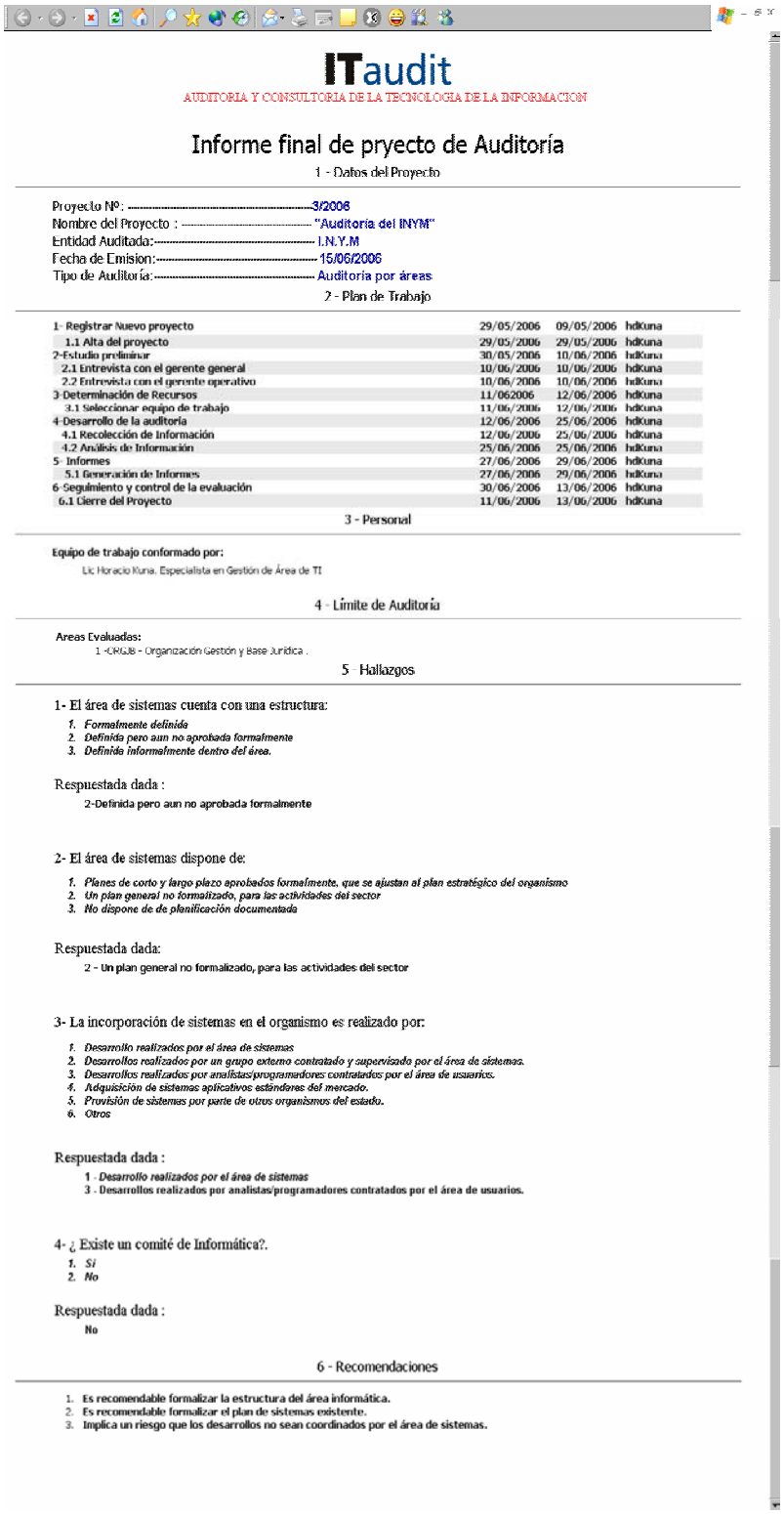
Se debe elegir dentro de la categoría "Proyectos" la opción "Informe final", una vez determinado el tipo de reporte a generar se debe elegir el nivel de detalle que debe tener el mismo, las alternativas son:

- Informe resumido
- Informe detallado

A través de un combo desplegable se debe elegir la opción "informe detallado".

Una vez elegido el reporte a generar y el nivel de detalle existen dos alternativas, cancelar o generar el informe, en la parte inferior se encuentra el botón "Cancelar" y a la derecha de la categoría de reporte a realizar el botón "Generar Informe", después de determinar el reporte se debe elegir la opción "generar Informe".

Como resultado de este proceso el sistema propone un informe final, como se muestra en la figura 5.15, que servirá de base para el informe definitivo que se le entregará al usuario final.



ITaudit

AUDITORIA Y CONSULTORIA DE LA TECNOLOGIA DE LA INFORMACION

Informe final de pryecto de Auditoría

1 - Datos del Proyecto

Proyecto Nº: ----------3/2006
Nombre del Proyecto : ---------- "Auditoria del INYM"
Entidad Auditada:---------- I.N.Y.M
Fecha de Emision:---------- 15/06/2006
Tipo de Auditoría:---------- Auditoría por áreas

2 - Plan de Trabajo

1- Registrar Nuevo proyecto	29/05/2006	09/05/2006	hdKuna
1.1 Alta del proyecto	29/05/2006	29/05/2006	hdKuna
2-Estudio preliminar	30/05/2006	10/06/2006	hdKuna
2.1 Entrevista con el gerente general	10/06/2006	10/06/2006	hdKuna
2.2 Entrevista con el gerente operativo	10/06/2006	10/06/2006	hdKuna
3-Determinación de Recursos	11/062006	12/06/2006	hdKuna
3.1 Seleccionar equipo de trabajo	11/06/2006	12/06/2006	hdKuna
4-Desarrollo de la auditoría	12/06/2006	25/06/2006	hdKuna
4.1 Recolección de información	12/06/2006	25/06/2006	hdKuna
4.2 Análisis de información	25/06/2006	25/06/2006	hdKuna
5- Informes	27/06/2006	29/06/2006	hdKuna
5.1 Generación de Informes	27/06/2006	29/06/2006	hdKuna
6-Seguimiento y control de la evaluación	30/06/2006	13/06/2006	hdKuna
6.1 Cierre del Proyecto	11/06/2006	13/06/2006	hdKuna

3 - Personal

Equipo de trabajo conformado por:
Lic Horacio Kuna. Especialista en Gestión de Área de TI

4 - Límite de Auditoría

Areas Evaluadas:
1 -ORGJB - Organización Gestión y Base Jurídica .

5 - Hallazgos

1- El área de sistemas cuenta con una estructura:
1. *Formalmente definida*
2. *Definida pero aun no aprobada formalmente*
3. *Definida informalmente dentro del área.*

Respuestada dada :
2-Definida pero aun no aprobada formalmente

2- El área de sistemas dispone de:
1. *Planes de corto y largo plazo aprobados formalmente, que se ajustan al plan estratégico del organismo*
2. *Un plan general no formalizado, para las actividades del sector*
3. *No dispone de de planificación documentada*

Respuestada dada:
2 - Un plan general no formalizado, para las actividades del sector

3- La incorporación de sistemas en el organismo es realizado por:
1. *Desarrollo realizados por el área de sistemas*
2. *Desarrollos realizados por un grupo externo contratado y supervisado por el área de sistemas.*
3. *Desarrollos realizados por analistas/programadores contratados por el área de usuarios.*
4. *Adquisición de sistemas aplicativos estándares del mercado.*
5. *Provisión de sistemas por parte de otros organismos del estado.*
6. *Otros*

Respuestada dada :
1 - *Desarrollo realizados por el área de sistemas*
3 - Desarrollos realizados por analistas/programadores contratados por el área de usuarios.

4- ¿ Existe un comité de Informática?.
1. *Si*
2. *No*

Respuestada dada :
No

6 - Recomendaciones

1. Es recomendable formalizar la estructura del área informática.
2. Es recomendable formalizar el plan de sistemas existente.
3. Implica un riesgo que los desarrollos no sean coordinados por el área de sistemas.

Figura 5.15. Informe final

5.3.7. Conclusiones de la experimentación

La experimentación permitió comprobar el funcionamiento del sistema en un entorno real, si bien para el caso de estudio realizado se ingresaron un set reducido de preguntas tanto del relevamiento inicial como para el desarrollo de la auditoría, se pudo comprobar que efectivamente el sistema cumplió los objetivos para los cuales fue creado, permitiendo asistir y guiar al auditor desde el punto de vista metodológico en su tarea.

Capítulo 6

Conclusiones y futuras líneas de investigación

6. CONCLUSIONES Y FUTURAS LÍNEAS DE INVESTIGACIÓN

En este capitulo se describen las conclusiones generales a las que se llego y las futuras líneas de investigación que es posible seguir.

6.1. Conclusiones generales

La metodología aplicada, Métrica V3, se adaptó perfectamente a un proyecto de características particulares y aportó a través de cada una de sus etapas, actividades y tareas a lograr el objetivo propuesto, demostrando la ventaja enorme que implica el uso de una metodología en el desarrollo de sistemas.

El desarrollo realizado permite afirmar que es posible contar con una herramienta software que incorpore los estándares que actualmente se utilizan a nivel global para realizar auditoría de sistemas.

La arquitectura del sistema y el hecho que el mismo funcione en un entorno Web, posibilita a auditores de sistemas en general, y a aquellos en particular que realizan sus actividades lejos de las grandes ciudades y tienen dificultades en su actualización profesional, contar con una herramienta software que les posibilita realizar su tarea con mayor calidad y de manera eficaz y eficiente.

Es posible desarrollar un producto software, utilizando herramientas basadas en la filosofía Open Source, que den soporte a las técnicas de auditoría de sistemas asistida por computadora.

El sistema desarrollado demuestra que se puede contar con una única herramienta software que asista desde el punto de vista metodológico al auditoría de sistemas y se adapte a los distintos entornos a auditar.

Es necesario difundir el uso de las Técnicas de auditoría asistidas por computadora, ya que las mismas son un soporte fundamental en la tarea que realiza el auditor de sistemas.

El sistema cuenta con los factores de calidad planificados:

- ✓ *Corrección:* El sistema cumple con sus especificaciones y satisface los objetivos de los usuarios.
- ✓ *Fiabilidad:* El sistema funciona sin errores.
- ✓ *Facilidad de uso:* El sistema es fácil de aprender y su operación se realiza sin inconvenientes, incluso para personas no expertas en la auditoría de sistemas.
- ✓ *Integridad:* Se controla el acceso ilegal al sistema y la base de datos.

- ✓ *Flexibilidad:* El sistema es fácil de modificar.

6.2. Futuras líneas de investigación y desarrollo

Considerando la experiencia obtenida a lo largo del desarrollo del sistema surgen varios elementos a considerar en futuras investigaciones:

- ✓ La depuración del prototipo generado permitirá tener un producto que asista efectivamente al auditor de sistemas en su tarea. Desarrollo de herramientas que asistan al auditor en la auditoría de bases de datos.
- ✓ Incorporación de un módulo especifico que permita asistir al auditor en los temas relacionados con las redes y telecomunicaciones, como por ejemplo escaneo de puertos, control de servicios, etc.
- ✓ Integración de la herramienta con otros software como por ejemplo Magerit, Idea, ACL, etc.
- ✓ Desarrollo de un módulo que permita asistir a las empresas en la generación de planes de contingencia.
- ✓ Desarrollo de un módulo estadístico.
- ✓ Estudio de la factibilidad que el sistema incorpore los conocimientos que se obtienen en las auditorias realizadas.

Capítulo 7

Referencias y Bibliografía

7.1. REFERENCIA

[Métrica V3, 2000] Metodología de Planificación, Desarrollo y Mantenimiento de sistemas de información. Ministerio de Administraciones Públicas Español. Disponible en http://www.csi.map.es/csi/metrica3/index.html, página vigente al 16 de abril de 2004.

[Rivas, 1988] Rivas, Auditoría Informática. 198 páginas. Ediciones Díaz de Santos. ISBN 84-87189-13

[ISACA, 2002] Information System Audit and Control Association. Disponible en http://www.isaca.org página vigente al 10 de mayo de 2004.

[SIGEN, 2004] Sindicatura General de la Nación. Disponible en http://www.sigen.gov.ar página vigente al 4 de setiembre de 2004.

[COBIT, 1996] Control Objectives for Information and related Technology. Disponible en http://www.isaca.org/cobit/ página vigente al 16 de abril de 2005.

[Piattini, 2003] Piattini Mario y del Peso Emilio, 2003. Auditoría Informática, un enfoque práctico. 659 páginas. Editorial Alfaomega-Rama. ISbn: 958-682-455-1

[ADACSI, 2004] Asociación de Auditoría y Control de Sistemas de Información. Disponible en http://www.adacsi.org.ar página vigente al 16 de abril de 2004.

[Fernández, 2006] Fernández Enrique, 2006. Asistente para la Gestión de Documentos de Proyectos de Explotación de Datos. Tesis de Magíster en Ingeniería del Software. Instituto Tecnológico de Buenos Aires. Disponible en http://www.itba.edu.ar/capis página vigente al 13 de mayo de 2006.

[Sueldo, 2006] Sueldo Alejandro José, 2006. Sistema Integrado de Gestión Estratégica. Tesis de Magíster en Ingeniería del Software. Instituto Tecnológico de Buenos Aires. Disponible en http://www.itba.edu.ar/capis página vigente al 13 de mayo de 2006

[Peralta, 2004] Peralta Mario Luis, 2004. Asistente para la Evaluación de CMMI-SW. Tesis de Magíster en Ingeniería del Software. Instituto Tecnológico de Buenos Aires. Disponible en http://www.itba.edu.ar/capis página vigente al 13 de mayo de 2006

[IDEA, 2004] Software de Auditoría. Disponible en www.usd.edu/idea/audit/, página vigente al 26 de abril de 2004.

[MAGERIT, 2004] MAGERIT – versión 2. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Disponible en www.csi.map.es/csi/pg5m20.htm , página vigente al 26 de abril de 2004.

[Horowitz, 1999] Horowitz E. "USC COCOMO II (1999)" Disponible en http://sunset.usc.edu/research/COCOMOII/index.html. página vigente al 17 de noviembre de 2005.

[ISO 9001:2000] International Organization for Standardization. Disponible en http://www.iso.org página vigente al 30 de marzo de 2005.

7.2. BIBLIOGRAFÍA

.

[Cansler, 2003] Cansler Leopoldo. 2003. Auditoría en contextos computarizados. 258 páginas. Editoriales Cooperativas. ISBN 9871076347.

[Castello, 1998] Castello Ricardo. 1998. Auditoría en entornos informáticos. 271 páginas. Editorial Universidad Nacional de Córdoba. ISBN en trámite.

[Echenique G., 2004] Echenique García José Antonio. 2004. Auditoría en Informática. 299 páginas. Editorial McGraw-Hill. ISBN 970-10-3356-6.

[García M. & Pasquín, 2003] García Martínez, R. y Pasquini, D. 2003. Sistemas Inteligentes. 352 páginas. Editorial Nueva Librería. ISBN 9871104057.

[Gomez & Jurista, 1997] Gomez Asunción y Jurista Natalia. 1997. Ingeniería del conocimiento. 828 páginas. Editorial Centro de Estudio Ramón Areses. ISBN 84-8004-269-9

[Hernández, 1998] Hernández Enrique. 1998. Auditoría en Informática, un enfoque práctico. 315 páginas. Editorial CECSA. ISBN 968-26-1283-7

[Kell W., 1996] Kell Walter G. 1996. Auditoría Moderna. 856 páginas. Editorial C.E.C.S.A. ISBN 968261144X

[Mendivil E., 2002] Mendivil Escalante Victor Manuel. 2002. Elementos de Auditoría. 160 páginas. Editorial Thomson Internacional. ISBN 9706861726.

[Pressman, 2002] Pressman Roger. 2002. Ingeniería del Software un enfoque práctico. 600 páginas. Editorial McGraw-Hill. ISBN 0-07-709677-0.

[Rich & Knight, 1994] Rich Elaine y Knight Kevin. 1994. Inteligencia Artificial. 703 páginas. Editorial McGraw-Hill. ISBN 0-07-052263-4.

Anexos

Anexo 1

Guías de Auditoría COBIT

Planificación y Organización

PO 1 Definir un Plan Estratégico para las Tecnologías de la Información

OBJETIVOS DE CONTROL:

1. Tecnología de la información como parte del Plan a largo y corto plazo de la Organización.
2. Plan de la tecnología de la Información a largo plazo.
3. Planificación de la tecnología de la Información a largo plazo - Enfoque y Estructura.
4. Cambios en el Plan a largo plazo de la tecnología de la información.
5. Planificación a corto plazo de la Tecnología de la Información.
6. Evaluación de los sistemas existentes.

TANTO LOS OBJETIVOS DE CONTROL DETALLADOS COMO LOS DE ALTO NIVEL SON AUDITADOS MEDIANTE:

Obtención de conocimiento a través de:

- **Entrevistas:**

  Director General.

  Director de Operaciones.

  Director de Finanzas.

  Director de las TI.

  Miembros del comité de planificación de los servicios de información.

  Dirección y personal de recursos humanos de los servicios de información.

- **Obteniendo:**

  Políticas y procedimientos inherentes al proceso de la planificación.

  Funciones y responsabilidades de planificación de la Dirección.

Objetivos y planes a corto y largo plazo de la organización.

Objetivos y planes a corto y largo plazo de la tecnología de la información.

Informes de estado y actas de las reuniones del comité de planificación.

Evaluación de los controles:

- **Considerando si:**

Las políticas y procedimientos de negocio de los servicios de información siguen un enfoque de planificación estructurado. Se ha establecido una metodología para formular y modificar los planes y que cubran, como mínimo:

- Misión y metas de la organización.

- Iniciativas de la tecnología de la información para soportar la misión y las metas de la organización.
- Oportunidades para las iniciativas de la tecnología de la información.
- Estudios de viabilidad de las iniciativas de la tecnología de la información.
- Evaluación de los riesgos de las iniciativas de la tecnología de la información.
- Inversión óptima en tecnología de la información actual y futura.
- Reingeniería de las iniciativas de la tecnología de la información para reflejar los cambios en la misión y las metas de la organización.
- Evaluación de las estrategias alternativas para las aplicaciones de datos, tecnología y organización.

Los cambios de la organización, la evolución tecnológica, los requerimientos regulatorios, la reingeniería de los procesos de negocio, las fuentes externas e internas, etc. están siendo consideradas y dirigidas adecuadamente en el proceso de planificación.

Existen planes de la tecnología de la información a corto y largo plazo, si éstos se actualizan, están dirigidos adecuadamente a la empresa en general, si su misión y proyectos de la tecnología de la información para las funciones clave del negocio están soportados por la documentación apropiada según lo definido en la metodología de planificación de la tecnología de la información.

Existe una revisión para asegurar que los objetivos de las tecnologías de la información y los planes a corto y largo plazo continúan satisfaciendo los objetivos y los planes a corto y largo plazo de la organización.

Los propietarios de los procesos y la Dirección de los planes de la tecnología de la información llevan a cabo las revisiones y aprobaciones formales.

El plan de la tecnología de la información evalúa los sistemas de información existentes en términos del grado de automatización, funcionalidad, estabilidad, complejidad, costes, fortalezas y debilidades del negocio.

Evaluación de la suficiencia:

- **Probando que:**

Las actas de las reuniones del comité de planificación de los servicios de información reflejan el proceso de planificación.

Existe una metodología de la planificación comunicada según lo indicado.

Se incluyen iniciativas de la tecnología de la información en los planes a corto y largo plazo de los servicios de información (por ejemplo, cambios de hardware, planificación de capacidad, arquitectura de la información, desarrollo u obtención de nuevos sistemas, planificación de recuperación en caso de desastre, instalación de plataformas para nuevos procesamientos, etc.).

Las iniciativas de la tecnología de la información soportan la investigación, la formación, la asignación de personal, las instalaciones, el hardware y el software

Se han identificado las implicaciones para las iniciativas de la tecnología de la información.

Se ha tenido en consideración la optimización de inversiones en tecnología de la información actuales y futuras.

Los planes a corto y largo plazo de la tecnología de la información son consistentes con los planes a corto y largo plazo de la organización, así como con los requerimientos de negocio de ésta.

Se han modificado los planes para reflejar los cambios.

Los planes a largo plazo de la tecnología de la información son traducidos periódicamente en planes a corto plazo.

Existen tareas para implementar los planes.

Evaluación del riesgo de que no se cumplan los objetivos de control:

- **Llevando a cabo:**

Mediciones ("Benchmarking") de los planes estratégicos de la tecnología de la información con respecto a organizaciones similares o buenas prácticas industriales reconocidas y estándares internacionales.

Una revisión detallada de los planes de las TI para asegurar que las iniciativas de la tecnología de la información reflejan la misión y las metas de la organización.

Una revisión detallada de los planes de las TI para determinar si, como parte de las soluciones de la tecnología de la información contenidas en los planes, se han identificado áreas de debilidad dentro de la organización que requieren ser mejoradas.

- **Identificando:**

Fallos en la tecnología de la información para satisfacer la misión y las metas de la organización.

Fallo en la tecnología de la información para concordar los planes a corto y largo plazo.

Fallos en la tecnología de la información para satisfacer planes a corto plazo.

Fallos en la tecnología de la información para satisfacer alineamientos de costes y tiempos.

Oportunidades de negocio no aprovechadas.

Oportunidades de la tecnología de la información no aprovechadas.

PO 2 Definir la Arquitectura de la Información

OBJETIVOS DE CONTROL:

1. Modelo de la arquitectura de la Información.
2. Diccionario de datos corporativo y reglas de sintaxis de los datos.
3. Esquema de Clasificación de los Datos.
4. Niveles de Seguridad.

TANTO LOS OBJETIVOS DE CONTROL DETALLADOS COMO LOS DE ALTO NIVEL SON AUDITADOS MEDIANTE:

Obtención de conocimiento mediante:

- **Entrevistas:**

Director de las TI.

Miembros del comité de planificación de los servicios de información.

Dirección de los servicios de información.

Responsable de Seguridad.

- **Obteniendo:**

Políticas y procedimientos sobre la arquitectura de la información.

Modelo de la arquitectura de la información.

Documentos que soportan el modelo de la arquitectura de la información, incluyendo el modelo de datos corporativo.

Diccionario de datos corporativo.

Política de propiedad de datos.

Funciones y responsabilidades de planificación de la Dirección. Objetivos y planes a corto y largo plazo de la tecnología de la información.

Informe de estado y actas de las reuniones del comité de planificación.

Evaluación de los controles:

- **Considerando si:**

Las políticas y procedimientos de los servicios de información dirigen el desarrollo y mantenimiento del diccionario de datos.

El proceso utilizado para actualizar el modelo de la arquitectura de la información se basa en los planes a corto y largo plazo, considera los costes y riesgos asociados y asegura que las aprobaciones formales de la Dirección se obtienen antes de hacer modificaciones al modelo.

Se utiliza algún proceso para mantener actualizados el diccionario de datos y las reglas de sintaxis de los datos.

Se utiliza algún medio para distribuir el diccionario de datos para asegurar que éste sea accesible para las áreas de desarrollo y que los cambios se reflejan inmediatamente.

Las políticas y procedimientos de los servicios de información dirigen la clasificación de los datos, incluyendo categorías de seguridad y propiedad de datos, y si las reglas de acceso para las clases de datos están claras y apropiadamente definidas.

Los estándares definen la clasificación por defecto de los datos que no contienen un identificador de clasificación de datos.

Las políticas y procedimientos de los servicios de información dirigen lo siguiente:

- La existencia de un proceso de autorización que requiere que el propietario de los datos (tal como lo define la política de propiedad de datos) autorice todos los accesos a éstos datos, así como los atributos de seguridad de los mismos.
- Los niveles de seguridad estén definidos para cada clasificación de datos.
- Los niveles de acceso están definidos y son apropiados para la clasificación de datos. El acceso a datos confidenciales requiere de niveles de acceso explícitos y que los datos únicamente se proporcionan si existe una verdadera necesidad de acceder a ellos.

Evaluación de la suficiencia:

- **Probando que:**

Están identificados los cambios realizados en el modelo de la arquitectura de la información para confirmar que dichos cambios reflejan la información de los planes a largo y corto plazo, así como los costes y los riesgos.

La evaluación del impacto de cualquier modificación o cambio realizado en el diccionario de datos para asegurar que éstos han sido comunicados efectivamente.

Existen varios sistemas de aplicación operacional y proyectos de desarrollo para confirmar que el diccionario de datos es utilizado para la definición de datos.

El diccionario de datos recoge toda la documentación para confirmar que éste define los atributos de los datos y los niveles de seguridad para cada uno.

Es apropiada cada clasificación de datos, los niveles de seguridad, los niveles de acceso y "defaults".

Cada clasificación de datos define claramente:

- Quién puede tener acceso.
- Quién es responsable de determinar el nivel de acceso apropiado.
- La aprobación específica requerida para el acceso.
- Los requerimientos especiales para el acceso (por ejemplo, acuerdo de confidencialidad).

Evaluación del riesgo de que no se cumplan los objetivos de control:

- **Llevando a cabo:**

Mediciones ("Benchmarking") del modelo de la arquitectura de la información en relación con organizaciones similares o estándares internacionales y buenas prácticas reconocidas en la industria del sector.

Una revisión detallada del diccionario de datos para asegurar que está completo en lo referente a los elementos clave.

Una revisión detallada de los niveles de seguridad definidos para los datos delicados, con el fin de verificar que se haya obtenido la autorización apropiada para el acceso y que el acceso sea consistente con los niveles de seguridad definidos en las políticas y procedimientos de los servicios de información.

- **Identificando:**

Inconsistencias en el modelo de la arquitectura de la información , en el modelo y diccionario de datos corporativo, en los sistemas de la información asociados y en los planes a largo y corto plazo de la tecnología de la información.

Elementos obsoletos en el diccionario de datos corporativo y reglas de sintaxis de los datos en las que se haya perdido tiempo debido a cambios realizados inadecuadamente en el diccionario de datos.

Elementos de datos en los que la propiedad no haya sido clara y apropiadamente determinada.

Clasificación de datos que han sido definidos de manera inapropiada.

Niveles de seguridad de datos inconsistentes con la regla de "necesidad de acceso" ("need to know").

PO 3 Determinar la Dirección Tecnológica

OBJETIVOS DE CONTROL:

1. Planificación de la Infraestructura Tecnológica.
2. Supervisión de Futuras Tendencias y Regulaciones.
3. Contingencia de la Infraestructura Tecnológica.
4. Planes de Adquisición de Hardware y Software.
5. Estándares Tecnológicos.

TANTO LOS OBJETIVOS DE CONTROL DETALLADOS COMO LOS DE ALTO NIVEL SON AUDITADOS MEDIANTE:

Obtención de un entendimiento a través de:

- **Entrevistas:**

  Director General.

  Director de Operaciones.

  Director de Finanzas.

  Director de las TI.

  Miembros del comité de planificación de los servicios de información.

  Dirección de los servicios de información.

- **Obteniendo:**

  - Políticas y procedimientos relacionados con la planificación y el seguimiento de la infraestructura tecnológica.
  - Tareas y responsabilidades de planificación de la Dirección.
  - Objetivos y planes a largo y corto plazo de la organización.

- Objetivos y planes a largo y corto plazo de la tecnología de la información.
- Plan de adquisición de hardware y software de la tecnología de la información.
- Plan de infraestructura tecnológica.
- Estándares de la tecnología.
- Informes de estado y actas de las reuniones del comité de planificación.

Evaluación de los controles:

- **Considerando si:**

Existe un proceso para la creación y la actualización regular del plan de infraestructura tecnológica para confirmar que los cambios propuestos están siendo examinados primero para evaluar los costes y riesgos inherentes, y que la aprobación de la Dirección se obtiene antes de realizar cualquier cambio en el plan.

El plan de infraestructura tecnológica está siendo comparado con los planes a largo y corto plazo de la tecnología de la información.

Existe un proceso para la evaluación de la situación tecnológica actual de la organización para asegurar que abarca aspectos tales como la arquitectura de sistemas, la dirección tecnológica y las estrategias de migración.

La política y procedimientos de los servicios de información aseguran la consideración de la necesidad de evaluar y realizan un seguimiento de las tendencias y condiciones regulatorias tecnológicas presentes y futuras, y si éstas se tienen en consideración durante el desarrollo y mantenimiento del plan de infraestructura tecnológica.

Se planifican el impacto logístico y ambiental de las adquisiciones tecnológicas.

Las políticas y procedimientos de los servicios de información aseguran que se considera la necesidad de evaluar sistemáticamente el plan tecnológico con respecto a contingencias (por ejemplo, redundancia, resistencia, adecuación y capacidad evolutiva de la infraestructura).

La dirección de los servicios de información evalúa tecnologías de vanguardia, e incorpora tecnologías apropiadas a la infraestructura de los servicios de información actual.

Los planes de adquisición de hardware y software suelen satisfacer las necesidades identificadas en el plan de infraestructura tecnológica y si éstos se aprueban apropiadamente.

Se encuentran establecidos los estándares de la tecnología para los componentes tecnológicos descritos en el plan de infraestructura tecnológica.

Evaluación de la suficiencia:

- **Probando que:**

La dirección de los servicios de información comprende y utiliza el plan de infraestructura tecnológica.

Se han realizado cambios en el plan de infraestructura tecnológica para identificar los costes y riesgos inherentes, y que dichos cambios reflejan las modificaciones a los planes a largo y corto plazo de la tecnología de la información.

La dirección de los servicios de información comprende el proceso de seguimiento y evaluación de las nuevas tecnologías e incorpora tecnologías apropiadas a la infraestructura de los servicios de información actual.

La dirección de los servicios de información comprende el proceso de evaluar sistemáticamente el plan tecnológico en cuanto a contingencias (por ejemplo, redundancia, resistencia, adecuación y capacidad evolutiva de la infraestructura).

Existe un espacio adecuado en los servicios de información adecuado para alojar el hardware y software actualmente instalado, así como nuevo hardware y software adquirido según el plan de adquisiciones actual aprobado.

El plan de adquisición de hardware y software cumple con los planes a largo y corto plazo de la tecnología de la información, reflejando las necesidades identificadas en el plan de infraestructura tecnológica. El plan de infraestructura tecnológica dirige la utilización de la tecnología actual y futura.

Se cumple con los estándares de la tecnología y que éstos son agregados e incorporados como parte del proceso de desarrollo.

El acceso permitido es consistente con los niveles de seguridad definidos en las políticas y procedimientos de los servicios de información, y se ha obtenido la autorización apropiada para el acceso.

Evaluación del riesgo de que no se cumplan los objetivos de control:

- **Llevando a cabo:**

Mediciones ("Benchmarking") de la planificación de la infraestructura tecnológica en relación con organizaciones similares o estándares internacionales y buenas prácticas reconocidas en la industria del sector.

Una revisión detallada del diccionario de datos para verificar que está completo en lo referente a elementos clave.

Una revisión detallada de los niveles de seguridad definidos para datos confidenciales.

- **Identificando:**

Inconsistencias en el modelo de la arquitectura de la información y en el modelo y el diccionario de datos corporativo, en los sistemas de información asociados y en los planes a largo y corto plazo de la tecnología de la información.

Elementos del diccionario de datos y reglas de sintaxis de datos obsoletos.

Contingencias que no han sido consideradas en el plan de infraestructura tecnológica.

Planes de adquisición de hardware y software de la tecnología de la información que no reflejan las necesidades del plan de infraestructura tecnológica.

Estándares de la tecnología que no son consistentes con el plan de infraestructura tecnológica o con los planes de adquisición de hardware y software de la tecnología de la información.

Un plan de infraestructura tecnológica o planes de adquisición de hardware y software de la tecnología de la información que no son consistentes con los estándares de la tecnología.

Elementos clave omitidos en el diccionario de datos.

PO 4 Definir la Organización de las TI y sus relaciones

OBJETIVOS DE CONTROL:

1. Comité de planificación o de dirección de las TI.
2. Ubicación organizativa de las TI.
3. Revisión de Logros De la organización.
4. Roles y Responsabilidades.
5. Responsabilidad del aseguramiento de la calidad.
6. Responsabilidad de la Seguridad Lógica y Física.
7. Propiedad y Custodia.
8. Propiedad de Datos y Sistemas.
9. Supervisión.
10. Segregación de Tareas.
11. Asignación de Personal para las TI.
12. Descripción de Puestos o Trabajos para el Personal de las TI.
13. Personal Clave de las Tecnologías de la información.
14. Políticas y Procedimientos para personal contratado.
15. Relaciones.

TANTO LOS OBJETIVOS DE CONTROL DETALLADOS COMO LOS DE ALTO NIVEL SON AUDITADOS MEDIANTE:

Obtención de conocimiento mediante:

- **Entrevistas:**

Director General.

Director de Operaciones.

Director de Finanzas.

Director de las TI.

Responsable de Asegurar la Calidad.

Responsable de Seguridad de la información.

Miembros del comité de planificación de los servicios de información, recursos humanos y Dirección.

- **Obteniendo:**

Funciones y responsabilidades de planificación de la Dirección.

Objetivos y planes a largo y corto plazo de la organización.

Objetivos y planes a largo y corto plazo de la tecnología de la información.

Organigrama de la organización que muestre la relación entre los servicios de información y otras funciones.

Políticas y procedimientos relacionados con la organización y las relaciones de la tecnología de la información.

Políticas y procedimientos relacionados con asegurar la calidad.

Políticas y procedimientos utilizados para determinar los requerimientos de asignación de personal de los servicios de información y Organigrama de la organización de los servicios de información.

Funciones y responsabilidades de los servicios de información**.**

Descripción de los puestos clave de los servicios de información.

Informes de estado y actas de las reuniones del comité de planificación.

Evaluación de los controles:

- **Considerando si:**

Las políticas y los comunicados de la Dirección aseguran la independencia y la autoridad de los servicios de información.

Se han definido e identificado los miembros, las funciones y las responsabilidades del comité de planificación de los servicios de información.

Los estatutos del comité de planificación de los servicios de información alinean las metas del comité con los objetivos y los planes a largo y corto plazo de la organización, y con los objetivos y planes a largo y corto plazo de la tecnología de la información.

Se han establecido procesos para aumentar el conocimiento la concienciación, la comprensión y la habilidad para identificar y resolver los problemas de dirección de la información.

Las políticas consideran la necesidad de evaluar y modificar la estructura de la organización para satisfacer los objetivos y circunstancias en continuo cambio.

Existen procesos e indicadores de rendimiento para determinar la efectividad y aceptación de los servicios de información.

La Dirección se asegura que las funciones y responsabilidades están siendo llevadas a cabo.

Existen políticas que determinan las funciones y responsabilidades para todo el personal dentro de la organización con respecto a sistemas de información, control y seguridad internos.

Existen campañas regulares para aumentar la concienciación y disciplina en cuanto al control y la seguridad interna.

Existen políticas y funciones para asegurar la calidad.

La función de asegurar la calidad cuenta con la independencia suficiente con respecto al personal de desarrollo de sistemas y con una asignación de personal y experiencia adecuados para llevar a cabo sus responsabilidades.

Existen procedimientos establecidos dentro de la función de asegurar la calidad para distribuir los recursos y asegurar el cumplimiento de las pruebas y la aprobación del aseguramiento de la calidad antes de que se implementen nuevos sistemas o cambios en los mismos.

La Gerencia ha asignado formalmente la responsabilidad a lo largo de toda la organización para la formalización de políticas y procedimientos de control y seguridad internos (tanto lógicos como físicos) a algún empleado de la seguridad de la información.

El responsable de la seguridad de la información comprende adecuadamente las funciones y responsabilidades y si éstas han mostrado consistencia con respecto a la política de seguridad de la información de la organización.

La política de seguridad de la organización define claramente las responsabilidades sobre la seguridad de la información que cada propietario de activos (por ejemplo, usuarios, dirección y administradores de seguridad) debe llevar a cabo.

Existen políticas y procedimientos que cubren los datos y la propiedad de los sistemas para todas las fuentes de datos y sistemas más importantes.

Existen procedimientos para revisar y mantener los cambios en la propiedad de los datos y los sistemas regularmente.

Existen políticas y procedimientos que describen las prácticas de supervisión para asegurar que las funciones y responsabilidades son ejercidas

apropiadamente y que todo el personal cuenta con suficiente autoridad y recursos para llevar a cabo sus funciones y responsabilidades.

Existe una segregación de funciones entre los siguientes pares de unidades:

- desarrollo y mantenimiento de sistemas.
- desarrollo y operaciones de sistemas.
- desarrollo y mantenimiento de sistemas y seguridad de la información.
- operaciones y control de datos.
- operaciones y usuarios.
- operaciones y seguridad de la información.

La asignación de personal y la competencia de los servicios de información se mantiene para asegurar su habilidad para proporcionar soluciones tecnológicas efectivas.

Existen políticas y procedimientos para la evaluación y validación de las descripciones de los puestos de los servicios de información.

Existen funciones y responsabilidades para procesos clave, incluyendo actividades del ciclo de vida de desarrollo de los sistemas (requerimiento, diseño, desarrollo, pruebas), seguridad de la información, adquisición y planificación de capacidad.

Se utilizan indicadores clave de rendimiento y factores críticos de éxito para medir los resultados de los servicios de información en el logro de los objetivos de las organizaciones.

Existen políticas y procedimientos en los servicios de información para controlar las actividades de los consultores y el resto del personal contratado, asegurando así la protección de los activos de la organización.

Existen procedimientos aplicables a la tecnología de la información contratada que son adecuados y consistentes con las políticas de adquisición de la organización.

Existen procesos para coordinar, comunicar y documentar los intereses dentro y fuera del directorio de los servicios de información.

Evaluación de la suficiencia:

- **Probando que:**

El comité de planificación de los servicios de información vigila a los mismos así como sus actividades.

Existe una jerarquía de la información de los servicios de información.

La localización de los servicios de información dentro de la organización es efectiva en cuanto a facilitar la relación con la alta Gerencia.

La Dirección de los servicios de información comprende cuáles son los procesos utilizados para seguir, medir e informar sobre la realización de los servicios de información.

Se utilizan los indicadores clave para evaluar el rendimiento.

Los procesos analizan los resultados reales comparándolos con las metas a conseguir, con el fin de determinar las acciones correctivas a realizar cuando los resultados reales no alcanzan las metas.

La dirección actúa ante cualquier variación significativa con respecto a los niveles esperados de resultado.

La dirección evalúa la capacidad de respuesta y la habilidad de los servicios de información para proporcionar soluciones de la tecnología de la información que satisfagan las necesidades de usuarios y propietarios.

La Gerencia de los servicios de información conoce sus funciones y responsabilidades.

Asegurar la calidad se involucra en la prueba y aprobación de los planes de los proyectos de los servicios de información.

El personal de seguridad de la información revisa los sistemas operativos y los sistemas de aplicación esenciales.

La adecuación de los informes o documentación al evaluar la seguridad de la información (tanto lógica como física) ya existe o esta en desarrollo.

Existe suficiente conocimiento, concienciación y una aplicación consistente de las políticas y procedimientos de seguridad de la información.

El personal asiste a la formación sobre seguridad y control interno.

La propiedad de los datos y sistemas se encuentra definida para todos los activos de la información.

Los propietarios de datos y sistemas han aprobado los cambios realizados en dichos datos y sistemas.

Todos los datos y sistemas cuentan con un propietario que es responsable del control sobre los datos y sistemas.

El acceso a todos los activos de datos y sistemas es aprobado por el reponsable o los responsables de dichos activos.

La línea directa de la autoridad y supervisión asociada con el puesto está en conformidad con las responsabilidades del responsable.

Las descripciones de los puestos definen claramente tanto la autoridad como la responsabilidad.

Las descripciones de los puestos definen claramente las aptitudes de los negocios, las relaciones y las técnicas necesarias.

Las descripciones de puestos han sido comunicadas con precisión y comprendidas por el personal.

Las descripciones de los puestos para la función de los servicios de información contienen indicadores clave de rendimiento que han sido comunicados al personal.

Las funciones y responsabilidades del personal de los servicios de información corresponden tanto a las descripciones publicadas de los puestos como al organigrama.

Existen las descripciones de los puestos clave y que éstas incluyen las ordenes de la organización relativas a los sistemas de información, control y seguridad internos.

Existe precisión en la descripción de los puestos en comparación con las responsabilidades actuales de los encargados de dichos puestos.

Existe una natural y suficiente segregación y limitación de funciones dentro de los servicios de información.

El personal de la tecnología de la información mantiene la competencia.

Es apropiada la descripción de los puestos como base para la adecuación y la claridad de las responsabilidades, autoridad y criterios de rendimiento.

Las responsabilidades de la dirección contratadas han sido asignadas al personal apropiado.

Los términos de los contratos son consistentes con los estándares de los contratos de la organización, y los términos y condiciones contractuales estándar han sido revisados y evaluados por un consultor legal, y se ha llegado a un acuerdo.

Los contratos contienen cláusulas apropiadas con respecto al cumplimiento de: políticas de seguridad corporativa y control interno, y estándares de la tecnología de la información.

Existen procesos y estructuras que garantizan una coordinación efectiva y eficiente para lograr relaciones con éxito.

Evaluación del riesgo de que no se cumplan los objetivos de control:

- **Llevando a cabo:**

Mediciones ("Benchmarking") de la organización y de las relaciones en comparación con otras organizaciones similares o estándares internacionales y buenas prácticas reconocidas por la industria.

Una revisión detallada para determinar el impacto sobre la organización causada por un comité de planificación de los servicios de información no efectivo.

Una revisión detallada para medir el progreso de los servicios de información al tratar con los problemas de los sistemas de la información e implementar soluciones tecnológicas.

Una revisión detallada para evaluar la estructura de la organización, las aptitudes del personal, las funciones y responsabilidades asignadas, la propiedad de datos y sistemas, la supervisión, la segregación de funciones, etc.

Una revisión detallada del aseguramiento de la calidad para determinar su efectividad en la satisfacción de los requerimientos de la organización.

Una revisión detallada de la seguridad de la información para determinar su efectividad para proporcionar seguridad general en la organización (tanto lógica como física) y formación de conocimiento y concienciación sobre seguridad.

Una revisión detallada de los contratos para confirmar que éstos han sido ejecutados apropiadamente por ambas partes y que cumplen con los términos contractuales estándar de la organización.

- **Identificando:**

Debilidades de los servicios de información y sus actividades ocasionadas por una vigilancia poco efectiva por parte del comité de planificación de dicha función.

Lagunas, deficiencias, etc. en la estructura de la organización que traen como resultado ineficacia e ineficiencia en los servicios de información.

Estructuras de la organización inapropiadas, falta de funciones, personal insuficiente, deficiencias en competencia, funciones y responsabilidades no apropiadas, confusión en la propiedad de los datos y los sistemas, problemas de supervisión, falta de segregación de funciones, etc.

Sistemas en proceso de desarrollo, modificados o implementados que cumplen con los requerimientos de seguridad de la calidad.

Sistemas en proceso de desarrollo, modificados o implementados que cumplen con los requerimientos de seguridad (lógica, física, o ambos).

Contratos que no cumplen con los requerimientos contractuales de la organización.

Coordinación y comunicación nada efectivas entre los servicios de información y otros intereses dentro y fuera de esta función.

PO 5 Administrar las Inversiones en Tecnología de la Información

OBJETIVOS DE CONTROL:

1 Presupuesto Operativo Anual para las TI.

2 Supervisión de Coste y Beneficio.

3 Justificación de Coste y Beneficio.

TANTO LOS OBJETIVOS DE CONTROL DETALLADOS COMO LOS DE ALTO NIVEL SON AUDITADOS MEDIANTE:

Obtención de un entendimiento a través de:

- **Entrevistas:**

  Director de Finanzas.

  Director de las TI.

  Miembros del comité de planificación de los servicios de información.

  Dirección de los servicios de información.

- **Obteniendo:**

Políticas, métodos y procedimientos de la organización relacionados con la elaboración del presupuesto y los costes.

Políticas y procedimientos de los servicios de información relacionados con la elaboración del presupuesto , las actividades y los costes.

Presupuesto actual y del año anterior para los servicios de información.

Objetivos y planes de la organización a corto y largo plazo.

Objetivos y planes a corto y largo plazo de la tecnología de la información.

Funciones y responsabilidades de planificación de la Dirección.

Informes sobre las variaciones producidas y otros informes relacionados con el control y el seguimiento de las variaciones que se producen.

Informes de estado y actas de las reuniones del comité de planificación.

Evaluación de los controles:

- **Considerando si:**

El proceso de elaboración del presupuesto de los servicios de información es consistente con el proceso de la organización.

Existen políticas y procedimientos para asegurar la preparación y la aprobación adecuada de un presupuesto anual para los servicios de información, que sea consistente con el presupuesto y los planes a corto y largo plazo de la organización y los planes a corto y largo plazo de la tecnología de la información.

El proceso de elaboración del presupuesto está vinculado con la dirección de las unidades más importantes de los servicios de información que contribuyen a su preparación.

Existen políticas y procedimientos para realizar un seguimiento regular de los costes reales y compararlos con los costes presupuestados y si los costes reales tienen como base el sistema de contabilidad de costes de la organización.

Existen políticas y procedimientos para garantizar que la entrega de los servicios por parte de los servicios de información están justificados en cuanto a costes y están en línea con los costes de la industria.

Evaluación de la suficiencia:

- **Probando que:**

El presupuesto de los servicios de información es el adecuado para justificar el plan operativo anual de dicha función.

Las categorías de gastos de los servicios de información son suficientes, apropiadas y han sido clasificadas adecuadamente.

El sistema habitual para registrar, procesar e informar sobre los costes asociados con las actividades de los servicios de información de forma rutinaria es adecuado.

El proceso de revisión de los costes compara adecuadamente los costes reales con los presupuestados.

Los análisis sobre el coste y beneficio, llevados a cabo por la dirección de los grupos de usuarios afectados, la función de los servicios de información y la Dirección de la organización son revisados adecuadamente.

Las herramientas utilizadas para el control de los costes son usadas de forma efectiva y apropiada.

Evaluación del riesgo de que no se cumplan los objetivos de control:

- **Llevando a cabo:**

Mediciones ("Benchmarking") de presupuestos y costes con respecto a otras organizaciones y buenas prácticas reconocidas en la industria y estándares internacionales apropiados.

Una revisión detallada del presupuesto actual y del año inmediato anterior con respecto a los resultados reales, variaciones y acciones correctivas aplicadas.

- **Identificando:**

Los presupuestos de los sistemas de información que no están en línea con el presupuesto y los planes a corto y largo plazo de la organización, y con los planes a corto y largo plazo de la tecnología de la información.

Los costes reales tenidos en cuenta de los servicios de información que no han sido capturados.

PO 6 Comunicar los objetivos y directrices de la Dirección

OBJETIVOS DE CONTROL:

1. Entorno Positivo de Control de la Información.
2. Responsabilidad de la Dirección en cuanto a Políticas.
3. Comunicación de las Políticas de la Organización.
4. Recursos para la Implementación de las Políticas.
5. Mantenimiento de Políticas.
6. Cumplimiento de Políticas, Procedimientos y Estándares.
7. Compromiso con la Calidad.
8. Política sobre el Marco de referencia para la Seguridad y el Control Interno.
9. Derechos de la Propiedad Intelectual.
10. Políticas para Situaciones Específicas.
11. Comunicación para la concienciación sobre Seguridad en las TI.

TANTO LOS OBJETIVOS DE CONTROL DETALLADOS COMO LOS DE ALTO NIVEL SON AUDITADOS MEDIANTE:

Obtención de un entendimiento a través de:

- **Entrevistas:**

  Director General.

  Director de Operaciones.

  Director de Finanzas.

Director de las TI.

Responsable de Seguridad.

Miembros del comité de planificación de los servicios de información.

Dirección de los servicios de información.

- **Obteniendo:**

Políticas y procedimientos relacionados con el marco de referencia de control positivo y el programa de conocimiento y concienciación de la dirección, con el marco de referencia de seguridad y control interno y con el programa de calidad de los servicios de información.

Las funciones y responsabilidades de planificación de la Dirección.

Objetivos y planes a corto y largo plazo de la organización.

Objetivos y planes a corto y largo plazo de la tecnología de la información.

Informes de estado y actas de las reuniones del comité de planificación.

Un programa de comunicación.

Evaluación de los controles:

- **Considerando si:**

Las políticas y procedimientos de la organización crean un marco de referencia y un programa de conocimiento y concienciación, prestando atención específica a la tecnología de la información, propiciando un entorno de control positivo y considerando aspectos como:

- Integridad.
- Valores éticos.
- Código de conducta.
- Seguridad y control interno.
- Competencia del personal.
- Filosofía y modo de actuar de la dirección.
- Responsabilidad, atención y dirección proporcionadas por el consejo directivo o su equivalente.

La alta gerencia promueve un entorno de control positivo a través del ejemplo.

La dirección ha aceptado la responsabilidad total sobre la formulación, el desarrollo, la documentación, la promulgación, el control y la revisión periódica de las políticas que rigen las metas y directivas generales.

Existe un programa de conocimiento y concienciación formal para proporcionar comunicación y formación relacionados con el entorno positivo de control de la dirección.

Existen políticas y procedimientos de la organización para asegurar que son asignados los recursos adecuados y apropiados para implementar las políticas de la organización de manera oportuna.

Existen procedimientos apropiados para asegurar que el personal comprende las políticas y procedimientos implementados, y que se cumple con dichas políticas y procedimientos.

Las políticas y procedimientos de los servicios de información definen, documentan y mantienen una filosofía, políticas y objetivos formales que rigen la calidad de los sistemas y servicios producidos, y que éstos son consistentes con la filosofía, políticas y objetivos de la organización.

La dirección de los servicios de información asegura que la calidad de la filosofía, las políticas y objetivos es comprendida, implementada y mantenidas a todos los niveles de los servicios de información.

Existen procedimientos que consideran la necesidad de revisar y aprobar periódicamente los estándares, directivas, políticas y procedimientos clave relacionados con la tecnología de la información.

La Dirección ha aceptado la responsabilidad total sobre el desarrollo de un marco de referencia para el enfoque general de seguridad y control interno.

El documento del marco de referencia de seguridad y control interno especifica la política, propósito, objetivos, estructura administrativa, alcance dentro de la organización, asignación de responsabilidades y definición de sanciones y acciones disciplinarias de seguridad y control interno asociados con la falta de cumplimiento de las políticas de seguridad y control interno.

Las políticas de seguridad y control interno identifican el proceso de control interno de la organización e incluyen componentes de control tales como:

- Entorno de control.
- Reevaluación de los riesgos.

- Actividades de control.
- Información y comunicación.
- Seguimiento.

Existen políticas para asuntos especiales para documentar las decisiones administrativas sobre actividades, aplicaciones, sistemas y tecnologías particulares.

Evaluación de la suficiencia:

- **Probando que:**

Los esfuerzos de la dirección para fomentar el control positivo cubren aspectos clave tales como: integridad, valores éticos, código de conducta, seguridad y control interno, competencia del personal, filosofía y forma de actuar de la dirección, responsabilidad, atención y dirección.

Los empleados han recibido el código de conducta y lo comprenden.

Se han comunicado las políticas de la dirección relacionadas con el entorno de control interno de la organización.

Existe el compromiso de la dirección en cuanto a los recursos para formular, desarrollar, documentar, promulgar y controlar las políticas relativas al control interno.

Existe propiedad y habilidad para adaptarse a las condiciones en continuo cambio de las revisiones regulares de los estándares, directivas, políticas y procedimientos por parte de la dirección.

Los esfuerzos de seguimiento de la dirección aseguran la asignación adecuada y apropiada de los recursos para implementar de manera oportuna las políticas de la organización.

Los esfuerzos de reforzamiento por parte de la dirección con respecto a los estándares, directivas, políticas y procedimientos relacionados el control interno están asegurando su cumplimiento a través de toda la organización.

La filosofía, políticas y objetivos de calidad determinan el cumplimiento y la consistencia con la filosofía, políticas y procedimientos corporativos y de los servicios de información.

La dirección de los servicios de información y el personal de desarrollo y operaciones determinan la filosofía de calidad y su política de relaciones, y que

los procedimientos y objetivos son comprendidos y cumplidos por todos los niveles dentro de los servicios de información.

Los procesos de medición aseguran que los objetivos de la organización son alcanzados.

Miembros seleccionados de la dirección están involucrados y comprenden el contenido de las actividades de seguridad y control interno (por ejemplo, informes de excepción, conciliaciones, comparaciones, etc.) que están bajo su responsabilidad.

Las funciones individuales, las responsabilidades y líneas de autoridad se comunican claramente y se comprenden en todos los niveles de la organización.

Los departamentos seleccionados evalúan procedimientos para realizar un seguimiento regular de forma rutinaria sobre actividades de seguridad y control interno (por ejemplo, informes de excepción, conciliaciones, comparaciones, etc.) y existe un proceso para proporcionar retroalimentación a la dirección.

La documentación del sistema seleccionado confirma que las decisiones administrativas del sistema específico han sido documentadas y aprobadas de acuerdo con las políticas y procedimientos de la organización.

La documentación del sistema seleccionado confirma que las decisiones administrativas con respecto a actividades, sistemas de aplicación o tecnologías particulares han sido aprobadas por la Dirección.

Evaluación del riesgo de que no se cumplan los objetivos de control:

- **Llevando a cabo:**

Mediciones ("Benchmarking") del marco de referencia del control de la información y del programa de conocimiento y concienciación de la dirección en relación con organizaciones similares o estándares internacionales y buenas prácticas de la industria reconocidas.

Una revisión detallada y de proyectos aprobados de seguridad y control interno para determinar que los proyectos fueron aprobados y tomaron como base un análisis de los riesgos y, coste y beneficio.

- **Identificando:**

Un marco de referencia de control débil que ponga en duda el compromiso de la dirección en cuanto al fomento de un entorno de control interno positivo a través de la organización.

Fallos en la dirección para comunicar de forma efectiva sus políticas relacionadas con el entorno de control interno de la organización.

Falta de recursos asignados para formular, desarrollar, documentar, promulgar y controlar políticas que cubren el entorno de control interno.

Estándares, directivas, políticas y procedimientos no actualizados.

Incumplimiento por parte de la dirección para asegurar el cumplimiento de los estándares, directivas, políticas y procedimientos a través de la organización.

Deficiencias en los servicios de información, en su compromiso con la calidad o en su habilidad para definir, documentar, mantener y comunicar efectivamente una filosofía, políticas y objetivos de calidad.

Debilidades en el marco de referencia de la seguridad y el control interno de la organización y en los servicios de información.

Ausencia de políticas para asuntos específicos requeridas para dirigir actividades, aplicaciones y tecnologías particulares.

PO 7 Administrar los Recursos Humanos

OBJETIVOS DE CONTROL:

1. Selección y Promoción de Personal.
2. Cualificaciones del Personal.
3. Roles y Responsabilidades.
4. Formación del Personal.
5. Formación Cruzado o copias de seguridad del Personal.
6. Procedimientos de acreditación del Personal.
7. Evaluación del Rendimiento del Trabajo del Empleado.
   Cambio de Puesto y Despido.

TANTO LOS OBJETIVOS DE CONTROL DETALLADOS COMO LOS DE ALTO NIVEL SON AUDITADOS MEDIANTE:

Obtención de un entendimiento a través de:

- **Entrevistas:**

Responsable de Recursos Humanos de la Organización y personal seleccionado.

Responsable de Seguridad.

Personal seleccionado de seguridad.

Director de los servicios de información.

Responsable de Recursos Humanos de los servicios de información.

Directores seleccionados de los servicios de información.

Personal seleccionado de los servicios de información.

Personal seleccionado asociado con posiciones sensibles en los servicios de información.

- **Obteniendo:**

Políticas y procedimientos relacionados con la dirección de los recursos humanos.

Descripciones de los puestos, formas de evaluación del trabajo realizado y formas de desarrollo y formación.

Expedientes de personal para puestos seleccionados y resto del personal.

Evaluación de los controles:

- **Considerando si:**

Se utilizan criterios para incorporar y seleccionar personal para cubrir puestos vacantes.

Las especificaciones de las habilidades y conocimientos necesarios para los puestos de staff tienen en consideración los requerimientos relevantes de los profesionales cuando sea apropiado.

La dirección y los empleados aceptan el proceso de las competencias del puesto.

Los programas de formación son consistentes con los requerimientos mínimos documentados de la organización relacionados con la educación, el

conocimiento y la concienciación generales que cubren los temas de seguridad de la información.

La dirección está comprometida con la formación y el desarrollo profesional de sus empleados.

Las brechas técnicas y administrativas están identificadas y si se están llevando a cabo las acciones apropiadas para manejar estas brechas.

Se dan los procesos de formación cruzado y copias de seguridad de personal habitualmente para las funciones de puestos críticos.

Se da un refuerzo de la política de vacaciones ininterrumpidas.

Si el proceso de liquidación de seguridad de la organización es adecuado.

Los empleados son evaluados tomando como base un conjunto estándar de perfiles de competencia para el puesto y si se llevan a cabo evaluaciones de forma periódica.

Los procesos de despido y cambio de puesto aseguran la protección de los recursos de la organización.

Las políticas y procedimientos de recursos humanos concuerdan con las leyes y regulaciones aplicables.

Evaluación de la suficiencia:

- **Probando que:**

Las acciones de incorporación y selección, así como los criterios de selección reflejan objetividad y relevancia con respecto a los requerimientos del puesto.

El personal cuenta con los conocimientos adecuados para desarrollar las funciones de su puesto o área de responsabilidad.

Existen descripciones de los puestos, y éstas son revisadas y se mantienen actualizadas.

Los expedientes del personal contienen un reconocimiento del mismo en cuanto a la comprensión del programa general de educación, concienciación y conocimiento de la organización.

Se da el proceso de formación y educación continua para el personal asignado a funciones clave.

El personal de seguridad de la información ha recibido la formación apropiada en procedimientos y técnicas de seguridad.

La dirección y el personal de los servicios de información tienen conocimiento, concienciación y comprenden las políticas y procedimientos de la organización.

Los procedimientos de investigación de los despidos son consistentes con las leyes aplicables que rigen la confidencialidad.

El conocimiento de los objetivos del negocio por parte del personal asignado a las funciones clave de los servicios de información incluye la filosofía de los controles internos y los conceptos de control y seguridad de los sistemas de información.

Evaluación del riesgo de que no se cumplan los objetivos de control:

- **Llevando a cabo:**

Mediciones ("Benchmarking") de las actividades de recursos humanos en relación con organizaciones similares o estándares internacionales y buenas prácticas reconocidas en la industria del sector.

Una revisión detallada de las actividades de la dirección de recursos humanos de los servicios de información.

- **Identificando:**

Causas y objeciones o quejas por parte de los candidatos potenciales y reales al puesto.

Discrepancias en las actividades de selección, transferencia, promoción y despido relacionadas con:

- Políticas y procedimientos no seguidos.
- Acciones no aprobadas por parte de la dirección correspondiente.
- Acciones no basadas en especificaciones de puestos y calificación del personal.

Personal:

- Calificado inapropiadamente.

- Cuyas oportunidades de formación y desarrollo no están ligados a las diferencias con respecto a la competencia.
- Cuyas evaluaciones de rendimiento no existen o no dan soporte al puesto ocupado y las funciones llevadas a cabo.
- Cuya investigación de seguridad asociada a la contratación no fue llevada a cabo.
- Cuyas investigaciones periódicas de seguridad no han sido llevadas a cabo.

Insuficiencias en los programas de formación y en las actividades de desarrollo personal.

Insuficiencias en la formación cruzada y copias de seguridad del personal clave.

Reconocimientos de políticas de seguridad que no han sido firmadas.

Presupuestos y tiempos inadecuados asignados a la formación y desarrollo del personal.

Informes de asistencia del personal que lleva a cabo funciones clave que no indican que se han tomado días de asueto y vacaciones.

PO 8 Asegurar el Cumplimiento con los requerimientos Externos

OBJETIVOS DE CONTROL:

1. Revisión de los requerimientos Externos.
2. Prácticas y Procedimientos para el Cumplimiento de Requerimiento Externos.
3. Cumplimiento de Seguridad y Ergonomía.
4. Privacidad, Propiedad Intelectual y Flujo de Datos.
5. Comercio Electrónico.
6. Cumplimiento con los Contratos de Seguros.

TANTO LOS OBJETIVOS DE CONTROL DETALLADOS COMO LOS DE ALTO NIVEL SON AUDITADOS MEDIANTE:

Obtención de un entendimiento a través de:

- **Entrevistas:**

  Consejo legal de la organización.

  Responsable de Recursos Humanos de la Organización.

Dirección de los servicios de información.

- **Obteniendo:**

Requerimiento relevantes gubernamentales o externos (por ejemplo, leyes, legislaciones, guías, regulaciones y estándares) con respecto a relaciones y revisiones de requerimiento externos, aspectos de seguridad y salud (incluyendo ergonomía), aspectos de confidencialidad, requerimiento de seguridad de los sistemas de información y transmisión de datos criptográficos - tanto nacional como internacional.

Estándares y declaraciones contables nacionales o internacionales relacionadas con el uso de comercio electrónico.

Reglamentos sobre impuestos relacionados con el uso del comercio electrónico.

Estándares, políticas y procedimientos sobre:

- Revisiones de requerimiento externos.
- Seguridad y salud (incluyendo ergonomía).
- Confidencialidad.
- Seguridad.
- Datos clave introducidos, procesados, almacenados, extraídos y transmitidos.
- Comercio electrónico.
- Seguros.

Copias de todos los contratos con socios de comercio electrónico y con el proveedor de intercambio electrónico de datos (EDI), si aplica copias de todos los contratos de seguros relacionados con la función de los servicios de información

Orientación del consejo sobre los requerimientos "uberrimae fidei" (de buena fe) para los contratos de seguros (Uberrimae fidei requiere que ambas partes divulguen completamente a la otra todo lo relacionado con el riesgo. En caso de no mostrarse buena fe en este sentido, el contrato será anulable por la parte agraviada y no podrá se puesto en vigor nuevamente por la parte culpable).

Informes de auditoría de auditores externos, proveedores de servicios como terceras partes y dependencias gubernamentales.

Evaluación de los controles:

- **Considerando si:**

Existen políticas y procedimientos para:

- Asegurar las acciones correctivas apropiadas relacionadas con la revisión oportuna de los requerimientos externos y si existen procedimientos para asegurar el cumplimiento continuo.
- Coordinar la revisión de los requerimientos externos, con el fin de asegurar que se aplican oportunamente las acciones correctivas que garantizan el cumplimiento de estos requerimiento externos.
- Dirigir protección apropiada, así como objetivos de seguridad y salud.
- Asegurar que se proporciona formación y educación en seguridad y salud apropiadamente a todos los empleados.
- Controlar el cumplimiento de las leyes y regulaciones aplicables de seguridad y salud.
- Proporcionar la dirección y enfoque adecuados sobre confidencialidad de tal manera que todos los requerimientos legales caigan dentro de este alcance.
- Informar a los aseguradores acerca de todos los cambios materiales realizados en el entorno de los servicios de información.
- Asegurar el cumplimiento con los requerimientos de los contratos de seguros
- Asegurar que se lleven a cabo las actualizaciones necesarias cuando se inicia un contrato de seguros nuevo o modificado.

Los procedimientos de seguridad están de acuerdo con todos los requerimientos legales y si éstos están siendo tomados en cuenta adecuadamente, incluyendo:

- Protección con "passwords" o contraseñas y software para limitar el acceso.
- Procedimientos de autorización.
- Medidas de seguridad de los terminales.
- Medidas de encriptamiento de los datos.
- Controles contra incendios.
- Protección contra virus.
- Seguimiento oportuno de los informes de violaciones.

Evaluación de la suficiencia:

- **Probando que:**

Las revisiones de los requerimientos externos:

- Son actuales, completas y suficientes en cuanto a aspectos legales, gubernamentales y regulatorios.
- Traen como resultado una rápida acción correctiva.

Las revisiones de seguridad y salud son llevadas a cabo dentro de los servicios de información para asegurar el cumplimiento de los requerimientos externos.

Las áreas problemáticas que no cumplan con los estándares de seguridad y salud son rectificadas.

El cumplimiento de los servicios de información en cuanto a las políticas y procedimientos de confidencialidad y seguridad.

Los datos transmitidos a través de las fronteras internacionales no violan las leyes de exportación.

Los contratos existentes con los proveedores de comercio electrónico consideran adecuadamente los requerimientos especificados en las políticas y procedimientos de la organización.

Los contratos de seguros existentes consideran adecuadamente los requerimientos especificados en las políticas y procedimientos de la organización.

En donde se han impuesto límites regulatorios a los tipos de encriptamiento que pueden ser utilizados (por ejemplo, la longitud de la llave), el encriptamiento aplicado cumple con las regulaciones.

En donde las regulaciones o procedimientos internos requieran la protección o encriptamiento especial de ciertos elementos de datos (por ejemplo, números PIN bancarios, Números de expedientes de Impuestos, de Inteligencia Militar), dicha protección y encriptamiento son proporcionados a estos datos.

Los procesos EDI reales desplegados por la organización aseguran el cumplimiento con las políticas y procedimientos de la organización y con los contratos individuales del socio de comercio electrónico (y del proveedor EDI).

Evaluación del riesgo de que no se cumplan los objetivos de control:

- **Llevando a cabo:**

Mediciones ("Benchmarking") del cumplimiento de los requerimientos externos, actividades EDI y requerimiento de contratos de seguros comparando con

organizaciones similares o estándares internacionales y buenas prácticas reconocidas en la industria correspondiente

Una revisión detallada de los archivos de requerimiento externos para asegurar que se han llevado a cabo acciones correctivas, o bien, que están siendo implementadas.

Una revisión detallada de los informes de seguridad para evaluar si la información clave y confidencial (definida como tal por procedimientos internos o por regulaciones externas) está siendo protegida apropiadamente en cuanto a seguridad y confidencialidad.

- **Identificando:**

Requerimiento externos que no han sido cumplidos por la organización.

Acciones significativas ni resueltas, ni corregidas en respuesta a las revisiones de requerimiento externos.

Riesgos de seguridad y salud (incluyendo ergonomía) en el entorno de trabajo que no han sido considerados.

Debilidades en la confidencialidad y la seguridad relacionadas con flujos de datos y flujo de datos internacionales.

Interrupciones en el comercio electrónico.

Debilidades en los contratos con socios comerciales relacionadas con los procesos de comunicación, mensajes de transacción, seguridad y almacenamiento de datos.

Debilidades en las relaciones de confianza con socios comerciales.

Debilidades y equivocaciones en la cobertura del seguro.

Incumplimientos de los términos del contrato.

PO 9 Evaluar Riesgos

OBJETIVOS DE CONTROL:

1. Evaluación de los riesgos del Negocio.
2. Enfoque de Evaluación de los riesgos.
3. Identificación de los riesgos.
4. Medición de los riesgos.
5. Plan de Acción de los riesgos.
6. Aceptación de los riesgos.
7. Selección de Protección.
8. Compromiso de Evaluación de los riesgos.

TANTO LOS OBJETIVOS DE CONTROL DETALLADOS COMO LOS DE ALTO NIVEL SON AUDITADOS MEDIANTE:

Obtención de un entendimiento a través de:

- **Entrevistas:**

  Dirección de los servicios de información.

  Personal seleccionado de los servicios de información.

  Personal seleccionado de gestión de los riesgos.

- **Obteniendo:**

  Políticas y procedimientos relacionados con la evaluación de los riesgos.

  Documentos de evaluación de los riesgos del negocio.

  Documentos de evaluación de los riesgos operativos.

  Documentos de evaluación de los riesgos de los servicios de información.

  Detalles de la base sobre la cual se miden los riesgos y la exposición a los riesgos.

  Expedientes de evaluación de los riesgos para personal seleccionado

  Políticas de seguros que cubren el riesgo residual.

Evaluación de los controles:

- **Considerando si:**

Existe un marco de referencia para la evaluación sistemática de los riesgos, incorporando los riesgos de la información relevantes para el logro de los objetivos de la organización y formando una base para determinar la forma en la que los riesgos deben ser manejados a un nivel aceptable.

El enfoque de evaluación de los riesgos asegura la evaluación actualizada regular de los mismos tanto a nivel global como a nivel específico de sistemas.

Existen procedimientos de evaluación de los riesgos para determinar que los riesgos identificados incluyen factores tanto externos como internos y toman en consideración los resultados de las auditorías, inspecciones, e incidentes identificados.

Los objetivos de toda la organización están incluidos en el proceso de identificación de riesgos.

Los procedimientos para el seguimiento de los cambios en la actividad de procesamiento de los sistemas determinan que los riesgos y la exposición de los sistemas son ajustados oportunamente.

Existen procedimientos para el seguimiento y mejorar continuos de la evaluación de los riesgos y controles de mitigación.

La documentación de evaluación de los riesgos incluye:

- Una descripción de la metodología de evaluación de los riesgos.
- La identificación de exposiciones significativas y los riesgos correspondientes.
- Los riesgos y exposiciones correspondientes considerados.

Se incluyen técnicas de probabilidad, frecuencia y análisis de amenazas en la identificación de los riesgos.

El personal asignado para la evaluación de los riesgos está adecuadamente cualificado.

Existe un enfoque cuantitativo , o cualitativo (o ambos) formal para la identificación y medición de los riesgos, amenazas y exposiciones.

Se utilizan cálculos y otros métodos en la medición de los riesgos, amenazas y exposiciones.

El plan de acción contra riesgos se utiliza en la implementación de las medidas apropiadas para mitigar los riesgos, amenazas y exposiciones.

La aceptación del riesgo residual tiene en cuenta:

- La política de la organización.
- La identificación y medición de los riesgos.
- La incertidumbre inherente al enfoque de evaluación de los riesgos.
- El coste y la efectividad de implementar medidas de seguridad y controles.

La cobertura de los seguros compensa el riesgo residual.

Evaluación de la suficiencia:

- **Probando que:**

Se cumple con el marco de referencia de evaluación de los riesgos en cuanto a que las evaluaciones de los mismos son actualizadas regularmente para reducir el riesgo a un nivel aceptable.

La documentación de evaluación de los riesgos cumple con el marco de referencia de evaluación de los mismos y se mantiene y prepara apropiadamente.

La dirección y el personal de los servicios de información tienen conocimiento y concienciación y están involucrados en el proceso de evaluación de los riesgos.

La dirección comprende los factores relacionados con los riesgos y la probabilidad de amenazas

El personal relevante comprende y acepta formalmente el riesgo residual.

Los informes emitidos a la Dirección para su revisión y acuerdo, con los riesgos identificados y utilización del seguimiento de actividades, de reducción de los riesgos, son oportunos

El enfoque utilizado para analizar los riesgos tiene como resultado una medida cuantitativa o cualitativa (o ambas) de la exposición al riesgo.

Los riesgos, amenazas y exposiciones identificados por la dirección y los atributos relacionados con ellos son utilizados para detectar cualquier amenaza específica.

El plan de acción contra riesgos esta actualizado e incluye controles económicos y medidas de seguridad para mitigar la exposición al mismo.

Existen prioridades desde la más alta hasta la más baja, y que existe una respuesta apropiada para cada riesgo:

- Control planificado preventivo de mitigación.
- Control secundario detectivo.
- Control terciario correctivo.

Los escenarios de riesgo frente al control están documentados, actualizados y comunicados al personal apropiado.

Existe suficiente cobertura de los seguros con respecto al riesgo residual aceptado y éste se considera respecto a varios escenarios de amenaza, incluyendo:

- Incendio, inundaciones, terremotos, tornados, terrorismo y otros desastres naturales no predecibles.
- Violaciones de responsabilidades fiduciarias del empleado.
- Interrupción del negocio, ganancias, perdidas, clientes perdidos, etc.
- Otros riesgos no cubiertos generalmente por la tecnología de la información y planes de riesgo y continuidad del negocio.

Evaluación del riesgo de que no se cumplan los objetivos de control:

- **Llevando a cabo:**

Mediciones ("Benchmarking") del marco de referencia de evaluación de los riesgos con respecto a organizaciones similares o estándares internacionales y buenas prácticas reconocidas en la industria.

Una revisión detallada del enfoque de la evaluación de los riesgos utilizado para identificar, medir y mitigar los riesgos a un nivel aceptable de riesgo residual.

- **Identificando:**

Riesgos no identificados.

Riesgos que no han sido medidos.

Riesgos no considerados y manejados a un nivel aceptable.

Evaluaciones de los riesgos obsoletos y evaluaciones de la información de riesgo obsoleta.

Medidas incorrectas cuantitativas y cualitativas de los riesgos, amenazas y exposiciones.

Planes de acción contra riesgos que no aseguren controles económicos y medidas de seguridad.

Falta de aceptación formal del riesgo residual.

Cobertura inadecuada de seguros.

PO 10 Gestionar los Proyectos

OBJETIVOS DE CONTROL:

1. Estructura de la Gestión de Proyectos.
2. Participación del Departamento de Usuario en el Inicio del Proyecto.
3. Miembros del Equipo del Proyecto y Responsabilidades.
4. Definición del Proyecto.
5. Aprobación del Proyecto.
6. Aprobación de las Fases del Proyecto.
7. Plan Maestro del Proyecto.
8. Plan para asegurar la Calidad del Sistema.
9. Planificación de los Métodos de Aseguramiento.
10. Gestión Formal del Riesgo del Proyecto.
11. Plan de Pruebas.
12. Plan de Formación.
13. Plan de Revisión Post-implementación.

TANTO LOS OBJETIVOS DE CONTROL DETALLADOS COMO LOS DE ALTO NIVEL SON AUDITADOS MEDIANTE:

Obtención de un entendimiento a través de:

- **Entrevistas:**

  Director de Calidad de la Organización.

  Director o Coordinador de Calidad de los Proyectos.

  Equipo del proyecto.

  Jefe de Proyecto.

Coordinador de Aseguramiento de Calidad.

Director de Seguridad.

Miembros del comité de planificación de los servicios de información.

Dirección de los servicios de información.

- **Obteniendo:**

Políticas y procedimientos relacionados con el marco de referencia de la dirección de proyectos.

Políticas y procedimientos relacionados con la metodología de dirección de proyectos.

Políticas y procedimientos relacionados con los planes para asegurar la calidad.

Políticas y procedimientos relacionados con los métodos para asegurar la calidad.

Plan Maestro del Proyecto de Software (Software Project Master Plan (SPMP)).

Plan para asegurar la Calidad del Software (Software Quality Assurance Plan (SQAP)).

Informes de estado del proyecto.

Informes de estado y actas de las reuniones del comité de planificación.

Informes de Calidad del Proyecto.

Evaluación de los controles:

- **Considerando si:**

El marco de referencia de la dirección de proyectos:

- Define el alcance y los límites para la dirección de proyectos.
- Asegura que las demandas del proyecto son revisadas en cuanto a su consistencia con el plan operativo aprobado y si los proyectos son priorizados de acuerdo con este plan.

- Define la metodología de la dirección de los proyectos que debe ser adoptada y aplicada en cada proyecto emprendido, incluyendo:

- Planificación del proyecto.
- Asignación del personal.
- Asignación de responsabilidades y autoridad.
- Distribución de tareas.
- Presupuestos de los Tiempos y recursos.
- Puntos de revisión.
- Puntos de verificación.
- Aprobaciones.

- Es suficiente y esta actualizado.
- Asegura la participación de la dirección del departamento de usuario afectado en la definición y autorización de un proyecto de desarrollo, implementación o modificación.
- Especifica la base sobre la cual el personal es asignado a los proyectos
- Define las responsabilidades y la autoridad de los miembros del equipo del proyecto.
- Asegura la creación clara y por escrito de los estatutos que definen la naturaleza y alcance del proyecto antes de comenzar a trabajar sobre el mismo.
- Proporciona un documento inicial de definición del proyecto que incluye los estatutos sobre la naturaleza y alcance del mismo.
- Incluye las siguientes razones para llevar a cabo el proyecto, entre ellas:

- Una definición del problema a ser resuelto o del proceso a ser mejorado.
- Una definición de la necesidad del proyecto expresada en términos de incrementar la habilidad de la organización para alcanzar las metas.
- Un análisis de las deficiencias relevantes de los sistemas existentes.
- Las oportunidades que se abren al incrementar la eficiencia y hacer más económica la operación.
- El control interno y la necesidad de seguridad deben satisfacerse por los proyectos.

- Considera la manera en que los estudios de viabilidad de los proyectos propuestos deben ser preparados y aprobados por la Dirección, incluyendo:

- El entorno del proyecto - hardware, software, telecomunicaciones.
- El alcance del proyecto - lo que este incluirá y excluirá en la primera implementación y en las subsecuentes.
- Las limitaciones del proyecto - lo que debe retenerse durante este proyecto, aún cuando las oportunidades de mejora a corto plazo parezcan obvias.

- Los beneficios y costes del proyecto.

- Delinea la manera en la que cada fase del proceso de desarrollo (por ejemplo, preparación de estudios de viabilidad, definición de requerimiento, diseño del sistema, etc.) debe ser aprobada antes de proceder a la siguiente fase del proyecto (por ejemplo, programación, pruebas del sistema, pruebas de transacciones, pruebas en paralelo, etc.).
- Requiere el desarrollo de un SPMP para cada proyecto y especifica la manera en la que el control debe mantenerse a través de la vida del proyecto, así como períodos (puntos de revisión) y presupuestos del mismo.
- Cumple con el estándar de la organización para SPMPs o, en caso de no existir éste, con algún otro estándar apropiado.
- Requiere el desarrollo de un SQAP para cada proyecto, asegura que éste se encuentre integrado con el SPMP y que sea revisado y acordado formalmente por todas las partes involucradas.
- Delinea la manera en la que el programa de gestión formal de los riesgos del proyecto elimina o minimiza los riesgos relacionados con el mismo.
- Asegura el desarrollo de un plan de pruebas para cada proyecto de desarrollo, implementación y modificación.
- Asegura el desarrollo de un plan adecuado para la formación de personal y de las funciones de los servicios de información para cada proyecto de desarrollo, implementación y modificación. Se realiza un seguimiento y se informa a la Dirección sobre los puntos de revisión y compra de software, compra de hardware, programación por contrato, actualizaciones de redes, etc.).

Los puntos de revisión y costes que exceden los importes y tiempos presupuestados requieren la aprobación de la dirección correspondiente de la organización.

SQAP cumple con el estándar de la organización para SQAPs, o en caso de no existir éste, con los criterios seleccionados anteriormente.

Las tareas de aseguramiento SQAP soportan la acreditación de los sistemas nuevos o modificados y aseguran que los estatutos de control interno y seguridad cumplen con los requerimientos .

Todo el personal asignado al proyecto ha sido informado sobre el SPMP y el SQAP y está de acuerdo sobre el resultado final.

El proceso de post-implementación es una parte integral del marco de referencia de la dirección del proyecto para asegurar que los sistemas de información nuevos o modificados han aportado los beneficios planificados.

Evaluación de la suficiencia:

- **Probando que:**

La metodología de la dirección de proyectos y todos los requerimientos son seguidos con consistencia.

La metodología de la dirección de proyectos se comunica a todo el personal apropiado involucrado en el proyecto.

La definición escrita de la naturaleza y alcance del proyecto concuerda con un patrón estándar.

La naturaleza y el alcance del personal involucrado en la definición y autorización del proyecto, así como la conformidad con la participación esperada de dicho personal se ajusta a lo estipulado por el marco de referencia de gestión de proyectos.

La asignación de los miembros del personal al proyecto y la definición de responsabilidades y autoridad de los miembros del equipo son respetados.

Existe evidencia de una definición clara y por escrito de la naturaleza y alcance del proyecto antes de comenzar a trabajar sobre el mismo.

Se ha aprobado y preparado un estudio de viabilidad.

Se obtienen las aprobaciones por parte de la dirección de los sistemas de información y de los responsables para cada fase del proyecto de desarrollo.

Cada fase del proyecto se completa y se obtienen las aprobaciones apropiadas según los requerimientos del SPMP.

Se han desarrollado y aprobado el SPMP y el SQAP de acuerdo con el marco de referencia de la dirección de proyectos.

El SPMP y el SQAP son suficientemente específicos y detallados.

Las actividades e informes obligatorios identificados han sido realmente ejecutados (por ejemplo, que se han llevado a cabo reuniones del Comité Ejecutivo de Planificación, reuniones para el proyecto o similares, se han registrado actas de las reuniones y éstas han sido distribuidas a las partes relevantes, se preparan y distribuyen informes a dichas partes relevantes).

Se ha desarrollado y aprobado un plan de pruebas de acuerdo con el marco de referencia de la dirección de proyectos y éste es suficientemente específico y detallado.

Las actividades e informes obligatorios identificados en el plan de pruebas han sido realmente ejecutados.

Existen criterios de acreditación utilizados para el proyecto y éstos:

- Se derivan de metas e indicadores de rendimiento.
- Se derivan de requerimiento cuantitativos acordados.
- Aseguran que se satisfacen los requerimientos de control interno y seguridad.
- Están relacionados con el "Qué" esencial frente el "cómo" arbitrario.
- Definen un proceso formal de aprobación y no aprobación.
- Son capaces de una demostración objetiva dentro de un período del tiempo limitado.
- No redefinen simplemente los requerimientos para el diseño de los documentos.

El programa de gestión de los riesgos ha sido utilizado para identificar y eliminar o por lo menos minimizar los riesgos relacionados con el proyecto.

Se ha cumplido con el plan de pruebas, así como las funciones de programación y seguridad de la calidad que el personal asignado al proyecto, ha creado y revisado, y se ha cumplido con el proceso de aprobación según lo esperado.

Se ha preparado un plan para la formación del personal de los servicios de información y para el personal asignado al proyecto, se ha dado el tiempo suficiente para completar las actividades de formación necesarias, y ha sido utilizado para el proyecto.

Se ha cumplido y seguido un plan de revisión post-implementación para el proyecto.

Evaluación del riesgo de que no se cumplan los objetivos de control:

- **Llevando a cabo:**

Mediciones ("Benchmarking ") del marco de referencia de dirección de proyectos respecto a organizaciones similares o estándares internacionales y buenas prácticas reconocidas en la industria.

Una revisión detallada de:

El plan maestro del proyecto para determinar el alcance de la participación del personal y la adecuación del proceso general para definir, autorizar y ejecutar el proyecto, incluyendo:

- Definición de las funciones del sistema.
- Viabilidad, dadas las limitaciones del proyecto.
- Determinación de los costes y beneficios del sistema.
- Propiedad de los controles del sistema.
- Impacto e integración en otros sistemas.
- Compromiso de los recursos (de personal y económicos) por parte del jefe del proyecto.
- Definición de las responsabilidades y autoridad de los participantes en el proyecto.
- Criterios de aceptación deseables y alcanzables.
- Puntos de revisión y verificación en la autorización de las diferentes fases del proyecto.

- Elaboración de las gráficas de Gantt, logs de problemas, resúmenes de reuniones, etc. en la dirección del proyecto.
- Informes de calidad para determinar si existen problemas sistemáticos en el proceso de planificación de la seguridad de la calidad de los sistemas en la organización.
- El programa de gestión formal de los riesgos del proyecto para determinar si se han identificado y eliminado, o por lo menos minimizado.
- La ejecución del plan de formación para determinar que se ha aprobado completamente todo el proyecto de desarrollo, implementación o modificación del sistema.
- La ejecución del plan de formación para determinar que éste ha preparado adecuadamente a todo el personal en el uso del sistema.
- La revisión post-implementación para determinar si los beneficios otorgados corresponden con los planificados.

- **Identificando:**

Proyectos que:

- Son administrados inadecuadamente.
- Han excedido fechas claves.
- Han excedido costes.
- Son obsoletos.
- No han sido autorizados.
- No son técnicamente factibles.
- No son económicos.
- No consiguen los beneficios planificados.
- No contienen puntos de verificación.
- No son aprobados en puntos de verificación claves.
- No han sido acreditados para implementación.
- No satisfacen los requerimientos de control interno y seguridad.
- No eliminan o mitigan los riesgos.
- No han sido probados completamente.
- Necesitan una formación no llevada a cabo o inadecuada para el sistema en Proceso de implementación.
- No han contado con una revisión post-implementación.

PO 11 Gestionar la Calidad

OBJETIVOS DE CONTROL:

1. Plan General de Calidad.
2. Enfoque de Aseguramiento de la Calidad.
3. Planificación del Aseguramiento de la Calidad.
4. Revisión de Adherencia del Aseguramiento de la Calidad a los Estándares y Procedimientos de las TI.
5. Metodología del Ciclo de vida de desarrollo de los sistemas.
6. Metodología del Ciclo de vida de desarrollo de los sistemas para los cambios importantes en la Tecnología Existente.
7. Actualización de la Metodología del Ciclo de vida de desarrollo de los sistemas.
8. Coordinación y Comunicación.
9. Estructura de Adquisición y Mantenimiento para la Infraestructura de la Tecnología.
10. Relaciones del Implementador de la tercera parte.
11. Estándares de Documentación del Programa.
12. Estándares de Prueba del Programa.
13. Estándares de Pruebas del Sistema.
14. Pruebas en Paralelo/Piloto.

15. Documentación de Pruebas del Sistema.
16. Evaluación de Adherencia del Aseguramiento de la Calidad a los Estándares de desarrollo.
17. Revisión del Aseguramiento de la Calidad para la consecución de los Objetivos de las TI.
18. Métricas de Calidad.
19. Informes de las Revisiones de Aseguramiento de la Calidad.

TANTO LOS OBJETIVOS DE CONTROL DETALLADOS COMO LOS DE ALTO NIVEL SON AUDITADOS MEDIANTE:

Obtención de un entendimiento a través de:

- **Entrevistas:**

  Director General

  Miembros del comité de planificación de los servicios de información

  Director de las TI

  Responsable de Seguridad

  Director de Calidad de la Organización

  Director de Calidad de los servicios de información

  Dirección de los servicios de información

  Propietarios y patrocinadores del sistema

- **Obteniendo:**

  Políticas y procedimientos relacionados con la seguridad de la calidad, el ciclo de vida de desarrollo de los sistemas y la documentación de éstos.

  Funciones y responsabilidades de planificación de la dirección.

  Plan estratégico, política de calidad, manual de calidad y plan de calidad de la organización del Plan estratégico, política de calidad, manual de calidad, plan de calidad y plan de dirección de la configuración de los servicios de información.

  Gráficas de todas las funciones de aseguramiento de la calidad.

Actas de las reuniones individuales de planificación de la calidad.

Actas de las reuniones convocadas para la revisión de la metodología del ciclo de vida de desarrollo de los sistemas.

Copias de las revisiones de metodología del ciclo de vida de desarrollo de los sistemas.

Informes de estado y actas de las reuniones del comité de planificación.

Evaluación de los controles:

- **Considerando si:**

El plan de calidad:

- Toma como base los planes a corto y largo plazo de la organización.
- Fomenta la filosofía de mejora continua y responde a las preguntas básicas de qué, quién y cómo.
- Está completo y actualizado.

El plan de calidad de los servicios de información:

- Se basa en el plan general de calidad de la organización y los planes a corto y largo plazo de la tecnología de la información.
- Fomenta la filosofía de mejora continua y responde a las preguntas básicas qué, quién y cómo.
- Está completo y actualizado.

Si el enfoque estándar de calidad existe, y si éste:

- Es aplicable tanto a las actividades generales como a las específicas del proyecto.
- Es escalable y, de esta manera, aplicable a todos los proyectos.
- Se comprende por todo el personal involucrado en un proyecto y en las actividades de para asegurar la calidad.
- Es aplicable a través de todas las fases de un proyecto.

El enfoque estándar sobre seguridad de la calidad indica los tipos de actividades para asegurar la calidad (y especifica revisiones, auditorías, inspecciones, etc.) a ser llevados a cabo para alcanzar los objetivos del plan general de calidad.

La planificación para asegurar la calidad recoge el alcance y calendario de las actividades para asegurar la calidad.

Las revisiones de la calidad evalúan el cumplimiento general de los estándares, políticas y procedimientos de los servicios de información.

La Dirección ha definido e implementado estándares, políticas y procedimientos de los servicios de información, incluyendo una metodología formal del ciclo de vida de desarrollo de los sistemas adquirida, desarrollada internamente o una combinación de ambas.

La metodología del ciclo de vida de desarrollo de los sistemas:

- Dirige el proceso de desarrollar, adquirir, implementar y mantener sistemas de la información automatizados y tecnología afín.
- Soporta y fomenta los esfuerzos de desarrollo y modificación que cumplen con los planes a corto y largo plazo de los servicios de información y de la organización.
- Requiere un proceso de desarrollo y modificación estructurado que contenga los puntos de revisión en momentos clave de decisión, así como la autorización para proceder con el proyecto en cada punto de revisión.
- Está completa y actualizada.

- Es capaz de ser adaptada para acoplarse a todos los tipos de desarrollo llevados a cabo dentro de la organización.
- Es aplicable a la creación y mantenimiento tanto del software adquirido como el desarrollado internamente.
- Cuenta con provisiones documentadas para cambios tecnológicos
- Ha construido un marco de referencia general en cuanto a la adquisición y mantenimiento de la infraestructura tecnológica.
- Cuenta con los pasos a seguir (tales como adquisición, programación, documentación y pruebas, establecimiento de parámetros, ofertas fijas) que deben ser guiados y estar en línea con el marco de referencia de adquisición y mantenimiento de la infraestructura tecnológica.
- Fomenta la aportación de criterios para la aceptación de terceras partes como implementadores, gestión de cambios, gestión de problemas, funciones participantes, instalaciones, herramientas y estándares, y procedimientos de software.
- Requiere el mantenimiento de documentación detallada de programación y de sistemas (por ejemplo, diagramas de flujo, diagramas de flujo de datos, programación, etc.), y dichos requerimiento han sido comunicados a todo el personal involucrado.

- Necesita que la documentación se mantenga actualizada al producirse cambios.
- Requiere la aplicación de pruebas rigurosas y sólidas de programas y sistemas.
- Define las circunstancias bajo las cuales deben realizarse pruebas piloto o en paralelo a sistemas nuevos o modificados.
- Requiere, como parte de cada proyecto de desarrollo, implementación o modificación de los sistemas, que las pruebas sean verificadas, documentadas y guardadas de forma independiente

El enfoque de asegurar la calidad de la organización:

- Necesita que se lleve a cabo una revisión post-implementación para asegurar que todos los sistemas nuevos o modificados se desarrollan y son puestos en producción de acuerdo con la metodología del ciclo de vida de desarrollo de los sistemas, además debe ser respetado por el equipo del proyecto.
- Requiere una revisión de la medida en la que los sistemas nuevos o modificados han alcanzado los objetivos establecidos por la dirección.
- Tiene como resultado informes, los cuales propician el llevar a cabo el desarrollo de los sistemas y las recomendaciones de efectividad para la dirección (tanto para los usuarios como para la función de los servicios de información).
- Cuenta con recomendaciones a las que se les hace un seguimiento periódicamente y son comunicadas a los responsables correspondientes.

La administración de los servicios de información de la Dirección revisa y actualiza apropiadamente la metodología del ciclo de vida de desarrollo de los sistemas con regularidad para asegurar su suficiencia para la nueva tecnología y el desarrollo y modificación.

Existe una variación de los niveles de control para los distintos tipos de proyectos de desarrollo y mantenimiento (por ejemplo, si los proyectos grandes reciben mayor control que los pequeños).

El logro de una coordinación y comunicación estrecha a través del ciclo de vida de desarrollo de los sistemas se da entre los clientes de los servicios de información y los que implementan el sistema.

Existe un compromiso apropiado por parte de las diferentes funciones y personas dentro de la organización (por ejemplo, administración de los servicios de información, responsable de seguridad, personal legal, personal de seguridad de la calidad, personal de auditoría, usuarios, etc.).

Existen medidas para aplicar a los resultados de las actividades, permitiendo una evaluación sobre si se han logrado las metas de calidad.

Evaluación de la suficiencia:

- **Probando que:**

  Los procedimientos para el desarrollo del Plan de Calidad de los servicios de información incluyen las siguientes entradas:

- Planes a corto y largo plazo de la organización.
- Planes a corto y largo plazo de los servicios de información.
- Política de Calidad de la organización.
- Política de Calidad de los servicios de información.
- Plan de Calidad de la organización.
- Plan de dirección de la configuración de los servicios de información.

El Plan de Calidad de los servicios de información toma como base los planes a corto y largo plazo de los servicios de información, los cuales definen:

- Los esfuerzos y adquisiciones de desarrollo de los sistemas de aplicación.
- Interfaces con otros sistemas (internos y externos).
- La plataforma e infraestructura de los servicios de información necesaria para soportar los sistemas e interfaces.
- Los recursos (tanto financieros como humanos) para desarrollar y soportar el entorno de los servicios de información planificado.
- La formación necesaria para desarrollar y dar soporte al entorno de los servicios de información planificado .

El Plan de Calidad de los servicios de información considera lo siguiente:

- En términos medibles no ambiguos, el nivel planificado del servicio que debe otorgarse a los clientes (internos o externos).
- En términos medibles no ambiguos, los "outages" planificados máximos para cada sistema y plataforma.
- Las estadísticas de actividad para realizar un seguimiento necesario de los objetivos planificados de rendimiento y "outage", incluyendo la manera en la que se deben comunicar y a quién de deben distribuir.
- Los procesos de seguimiento y revisión necesarios para asegurar el desarrollo, modificación, transición en el entorno e infraestructura de los servicios de información identificados en los planes a corto y largo plazo de los mismos están correctamente planificados, comprobados, probados,

documentados, implementados y cuentan con la formación y los recursos necesarios.
- Los intervalos en los que el Plan de Calidad debe actualizarse.

El personal asignado para asegurar la Calidad cumple consistentemente con el enfoque y el plan de asegurar la calidad y otros procedimientos operativos establecidos.

La metodología del ciclo de vida de desarrollo de los sistemas asegura apropiadamente:

- Controles suficientes durante el proceso de desarrollo para los nuevos sistemas y tecnologías.
- Comunicación con todos los empleados involucrados en el desarrollo y mantenimiento de los sistemas.
- Se utilizan procedimientos para los cambios tecnológicos.
- Se utilizan procedimientos para asegurar la aceptación y aprobación de los usuarios.
- La adecuación de los acuerdos de terceros para realizar implementaciones.

Los usuarios comprenden los controles y requerimiento de la metodología del ciclo de vida de desarrollo de los sistemas.

Los mecanismos de control de los cambios dentro de la metodología del ciclo de vida de desarrollo de los sistemas, permiten llevar a cabo cambios en la metodología y ésta es un documento "vivo".

El registro de las revisiones y modificaciones en la metodología del ciclo de vida de desarrollo de los sistemas de la organización refleja los nuevos sistemas y tecnologías considerados actualmente y esperados en el futuro.

Los resultados completos de las pruebas de los programas y sistemas (incluyendo resultados de pruebas en paralelo y piloto) son revisados y guardados para pruebas futuras.

Existe un proceso para resolver los problemas encontrados durante las pruebas.

Se ha llevado a cabo una revisión post-implementación por parte del personal asignado para asegurar la calidad.

Los representantes del departamento involucrado en los proyectos de desarrollo de los sistemas están satisfechos con el uso actual de la metodología.

El personal de aseguramiento de la calidad comprende claramente su función dentro de la organización.

Se necesita llevar a cabo una revisión sobre asegurar la calidad al término de todas las mismas del sistema y de la revisión y aprobación de los resultados de las pruebas por parte del personal de la dirección de los servicios de información, de asegurar la calidad y de los usuarios.

La revisión sobre la función de asegurar la calidad lleva como resultado acciones correctivas por parte de la dirección.

Se llevan a cabo revisiones post-implementación, los resultados son comunicados a la Dirección y se solicitan planes de acción para las áreas de implementación con necesidad de mejoras.

Los resultados de las mediciones de los objetivos de calidad, existen y se trabaja con ellos.

Evaluación del riesgo de que no se cumplan los objetivos de control:

- **Llevando a cabo:**

Mediciones ("Benchmarking") de la metodología del ciclo de vida de desarrollo de los sistemas en comparación con organizaciones similares o estándares internacionales y buenas prácticas reconocidas en la industria.

Una revisión detallada de las medidas a llevar a cabo incluidas en el Plan de Calidad y asegurar si éstas:

- Son alcanzables.
- Satisfacen los requerimientos y expectativas de la corporación.
- Satisfacen los requerimientos y expectativas de los usuarios.
- Son medibles.

Una revisión detallada de una muestra de proyectos para asegurar que:

- Se ha cumplido con la metodología del ciclo de vida de desarrollo de los sistemas.
- Toda la adaptación y priorización de la metodología del ciclo de vida de desarrollo de los sistemas es apropiada y ha sido aprobada.

- Se han obtenido aprobaciones en todos los puntos de revisión y por parte de todo el personal clave de control (por ejemplo, responsable de seguridad de los servicios de información, personal asignado a asegurar la calidad, representantes de los usuarios, etc.).
- Se ha dado una coordinación y comunicación estrecha entre los usuarios de los servicios de información y los que implementan los sistemas (internos o terceros).
- Se ha seguido el marco de la referencia para la adquisición y el mantenimiento de la infraestructura técnica, junto con cualquier paso relevante involucrado.
- El desarrollo y las modificaciones han sido terminados satisfactoria y oportunamente.
- Se terminaron los informes apropiados en relación a la función de asegurar la calidad y se llevaron a cabo las acciones correctivas necesarias de manera oportuna.

Una revisión detallada sobre como la documentación de la programación y los sistemas debe ser preparada, revisada, aprobada y mantenida.

Una revisión detallada de como las pruebas de los programas y los sistemas (incluyendo pruebas piloto y en paralelo) y la documentación son preparadas, aprobadas y mantenidas.

Una revisión detallada del proceso de verificación de post-implementación del aseguramiento de la calidad para confirmar que los informes tienen en cuenta el cumplimiento del proceso del ciclo de vida de desarrollo de los sistemas, así como la efectividad y calidad de los sistemas nuevos como de los modificados.

- **Identificando:**

Planes de calidad que no se relacionen con los planes a corto y largo plazo.

Donde no se utiliza la metodología del ciclo de vida de desarrollo de los sistemas y aquellas situaciones de sobreutilización de la metodología (por ejemplo demasiada estructura en proyectos pequeños, e insuficiente en proyectos mayores).

Cuándo la metodología del ciclo de vida de desarrollo de los sistemas ha sido utilizada inapropiadamente (por ejemplo, aplicar la metodología del ciclo de vida de desarrollo de los sistemas para desarrollos internos en la implementación de un paquete de software "off-the-shelf", sin modificarla según corresponda).

Si la coordinación y la comunicación entre el personal involucrado en el proceso del ciclo de vida de desarrollo de los sistemas (incluyendo terceros como implementadores) existente o no.

Momentos en los que los distintos pasos a seguir en la adquisición y mantenimiento de la infraestructura de la tecnología (por ejemplo, adquisición, programación, documentación y pruebas; establecimiento de parámetros; mantenimiento y "applying fixes") no han sido seguidas adecuadamente.

Situaciones en las que no existe documentación de los programas y sistemas, o donde ésta es inadecuada o no está actualizada.

Cuando las pruebas de los programas y sistemas (incluyendo pruebas piloto y en paralelo) no han sido llevadas a cabo, se han realizado inadecuadamente, no han sido documentadas o han sido documentadas inadecuadamente.

Situaciones en las que las verificaciones de las revisiones post-implementación para asegurar la calidad no han sido llevadas a cabo o han sido realizadas inadecuadamente.

Situaciones en las que las verificaciones de revisiones y post-implementación para asegurar la calidad han sido ignoradas por la dirección y en las que se han implementado sistemas que no debían haber sido implementados.

Adquisición e Implementación

AI 1 Identificar Soluciones susceptibles de Automatización

OBJETIVOS DE CONTROL:

1. Definición de Requerimiento de la información.
2. Formulación de Acciones Alternativas.
3. Formulación de la Estrategia de Adquisición.
4. Requerimiento de Servicios de terceros.
5. Estudio de Viabilidad Tecnológica.
6. Estudio de Viabilidad Económica.
7. Arquitectura de la información.
8. Informe de Análisis de los riesgos.
9. Controles de Seguridad Eficaces en coste.
10. Diseño de Guías de Auditoría.
11. Ergonomía.
12. Selección del Software del Sistema.
13. Control de Abastecimiento.

14. Adquisición de Productos de Software.
15. Mantenimiento de Software de Terceros.
16. Programación de Aplicaciones por Contrato.
17. Aceptación de Instalaciones.
18. Aceptación de la Tecnología.

TANTO LOS OBJETIVOS DE CONTROL DETALLADOS COMO LOS DE ALTO NIVEL SON AUDITADOS MEDIANTE:

Obtención de un entendimiento a través de:

- **Entrevistas:**

  Director de las TI.

  Responsable de Seguridad.

  Dirección de los servicios de información.

  Patrocinadores del proyecto.

  Gestión de contratos.

- **Obteniendo:**

  Políticas y procedimientos relacionados con el ciclo de vida de desarrollo de los sistemas y con la adquisición de software.

  Objetivos y planes a corto y largo plazo de la tecnología de la información.

  Documentación seleccionada del proyecto, incluyendo definición de requerimiento, análisis de alternativas, estudios de viabilidad tecnológica, estudios de viabilidad económica, análisis de modelos de datos de la empresa y arquitectura de la información, análisis de los riesgos, estudios de economía sobre control y seguridad interna, análisis de pistas de auditoría, estudios ergonómicos, y planes de aceptación y resultados de pruebas de instalaciones y tecnología específica.

  Contratos seleccionados relacionados con la compra, desarrollo o mantenimiento del software.

Evaluación de los controles:

- **Considerando si:**

Existen políticas y procedimientos que requieren que:

- Los requerimientos de los usuarios satisfechos por el sistema existente o a ser satisfechos por el nuevo sistema propuesto o modificado están claramente definidos antes de la aprobación de cualquier proyecto de desarrollo, implementación o modificación.
- Los requerimientos de los usuarios son revisados y aprobados por escrito antes de la aprobación de cualquier proyecto de desarrollo, implementación o modificación.
- Los requerimientos operativos y funcionales de la solución son satisfechos incluyendo rendimiento, seguridad, confiabilidad, compatibilidad y legislación.
- Las soluciones alternativas a los requerimientos de los usuarios son estudiadas y se estudian y analizan antes de seleccionar una u otra solución de software.
- Se lleva a cabo la identificación de paquetes de software comercial que satisfacen los requerimientos del usuario para un proyecto específico de desarrollo o modificación antes de tomar la decisión final.
- Las alternativas para la adquisición de los productos de software están claramente definidas en términos de practicidad, internamente desarrollados, a través del contacto o mejora del software existente o una combinación de todos los anteriores.
- El patrocinador prepara, analiza y aprueba un estudio de viabilidad técnica para cada alternativa con el fin de satisfacer los requerimientos del usuario establecidos para el desarrollo de un proyecto de los sistemas tanto nuevos como modificados.
- En cada proyecto de desarrollo, modificación o implementación de los sistemas, se lleva a cabo un análisis de los costes y beneficios asociados con cada alternativa considerada para satisfacer los requerimientos del usuario.
- El patrocinador prepara, analiza y aprueba un estudio de viabilidad económica antes de tomar la decisión respecto a desarrollar o modificar un proyecto de los sistemas tanto nuevos como modificados.
- Se presta atención al modelo de datos de la empresa mientras se identifica y analiza la viabilidad de las soluciones.
- En cada proyecto de desarrollo, implementación o modificación de los sistemas propuestos, se prepara y documenta un análisis de las amenazas a la seguridad, de las debilidades y los impactos potenciales y las medidas factibles de seguridad y control interno para reducir o eliminar el riesgo identificado.

- Los costes y los beneficios de seguridad son examinados cuidadosamente para garantizar que los costes de los controles no exceden los beneficios.
- Se obtiene una aprobación formal del estudio de los costes y beneficios por parte de la dirección.
- Se requieren controles y pistas de auditoría apropiados para ser aplicados en todos los sistemas modificados o nuevos propuestos durante la fase de diseño del proyecto.
- Las pistas de auditoría y los controles dan la posibilidad de proteger a los usuarios contra la identificación o mal uso de su identidad por parte de otros usuarios (ej., ofreciendo anonimato, pseúdonimos, ausencia de vínculos y confidencialidad).
- Cada proyecto de desarrollo, implementación o modificación de los sistemas propuesto presta atención a los problemas ergonómicos asociados con la introducción de los sistemas automatizados.
- La dirección de los servicios de información identifica todos los programas de software de los sistemas potenciales que satisfacen sus requerimientos.
- Los productos son revisados y probados antes de ser adquiridos y utilizados.
- La compra de productos de software cumple con las políticas de adquisición de la organización definiendo el marco de referencia para la solicitud de propuesta, la selección del proveedor de software y la negociación del contrato.
- Para el software con licencia adquirido a terceros, los proveedores cuenten con procedimientos apropiados para validar, proteger y mantener los derechos de integridad de los productos de software.
- La adquisición de servicios de programación se justifica a través de un requerimiento de servicios escrito por parte de un miembro designado de los servicios de información.
- Se acuerda en el contrato con el proveedor un plan de aceptación de las instalaciones y que dicho plan defina los procedimientos y criterios de aceptación.
- Los productos finales de los servicios de programación contratados se han terminado, son revisados y probados de acuerdo con los estándares establecidos por el grupo encargado de asegurar la calidad de los servicios de información y otras partes interesadas antes de pagar por el trabajo realizado y aprobar el producto final.
- Se acuerda en el contrato con los proveedores un plan de aceptación para tecnología específica, y que dicho plan defina los procedimientos y criterios de aceptación.
- La adquisición de servicios de programación adquiridos a terceros se justifica a través de una solicitud por escrito de los servicios por parte de un miembro designado de los servicios de información.

Se lleva a cabo un análisis de los riesgos en línea con el marco de referencia general de evaluación de los riesgos.

Existen los mecanismos para asignar o mantener los atributos de seguridad para la exportación e importación de datos, y para interpretarlos correctamente.

La dirección ha desarrollado e implementado un enfoque de adquisición central, que describe un conjunto común de procedimientos y estándares que deben ser seguidos, en la adquisición de servicios de hardware, software y servicios de la tecnología de la información.

Los contratos estipulan que el software, la documentación y las entregas están sujetos a pruebas y revisiones antes de ser aceptados.

Las pruebas incluidas en las especificaciones del contrato consisten en pruebas de sistema, pruebas de integración, pruebas de hardware y componentes, pruebas de procedimientos, pruebas de carga y estrés, pruebas de rendimiento, pruebas de regresión, pruebas de aceptación del usuario, y finalmente, pruebas piloto del sistema total para evitar cualquier fallo inesperado del sistema.

Las pruebas de aceptación de las instalaciones son llevadas a cabo para garantizar que éstas y el entorno, satisfacen los requerimientos especificados en el contrato.

Las pruebas de aceptación de la tecnología específica deberían incluir inspección, pruebas de funcionalidad y carga de trabajo.

Evaluación de la suficiencia:

- **Probando que:**

Los requerimientos de los usuarios satisfechos por el sistema existente y a ser satisfechos por el sistema nuevo o modificado han sido claramente definidos, revisados y aprobados por escrito por parte del usuario antes del desarrollo, implementación o modificación del proyecto.

Los requerimientos de las soluciones funcionales se satisfacen incluyendo rendimiento, seguridad, confiabilidad, compatibilidad y legislación.

Todas las debilidades y deficiencias de procesamiento en el sistema existente son identificadas y tomadas en cuenta y resueltas completamente por el sistema nuevo o el modificado.

Los cursos alternativos que satisfacen los requerimientos de los usuarios, establecidos para un sistema nuevo o modificado, son analizados apropiadamente.

Los paquetes de software comercial que satisfacen las necesidades de un proyecto particular de desarrollo o modificación de los sistemas son identificados y considerados apropiadamente.

Todos los costes y beneficios identificados asociados con cada alternativa han sido soportados apropiadamente e incluidos como parte del estudio de viabilidad económica.

Se ha prestado atención al modelo de datos de la arquitectura de la información y de la empresa al identificar y analizar su viabilidad.

El informe del análisis de los riesgos en cuanto a las amenazas de la seguridad, vulnerabilidades e impactos potenciales y las medidas factibles de seguridad y control interno es preciso, completo y suficiente.

Los problemas de seguridad y control interno se han tenido en cuenta apropiadamente en la documentación de diseño del sistema.

La aprobación de la dirección de los controles existentes y planificados son suficientes y aportan beneficios apropiados comparados con los costes de compensación.

Existen mecanismos disponibles para las pistas de auditoría o éstos pueden ser desarrollados para la solución identificada y seleccionada.

Se ha tomado en cuenta un diseño amigable para el usuario para mejorar las habilidades finales de éste durante el diseño del sistema y el desarrollo del diseño de las pantallas, formato de informe, instalaciones de ayuda en línea, etc.

Se han considerado aspectos ergonómicos durante el diseño y el desarrollo del sistema.

Se han incluido aspectos de utilización de los usuarios (por ejemplo, tiempo de respuesta del sistema, capacidades de carga y descarga, e informes "ad hoc") en las especificaciones de requerimiento del sistema antes de su diseño y desarrollo.

La identificación de todos los programas de software de los sistemas potenciales que satisfacen los requerimientos.

La función de los servicios de información cumple con un conjunto común de procedimientos y estándares en la adquisición del hardware, software y los servicios relacionados con la tecnología de la información.

Los productos adquiridos son revisados y probados antes de ser usados y pagados completamente.

El acuerdo de compra del software permite al usuario tener una copia del código fuente del programa, aplica las actualizaciones, renovaciones de la tecnología y los "fixes" son especificados en los documentos de adquisición.

El mantenimiento de terceros incluye los requerimientos de validación, protección y mantenimiento de la integridad del producto de software.

El personal de programación contratado trabaja sujetándose al mismo nivel de pruebas, revisión y aprobaciones que se exige a los programadores propios de la organización.

La función para asegurar la calidad de la organización es responsable de la revisión y aprobación del trabajo llevado a cabo por los programadores externos.

Es suficiente el plan de aceptación de las instalaciones, incluyendo los procedimientos y criterios.

Es suficiente el plan específico de aceptación de la tecnología, incluyendo inspecciones, pruebas de funcionalidad y pruebas de carga de trabajo.

Evaluación del riesgo de que no se cumplan los objetivos de control:

- **Llevando a cabo:**

Mediciones ("Benchmarking") de la identificación de los requerimientos de los usuarios para lograr soluciones automatizadas con respecto a organizaciones similares o estándares internacionales y buenas prácticas reconocidas en la industria.

Una revisión detallada de:

- La identificación de soluciones automatizadas para satisfacer los requerimientos del usuario (incluyendo la definición de los requerimientos

del usuario, formulación de los cursos de acción alternativos; identificación de los paquetes de software comercial y elaboración de los estudios de viabilidad del desarrollo tecnológico, de viabilidad económica, de la arquitectura de la información y de los análisis de los riesgos).

- La seguridad, los controles internos (incluyendo la consideración de diseños familiares al usuario, ergonomía, etc.) y las pistas de auditoría disponibles o "desarrollables" para la solución identificada y seleccionada.
- La selección e implementación del software del sistema.
- Las políticas y procedimientos existentes de adquisición de software para la adecuación y el cumplimiento del control interno de la organización.
- La manera en que se administra el mantenimiento de terceros.
- La manera en que la programación de aplicación contratada ha sido revisada y administrada.
- La identificación de todo lo especificado en el contrato por parte de la dirección de los servicios de información.
- El proceso de aceptación de la tecnología específica para asegurar que las inspecciones, pruebas de funcionalidad y pruebas de carga de trabajo satisfacen los requerimientos especificados en el contrato.

- **Identificando:**

Las deficiencias en la metodología del ciclo de vida de desarrollo de los sistemas de la organización.

Soluciones que no satisfacen los requerimientos del usuario.

Tentativas de desarrollo de los sistemas que:

- No han considerado cursos alternativos, trayendo como resultado una solución más costosa.
- No han considerado los paquetes de software comercial que podrían haber sido implementados en menos tiempo y a un menor coste.
- No han considerado la viabilidad tecnológica de las alternativas o han considerado inapropiadamente la viabilidad tecnológica de la solución elegida, dando como resultado la incapacidad para implementar la solución como fue diseñada originalmente.
- Han hecho suposiciones equivocadas en el estudio de la viabilidad económica, dando como resultado la elección del curso de acción incorrecto.
- No han considerado el modelo de datos de la arquitectura de la información de la empresa, teniendo como resultado la elección del curso incorrecto.
- No han realizado análisis de los riesgos sólidos, y consecuentemente, no han identificado adecuadamente los riesgos (incluyendo amenazas,

vulnerabilidades e impactos potenciales) o los controles internos y de seguridad para reducir o eliminar los riesgos identificados.

Soluciones que:

- Están sobre controladas o controladas insuficientemente debido a que la economía de los controles y la seguridad son examinados inapropiadamente.
- No han contado con pistas de auditoría adecuadas.
- No han considerado los aspectos ergonómicos y de diseño familiar para el usuario, dando como resultado errores en la entrada de datos que podrían haber sido evitados.
- No han seguido el enfoque de adquisiciones establecido por la organización, dando como resultado costes adicionales creados por la organización.

La falta de software necesario de los sistemas.

La inefectividad del software de los sistemas debido al establecimiento incorrecto de parámetros.

Mantenimiento del software de terceros que no ha satisfecho los términos del contrato, afectando negativamente a la organización en el logro de su misión y metas.

Programas de aplicación contratados que no han satisfecho los términos del contrato, dando lugar a costes adicionales a la organización, atraso en la implementación de los sistemas, etc.

Situaciones en las que las instalaciones han sido aceptadas sin probar completamente el entorno, y por tanto no satisfacen los requerimientos de los usuarios y no cumplen con los términos del contrato.

Las instancias en las que se ha aceptado una tecnología específica, pero que no se han llevado a cabo adecuadamente inspecciones, pruebas de funcionalidad y pruebas de carga de trabajo, teniendo como resultado que la tecnología no satisface los requerimientos del usuario y no cumple con los términos del contrato.

Cualquier fallo del sistema.

AI 2 Adquirir y Mantener el Software de Aplicación

OBJETIVOS DE CONTROL:

1. Métodos de Diseño.
2. Cambios Importantes a los Sistemas Existentes.
3. Aprobación del Diseño.
4. Definición y Documentación de Requerimiento para Ficheros.
5. Especificaciones del Programa.
6. Diseño de la Recopilación de Datos Fuente.
7. Definición y Documentación de los requerimientos de Entrada.
8. Definición de Interfaces.
9. Interfaz Usuario – Máquina.
10. Definición y Documentación de los requerimientos de Procesamiento.
11. Definición y Documentación de los requerimientos de Salida.
12. Controlabilidad.
13. Disponibilidad como Factor Clave de Diseño.
14. Disposiciones sobre Integridad de las TI en el Software de Aplicación.
15. Pruebas del Software de Aplicación.
16. Materiales de Soporte y Referencia para los Usuarios.
17. Reevaluación del Diseño del Sistema.

TANTO LOS OBJETIVOS DE CONTROL DETALLADOS COMO LOS DE ALTO NIVEL SON AUDITADOS MEDIANTE:

Obtención de un entendimiento a través de:

- **Entrevistas:**

  Director de las TI.

  Responsable de Seguridad.

  Dirección de los servicios de información.

  Patrocinadores de los proyectos.

- **Obteniendo:**

  Políticas y procedimientos relacionados con la metodología del ciclo de vida de desarrollo de los sistemas.

  Objetivos y planes a corto y largo plazo de la tecnología de la información.

  Documentación seleccionada del proyecto, incluyendo aprobaciones de diseños, definición de requerimiento de archivo, especificaciones de los

programas, los diseño de recopilación de los datos fuente, definición de los requerimientos de entrada, interface usuario-máquina, definición de los requerimientos de procesamiento, definición de los requerimientos de salida, los requerimientos de control interno y seguridad, requerimiento de disponibilidad, provisiones para la integridad de la tecnología de la información, plan de pruebas y resultados del software de aplicación, materiales de soporte y referencia para usuarios y reevaluación del diseño del sistema.

Evaluación de los controles:

- **Considerando si:**

Las políticas y procedimientos aseguran:

- La metodología del ciclo de vida de desarrollo de los sistemas de la organización aplicada tanto para el desarrollo de los nuevos sistemas como para la modificación de los sistemas existentes y participación del usuario.
- El vínculo con el usuario al crear las especificaciones de diseño y al verificar éstas respecto a los requerimientos del usuario.
- En el caso de cambios mayores en los sistemas existentes, se observa un proceso de ciclo de vida de desarrollo de los sistemas similar al utilizado en los casos de desarrollo de los nuevos sistemas.
- Las especificaciones de diseño son aprobadas por la dirección, los departamentos de usuarios afectados y la Dirección de la organización, cuando esto es apropiado para todos los proyectos nuevos de modificación y desarrollo de los sistemas.
- Se aplica un proceso apropiado para definir y documentar el formato de los archivos para cada proyecto nuevo de desarrollo o modificación de los sistemas, incluyendo el respeto de las reglas del diccionario de datos.
- Se preparan especificaciones detalladas de los programas para cada proyecto de desarrollo o modificación de la información, y las especificaciones concuerdan con las especificaciones del diseño del sistema.
- Se especifican los mecanismos adecuados para la recolección y captura de datos para cada desarrollo nuevo del sistema o proyecto de modificación.
- Se especifican los mecanismos adecuados para la recopilación y entrada de datos para cada nuevo proyecto de desarrollo o modificación de los sistemas.
- Existen mecanismos adecuados para la definición y documentación de los requerimientos de entrada para cada proyecto nuevo de desarrollo o modificación de los sistemas.

- Existe el desarrollo de una interface entre el usuario y la máquina fácil de utilizar y autodocumentable (por medio de funciones de ayuda en línea).
- Existen mecanismos adecuados para la definición y documentación de los requerimientos de procesamiento para cada nuevo proyecto de desarrollo o modificación de los sistemas.
- Existen mecanismos adecuados para la definición y documentación de los requerimientos de salida para cada nuevo proyecto de desarrollo o modificación de los sistemas.
- Se especifican mecanismos adecuados para asegurar los requerimientos de seguridad y control interno para cada proyecto nuevo de desarrollo o modificación de los sistemas.
- Los requerimientos de seguridad y control interno incluyen controles de aplicación que garantizan la precisión, suficiencia y autorización de las entradas y salidas.
- Se considera la disponibilidad en el proceso de diseño de los sistemas nuevos o modificados en la etapa más temprana posible, y esta consideración debe analizar, en caso necesario, un incremento a través de mejoras de mantenimiento y confiabilidad.
- Los programas de aplicación contienen provisiones que verifican rutinariamente las tareas llevadas a cabo por el software para ayudar a asegurar la integridad de los datos.
- El software de aplicación se aprueba de acuerdo con el plan de pruebas del proyecto y los estándares establecidos antes de ser aprobados por el usuario.
- Se preparan manuales adecuados como soporte y referencia para los usuarios (preferiblemente en formato electrónico) como parte del proceso de desarrollo o modificación de cada sistema.
- El diseño del sistema es reevaluado siempre que ocurren discrepancias tecnológicas y lógicas significativas durante el desarrollo o el mantenimiento del sistema.

La metodología del ciclo de vida de desarrollo de los sistemas asegura que los materiales de soporte y referencia para los usuarios se actualizan de manera precisa y oportuna.

La metodología del ciclo de vida de desarrollo de los sistemas necesita una evaluación de sensibilidad durante la iniciación del desarrollo o modificación de los nuevos sistemas.

La metodología del ciclo de vida de desarrollo de los sistemas precisa la evaluación de los aspectos básicos de seguridad y control interno de un sistema nuevo a ser desarrollado o modificado, junto con el diseño conceptual

del sistema, con el fin de integrar en el diseño los conceptos de seguridad lo más pronto posible.

La metodología del ciclo de vida de desarrollo de los sistemas requiere que los aspectos de seguridad lógica y de las aplicaciones son considerados e incluidos en el diseño de los nuevos sistemas o modificaciones de los sistemas existentes.

La evaluación de los aspectos de control interno y de seguridad está basada en un buen marco de referencia.

Los sistemas de Inteligencia Artificial están funcionando en interacción o en el marco de referencia con los empleados asignados para asegurar que las decisiones importantes son aprobadas.

La exposición de la información clave que se utiliza durante las pruebas de la aplicación se reduce ya sea con limitaciones severas de acceso o la despersonalización de los datos históricos.

Evaluación de la suficiencia:

- **Probando que:**

La participación del usuario en el proceso del ciclo de vida de desarrollo de los sistemas es significativa.

La metodología del ciclo de vida de desarrollo de los sistemas asegura que existe un proceso que considera apropiadamente todos los aspectos de diseño de los sistemas (por ejemplo, entrada, procesamiento, salida, controles internos, seguridad, recuperación en caso de desastre, tiempo de respuesta, informes, control de cambios, etc.).

Los usuarios clave de los sistemas están involucrados en el proceso de diseño del sistema.

Que la revisión del diseño y el proceso de aprobación aseguran que todos los problemas han sido resueltos antes de comenzar a trabajar sobre la siguiente fase del proyecto.

Los cambios mayores de los sistemas existentes que aseguran que éstos han sido desarrollados utilizando una metodología de ciclo de vida de desarrollo de los sistemas similar a la utilizada para el desarrollo de los nuevos sistemas.

Procedimientos de aprobación del diseño, para asegurar que la programación del sistema no se inicia hasta que se han obtenido las aprobaciones correspondientes.

Los requerimientos de archivo y la documentación del sistema, así como el diccionario de datos que son consistentes con los estándares.

Aprobación de las especificaciones finales de los archivos.

Las especificaciones de programación concuerdan con las especificaciones del diseño del sistema.

Las especificaciones del diseño de recolección de datos y de entrada de datos concuerdan.

Existen las especificaciones del diseño de la interface usuario – máquina.

Las especificaciones usuario - máquina son fáciles de utilizar y la autodocumentación (utilizando instalaciones de ayuda en línea) funciona.

Se documentan las interfaces internas y externas.

Los requerimientos de procesamiento forman parte de las especificaciones del diseño.

Los requerimientos de salida forman parte de las especificaciones del diseño.

Los requerimientos de seguridad y control interno forman parte de las especificaciones del diseño.

Las especificaciones del diseño de los requerimientos de los controles de aplicación garantizan la precisión, suficiencia, oportunidad y autorización de las entradas y las salidas.

Los requerimientos de seguridad y control interno han sido incluidos en el diseño conceptual del sistema (ya sea nuevo o modificado) lo más rápidamente posible.

El responsable de seguridad está involucrado activamente en el proceso de diseño, desarrollo e implementación del proyecto del nuevo sistema o de modificación del mismo.

El diseño del sistema determina si se han cuantificado las mejoras de disponibilidad y confiabilidad en términos de tiempo y de procedimientos más eficientes en comparación con los métodos anteriores.

Las provisiones de los programas de aplicación verifican rutinariamente las tareas llevadas a cabo por el software para asegurar la integridad de los datos.

Existen estándares de pruebas establecidos.

Existe un plan de pruebas del proyecto y un proceso de aprobación del usuario.

Los materiales de soporte y referencia para los usuarios, así como las instalaciones de ayuda en línea están disponibles.

La función de "help desk" apoya efectivamente a los usuarios para solucionar los problemas de procesamiento cada vez más complejos.

El proceso para priorizar los problemas del “help desk” incluye el seguimiento e informe de tales problemas a la dirección de los servicios de información apropiada.

Se requiere la existencia de mecanismos para actualizar la documentación de los usuarios.

Existe la comunicación sobre los cambios en la documentación de los usuarios.

Se da el proceso de reevaluación siempre que ocurren discrepancias tecnológicas o lógicas significativas.

Evaluación del riesgo de que no se cumplan los objetivos de control:

- **Llevando a cabo:**

Mediciones ("Benchmarking") de los costes de adquirir y desarrollar el software de aplicación con respecto a organizaciones similares o estándares internacionales y buenas prácticas reconocidas en la industria.

Una revisión detallada de:

- Documentación seleccionada del diseño del sistema para evaluar la adecuación de las especificaciones y el cumplimiento del diseño en cuanto a dichas especificaciones.

- Proyectos seleccionados de desarrollo o modificación de los nuevos sistemas, determinando si los documentos de especificación del diseño han sido revisados y aprobados por la dirección de los servicios de información y las funciones de los usuarios afectados, así como por la Dirección de la organización cuando esto sea apropiado.
- Documentación seleccionada del software para asegurar que los requerimientos de archivo (por lo menos para los archivos mencionados a continuación) son comprendidos claramente por el equipo de implementación del proyecto y están siendo estructurados por el sistema y los requerimientos del usuario, así como por las reglas del diccionario de datos de la organización:

- Maestro
- Transacciones
- Comando
- Programa
- Control
- Tablas
- Informes
- Impresión
- Log

- Transmisión
- Proyectos de desarrollo o modificación de los nuevos sistemas para asegurar que los archivos, programas, instrumentos de recopilación de datos fuente, entradas, interfaces usuario - máquina, pasos de procesamiento y salidas identificados en los diagramas de flujo y diagramas de flujo de datos, corresponden a las varias especificaciones del diseño del sistema.
- Proyectos de desarrollo o modificación de los nuevos sistemas para determinar que siempre que se identifiquen discrepancias técnicas o lógicas, ocurra un proceso efectivo de reevaluación del diseño del sistema.
- Proyectos de desarrollo o modificación de los nuevos sistemas para determinar la existencia de cualquier discrepancia de diseño técnico o cualquier cambio funcional necesario.
- Proyectos de desarrollo o modificación de los nuevos sistemas y diseños conceptuales de los mismos para evaluar la adecuación de las provisiones de seguridad y control interno que aseguran la precisión, la suficiencia, la oportunidad y la autorización de las entradas y salidas, así como la integración de los conceptos de seguridad en el diseño lo mas tempranamente posible.

- Proyectos de desarrollo o modificación de los nuevos sistemas para evaluar el diseño a la luz de una mayor confiabilidad y disponibilidad para el usuario final, así como de "mantenibilidad" para el personal de mantenimiento de los servicios de información.
- Proyectos para evaluar la adecuación de la verificación de integridad de los datos de los programas de aplicación.
- Proyectos de desarrollo o modificación de los nuevos sistemas para asegurar que los materiales de referencia para los usuarios son actuales y consistentes con la documentación del sistema y que éstos satisfacen completamente las necesidades del usuario.

Una revisión detallada de la efectividad de:

- El proceso de especificación de los programas para asegurar que éstos están escritos de acuerdo con las especificaciones del diseño del usuario.
- El proceso de especificación de las entradas para asegurar que los programas están escritos de acuerdo con las especificaciones del diseño del usuario.
- El proceso de especificación de interface usuario - máquina para asegurar que los programas están escritos de acuerdo a las especificaciones del diseño del usuario.
- El proceso de especificación de procesamiento para asegurar que los programas están escritos de acuerdo con las especificaciones del diseño del usuario.
- El proceso de especificación de salidas para asegurar que los programas están escritos de acuerdo con las especificaciones del diseño del usuario

Una revisión detallada de los estándares de prueba de la organización y la implementación de los planes de prueba relacionados para proyectos seleccionados de desarrollo y modificación de los nuevos sistemas.

Una revisión detallada de la satisfacción del usuario con el sistema, sus informes, la documentación y el material de referencia para el usuario, las instalaciones de ayuda, etc.

- **Identificando:**

Deficiencias en la metodología del ciclo de vida de desarrollo de los sistemas utilizada para los proyectos de desarrollo o modificación de los nuevos sistemas.

Especificaciones de diseño que no reflejan los requerimientos del usuario.

Requerimiento de archivo que no son consistentes con las reglas del diccionario de datos de la organización.

Proyectos de desarrollo o modificación de los nuevos sistemas que contienen archivos, programas, selección de datos fuente, entradas, interfaces usuario - máquina, procesamiento, requerimiento de salida o controles inadecuadamente definidos.

Proyectos de desarrollo o modificación de los nuevos sistemas en los que la disponibilidad no ha sido considerada en el proceso de diseño.

Deficiencias en la integridad de los datos en el software de programas de aplicación en proyectos de desarrollo o modificación de los nuevos sistemas.

Deficiencias en los estándares de pruebas de la organización, trayendo como consecuencia la implementación de los sistemas que procesan incorrectamente los datos, y emiten incorrectamente informes.

Deficiencias en los planes de prueba en proyectos nuevos de desarrollo o modificación de los sistemas.

Deficiencias en los materiales de soporte y referencia para los usuarios en proyectos nuevos de desarrollo o modificación de los sistemas.

Discrepancias técnicas o lógicas significativas que han ocurrido durante el desarrollo o mantenimiento del sistema que no han traído como consecuencia la reevaluación del diseño del sistema, y por lo mismo, no han sido corregidos o han dado como resultado correcciones provisionales no económicas en el sistema.

AI 3 Adquirir y Mantener la Arquitectura Tecnológica

OBJETIVOS DE CONTROL:

1. Evaluación del Nuevo Hardware y Software.
2. Mantenimiento Preventivo para Hardware.
3. Sistema de Seguridad del Software.
4. Instalación del Software del Sistema.
5. Mantenimiento del Software del Sistema.
6. Controles del Cambio del Software del Sistema.
7. Utilización y Supervisión de Utilidades del Sistema.

TANTO LOS OBJETIVOS DE CONTROL DETALLADOS COMO LOS DE ALTO NIVEL SON AUDITADOS MEDIANTE:

Obtención de un entendimiento a través de:

- **Entrevistas:**

  Director de las TI.

  Responsable de Seguridad.

  Dirección de los servicios de información.

  Propietarios y patrocinadores de los proyectos.

- **Obteniendo:**

  Políticas y procedimientos relacionados con la metodología del ciclo de vida de desarrollo de los sistemas.

  Objetivos y planes a corto y largo plazo de la tecnología de la información.

  Documentación seleccionada del proyecto, incluyendo aprobaciones de diseños, definición de requerimiento de archivo, especificaciones de programas, diseño de recopilación de datos fuente, definición de requerimiento de entrada, interface usuario-máquina, definición de requerimiento de procesamiento, definición de requerimiento de salida, requerimiento de control interno y seguridad, requerimiento de disponibilidad, provisiones para la integridad de la tecnología de la información, plan de pruebas y resultados del software de aplicación, materiales de soporte y referencia para usuarios y reevaluación del diseño del sistema.

Evaluación de los controles:

- **Considerando si:**

  Existen políticas y procedimientos que aseguran que:

- Se prepara un plan de evaluación formal para evaluar el nuevo hardware y software en cuanto a cualquier impacto sobre el rendimiento global del sistema.
- La posibilidad de acceso al software del sistema y con ella, la posibilidad de interrumpir los sistemas de la información es limitada.
- La preparación, instalación y mantenimiento del software del sistema no amenaza la seguridad de los datos y programas almacenados en el sistema.
- Se seleccionan parámetros del software del sistema para asegurar la integridad de los datos y programas almacenados en el sistema.
- El software del sistema se instala y mantiene de acuerdo con el marco de referencia de adquisición y mantenimiento de la infraestructura de la tecnología.
- Los proveedores de software del sistema proporcionan estatutos para asegurar la integridad como parte de su software y todas las modificaciones del mismo.
- La prueba global (por ejemplo, utilizando una metodología de ciclo de vida de desarrollo de los sistemas) de software del sistema se realiza antes de que éste sea implantado.
- Los passwords o contraseñas de instalación proporcionadas por el proveedor del software se modifican en el momento de la instalación y los cambios del software del sistema se controlan y están en línea con los procedimientos de gestión de cambios de la organización.

Existen políticas y procedimientos para el mantenimiento del hardware para reducir la frecuencia y el impacto de los fallos de aplicación.

Se cumple con los pasos y el mantenimiento preventivo prescritos por el proveedor para cada dispositivo de hardware de los servicios de información los usuarios afectados.

Evaluación de la suficiencia:

- **Probando que:**

Existen estatutos para asegurar la integridad del software entregados por el proveedor de software del sistema (incluyendo todas las modificaciones) y considera las exposiciones resultantes del software del sistema.

La evaluación de la aplicación tiene como resultado la comparación con los requerimientos del sistema.

Existe un proceso formal de evaluación de la aplicación.

El calendario de mantenimiento preventivo asegura que el mantenimiento del hardware programado no tendrá ningún impacto negativo sobre las aplicaciones críticas.

El mantenimiento programado asegura que no ha sido planificado para los períodos de máxima carga de trabajo y de los servicios de información y las operaciones de los grupos de usuarios afectados son suficientemente flexibles para adaptar el mantenimiento preventivo rutinario planificado.

Los programas operativos de los servicios de información aseguran que existe la preparación adecuada para controlar anticipadamente los tiempos muertos de hardware ocasionados por el mantenimiento no programado.

Los parámetros del software del sistema aseguran que fueron elegidos correctamente por parte del personal apropiado de los sistemas de la información con el fin de asegurar la integridad de los datos y los programas almacenados en el sistema.

El acceso se restringe únicamente a un número limitado de operadores dentro de los servicios de información.

El software del sistema es instalado y mantenido de acuerdo con el marco de referencia de adquisición y mantenimiento para la infraestructura de la tecnología.

Se llevan a cabo pruebas completas (utilizando una metodología de ciclo de vida de desarrollo de los sistemas) para todo el software del sistema antes de autorizar su introducción al ambiente de producción.

Todas las passwords o contraseñas de instalación del software del sistema proporcionadas por los proveedores se cambian en el momento de la instalación.

Todos los cambios del software del sistema son controlados de acuerdo con los procedimientos de gestión de cambios de la organización.

La dirección del sistema (por ejemplo, adición de los nuevos usuarios al sistema y a las redes; creación y copias de seguridad de las bases de datos, asignación de espacio para el almacenamiento de los datos, prioridades del sistema, etc.) se restringe únicamente a un número limitado de operadores dentro de los servicios de información.

Evaluación del riesgo de que no se cumplan los objetivos de control:

- **Llevando a cabo:**

Mediciones ("Benchmarking") de la adquisición, implementación y mantenimiento del hardware y software en comparación con organizaciones similares o estándares internacionales y buenas prácticas reconocidas en la industria.

Una revisión detallada de:

- La documentación seleccionada de los sistemas operacionales o los proyectos de desarrollo o modificación de los sistemas para determinar si los requerimientos formales de utilización del hardware y software (incluyendo referencias para el volumen de transacción, los tiempos de procesamiento y respuesta, los tamaños de los archivos y bases de datos, los volúmenes de redes y la compatibilidad de los protocolos de las comunicaciones) existen para todos los sistemas.
- Las prácticas de mantenimiento del hardware para determinar si el mismo se lleva a cabo de acuerdo con lo establecido por el proveedor y el calendario de fechas de tal manera que no afecte el rendimiento global del sistema.
- La documentación seleccionada de los sistemas operativos y sistemas en desarrollo o modificación para evaluar las habilidades potenciales para burlar las existentes restricciones de seguridad de acceso lógicas proporcionadas por el software del sistema.
- La instalación, mantenimiento del sistema y controles de cambio para asegurar el cumplimiento con el marco de referencia de adquisición y mantenimiento de la infraestructura de la tecnológica y la integridad del sistema.

- **Identificando:**

Evaluaciones de utilización que han afectado a la utilización global del sistema.

Problemas de mantenimiento preventivo que han afectado a la utilización global del sistema.

Debilidades en la preparación, instalación y mantenimiento del software del sistema (incluyendo la selección de parámetros inapropiados del software del sistema) que han amenazado la seguridad de los datos y los programas almacenados en el sistema.

Debilidades en las pruebas del software del sistema que pueden amenazar la seguridad de los datos y los programas almacenados en dicho sistema.

Debilidades en el proceso de control de cambios del software del sistema que pueden amenazar la seguridad de los datos y los programas almacenados en el sistema.

AI 4 Desarrollar y Mantener los procedimientos de la Tecnología de la Información

OBJETIVOS DE CONTROL:

1. Requerimiento Operacionales y Niveles de Servicio.
2. Manual de Procedimientos de Usuario.
3. Manual de Operaciones.
4. Manual de Formación.

TANTO LOS OBJETIVOS DE CONTROL DETALLADOS COMO LOS DE ALTO NIVEL SON AUDITADOS MEDIANTE:

Obtención de un entendimiento a través de:

- **Entrevistas:**

  Desarrollo de aplicaciones de los servicios de información.

  Mantenimiento de los servicios de información.

  Control de los cambios de los servicios de información.

  Operaciones de los servicios de información.

  Recursos humanos y formación de los servicios información.

  Dirección de aseguramiento de la calidad de los servicios información.

  Usuarios seleccionados como recursos de los sistemas de información.

Obteniendo:

Políticas y procedimientos de la organización relacionados con:

planificación estratégica y objetivos del negocio, planificación de los sistemas de información y desarrollo de las aplicaciones.

Políticas y procedimientos de los servicios de información relacionados con el desarrollo del sistema, incluyendo: organigrama, metodología del ciclo de

vida de desarrollo de los sistemas, planificación de capacidad, manuales de usuarios y operaciones, materiales de formación, pruebas y migración a estado de producción y documentos de planificación de reanudación y contingencia.

Evaluación de los controles:

- **Considerando si:**

Los requerimientos operativos se determinan con estadísticas históricas de aplicaciones disponibles y entradas del usuario con respecto a incrementos y decrementos esperados.

El nivel de servicio y las expectativas de utilización están suficientemente detallados para permitir el seguimiento, la emisión de informes y las oportunidades de mejora.

Los requerimientos operativos y los niveles de servicio se determinan utilizando tanto datos históricos y ajustes del usuario como mediciones o "benchmarks" de la industria.

Los niveles de servicio y requerimiento de procesamiento son un paso integral en la planificación de los nuevos sistemas.

Los manuales de procedimientos de los usuarios, el manual de operaciones y los materiales de formación se desarrollan como parte de cada proyecto de desarrollo, implementación o modificación de los sistemas de la información, y se mantienen actualizados.

Evaluación de la suficiencia:

- **Probando que:**

Existen requerimientos operacionales y éstos reflejan tanto las expectativas de operación como las de los usuarios.

La utilización operacional está siendo medida, comunicada y corregida en donde existen deficiencias.

El personal de operaciones y los usuarios son conscientes y conocen los requerimientos de la aplicación.

El personal de operaciones cuenta con los manuales de operaciones para todos los sistemas y procesos bajo su responsabilidad.

Todo el movimiento de programas de desarrollo de aplicaciones a producción requiere la actualización o creación de un manual de operaciones.

Existen manuales de formación de usuarios para todas las aplicaciones, y reflejan la funcionalidad actual de la aplicación.

Existen manuales de formación para todos los sistemas tanto existentes como nuevos, y éstos dan soporte a los usuarios, reflejando el uso del sistema en la práctica diaria.

Los manuales del usuario incluyen, pero no se limitan a dar:

- Una visión global de los sistemas y el entorno.
- Explicación de todas las entradas, programas, salidas e integración de los sistemas.
- Explicación de todas las pantallas de entrada y despliegue de datos.
- Explicación de todos los mensaje de error y la respuesta apropiada.
- Procedimientos y recursos de estructuración de los problemas.

El manual de operación incluye, pero no se limita a:

- Dar nombre al sistema, a los programas, secuencia de ejecución.
- Definir los nombres de todos los archivos de entrada, proceso y salida, y de formato.
- Ofrecer un calendario diario, semanal, mensual, trimestral, cuatrimestral, fin de año, etc.
- Los comandos y parámetros que necesitan entradas por parte del operador.
- Los mensajes y respuestas de mensaje de error.
- Procedimientos de copias de seguridad, reinicio y recuperación en varios puntos o a dar una terminación anormal.
- Formatos o procedimientos de salidas especiales; distribución de informes y salidas.
- Dar un procedimiento de solución en caso de emergencia.

Se llevan a cabo la formación y el mantenimiento continuo de la documentación de aplicación, manuales de operación y de usuario.

Evaluación del riesgo de que no se cumplan los objetivos de control:

- **Llevando a cabo:**

Para una selección de proyectos de desarrollo de los sistemas, revisiones y aprobaciones de documentación:

- La consideración de futuros requerimientos y niveles de los servicios de los usuarios.
- La tarea, entrega y liberación para la creación y el mantenimiento de los manuales de usuario.
- La tarea, entrega y liberación para la creación y el mantenimiento del manual de operaciones.
- La tarea, entrega y liberación de la formación para el usuario para comprender y utilizar nuevos sistemas o nuevas modificaciones.

Entrevistas a los usuarios para confirmar la suficiencia de las tentativas de desarrollo de los sistemas, incluyendo los manuales desarrollados y la formación proporcionada.

El análisis tanto de los manuales del usuario como de operaciones en cuanto a su continua actualización y mantenimiento.

- **Identificando:**

- Deficiencias en los manuales de los usuarios, las operaciones y la formación.
- La inexistencia de acuerdos sobre servicios entre el proveedor y los servicios de información, y la función y usuarios de los servicios de información.
- Debilidades de la organización para desarrollar y hacer funcionar las aplicaciones requeridas.

AI 5 Instalar y Validar los Sistemas

OBJETIVOS DE CONTROL:

1 Formación.

2 Dimensión del rendimiento del software de la aplicación.

3 Plan de Implementación.

4 Conversión del Sistema.

5 Conversión de Datos.

6 Estrategias y Planes de Pruebas.

7 Pruebas de Cambios.

8 Criterios y Rendimiento de Pruebas en Paralelo/Piloto.

9 Prueba Final de Aceptación.

10 Prueba de Seguridad y Acreditación.

11 Prueba Operacional.

12 Promoción de Producción.

13 Evaluación de Cumplimiento de los requerimientos del Usuario.

14 Revisión Post-implementación de la Dirección.

TANTO LOS OBJETIVOS DE CONTROL DETALLADOS COMO LOS DE ALTO NIVEL SON AUDITADOS MEDIANTE:

Obtención de un entendimiento a través de:

- **Entrevistas:**

  Director de las TI.

  Dirección de los servicios de información.

  Departamento de formación, desarrollo de aplicaciones, seguridad, asegurar la calidad y dirección de operaciones de los servicios de información.

  Responsable de Seguridad.

  Dirección seleccionada de los sistemas recientemente desarrollados o en desarrollo.

  Contratos con proveedores de desarrollo de sistemas.

- **Obteniendo:**

Políticas y procedimientos de la organización relacionados con la planificación del ciclo de vida de desarrollo de los sistemas.

Políticas y procedimientos de los servicios de información relacionados con las políticas y los comités de seguridad, planificación del ciclo de vida de desarrollo

de los sistemas para los programas, unidades, planes de prueba del sistema, formación de usuarios, migración de los sistemas de prueba a los de producción, asegurar la calidad y formación.

Plan y calendario del ciclo de vida de desarrollo de los sistemas, estándares de programación del ciclo de vida de desarrollo de los sistemas, incluyendo procesos de solicitud de cambios.

Informes sobre la muestra del estado de desarrollo de los sistemas.

Informes post-implementación sobre los anteriores esfuerzos de desarrollo.

Evaluación de los controles:

- **Considerando si:**

Existen políticas y procedimientos relacionados con el proceso del ciclo de vida de desarrollo de los sistemas.

Existe una metodología formal del ciclo de vida de desarrollo de los sistemas para la instalación y acreditación de los mismos, incluyendo, pero no limitándose a un enfoque por fases sobre: formación, adecuación del resultado, plan de conversión, pruebas de los programas, grupos de programas y del sistema total, un plan de pruebas prototipo o paralelo, pruebas de aceptación, pruebas y certificación de la seguridad, pruebas operativas, controles de cambio, revisión y modificación de la implementación y post-implementación.

Se lleva a cabo la formación de los usuarios como parte del esfuerzo de desarrollo.

Los controles de los programas y sistema son consistentes con los estándares de seguridad de la organización y con las políticas, procedimientos y estándares de los servicios de información.

Existen varias librerías de desarrollo, prueba y producción para los sistemas en proceso.

Existen criterios predeterminados para probar el acierto, los fallos y la terminación de futuros esfuerzos.

El proceso para asegurar la calidad incluye la migración independiente de desarrollo a las librerías de producción y la aceptación requerida de los usuarios y grupos de operación.

Los planes de prueba para simulación de volúmenes, intervalos de proceso y salidas disponibles, instalación y acreditación forman parte del proceso.

El programa de formación asociado con una muestra de varios esfuerzos de desarrollo de sistemas contiene: diferencias con respecto al sistema anterior, cambios que afectan a las entradas, procesamiento, calendario, distribución, interfaces con otros sistemas, errores y corrección de errores.

Las herramientas automatizadas optimizan los sistemas desarrollados, en producción, y si estas herramientas se utilizan para oportunidades de eficiencia.

La solución de los problemas ocurre en relación con un resultado inferior al óptimo.

Evaluación de la suficiencia:

- **Probando que:**

Se ha incluido en todos los esfuerzos de desarrollo de los nuevos sistemas un plan formal para la formación de los usuarios.

El personal es consciente, comprende y tiene conocimiento de la necesidad de los controles formales de desarrollo de los sistemas y formación de los usuarios para cada instalación e implementación de desarrollo.

La consciencia, comprensión y conocimiento de los usuarios seleccionados con respecto a sus responsabilidades en el diseño, aprobación, pruebas, formación, conversión y proceso de implementación, es conocida y considerada.

Se realiza un seguimiento de los costes reales del sistema comparados con los costes estimados, y el resultado real respecto al esperado tanto de los sistemas nuevos como de los modificados.

Existe un plan de pruebas que cubre todas las áreas de recursos de los sistemas de información: software de aplicación, instalaciones, tecnología y usuarios.

Los usuarios comprenden todas las fases y responsabilidades en el desarrollo de los sistemas, incluyendo:

- Especificaciones de diseño, incluyendo iteraciones durante el ciclo de desarrollo.
- Análisis coste-beneficio y estudio de viabilidad.

- Aprobación en cada paso del proceso de desarrollo del sistema.
- Compromiso y evaluación del plan de pruebas y los resultados de las mismas.
- Aprobación y aceptación del sistema a través del ciclo de desarrollo.
- Aprobación final y aceptación del sistema.
- Evaluación de la suficiencia de la formación recibida para los sistemas recientemente entregados y terminados.

El personal de desarrollo y la dirección aseguran la estabilidad de los requerimientos de los usuarios una vez acordados.

La satisfacción del usuario se mide comparando las aplicaciones entregadas por los proveedores con los productos internos.

Evaluación del riesgo de que no se cumplan los objetivos de control:

- **Llevando a cabo:**

Mediciones ("Benchmarking") de la instalación y certificación de los sistemas comparándolos con organizaciones similares o estándares internacionales y buenas prácticas reconocidas en la industria.

Una revisión detallada de:

- El cumplimiento del equipo de trabajo con las fechas límite y tareas en relación con la satisfacción del usuario y la funcionalidad del sistema una vez terminado.
- El material de formación asociado con los sistemas anteriores.
- La revisión independiente y migración de los sistemas del entorno de prueba al estado y las librerías de producción por parte de la función encargada de asegurar la calidad.
- Las herramientas y el seguimiento de las redes y recursos utilizados para recopilar estadísticas para el mantenimiento y optimización, asegurando el soporte de las aplicaciones desarrolladas para lograr un resultado máximo a un coste mínimo.
- El registro del esfuerzo de desarrollo para determinar la disponibilidad de:

- Formación de los usuarios.
- Seguridad.
- Resultado del software.
- Documentación y resultados de las pruebas.
- Plan de conversión.
- Migración a producción.

- Control de los cambios durante el desarrollo.
- Satisfacción de las necesidades del usuario.
- Pruebas piloto o en paralelo.
- Revisión post-implementación.

- Conclusiones de la auditoría interna o externa con respecto al proceso de diseño de los sistemas.
- Resultados de las pruebas para confirmar si éstos satisfacen los criterios predefinidos y si todas las funciones del sistema fueron incluidas en los planes de prueba.
- Discusiones de la dirección sobre los resultados de las pruebas, así como sobre cualquier prueba realizada sobre un proyecto terminado o en desarrollo.
- Participación del usuario en el proceso de desarrollo.
- Pistas de auditoría dirigidas a recrear una actividad o el análisis de los errores según sea necesario.
- Participación del proveedor en el desarrollo incluyendo:

- Lo razonable de los costes.
- El cumplimiento con las fechas límite.
- La funcionalidad entregada.

- **Identificando:**

  Para una selección de los proyectos recientes del ciclo de vida de desarrollo de los sistemas:

- Compromiso del usuario y aprobación formal en cada fase del proceso de desarrollo de los sistemas.
- Plan de pruebas para programas, unidades, sistemas (incluyendo prototipo o en paralelo), conversión, implementación, y revisión post-implementación.
- Consistencia con los estándares de seguridad y control interno.
- Tareas y calendario apropiados para la conversión de datos.
- La realización de pruebas independientemente de las de desarrollo, modificación o mantenimiento del sistema.
- Aceptación formal por parte de los usuarios con respecto a la funcionalidad, seguridad, integridad y riesgo del sistema.

  Los manuales de operación para fijar las fechas, funcionamiento, recuperación y reinicio, copias de seguridad y "backup", y solución de errores consideran:

- La separación física y lógica de las librerías de productos con respecto a las de desarrollo o pruebas.
- Los procedimientos de solución entre las expectativas de los usuarios y la funcionalidad del sistema entregado, cuando éstos se encuentran en conflicto.

Para los proveedores:

- La formalidad de las relaciones con los proveedores y la existencia de contratos.
- La consideración de servicios específicos y costes.
- Que el resultado del proveedor está controlado también por la metodología del ciclo de vida de desarrollo de los sistemas de la organización.
- El cumplimiento del proveedor en cuanto al resultado, fechas límite y especificaciones de costes de los contratos.

AI 6 Gestionar Cambios

OBJETIVOS DE CONTROL:

1 Inicio y Control de la Solicitud de Cambio.

2 Evaluación del Impacto.

3 Control de Cambios.

4 Cambios de Emergencia.

5 Documentación y Procedimientos.

6 Mantenimiento Autorizado.

7 Políticas de liberación del Software.

8 Distribución del Software.

TANTO LOS OBJETIVOS DE CONTROL DETALLADOS COMO LOS DE ALTO NIVEL SON AUDITADOS MEDIANTE:

Obtención de un entendimiento a través de:

- **Entrevistas:**

Director de las TI.

Dirección de los servicios de información.

Dirección de desarrollo de los sistemas, control de la calidad de control de cambios, operaciones y seguridad.

Administración de los usuarios seleccionados involucrados en el diseño y utilización de las aplicaciones de los sistemas de información.

- **Obteniendo:**

Políticas y procedimientos de la organización relacionados con: la planificación de los sistemas de información, control de los cambios, seguridad y ciclo de vida de desarrollo de los sistemas.

Políticas y procedimientos de los servicios de los sistemas de información relacionados con: las metodología del ciclo de vida de desarrollo de los sistemas, los estándares de seguridad, el control independiente de la calidad, la implementación, la distribución, el mantenimiento, los cambios de emergencia, la liberación del software y el control de versiones del sistema.

Plan de desarrollo de aplicaciones.

Formato y logs de solicitud de control de cambios.

Contratos con proveedores relacionados con los servicios de desarrollo de la aplicación.

Evaluación de los controles:

- **Considerando si:**

Existe y se utiliza una metodología para priorizar los requerimientos de cambio en el sistema.

Se consideran los procedimientos de cambio de emergencia en los manuales de operaciones.

El control de los cambios es un procedimiento formal tanto para los usuarios como para los grupos de desarrollo.

El log del control de cambios asegura que todos los cambios mostrados han sido resueltos.

El usuario está satisfecho con el resultado de los cambios solicitados, calendario y costes.

Para una selección de cambios en el log de control de cambios:

- El cambio produce como resultado modificaciones en los programas y operaciones.
- Los cambios se han realizado como fueron documentados.
- La documentación actual refleja el entorno modificado.

El proceso de cambios se ha controlado en cuanto a las mejoras en el conocimiento, efectividad en el tiempo de respuesta y satisfacción del usuario con respecto al proceso.

El mantenimiento del sistema de intercambio de rama privada o Exchange Private Branch (PBX) se incluye en los procedimientos del control de cambios.

Evaluación de la suficiencia:

- **Probando que:**

Para una muestra de cambios, la administración ha aprobado los siguientes puntos:

- Solicitud de cambios.
- Especificación del cambio.
- Acceso al programa fuente.
- Finalización del cambio por parte del programador.
- Solicitud para mover el programa fuente al entorno de prueba.
- Finalización de las pruebas de aceptación.
- Solicitud de compilación y paso a producción.
- Determinación y aceptación del impacto general y específico.
- Desarrollo de un proceso de distribución.

La revisión del control de cambios en cuanto a la inclusión de:

- Fecha del cambio solicitado.
- Personas que lo solicitan.
- Solicitud aprobada de cambios.
- Aprobación del cambio realizado - función de servicios de información.
- Aprobación del cambio realizado - usuarios.
- Fecha de actualización de la documentación.
- Fecha de paso a producción.

- Aprobación del cambio por parte del control de la calidad.
- Aceptación por parte de operaciones.

Los tipos de análisis de los cambios realizados en el sistema para la identificación de las tendencias.

La evaluación de la adecuación de las librerías de los servicios de información y la determinación de los niveles de código base para prevenir la regresión de los errores.

Existen procedimientos de entradas y salidas ("check in/check out) para los cambios.

Todos los cambios en los logs se resuelven a satisfacción de los usuarios y no se realizan cambios que no sean registrados en los logs.

Los usuarios tienen consciencia y conocimiento de la necesidad de procedimientos formales para el control de cambios.

El proceso de reforzamiento del personal asegura el cumplimiento de los procedimientos de control de cambios.

Evaluación del riesgo de que no se cumplan los objetivos de control:

- **Llevando a cabo:**

Mediciones ("Benchmarking") de la dirección de control de cambios con respecto a organizaciones similares o estándares internacionales y buenas prácticas reconocidas en la industria.

Para sistemas seleccionados de los servicios de información:

- Una verificación sobre si la documentación determina los requerimientos o si el cambio del sistema ha sido aprobado y priorizado por parte de la dirección de las áreas afectadas y el proveedor de servicios.
- La confirmación de la existencia y adecuación de la evaluación del impacto en formas de control de cambios.
- La obtención del conocimiento del cambio a través de la recepción de la solicitud de cambios de los servicios de información.
- La asignación del cambio a los recursos apropiados de desarrollo.
- La adecuación de los sistemas y los planes de prueba de los usuarios y sus resultados.
- La migración de la aplicación de la fase de prueba a la producción controlada por el equipo de control de calidad.

- La actualización de los manuales del usuario y de operaciones para reflejar el cambio.
- La distribución de la nueva versión a los usuarios correspondientes.

- **Identificando:**

Para una selección de cambios de la información que:

- Sólo se llevaron a cabo cambios aprobados.
- Todos los cambios han sido considerados.
- Las librerías actuales reflejan los cambios más recientes.
- Las variaciones en el procedimiento de control de cambios entre:

- Aplicaciones adquiridas e internas.
- Software de aplicación y de los sistemas.
- Tratamiento del control de cambios por parte del proveedor.

Entrega y Soporte

DS 1 Definir y Gestionar los Niveles de Servicio

OBJETIVOS DE CONTROL:

1. Marco de Referencia para el Acuerdo de Nivel de Servicio.
2. Aspectos sobre los Acuerdos de Nivel de Servicio.
3. Procedimientos de Rendimiento.
4. Cambios de Emergencia.
5. Documentación y Procedimientos.
6. Mantenimiento Autorizado.
7. Políticas de liberación del Software.
8. Distribución del Software.

TANTO LOS OBJETIVOS DE CONTROL DETALLADOS COMO LOS DE ALTO NIVEL SON AUDITADOS MEDIANTE:

Obtención de un entendimiento a través de:

- **Entrevistas:**

Director de la información.

Dirección de los servicios de información.

Administrador del nivel de servicio contratado de los servicios de información.

Administrador de operaciones de los servicios de información.

Administración de usuarios.

- **Obteniendo:**

Políticas y procedimientos generales para la organización asociadas a las relaciones del proveedor con el usuario.

Políticas y procedimientos de los servicios de información relacionados con:

- Acuerdos de nivel de servicio.
- Contenido de emisión de informes operativos, tiempos y distribución.
- Métodos de seguimiento del resultado.
- Actividades correctivas.

Documentación de los servicios de información relacionada con:

- Informes de resultado del nivel de servicio.
- Algoritmos de cargo y metodología para calcular cargos.
- Programas de mejora del servicio.
- Recurso resultante de un bajo rendimiento.

Acuerdos de nivel de servicio con usuarios y proveedores internos y externos.

Evaluación de los controles:

- **Considerando si:**

Se identifica por política un proceso de acuerdo del nivel de servicio.

Es necesaria la participación en el proceso por parte del usuario para la creación y modificación de acuerdos.

Están definidas las responsabilidades de los usuarios y proveedores.

La administración realiza un seguimiento y emite informes sobre el logro de los criterios de desarrollo de servicio especificados y sobre todos los problemas encontrados

Existe un proceso de revisión regular llevado a cabo por la dirección.

Se identifica un proceso de recurso en caso de un bajo resultado.

Los acuerdos de nivel de servicio incluyen, pero no se limitan a contar con:

- Definición del servicio.
- Coste del servicio.
- Nivel de servicio mínimo cuantificable.
- Nivel de soporte por parte de los servicios de información.
- Disponibilidad, confiabilidad y capacidad de crecimiento.
- Planificación de recuperación en caso de desastre o contingencia.
- Requerimiento de seguridad.
- Procedimientos de cambio para cualquier parte del acuerdo.
- Acuerdo por escrito y formalmente aprobado entre el proveedor y el usuario del servicio.
- Revisión , renovación , no renovación del período efectivo y del nuevo período.
- Contenido y frecuencia del informe de resultados y pago de servicios.
- Cargos realistas comparados contra la historia, la industria y las buenas prácticas.
- Cálculo de cargos.
- Compromiso de mejoras al servicio.

Evaluación de la suficiencia:

- **Probando que:**

  Para una muestra de acuerdos pasados y en proceso, el contenido incluye:

- Definición del servicio.
- Coste del servicio.
- Nivel de servicio mínimo cuantificable.
- Nivel de soporte por parte de los servicios de información.
- Disponibilidad, confiabilidad y capacidad de crecimiento.
- Procedimiento de cambios para cualquier parte del acuerdo.
- Planificación de recuperación en caso de desastre o contingencia.
- Requerimiento de seguridad.
- Acuerdo por escrito y formalmente aprobado entre el proveedor y el usuario del servicio.
- Revisión , renovación , no renovación del período efectivo y nuevo período.
- Contenido y la frecuencia del informe de resultados para el pago de servicios.
- Cargos realistas comparados con la historia, la industria y las buenas prácticas.

- Cálculos de cargos.
- Compromiso de mejoras al servicio.
- Aprobación formal por parte de los usuarios y proveedores.

Los usuarios son conscientes, tienen conocimiento y comprenden los procesos y procedimientos del acuerdo del nivel de servicio.

El nivel de satisfacción del usuario en cuanto al proceso y acuerdos reales del nivel de servicio actuales es suficiente.

El servicio proporciona información para determinar las razones de un bajo rendimiento ("non-performance") y para asegurar que existe un programa para la mejora de dicho rendimiento.

Los cargos reales concuerdan con el contenido del acuerdo.

Se realiza un seguimiento del resultado histórico comparándolo con el compromiso de mejora del servicio determinado anteriormente.

Los informes sobre el logro del resultado de servicio especificado son utilizados apropiadamente por la dirección para asegurar un rendimiento satisfactorio.

Los informes sobre todos los problemas encontrados se utilizan apropiadamente para asegurar que se toman las acciones correctivas correspondientes.

Evaluación del riesgo de que no se cumplan los objetivos de control:

- **Llevando a cabo:**

Mediciones ("Benchmarking") de los acuerdos del nivel de servicio comparando con organizaciones similares o estándares internacionales y buenas prácticas reconocidas en la industria.

Una revisión:

- Del acuerdo de nivel de servicio para determinar que se definen y alcanzan las provisiones cualitativas y cuantitativas que confirman las obligaciones.
- Del acuerdo de nivel de servicio seleccionado para confirmar que los procedimientos de solución de los problemas, específicamente el resultado bajo, son incluidos y llevados a cabo.

- **Identificando:**

La conveniencia de las provisiones que describen, coordinan y comunican la relación entre el proveedor y el usuario de los servicios de información.

Cálculos incorrectos para las categorías seleccionadas de la información.

Revisiones continuas y acciones correctivas llevadas a cabo por la dirección de informes del nivel de servicio.

La conveniencia de las mejoras de los servicios propuestos en comparación con el análisis coste - beneficio.

La conveniencia de la capacidad de los proveedores para alcanzar en el futuro los objetivos de mejoras comprometidas.

DS 2 Gestionar servicios de terceros

OBJETIVOS DE CONTROL:

1. Interfaces del Proveedor.
2. Relaciones con el propietario.
3. Contratos con Terceros.
4. Calificaciones de los Subcontratados.
5. Contratos de Outsourcing.
6. Continuidad de los Servicios.
7. Relaciones de Seguridad.
8. Supervisión.

TANTO LOS OBJETIVOS DE CONTROL DETALLADOS COMO LOS DE ALTO NIVEL SON AUDITADOS MEDIANTE:

Obtención de un entendimiento a través de:

- **Entrevistas:**

Director de Información.

Dirección de los servicios de información.

Administrador de contratos y nivel de servicio de los servicios de información.

Dirección de las operaciones de los servicios de información.

Responsable de seguridad de los servicios de información.

- **Obteniendo:**

Políticas generales para la organización asociadas con los servicios adquiridos y en particular, con las relaciones con los proveedores como terceros.

Políticas y procedimientos de los servicios de información asociadas con: relaciones con terceros, procedimientos de selección de los proveedores, contenido del control de dichas relaciones, seguridad lógica y física, mantenimiento de la calidad por parte de los proveedores, planificación de las contingencias y fuentes externas.

Una lista de todas las relaciones actuales con terceros y de los contratos reales asociados con ellos.

El informe del nivel de servicio relacionado con las relaciones y servicios proporcionados por terceros.

Las actas de las reuniones en las que se discute la revisión de los contratos, la evaluación del resultado y la dirección de las relaciones.

Los acuerdos de confidencialidad para todas las relaciones con terceros.

Las listas de seguridad de acceso con los perfiles y recursos disponibles para los vendedores.

Evaluación de los controles:

- **Considerando si:**

Existen políticas y procedimientos de los servicios de información asociadas con las relaciones con terceros, y si éstas son consistentes con las políticas generales de la organización.

Existen políticas que consideran específicamente la necesidad de contratos, de una definición del contenido de los mismos, del propietario o administrador de las relaciones responsable de asegurar la creación, mantenimiento, seguimiento y renegociación de los contratos.

Las interfaces están definidas para agentes independientes involucrados en la dirección del proyecto y demás partes como los subcontratados.

Los contratos representan un registro completo de las relaciones con los proveedores como terceros.

Los contratos están establecidos específicamente para la continuidad de los servicios, y que dichos contratos incluyan una planificación de las contingencias por parte del proveedor para asegurar la continuidad del servicio a los usuarios.

El contenido de los contratos incluye por lo menos lo siguiente:

- Aprobación formal administrativa y legal.
- Entidad legal que proporciona los servicios.
- Servicios proporcionados.
- Acuerdos cualitativos y cuantitativos de nivel de servicio.
- Coste de los servicios y frecuencia de su pago.
- Proceso de solución de los problemas.
- Sanciones por bajo resultado.
- Proceso de disolución.
- Proceso de modificación.
- Informe de servicio - contenido, frecuencia y distribución.
- Funciones entre las partes del contrato durante la vida del mismo.
- Asegurar la continuidad que indica que el servicio será proporcionado por el proveedor.

- Usuarios de los servicios , procesos y frecuencia de las comunicaciones del proveedor.
- Duración del contrato.
- Nivel de acceso proporcionado por el proveedor.
- Requerimiento de seguridad.
- Garantías de confidencialidad.
- Derecho a acceso y a auditar.

Los acuerdos de depósito se han negociado en su momento.

Los terceros en potencia se han calificado adecuadamente mediante la evaluación de sus habilidades para proveer el servicio necesario (vencimiento del trabajo).

Evaluación de la suficiencia:

- **Probando que:**

La lista de contratos y los contratos actuales son acertados.

Ningún servicio es proporcionado por algún proveedor no incluido en la lista de contratos mencionada.

Los proveedores mencionados en los contratos efectivamente están llevando a cabo los servicios definidos.

La dirección y los proveedores comprenden su responsabilidades definidas en el contrato.

Las políticas y procedimientos de los servicios de información asociados con terceros existen y son consistentes con las políticas generales de la organización.

Existen políticas que consideran específicamente la necesidad de establecer contratos, la definición del contenido de los mismos, que la dirección se responsabilice de asegurarlos, mantenerlos así como de realizar un seguimiento y su posterior renegociación.

Los contratos suponen un registro completo de las relaciones con los proveedores como terceros.

Los contratos están establecidos para asegurar específicamente la continuidad de los servicios, y que dichos contratos incluyan una planificación de las contingencias por parte del proveedor para asegurar el servicio continuo a los usuarios.

El contenido de los contratos incluye por lo menos lo siguiente:

- Aprobación formal administrativa y legal.
- Entidad legal para proporcionar los servicios.
- Servicios proporcionados.

- Acuerdos cuantitativos y cualitativos del nivel de servicio.
- Coste y frecuencia de los servicios y su pago.
- Proceso de solución de los problemas.
- Sanciones por bajo resultado.
- Proceso de disolución.
- Proceso de modificación.
- Informe de servicios - contenido, frecuencia y distribución.
- Funciones entre las partes del contrato durante la vida del mismo.
- Asegurar la continuidad de los servicios prestados por el proveedor.
- Usuarios de los servicios y frecuencia del proceso de comunicaciones del proveedor.

- Duración del contrato.
- Nivel de acceso proporcionado por el proveedor.
- Requerimiento de seguridad.
- Garantías de confidencialidad.
- Derecho de acceso y de auditar.

Los usuarios tienen consciencia, conocimiento y comprenden la necesidad de contar con políticas de contratos y con los contratos mismos para proporcionar servicios.

Existe una independencia adecuada entre el proveedor y la organización.

Se dan independientemente la búsqueda y la selección de los proveedores.

La lista de seguridad de acceso incluye únicamente un número mínimo de proveedores, y que dicho acceso es el mínimo necesario.

El acceso a los recursos de hardware y software de la organización es administrado y controlado para minimizar la utilización de proveedores.

El nivel real de los servicios proporcionados se compara en gran medida con las obligaciones contractuales.

Las instalaciones, personal, operaciones y controles de las fuentes externas aseguran un nivel de resultado comparable con el esperado.

El seguimiento continuo de liberación y entrega de los servicios por parte de terceros es llevado a cabo por la dirección.

Se llevan a cabo auditorías independientes de las operaciones de la parte contratante.

Existen los informes de evaluación de terceros con el fin de estudiar su capacidad para entregar el servicio solicitado.

Las interfaces de los agentes independientes involucrados en el desarrollo del proyecto están documentadas en el contrato.

La historia de la actividad de litigación - actual y anterior.

Los contratos con proveedores PBX están y son cubiertos.

Evaluación del riesgo de que no se cumplan los objetivos de control:

- **Llevando a cabo:**

Mediciones ("Benchmarking") de los servicios de terceros en relación con organizaciones similares o estándares internacionales y buenas prácticas reconocidas en la industria.

Una revisión detallada de cada uno de los contratos de terceros para determinar provisiones cualitativas y cuantitativas que confirman la definición de las obligaciones.

- **Identificando:**

Provisiones que describen, coordinan y comunican la relación entre el proveedor y el usuario de los servicios de información.

Facturas de terceros que reflejan cargos precisos por los servicios contratados.

El vínculo de la organización con los proveedores como terceros que asegura la comunicación de los problemas contractuales entre las partes y los usuarios de los servicios.

La aprobación de todos los contratos por parte de la dirección y el consejo.

La puesta en práctica de las evaluaciones de los riesgos para confirmar la necesidad de estas relaciones y su modificación.

La revisión continua y las acciones correctivas sobre los informes de los contratos llevadas a cabo por la dirección.

Lo razonable de la aplicación de los cargos en comparación con el resultado interno, externo y de la industria.

La existencia de planes de contingencia para todos los servicios contratados, específicamente para los servicios de recuperación en caso de desastre de los servicios de información.

Las funciones de fuentes externas, defectos u oportunidades para mejorar el resultado o reducir costes.

La implementación de las recomendaciones de las auditorías independientes llevadas a cabo por la parte contratante.

DS 3 Gestionar Rendimientos y Capacidades

OBJETIVOS DE CONTROL:

1. Requerimiento de Disponibilidad y Rendimiento.
2. Plan de Disponibilidad.
3. Supervisión e Informe.
4. Herramientas de Modelado.
5. Gestión Proactiva del Rendimiento.
6. Pronóstico de Carga de Trabajo
7. Gestión de la Capacidad de los Recursos.
8. Disponibilidad de Recursos.
9. Calendario de Recursos.

TANTO LOS OBJETIVOS DE CONTROL DETALLADOS COMO LOS DE ALTO NIVEL SON AUDITADOS MEDIANTE:

Obtención de un entendimiento a través de:

- **Entrevistas:**

  Dirección de los servicios de información.

  Dirección de las operaciones de los servicios de información.

  Dirección de la capacidad de los servicios de información.

  Dirección de redes de los servicios de información.

- **Obteniendo:**

Políticas y procedimientos globales para la organización relacionados con la disponibilidad, seguimiento e informe del resultado, pronóstico de la carga de trabajo, dirección de la capacidad y calendario.

Políticas y procedimientos de los servicios de información relacionados con: el enlace de la capacidad con el plan del negocio, la disponibilidad de los servicios, la planificación de la disponibilidad, el seguimiento continuo y la dirección del rendimiento.

Representaciones del producto por parte del proveedor con respecto a las normas de capacidad y desarrollo.

Una lista de todos los productos actuales del proveedor en lo referente a hardware, software, comunicaciones y periféricos.

Informes de seguimiento de las redes de comunicación.

Actas de las reuniones en las que se discute la planificación de la capacidad, las expectativas de resultado y la "afinación" del resultado.

Documentos de disponibilidad, capacidad, carga de trabajo y planificación de recursos.

Presupuesto anual de las TI incluyendo las suposiciones relacionadas con la capacidad y el resultado.

Informes relacionados con el desarrollo operativo dentro de los servicios de información, incluyendo el informe y la historia de la solución de problemas.

Evaluación de los controles:

- **Considerando si:**

Los períodos de tiempo y el nivel de servicio están definidos para todos los servicios proporcionados por la función de los servicios de información.

Los períodos de tiempo y los niveles de servicio reflejan los requerimientos del usuario.

Los períodos de tiempo y los niveles de servicio son consistentes con las expectativas de resultado del equipo.

Existe un plan de disponibilidad, si éste es actual y refleja los requerimientos del usuario.

Se lleva a cabo y se informa sobre el seguimiento continuo del resultado de todo el equipo y de la capacidad, y si la falta de un resultado adecuado se tiene en consideración por la dirección y si se considera formalmente las oportunidades de mejoras del mismo.

Se realiza un seguimiento del resultado óptimo de la configuración utilizando herramientas para maximizar el rendimiento y al mismo tiempo, minimizar la capacidad a los niveles necesarios.

Los usuarios y los grupos de desarrollo operativo revisan proactivamente la capacidad, el rendimiento, y si se llevan a cabo modificaciones en el calendario de trabajo.

El pronóstico de la carga de trabajo incluye las entradas hechas por los usuarios debido a variaciones en las demandas y por los proveedores debido a nueva tecnología o a mejoras de los productos actuales.

Evaluación de la suficiencia:

- **Probando que:**

Las estadísticas sobre informes de desarrollo, capacidad y disponibilidad son precisas, incluyendo una comparación entre las explicaciones de las variaciones de desarrollo históricas y las pronosticadas.

El proceso de cambios para modificar los documentos de planificación de la disponibilidad, capacidad y carga de trabajo refleja los cambios en la tecnología o los requerimientos del usuario.

Los informes del análisis de flujo de trabajo consideran las oportunidades de eficiencia de procesos adicionales.

El informe sobre el uso y disponibilidad realizado por los usuarios existe, incluyendo el calendario de carga de trabajo y las tendencias.

Existen procedimientos de priorización, éstos se siguen y son apropiados para la solución de problemas.

La fase de post-implementación de la metodología de desarrollo de los sistemas incluye los criterios para determinar el crecimiento futuro y los cambios en las expectativas de desarrollo.

Los niveles de soporte proporcionados por los servicios de información son suficientes para apoyar las metas de la organización.

Evaluación del riesgo de que no se cumplan los objetivos de control:

- **Llevando a cabo:**

Mediciones ("Benchmarking") de la dirección del desarrollo y la capacidad para comparar con organizaciones similares o estándares internacionales y buenas prácticas reconocidas en la industria.

Pruebas sobre las necesidades continuas del negocio, para asegurar que los términos y requerimiento de disponibilidad de las TI reflejan adecuadamente estas necesidades.

Una revisión del proceso de planificación de la capacidad y los recursos para asegurar la modificación oportuna de los planes, tomando como base las necesidades cambiantes del negocio.

Una verificación para asegurar que las expectativas de desarrollo están siendo alcanzadas en lo referente a la capacidad, respuesta y disponibilidad.

Una comparación de los requerimientos de desarrollo desde una perspectiva de análisis coste y beneficio, para asegurar que no existen excedentes de capacidad o recursos.

Una verificación periódica del informe de desarrollo producido y revisado por la dirección.

Identificando:

Informes de desarrollo en cuanto a oportunidades de mejora o solución de las debilidades.

Las expectativas de desarrollo de los usuarios están siendo satisfechas, y las modificaciones basadas en los cambios de los requerimientos están siendo reflejadas en el los logs o informes de los problemas que confirman que los problemas ocurridos durante el procesamiento son considerados oportunamente y se llevan a cabo las acciones correctivas apropiadas.

Problemas específicos encontrados y el control de la efectividad del proceso de la solución de los problemas.

DS 4 Asegurar el Servicio Continuo

OBJETIVOS DE CONTROL:

1. Marco de Continuidad de las TI.
2. Filosofía y Estrategia del Plan de Continuidad de las TI.
3. Contenidos del Plan de Continuidad de las TI.
4. Minimización de los requerimientos de Continuidad de las TI.
5. Mantenimiento del Plan de Continuidad de las TI.
6. Pruebas del Plan de Continuidad de las TI.
7. Formación del Plan de Continuidad de las TI.
8. Distribución del Plan de Continuidad de las TI.

9. Procedimientos de Procesamiento Alternativos de Backup del Departamento de usuarios.
10. Recursos Críticos de las TI.
11. Lugar y Hardware de Backup.
12. Almacenamiento de Backup fuera de la Institución.
13. Procedimientos de Terminación.

TANTO LOS OBJETIVOS DE CONTROL DETALLADOS COMO LOS DE ALTO NIVEL SON AUDITADOS MEDIANTE:

Obtención de un entendimiento a través de:

- **Entrevistas:**

  Dirección de los servicios de información.

  Dirección de operaciones de los servicios de información.

  Dirección de contingencias de los servicios de información.

  Dirección de recursos humanos o formación.

  Organizaciones de usuarios con necesidades de reanudación y contingencia.

  Administrador del centro de cómputo de recuperación del proveedor.

  Administrador del almacenamiento fuera del centro de cómputo.

  Administrador de los riesgos y seguros.

- **Obteniendo:**

Políticas y procedimientos generales para la organización relacionados con el proceso de planificación de solución de contingencias.

Políticas y procedimientos de los servicios de información relacionados con: el marco de referencia, el plan, la filosofía, la estrategia, la priorización de aplicaciones, el plan de pruebas, las copias de seguridad y rotaciones regulares y la formación de recuperación en caso de desastres y contingencias.

El plan de solución de desastres y contingencia de los servicios de información.

Los usuarios de los servicios de los planes de continuidad del negocio y superación de las contingencias.

Los resultados de las pruebas sobre estos planes.

La metodología para determinar la priorización de las aplicaciones en caso de fallo.

Los contratos de los proveedores que proporcionan continuidad y dan soporte.

Pólizas de seguros por interrupción del negocio.

Evaluación de los controles:

- **Considerando si:**

Las políticas de la organización necesitan de un marco de referencia un plan como parte de los requerimientos normales de operación tanto para los servicios de información como para todas las organizaciones dependientes de los recursos de los sistemas de la información.

Las políticas y procedimientos de los servicios de información requieren de:

- Una filosofía y un marco de referencia consistentes en relación con el desarrollo de un plan de continuidad del servicio.
- Una priorización de las aplicaciones con respecto a los tiempos de recuperación y retorno.
- Una evaluación de los riesgos y la consideración de seguros para pérdidas del negocio en situaciones de continuidad de los servicios de información, así como para los usuarios de los recursos.
- Una determinación de las funciones y responsabilidades específicas con respecto a la planificación de recuperación de desastres y contingencias con pruebas, mantenimiento y requerimiento de actualización específicos.
- Un acuerdo de contrato formal con los proveedores que prestan servicios para proporcionar servicios en caso de desastre, incluyendo instalaciones de la sala de servidores o relaciones de copias de seguridad, anticipándose a una necesidad real.

La inclusión de los siguientes puntos como contenido mínimo en cada plan de recuperación de desastre y contingencias:

- Procedimientos de emergencia para garantizar la seguridad de todos los miembros del personal afectados.

- Funciones y responsabilidades de los servicios de información, de los proveedores que prestan los servicios de recuperación de desastres, de los usuarios de los servicios y del personal administrativo soporte.
- Un marco de referencia de recuperación de los desastres consistente con un plan de contingencias a largo plazo.
- Una lista de los recursos de los sistemas que necesitan alternativas (hardware, periféricos, software).
- Una lista de las aplicaciones mayores y menores, de los tiempos de recuperación necesarios y de las normas de actuación esperadas.
- Funciones administrativas para comunicar y proporcionar servicios soporte tales como beneficios, nómina, comunicación externa, seguimiento de los costes, etc. en caso de desastre.
- Varios escenarios de desastre, desde las pérdidas mínimas hasta la pérdida total de la capacidad y respuesta en suficiente detalle para llevar a cabo una ejecución paso a paso.
- La identificación del equipo específico y necesidades de suministros tales como impresoras de alta velocidad, firmas, formatos, equipo de comunicación, teléfonos, etc.
- La formación, la conciencia y el conocimiento de las funciones individuales y del equipo en el plan de recuperación de desastres.
- El calendario de las pruebas, los resultados de la última prueba y las acciones correctivas llevadas a cabo tomando como base la prueba anterior.
- El detalle de los proveedores de servicios contratados, de los servicios y de las expectativas de respuesta.
- La información logística sobre la localización de los recursos clave, incluyendo la sala de servidores y copias de seguridad para la recuperación de los sistemas operativos, aplicaciones, archivos de datos, manuales de operación y documentación de programas, sistemas y usuarios.
- Los nombres, direcciones, números de teléfono y "localizadores" (pagers) actuales del personal clave.
- La inclusión de los planes de reconstrucción para la recuperación en la localidad original de todos los sistemas y recursos.
- Las alternativas de reanudación del negocio para todos los usuarios para el establecimiento de lugares de trabajo alternativos, una vez que los recursos de los sistemas de información están disponibles (por ejemplo, el sistema ha sido recuperado en una sala de servidores alternativo pero el edificio de los usuarios sufrió un incendio y no está disponible).

Los requerimientos de la agencia reguladora con respecto a la planificación de contingencia están siendo satisfechos.

Los planes de contingencia para los usuarios son desarrollados tomando como base la indisponibilidad de los recursos físicos para llevar a cabo procesamientos críticos - manuales y automatizados.

Los sistemas de telefonía, Correo de Voz, fax y sistemas de imágenes son parte del plan de continuidad.

Los sistemas de imágenes, fax, los documentos en papel y los medios de almacenamiento masivo son parte del plan de continuidad.

Evaluación de la suficiencia:

- **Probando que:**

Existen planes de recuperación de desastre y contingencias, que están actualizados y que se comprenden por todas las partes afectadas.

Se ha proporcionado a todas las partes involucradas un plan regular de formación sobre contingencias y recuperación en caso de desastre.

Se han seguido todas las políticas y procedimientos relacionados con el desarrollo del plan.

El contenido del plan tiene como base el contenido descrito anteriormente, y que:

- Los objetivos del plan de contingencia han sido alcanzados.
- Se ha seleccionado a las personas apropiadas para llevar a cabo las funciones de liderazgo.
- El plan ha recibido las revisiones y aprobaciones apropiadas por parte de la dirección.
- El plan ha sido probado recientemente y éste funcionó de acuerdo con lo esperado, o que cualquier deficiencia encontrada trajo como resultado la aplicación de correcciones en el plan.
- Existe un vínculo entre el plan de recuperación en caso de desastre y el plan de negocio de la organización.
- Los procedimientos manuales alternativos son documentados y probados como parte de la prueba global.

Se ha proporcionado la formación, la consciencia y el conocimiento a los usuarios y personal de los servicios de información en cuanto a funciones, tareas y responsabilidades específicas dentro del plan.

Las relaciones y tiempos del proveedor contratado son consistentes con las expectativas y necesidades del usuario.

El contenido de la sala de servidores y copias de seguridad está actualizado y es suficiente con respecto a los procedimientos normales de rotación.

Evaluación del riesgo de que no se cumplan los objetivos de control:

- **Llevando a cabo:**

Mediciones ("Benchmarking") de la planificación de recuperación de desastres y contingencias con respecto a organizaciones similares o estándares internacionales y buenas prácticas reconocidas en la industria.

Una revisión detallada de:

- Los objetivos del plan para asegurar una estrategia apropiada y una interface con la estrategia de continuidad general del negocio.
- La comprensión apropiada del personal con respecto a proporcionar liderazgo como coordinadores del plan.
- El plan verificado y aprobado por los niveles apropiados de la Dirección.
- Los miembros seleccionados de los servicios de información y del departamento usuario para verificar que las necesidades del negocio están incluidas en el plan de contingencia.
- Los procedimientos de los usuarios para el procesamiento de datos manual alternativo para asegurar que éstos están documentados por los departamentos de usuarios con el fin de ser utilizados cuando ocurra un desastre, y hasta que haya posibilidad de restaurar las operaciones después de dicho desastre.
- Los suministros de aplicación específicos, para asegurar que existe inventario suficiente en un centro de cómputo exterior (por ejemplo, cintas magnéticas, reserva de cheques, reserva de certificados, etc.).

- **Identificando:**

Los contratos de los proveedores para verificar los tiempos para obtener suministros y la suficiencia de detalles del servicio, oportunidad, niveles de servicio y costes.

Las provisiones para adquirir componentes de redes o de telecomunicaciones especializadas.

Escenarios varios a corto plazo y permanentes como parte del plan.

La priorización de aplicaciones de forma consistente con las expectativas de los usuarios.

Que existen contratos por escrito para instalaciones externas de la sala de servidores proporcionales a las necesidades.

Velocidad, respuesta, disponibilidad y soporte del procesamiento de la sala de servidores alternativa, suficientes para los requerimientos de los usuarios.

Plan de recuperación de desastre de los proveedores para asegurar la continuidad de sus servicios en caso de desastre.

La lejanía de los servicios alternativos del proveedor con respecto a la sala de servidores original, con el fin de eliminar la posibilidad de desastres mutuos.

Pruebas periódicas del plan, ajustes en el mismo basándose en las pruebas.

Al personal usuario y de los servicios de información, asegurándose que han recibido regularmente formación sobre recuperación por desastres.

La existencia de equipos, funciones y responsabilidades de reconstrucción similares, así como pruebas para migrar el procesamiento desde el lugar de procesamiento alternativo al centro de control original.

DS 5 Garantizar la Seguridad de los Sistemas

OBJETIVOS DE CONTROL:

1. Administrar las Medidas de Seguridad.
2. Identificación, Autentificación y Acceso.
3. Seguridad de Acceso a Datos en Línea.
4. Dirección de Cuentas de Usuario.
5. Revisión Gerencial de Cuentas del Usuario.
6. Control del Usuario sobre Cuentas de Usuario.
7. Vigilancia de Seguridad.
8. Clasificación de Datos.
9. Identificación Central y Gestión de los Permisos de Acceso.
10. Informes sobre Actividades de Violación y Seguridad.
11. Gestión de Incidentes.
12. Reacreditación.
13. Confianza en la otra Parte.
14. Autorización de Transacción.
15. No Repudio.

16. Caminos con Confianza.
17. Protección de las Funciones de Seguridad.
18. Gestión de la Clave Criptográfica.
19. Prevención, Detección y Corrección de Software Dañino.
20. Arquitectura de Firewalls y Conexión con Redes Públicas.
21. Protección del Valor Electrónico.

TANTO LOS OBJETIVOS DE CONTROL DETALLADOS COMO LOS DE ALTO NIVEL SON AUDITADOS MEDIANTE:

Obtención de un entendimiento a través de:

- **Entrevistas:**

  Responsable Senior de seguridad de la organización.

  Dirección de la seguridad y Dirección de los servicios de información.

  Administrador de la base de datos de los servicios de información.

  Administrador de la seguridad de los servicios de información.

  Administración del desarrollo de las aplicaciones de los servicios de información.

- **Obteniendo:**

Políticas y procedimientos globales para la organización relacionados con la seguridad y el acceso a los sistemas de información.

Políticas y procedimientos de los servicios de información relacionados con: seguridad y acceso a los sistemas de información.

Políticas y procedimientos relevantes, así como requerimiento de seguridad legales y regulatorios de los sistemas de información (por ejemplo, leyes, regulaciones, alineamientos, estándares industriales) incluyendo:

- Procedimientos de dirección de las cuentas del usuario.
- Política de seguridad del usuario o de protección de la información.
- Estándares relacionados con el comercio electrónico.
- Esquema de clasificación de los datos.
- Inventario del software de control de acceso.
- Plano de los edificios y habitaciones que contienen los recursos de los sistemas de información.

- Inventario o esquema de los puntos de acceso físico a los recursos de los sistemas de información (por ejemplo, modems, líneas telefónicas y terminales remotas).
- Procedimientos de control de cambios del software de seguridad.
- Procedimientos de seguimiento, solución y priorización de problemas.
- Informes sobre violaciones a la seguridad y procedimientos de revisión administrativa.
- Inventario de los dispositivos de encriptación de datos y de los estándares de encriptación.
- Lista de los proveedores y clientes con acceso a los recursos del sistema.
- Lista de los proveedores de servicios utilizados en la transmisión de los datos.
- Prácticas de dirección de redes relacionadas con pruebas continuas de seguridad.
- Copias de los contratos de transmisión de datos de los proveedores de servicios.
- Copias de documentos firmados sobre seguridad y conocimiento de los usuarios.
- Contenido del material de formación sobre seguridad para nuevos empleados.
- Informes de auditoría de auditores externos, proveedores de servicios como terceros y dependencias gubernamentales relacionadas con la seguridad de los sistemas de información.

Evaluación de los controles:

- **Considerando si:**

Se cuenta con un plan de seguridad estratégico que proporcione una dirección y control centralizados sobre la seguridad de los sistemas de información, así como los requerimientos de seguridad de los usuarios con propósitos de consistencia.

Se cuenta con una organización de seguridad centralizada responsable de asegurar el acceso apropiado a los recursos del sistema.

Se cuenta con un esquema de clasificación de los datos en operación que indica que todos los recursos del sistema cuentan con un propietario responsable de su seguridad y contenido.

Se cuenta con perfiles de seguridad de usuario que representan “los menos accesos requeridos” y que muestran revisiones regulares de los perfiles por parte de la dirección con fines de reacreditación.

La formación de los empleados incluye el conocimiento y concienciación sobre seguridad, las responsabilidades de los propietarios y los requerimientos de protección contra virus.

Se cuenta con informes sobre violaciones de la seguridad y procedimientos formales de solución de problemas. Estos informes deberán incluir:

- Intentos no autorizados de acceso al sistema (sign on).
- Intentos no autorizados de acceso a los recursos del sistema.
- Intentos no autorizados para consultar o modificar las definiciones y reglas de seguridad.
- Privilegios de acceso a recursos por ID de usuario.
- Modificaciones autorizadas a las definiciones y reglas de seguridad.
- Accesos autorizados a los recursos (seleccionados por usuario o recurso).
- Cambio sobre el estado de la seguridad del sistema.
- Accesos a las tablas de parámetros de seguridad del sistema operativo.

Existen módulos criptográficos y procedimientos clave de mantenimiento, si éstos son administrados centralizadamente y si son utilizados para todas las actividades de acceso externo y de transmisión.

Existen estándares de dirección criptográfica claves tanto para la actividad centralizada como para la de los usuarios.

Los controles de cambios en el software de seguridad son formales y consistentes con los estándares normales de desarrollo y mantenimiento de los sistemas.

Los mecanismos de autenticidad en uso proveen las siguientes facilidades:

- Uso individual de los datos de autenticidad (ej., passwords y no re-utilizables).
- Autentificación múltiple (ej., se utilizan dos o más mecanismos de autenticidad diferentes)
- Autenticidad basada en la política (ej., capacidad para especificar procedimientos de autenticidad aparte en los eventos específicos).
- Autenticidad por demanda (ej., capacidad de volver a autentificar al usuario, en ocasiones, después de la autentificación inicial).

El número de sesiones concurrentes correspondientes al mismo usuario están limitadas.

Al entrar, aparece un mensaje de advertencia preventivo en relación al uso adecuado del hardware, software o conexión.

Se despliega una pantalla de advertencia antes de completar la entrada para informar al lector que los accesos no autorizados podrían causar responsabilidades legales.

Al lograrse la sesión con éxito, se despliega el historial de los intentos con éxito y fallidos de acceso a la cuenta del usuario.

La política de password incluye:

- Cambio inicial de la password la primera vez que se utiliza.
- Longitud adecuada mínima del password.
- La frecuencia obligatoria mínima de cambio de password.
- Verificación de la password en la lista de valores no permitidos (ej., verificación de diccionario).
- Protección adecuada para las passwords de emergencia.

El procedimiento formal para resolver los problemas incluye:

- ID de usuario suspendido después de 5 intentos de entrada fallidos.
- Fecha del último acceso y el número de intentos fallidos se despliega al usuario autorizado de las entradas.
- El tiempo de autenticidad se limita a 5 minutos, después de los cuales se concluye la sesión.
- Se le informa al usuario la suspensión, pero no la razón de la misma.

Los procedimientos de entrada en el sistema incluyen el rechazo o autentificación base.

Los métodos de control de localización se utilizan para aplicar restricciones adicionales a las localizaciones específicas.

El acceso al servicio VoiceMail y el sistema PBX está controlado con los mismos controles físicos y lógicos de los sistemas.

Éxito un refuerzo de las políticas de posición delicada, incluyendo que:

- Se les pide a los empleados en puestos delicados que permanezcan fuera de la organización durante un periodo de tiempo cada año; que durante este tiempo su ID de usuario se suspenda; y las personas que los sustituyen en caso de advertir cualquier anormalidad de seguridad deben notificarla a la administración.

- La rotación de personal dentro de estas áreas delicadas se realiza de vez en cuando.

El hardware y software de seguridad así como los módulos de encriptación, están protegidos contra la intromisión o divulgación, el acceso se limita a la base de la “necesidad de conocimiento”.

El acceso a los datos de seguridad como a la gestión de la seguridad, datos de transacción delicados, passwords y claves de encriptación se limita a la base de la “necesidad de conocimiento”.

Se utilizan rutas de confianza para transmitir información delicada sin encriptar.

Para evitar la suspensión del servicio por ataques con faxes basura, se toman medidas de seguridad como:

- Evitar la publicación de números de fax fuera de la organización en la base de “necesidad de conocimiento”.
- Las líneas de fax utilizadas para solicitudes del negocio no se utilizan con otros fines.

Se han establecido con respecto a los virus de ordenadores las medidas de control preventivas y detectoras.

Para reforzar la integridad de los valores electrónicos, se toman las medidas siguientes:

- Se protegen las facilidades del lector de tarjeta contra la destrucción, publicación o modificación de la información de la misma.
- La información de la tarjeta (NIP y demás información) se protege contra la divulgación.
- Se evita la falsificación de las tarjetas

Para reforzar la protección de la seguridad, se toman medidas como:

- El proceso de identificación y autentificación requiere ser repetido después de un cierto periodo de inactividad.
- Un sistema de candado, un botón de fuerza o una secuencia de salida que se puede activar cuando el terminal se deja encendido.

Evaluación de la suficiencia:

- **Probando que:**

Los servicios de información cumplen con los estándares de seguridad relacionados con:

- Autentificación y acceso.
- Dirección de clasificación de los perfiles de usuario y seguridad de datos.
- Informes y revisión gerencial de las violación e incidentes de seguridad.
- Estándares criptográficos administrativos clave.
- Detección de virus, solución y comunicación.
- Clasificación y propiedad de los datos.

Existen procedimientos para la solicitud, establecimiento y mantenimiento del acceso de los usuarios al sistema.

Existen procedimientos para el acceso externo de los recursos del sistema, por ejemplo, "logon", "ID", "password" o contraseña y "dial back".

Se lleva un inventario de los dispositivos del sistema para verificar su suficiencia.

Los parámetros de seguridad del sistema operativo tienen como base estándares locales y del proveedor.

Las prácticas de dirección de la seguridad de la red son comunicadas, comprendidas e impuestas.

Los contratos de los proveedores de acceso externo incluyen consideraciones sobre responsabilidades y procedimientos de seguridad.

Existen procedimientos de "logon" reales para sistemas, usuarios y para el acceso de proveedores externos.

Se emiten informes de seguridad en cuanto a la oportunidad, precisión y respuesta gerencial a incidentes.

El acceso a las llaves y módulos criptográficos se limita a necesidades reales de consulta.

Existen llaves secretas para utilizar en transmisiones.

Los procedimientos para la protección contra el software dañino incluyen:

- Todo el software adquirido por la organización se revisa contra los virus antes de su instalación y uso.
- Existe una política por escrito para bajar archivos (downloads), aceptación o uso de aplicaciones gratuitas y compartidas y esta política está vigente.
- El software para aplicaciones altamente sensibles está protegido por MAC (Messsage Authentication Code - Código de Autentificación de Mensajes) o firma digital, y fallos de verificación para evitar el uso del software.
- Los usuarios tienen instrucciones para la detección e información sobre virus, como el desarrollo lento o crecimiento misterioso de archivos.
- Existe una política y un procedimiento vigente para la verificación de los disquetes externos al programa de compra normal de la organización.

Los firewalls poseen por lo menos las siguientes propiedades:

- Todo el tráfico de adentro hacia fuera y viceversa debe pasar por estos firewalls (esto no debe limitarse a los controles digitales, debe reforzarse físicamente).
- Sólo se permitirá el paso del tráfico autorizado, como se define en la política de seguridad local.
- Los firewalls por si mismos son inmunes a la penetración.
- El tráfico se intercambia únicamente en firewalls a la capa de aplicación.
- La arquitectura del firewall combina las medidas de control tanto a nivel de la red como de la aplicación.
- La arquitectura del firewall refuerza la discontinuidad de un protocolo en la capa de transporte.
- La arquitectura del firewall debe estar configurada de acuerdo a la “filosofía de arte mínima”.
- La arquitectura del firewall debe desplegar una sólida autentificación para la dirección y sus componentes.
- La arquitectura del firewall oculta la estructura de la red interna.
- La arquitectura del firewall provee una auditoría de todas las comunicaciones hacia o a través del sistema del firewall y activará las alarmas cuando se detecte alguna actividad sospechosa.
- El host de la organización, que provee el soporte para las solicitudes de entrada al servicio de las redes públicas, permanece fuera del firewall.
- La arquitectura del firewall se defiende de los ataques directos (ej., a través del seguimiento activo de la tecnología de reconocimiento de los patrones y tráfico).
- Todo código ejecutable se explora en busca de códigos dañinos ej., virus, applets dañinos antes de introducirse en la red interna.

Evaluación del riesgo de que no se cumplan los objetivos de control:

- **Llevando a cabo:**

Mediciones (“Benchmarking”) de la seguridad de los sistemas de información con respecto a organizaciones similares o estándares internacionales y buenas prácticas reconocidas en la industria.

Una revisión detallada de la seguridad de los sistemas de la información, incluyendo evaluaciones de penetración de la seguridad física y lógica de los recursos informáticos, de comunicación, etc.

Entrevistas a los nuevos empleados para asegurar el conocimiento y la concienciación en cuanto a seguridad y en cuanto a las responsabilidades individuales, por ejemplo, confirmar la existencia de declaraciones de seguridad firmadas y la formación para nuevos empleados en cuanto a seguridad.

Entrevistas a los usuarios para asegurar que el acceso está determinado tomando como base la necesidad (“menor necesidad”) y que la precisión de dicho acceso es revisada regularmente por la gerencia.

- **Identificando:**

Accesos inapropiados por parte de los usuarios a los recursos del sistema.

Inconsistencias con el esquema o inventario de redes en relación con puntos de acceso faltantes, accesorios perdidos, etc.

Deficiencias en los contratos en cuanto a la propiedad y responsabilidades relacionadas con la integridad y seguridad de los datos en cualquier punto de la transmisión entre el envío y la recepción.

Empleados no verificados como usuarios legítimos o antiguos empleados que cuentan aún con acceso.

Solicitudes informales o no aprobadas de acceso a los recursos del sistema y Software de seguimiento de redes que no indican a la dirección de redes las violaciones de la seguridad.

Defectos en los procedimientos de control de los cambios del software de redes.

La no utilización de llaves secretas en los procedimientos de emisión y recepción de terceros.

Deficiencias en los protocolos para generación de llaves, almacenamiento de distribución, entrada, uso, archivo y protección.

La falta de software actualizado para la detección de virus o de procedimientos formales para prevenir, detectar, corregir y comunicar contaminaciones.

DS 6 Identificar y asignar costes

OBJETIVOS DE CONTROL:

1. Elementos con Cargo.
2. Procedimientos de Coste.
3. Facturas de Usuarios y Procedimientos de Reembolso.

TANTO LOS OBJETIVOS DE CONTROL DETALLADOS COMO LOS DE ALTO NIVEL SON AUDITADOS MEDIANTE:

Obtención de un entendimiento a través de:

- **Entrevistas:**

Gerencia administrativa o de asignación de costes de los servicios de información.

Administración de los usuarios en relación a la facturación y absorción de costes.

- **Obteniendo:**

Políticas y procedimientos generales para la organización relacionados con la planificación y la preparación del presupuesto.

Políticas y procedimientos de los servicios de información relacionados con la agregación de costes, facturación, metodología e informes de desarrollo y costes.

Los siguientes elementos de los servicios de información:

- Presupuesto actual y del año anterior.
- Informes de seguimiento de la utilización de los recursos de los sistemas de información.
- Datos fuente utilizados en la preparación de los informes de seguimiento.
- Metodología o algoritmo de asignación de costes.
- Informes históricos de facturación.

Los siguientes elementos de la dirección de usuarios:

- Presupuesto actual y del año anterior para los costes de los servicios de información.
- Plan de desarrollo y mantenimiento de los sistemas de información del año en curso.
  Gastos presupuestados para los recursos de los sistemas de información, incluyendo aquellos facturados o absorbidos.

Evaluación de los controles:

- **Considerando si:**

Los servicios de información cuentan con un grupo responsable de la información y emisión de facturar a los usuarios.

Existen procedimientos que:

- Crean un plan anual de desarrollo y mantenimiento con la identificación de las prioridades por parte del usuario en cuanto al desarrollo, mantenimiento y gastos operacionales.
- Permiten a los usuarios una determinación de muy alto nivel en cuanto a en qué se gastan los recursos de los servicios de información.
- Generen un presupuesto anual para la función de los servicios de información, incluyendo:

- Cumplimiento con los requerimientos de la organización en cuanto a la preparación de los presupuestos.
- Consistencia en cuanto a qué costes deben ser asignados por los departamentos usuarios.
- Comunicación de los costes históricos, previsión de los nuevos costes – para la comprensión del usuario en cuanto a qué costes son incluidos y facturados.
- Autorización del usuario de todos los costes presupuestados que deben ser asignados por la función de los servicios de información.
- Frecuencia de la emisión de informes y cargo real de costes a los usuarios.

- Seguimiento de los costes asignados de todos los recursos de los sistemas de información en cuanto pero sin limitarse a:

- Hardware operacional.
- Equipo periférico.
- Utilización de telecomunicaciones.

- Desarrollo y soporte de aplicaciones.
- Generales administrativos.
- Costes por servicios de proveedores externos.
- Help desk.
- Instalaciones y mantenimiento.
- Costes directos e indirectos.
- Gastos fijos y variables.
- Costes discrecionales.

- Asisten en la emisión regular de informes para los usuarios en cuanto al rendimiento para las distintas categorías de coste.
- Informan a los usuarios en cuanto a mediciones ("benchmarks") externas relacionadas con la efectividad de los costes, con el fin de permitir una comparación con respecto a las expectativas de la industria u otras fuentes alternativas de servicios para los usuarios.
- Permiten la modificación oportuna de la asignación de costes para reflejar los cambios en las necesidades del negocio.
- Aprueban y aceptan formalmente los cargos al ser recibidos.
- Identifican las oportunidades de mejora de los servicios de información para reducir las facturaciones o para obtener un mejor valor por los cargos.

Los informes aseguran que los elementos sujetos a coste son identificables, medibles y predecibles.

Los informes capturan y resaltan los cambios en los componentes de coste o en el algoritmo de asignación.

Evaluación de la suficiencia:

- **Probando que:**

Existe una metodología de asignación de costes, que los usuarios están de acuerdo en cuanto a su equidad, y que genera tanto costes como informes.

Existe un programa de mejora para reducir costes o aumentar el resultado de los recursos de los sistemas de información.

Los procesos de asignación e informe fomentan el uso más apropiado, efectivo y consistente de los recursos de las TI, éstos aseguran el tratamiento justo de los departamentos de usuarios y sus necesidades, y los cargos reflejan los costes asociados con la prestación de servicios.

Evaluación del riesgo de que no se cumplan los objetivos de control:

- **Llevando a cabo:**

Mediciones (“Benchmarking”) de la contabilidad de costes y de la metodología de facturación comparando con organizaciones similares o estándares internacionales y buenas prácticas reconocidas en la industria.

Un cálculo de la facturación a partir de datos fuente, a través de un algoritmo de asignación de facturación y dentro del flujo de informes a usuarios.

La precisión de los datos en el informe de resultados, como:

- Utilización de la CPU.
- Utilización de los periféricos.
- Utilización de DASD.
- Líneas de código escritas.
- Líneas y páginas impresas.
- Modificaciones de programas llevados a cabo.
- Número de PCs, teléfonos, archivos de datos.
- Consultas al help desk.
- Número, duración de las transmisiones.

La compilación de los datos fuente de recursos en el informe de resultado es correcta.

Utilización de un algoritmo real para compilar y asignar costes a la facturación.

La comprobación frecuente de la precisión de la facturación de los usuarios específicos.

Las facturaciones a los usuarios sean aprobadas.

Se lleven a cabo revisiones consistentes de la facturación entre los diferentes usuarios.

El progreso en el plan de desarrollo de los usuarios tenga como base los costes expendidos.

Se lleve a cabo una revisión de la distribución de informes en cuanto a la utilización e información sobre los costes.

La satisfacción del usuario en cuanto a :

- Lo razonable de la facturación comparada con las expectativas presupuestadas.

- El plan de desarrollo anual con respecto a los costes.
- Lo razonable de la facturación comparada con las fuentes alternativas, por ejemplo “benchmarks”.
- La comunicación de las tendencias que incrementaría o disminuiría la facturación.
- Solución de las variaciones comparadas con la facturación esperada.

Identificando:

Oportunidades para una mayor efectividad y propiedad de la metodología de facturación:

- Incluyendo más componentes de costes.
- Modificando los índices o unidades de medida de asignación de costes.
- Modificando el algoritmo mismo de los costes.
- Mecanizando o integrando la función de contabilidad y los informes generados por aplicaciones.

Inconsistencias dentro del algoritmo de asignación.

Inconsistencias de asignación entre los diferentes usuarios.

Oportunidades para la mejora de los recursos de los sistemas.

Oportunidades para el usuario con el fin de aplicar de una mejor manera los recursos de los servicios de información para alcanzar los requerimientos de negocios del usuario.

Mejoras en la eficiencia de los procesos de recopilación, acumulación, asignación, informe y comunicación, los cuales se traducirán en un mejor resultado o menor coste para los usuarios de los servicios proporcionados.

Que las tendencias de costes reflejadas por las variaciones y el análisis hayan sido traducidas a cargos modificados en los períodos siguientes y hayan sido reflejadas en la estructura de costes.

Que existen oportunidades para hacer de los servicios de información un centro de provecho y beneficios al proporcionar servicios a otros usuarios internos o externos.

Si la función de los servicios de información es un centro de provecho y beneficios, que la contribución de dichos beneficios se ajusten al plan y el presupuesto y que destaquen las oportunidades para aumentar los beneficios.

DS 7 Educar y Capacitar a los Usuarios

OBJETIVOS DE CONTROL:

1 Identificación de las necesidades de formación.

2 Organización del Formación.

3 Principio de Seguridad y Conciencia del Formación.

TANTO LOS OBJETIVOS DE CONTROL DETALLADOS COMO LOS DE ALTO NIVEL SON AUDITADOS MEDIANTE:

Obtención de un entendimiento a través de:

- **Entrevistas:**

Director de formación o de recursos humanos de la organización.

Director de formación o de recursos humanos de los servicios de información.

Responsable y empleados seleccionados de los servicios de información.

Responsables y empleados seleccionados de los departamentos de usuarios.

- **Obteniendo:**

Políticas y procedimientos generales para la organización con respecto a la formación sobre controles y conciencia sobre seguridad, beneficios para los empleados enfocados al desarrollo, programas de formación para los usuarios de los servicios, instalaciones educacionales y requerimientos de educación continua profesional.

Programas, políticas y procedimientos de formación y de educación de los servicios de información relacionados con controles y concienciación sobre seguridad, seguridad técnica y controles.

Programas de formación disponibles (tanto internos como externos) sobre seguridad y conciencia sobre controles introductorios y continuos, así como para formación dentro de la organización.

Evaluación de los controles:

- **Considerando si:**

Existen políticas y procedimientos relacionados con una concienciación continuada sobre seguridad y controles.

Se cuenta con un programa de educación y formación enfocado a los principios de seguridad de los sistemas de información y de control.

Los nuevos empleados tienen conocimiento y conciencia de la responsabilidad sobre seguridad y control con respecto a la utilización y la custodia de los recursos de los sistemas de información.

Se cuenta con políticas y procedimientos vigentes relacionados con la formación y si éstos están actualizados con respecto a la configuración técnica de los recursos de los sistemas de información.

Existe disponibilidad de oportunidades de formación interna, considerando también la asistencia a los empleados.

Existe disponibilidad de oportunidades de formación técnica externa, considerando también la asistencia a los empleados.

Si una función de formación asesora sobre las necesidades de formación del personal con respecto a la seguridad y controles, trasladando estas necesidades en oportunidades de formación tanto interna como externa.

Se requiere a todos los empleados asistir a la formación sobre concienciación de la necesidad de control y seguridad continuamente, esta información incluirían, sin limitarse a:

- Principios generales de seguridad de los sistemas.
- Conducta ética de los servicios de información.
- Prácticas de seguridad para la protección contra daños ocasionados por fallos que afectan la disponibilidad, confidencialidad, integridad y resultado de las funciones de una forma segura.
- Existen las responsabilidades asociadas con la custodia y utilización de los recursos de los sistemas de información.
- La seguridad de la información y los sistemas de información cuando se utilizan externamente.

La capacitación sobre la sensibilización respecto a la seguridad incluye una política para evitar la exposición de la información sensible a través de conversaciones (ej., avisando sobre el estado de la información a todas las personas que toman parte en la conversación).

Evaluación de la suficiencia:

- **Probando que:**

Los nuevos empleados tienen conciencia y conocimiento sobre seguridad, controles y responsabilidades fiduciarias de poseer y utilizar recursos de los sistemas de información.

Las responsabilidades de los empleados con respecto a la confiabilidad, integridad, disponibilidad, confidencialidad y seguridad de todos los recursos de los sistemas de información es comunicada continuamente.

Un grupo de los servicios de información es formalmente responsable de la formación, concienciación sobre seguridad y controles, y mantenimiento de programas de educación continua para certificaciones profesionales.

Se considera continuamente la evaluación de las necesidades de formación para los empleados.

El desarrollo o la participación en los programas de formación relacionados con la seguridad y los controles es parte de los requerimientos de formación.

Existen programas reales nuevos y a largo plazo de formación y concienciación sobre seguridad para los empleados.

Los acuerdos de confidencialidad son firmados por todos los empleados.

No faltan estatutos de confidencialidad y conflicto de intereses para los empleados.

No faltan evaluaciones de necesidades de formación para los empleados.

Evaluación del riesgo de que no se cumplan los objetivos de control:

- **Llevando a cabo:**

Una revisión de los manuales de formación en cuanto a su adecuación y suficiencia con respecto a los controles de seguridad, confidencialidad, confiabilidad, disponibilidad e integridad.

Entrevistas al personal de los servicios de información para determinar la identificación de las necesidades de formación y la extensión o satisfacción de tales necesidades

- **Identificando:**

Inconsistencias en el currículum ofrecido como respuesta a las necesidades de formación.

Deficiencias en la concienciación de los usuarios en cuanto a los problemas de seguridad relacionados con la utilización de los recursos de los sistemas de información.

DS 8 Asistir y Orientar a los Clientes de las TI

OBJETIVOS DE CONTROL:

1 Ayuda.

2 Registro de preguntas de los Clientes.

3 Escalación de las preguntas de los clientes.

4 Supervisión de Aprobación.

5 Análisis de Tendencias e Informes.

TANTO LOS OBJETIVOS DE CONTROL DETALLADOS COMO LOS DE ALTO NIVEL SON AUDITADOS MEDIANTE:

Obtención de un entendimiento a través de:

- **Entrevistas:**

  Director de soporte del help desk de los sistemas de información.

  Usuarios seleccionados de los servicios de información.

- **Obteniendo:**

Políticas y procedimientos generales para la organización relacionados con el soporte proporcionado a los usuarios de los servicios de información.

Organigrama, misión, políticas y procedimientos de los servicios de información relacionados con las actividades del help desk.

Informes relacionados con la preguntas de los usuarios, su solución y estadísticas de resultado del help desk.

Cualquier estándar de resultado para las actividades del help desk.

Acuerdos de nivel de servicios entre los servicios de información y los diversos usuarios.

Archivos personales que muestran las credenciales y experiencia profesional del personal del help desk.

Evaluación de los controles:

- **Considerando si:**

La función del help desk (por ejemplo, la forma en la que las solicitudes de ayuda son procesadas y la ayuda es proporcionada) es efectiva.

Existen instalaciones reales, divisiones o departamentos que lleven a cabo la función del help desk, así como personal o posiciones responsables del help desk.

El nivel de documentación para las actividades del help desk es el adecuado y está actualizado.

Existe un proceso real para registrar solicitudes de los servicios y si se hace uso de dicho log.

El proceso para la priorización de preguntas y la intervención de la administración para su solución son suficientes.

El período de los tiempos para atender las preguntas recibidas es adecuado.

Existen los procedimientos para el seguimiento de las tendencias e informes proporcionados por el help desk.

Se identifican y ejecutan formalmente iniciativas de mejora del resultado.

Se alcanzan y se cumple con los acuerdos de nivel de servicio y los estándares.

El nivel de satisfacción del usuario se revisa periódicamente y se informa.

Evaluación de la suficiencia:

- **Probando que:**

Las políticas y procedimientos están actualizados y son precisos en relación con las actividades del help desk.

Los compromisos de nivel de servicio se conservan y las variaciones se explican.

Las preguntas son atendidas de una forma oportuna.

El análisis e informe de las tendencias asegura que los informes:

- Son emitidos y que se toman las medidas necesarias para mejorar el servicio.
- Incluyen problemas específicos, análisis de tendencias y tiempos de respuesta.
- Son enviados a las personas responsables con la autoridad suficiente para resolver los problemas.

Se obtienen para una muestra de solicitudes de ayuda, confirmación de la precisión, oportunidad y suficiencia de la respuesta.

Las encuestas sobre el nivel de satisfacción del usuario existen y se trabaja con ellas.

Evaluación del riesgo de que no se cumplan los objetivos de control:

- **Llevando a cabo:**

Entrevistas con los usuarios seleccionados para determinar su satisfacción en cuanto a:

- Actividades de help desk.
- Informe de actividades.
- Cumplimiento de los compromisos del nivel de servicio.

Una revisión de la competencia y capacidad del personal del help desk con respecto a la realización de sus tareas.

Una revisión de las preguntas seleccionadas priorizadas en cuanto a lo adecuado de sus respuestas.

Una revisión de los informes de las tendencias y posibles oportunidades de mejoras del resultado.

- **Identificando:**

Interacciones inadecuadas de las actividades del help desk con respecto a otras funciones dentro de los servicios de información, así como con las organizaciones usuarias.

Procedimientos y actividades insuficientes relacionados con problemas en el informe de recepción, registro, seguimiento, priorización y solución de preguntas.

Deficiencias en el proceso de priorización con respecto a la falta de involucramiento por parte de la administración o a acciones correctivas efectivas.

Oportunidad inadecuada del informe de problemas o insatisfacción del usuario en cuanto al proceso de información sobre los problemas.

DS 9 Gestionar la Configuración

OBJETIVOS DE CONTROL:

1 Registro de la Configuración.

2 Línea Base de la Configuración.

3 Contabilidad del Estado.

4 Control de la Configuración.

5 Software no Autorizado.

6 Almacenamiento de Software.

7 Procedimientos de Gestión de la Configuración.

8 Contabilidad Software.

TANTO LOS OBJETIVOS DE CONTROL DETALLADOS COMO LOS DE ALTO NIVEL SON AUDITADOS MEDIANTE:

Obtención de un entendimiento a través de:

- **Entrevistas:**

Dirección de operaciones de los servicios de Información.

Dirección de soporte de los sistemas de los servicios de información.

Dirección de desarrollo de las aplicaciones de los servicios de información.

Administración de las instalaciones.

Personal soporte de los proveedores de software.

Personal de administración de activos relacionados con ordenadores.

Director de seguridad de la calidad.

- **Obteniendo:**

Un inventario de la configuración: hardware, software del sistema operativo, software de aplicaciones, instalaciones y archivos de datos –dentro y fuera de las instalaciones.

Políticas y procedimientos de la organización relacionados con la adquisición, inventario y disposición de software y equipo informático comprado, o arrendado.

Políticas de la organización relacionadas con la utilización del software o equipo no autorizado.

Políticas y procedimientos de los servicios de información relacionados específicamente con la adquisición, disposición y mantenimiento de los recursos de la configuración.

Políticas y procedimientos de los servicios de información relacionados con asegurar la calidad y el control de los cambios en cuanto a la transferencia independiente y el registro de la migración del desarrollo del software nuevo y modificado hacia los archivos y estado de producción.

Información sobre las líneas básicas de la configuración.

Registros contables de los activos fijos y arrendamientos relacionados con los recursos de los sistemas.

Informes relacionados con adiciones, eliminaciones y cambios de la configuración de los sistemas.

Listas del contenido de las distintas librerías – prueba, desarrollo y producción.

Inventario del contenido del almacenamiento fuera de las instalaciones – equipo, archivos, manuales y formas – incluyendo material en manos de los proveedores.

Evaluación de los controles:

- **Considerando si:**

El proceso para crear y controlar las bases de la configuración (el punto en el diseño y desarrollo de un elemento de la configuración más allá del cual no se producen más avances sin llevar a cabo un estricto control de la configuración) es apropiado.

Existen funciones para mantener la base de la configuración.

Existe un proceso para controlar el estado de los recursos adquiridos y arrendados, incluyendo entradas, salidas e integración con otros procesos.

Los procedimientos de control de la configuración incluyen:

- Integridad en la base de la configuración.
- Controles de autorización de acceso programados en el sistema de administración de cambios.
- La recuperación de los elementos de la configuración y las solicitudes de cambios en cualquier momento.
- La terminación de la configuración y de los informes que evalúan lo adecuado de los procedimientos de registro de la configuración.
- Evaluaciones periódicas del registro de la configuración.
- El personal responsable de la revisión de que el control de la configuración satisfaga los requerimientos de conocimientos, destrezas y habilidades.
- La existencia de procedimientos para revisar el acceso a las bases del software.
- Los resultados de las revisiones proporcionados a la dirección para llevar a cabo acciones correctivas.

Se lleva a cabo regularmente una revisión periódica de la configuración con registros del inventario y de las cuentas.

La configuración cuenta con historia suficiente para realizar un seguimiento de los cambios.

Existen procedimientos de control de cambios del software para:

- Establecer y mantener una librería de programas con licencia.

- Asegurar que la librería de programas con licencia se controla adecuadamente.
- Asegurar la confiabilidad e integridad del inventario del software.
- Asegurar la confiabilidad e integridad del inventario del software autorizado y utilizado, y revisar la existencia del software no autorizado.
- Asignar responsabilidades sobre el control del software no autorizado a un miembro específico del personal.
- Registrar el uso del software no autorizado e informar a la administración para llevar a cabo acciones correctivas.
- Determinar si la administración llevó a cabo acciones correctivas sobre las violaciones.

Los procesos de migración de aplicaciones de desarrollo al entorno de pruebas y finalmente al estado de producción interactúan con el informe de la configuración.

El proceso de almacenamiento del software incluye:

- Definir un área segura de almacenamiento de los archivos (librería) válidos para todo el software y las distintas fases del ciclo de vida de desarrollo de los sistemas.
- Solicitar separación de las librerías de almacenamiento del software entre ellas y con respecto a las áreas de almacenamiento de los archivos de desarrollo, pruebas y producción.
- Requerir la existencia dentro de las librerías fuente que permiten la colocación temporal de módulos fuente a transferirse al período del ciclo de producción.
- Solicitar que cada miembro de todas las librerías cuente con un propietario designado.
- Definir controles de acceso lógicos y físicos.
- Establecer responsabilidades sobre el software.
- Establecer un seguimiento de la auditoría.
- Detectar, documentar e informar a la administración de todas las instancias en las que no se cumple con este procedimiento.
- Determinar si la administración llevó a cabo acciones correctivas.

Existe una coordinación entre el desarrollo de las aplicaciones, el proceso de asegurar la calidad y las operaciones con respecto a la actualización de la configuración base al realizarse cambios.

Evaluación de la suficiencia:

- **Probando que:**

Todos los elementos de la configuración se encuentran bajo control.

Las políticas y procedimientos relacionados con el informe sobre la configuración están actualizados y son precisos.

Se cumple con los estándares de resultado con respecto al mantenimiento e informe de la configuración.

Se lleva a cabo una comparación entre el inventario físico del equipo y los registros de contabilidad de los activos.

Existe independencia de la migración de pruebas a producción, y registro de los cambios.

Para una selección de salidas básicas:

- Se tiene una base precisa, apropiada y aprobada de los elementos de la configuración.
- Los registros de la configuración reflejan el estado actual de todos los elementos de la configuración, incluyendo la historia de los cambios.
- La administración revisa y evalúa periódicamente la consistencia de la configuración, y que se lleven a cabo acciones correctivas.
- Las librerías de archivos han sido definidas conveniente y adecuadamente y en las diferentes fases del ciclo de vida de desarrollo de los sistemas.
- Para todos los ordenadores personales que tienen software no autorizado se informa sobre las violaciones y la administración lleva a cabo las acciones correctivas oportunas.
- Los registros de la configuración con respecto al producto, versión y modificaciones de los recursos proporcionados por los proveedores son precisos.
- Los registros históricos de los cambios de la configuración son precisos.
- Existen mecanismos para asegurar que no existe un software no autorizado en los ordenadores, incluyendo:

- Políticas y estatutos.
- Formación y conciencia de las responsabilidades potenciales (legales y de producto).
- Formas firmadas de cumplimiento por parte de todo el personal que utilice los ordenadores.
- Control centralizado del software informático.
- Revisión continua del software informático.
- Informes de los resultados de la revisión.

- Acciones correctivas por parte de la administración basadas en los resultados de las revisiones.
- El almacenamiento de programas de aplicación y código fuente se define durante el ciclo de desarrollo y el impacto de los registros de la configuración se ha determinado.
- La suficiencia e integridad de los registros de los proveedores relacionados con la configuración, así como la precisión en los registros de la configuración anticipados y considerados.
- Se definen procedimientos base de la configuración para:

- Registrar lo que creó la base, el establecimiento de la base y los elementos de la configuración que deben ser controlados.
- Modificar la base, incluyendo la autoridad requerida para aprobar los cambios base de la configuración aprobadas previamente.
- Registrar los cambios base y los elementos de la configuración que deben ser controlados.
- Asegurar que todos los elementos de la configuración se registran dentro de los productos.

Existe el informe de estado de la cuenta para:

- El tipo de información que debe ser recopilada, almacenada, procesada y transmitida (Esto deberá incluir el estado de la base, los hallazgos en las revisiones, solicitudes de cambios y estados; revisión y aprobación, y desaprobación del control de la configuración; modificaciones realizadas; informes de los problemas y estado y la historia de la revisión de la configuración).
- La manera en la que los problemas de las solicitudes de cambio se resuelven con un estado de cuenta incompleto.
- Los tipos de informes de estado de cuenta generados y su frecuencia.
- La manera en la que el acceso a estos datos de estado se controlan.

Evaluación del riesgo de que no se cumplan los objetivos de control:

- **Llevando a cabo:**

Una revisión detallada de la frecuencia y la oportunidad de las revisiones administrativas de los registros de la configuración, los cambios en los registros y la conciliación de los registros de inventario, contabilidad y proveedores.

Un análisis del software de varias librerías en cuanto a posible duplicidad, identificación del código objeto que falta y en cuanto a la eliminación de los

archivos de datos o programas innecesarios -- y su reflejo en los registros de la configuración.

- **Identificando:**

Las debilidades en la conciencia y en el conocimiento de la administración y el personal en cuanto a las políticas de la organización con respecto a:

- Los registros de la configuración y los cambios realizados en estos registros.
- El establecimiento de los controles de configuración en el ciclo de vida de desarrollo de los sistemas. La integración de los registros de configuración, contabilización y proveedores.
- La no utilización del software no autorizado en ordenadores personales.

Posibles mejoras inadecuadas de la efectividad y la eficiencia de la creación y mantenimiento de la base de la configuración.

Deficiencias en los cambios de los proveedores al reflejarse en los registros de la configuración, en los registros de seguridad, o cambios en los registros por parte de los proveedores reflejados apropiadamente.

DS 10 Gestionar los Problemas e Incidencias

OBJETIVOS DE CONTROL:

1 Sistema de Gestión de Problemas.

2 Escalación del Problema.

3 Seguimiento del Problema y Pista de Auditoría.

4 Autorizaciones de acceso temporales y de emergencia

5 Prioridades del procesamiento de emergencia

TANTO LOS OBJETIVOS DE CONTROL DETALLADOS COMO LOS DE ALTO NIVEL SON AUDITADOS MEDIANTE:

Obtención de un entendimiento a través de:

- **Entrevistas:**

Personal soporte de las operaciones de los servicios de información.

Personal soporte del help desk de los servicios de información.

Personal soporte de los sistemas de los servicios de información.

Personal soporte de las aplicaciones de los servicios de información.

Usuarios seleccionados como recursos de los sistemas de información.

- **Obteniendo:**

Un resumen de las facilidades y posiciones de solución de los problemas que realiza la función de gestión de problemas.

Políticas y procedimientos de los servicios de información relacionados con el control de los problemas, incluyendo procesos de reconocimiento, registro, solución, priorización, seguimiento e informe.

Una lista informando sobre los problemas existentes durante un período representativo, incluyendo la fecha de aparición, la fecha de priorización, la fecha de solución y los tiempos de solución.

Una lista de las aplicaciones críticas que envían inmediatamente a la atención de la Dirección para darles prioridad de solución, o que son transmitidas como problemas críticos.

Un conocimiento de cualquier aplicación de solución de problemas, y en particular un método para asegurar que todos los problemas son capturados, resueltos y transmitidos según lo requerido.

Evaluación de los controles:

- **Considerando si:**

Existe un proceso de gestión de problemas que asegura que todos los hechos operacionales que no son parte de las operaciones estándar se registran, analizan y resuelven de forma oportuna, y se generan informes de incidentes y problemas significativos.

Existen procedimientos de gestión de problemas para:

- Definir e implementar un sistema de gestión de problemas.
- Registrar, analizar y resolver de manera oportuna todos los acontecimientos que no son estándar.

- Establecer informes sobre los incidentes en los eventos críticos y la emisión de informes para los usuarios.
- Identificar los tipos de problemas y metodología de priorización que permiten una variedad de soluciones tomando el riesgo como base.
- Definir controles lógicos y físicos de la información para la gestión de problemas.
- Distribuir salidas con una base de “necesidad de conocimiento”.
- Seguir las tendencias de los problemas para maximizar los recursos y reducir la rotación.
- Recolectar entradas de datos precisas, actualizadas, consistentes y utilizadas para la emisión de informes.
- Notificar las priorizaciones al nivel apropiado de la administración.
- Determinar si la administración evalúa periódicamente el proceso de gestión de los problemas en cuanto a una mayor efectividad y eficiencia.
- Asegurar la suficiencia del seguimientos de auditoría para los problemas de los sistemas.
- Asegurar la integración entre los cambios, la disponibilidad, el sistema y el personal que gestiona la configuración.

Evaluación de la suficiencia:

- **Probando que:**

Una muestra seleccionada de salidas de procesos cumple con los procedimientos establecidos relacionados con:

- Problemas no críticos.
- Problemas críticos y de alta prioridad que necesitan una priorización.
- El informe de los requerimientos, el contenido, la precisión, la distribución y las acciones llevadas a cabo.
- La satisfacción del usuario con el proceso de gestión de los problemas y los resultados.

Vía entrevistas, el conocimiento y la conciencia del proceso de gestión de los problemas.

Evaluación del riesgo de que no se cumplan los objetivos de control:

- **Llevando a cabo:**

Para una , incluyendo:

- Registro de todos los eventos no estándar por proceso.

- Seguimiento y solución de todos y cada uno de los eventos.
- Nivel apropiado de respuesta tomando como base la prioridad del echo.
- Priorización de problemas para eventos críticos.
- Informe apropiado dentro de los servicios de información y los grupos de usuarios.
- Revisiones regulares de la efectividad y eficiencia de los procesos en cuanto a mejoras.
- Expectativas y éxito del programa de mejoras del resultado.

- **Identificando:**

Problemas no controlados formalmente por el proceso de gestión de los problemas.

Problemas reconocidos pero no resueltos por el proceso de gestión de los problemas.

Variaciones entre los hechos de procesos reales y formales con respecto a la solución de los problemas.

Deficiencias de los usuarios en el proceso de gestión de los problemas, en la comunicación de los mismos y su solución - en cuanto a posibles oportunidades de mejora.

DS 11 Administrar Datos

OBJETIVOS DE CONTROL:

1 Procedimientos de Preparación de Datos.

2 Procedimientos de Autorización de Documentos Fuente.

3 Confección de Datos de Documentos Fuente.

4 Gestión de Errores de Documentos Fuente.

5 Retención de Documentos Fuente.

6 Procedimientos de Autorización de Entrada de Datos.

7 Chequeos de Exactitud, Compilación y Autorización.

8 Tratamiento de Errores de Entrada de Datos.

9 Integridad de Procesamiento de Datos.

10 Validación y Edición de Procesamiento de Datos.

11 Tratamiento de Errores del Procesamiento de Datos.

12 Tratamiento y Retención de la Salida.

13 Distribución de la Salida.

14 Balanceo y Reconciliación de la Salida.

15 Revisión de la Salida y Tratamiento de Errores.

16 Provisiones de Seguridad para los Informes de Salida.

17 Protección de la Información Sensible durante su Transmisión y Transporte.

18 Protección de la Información Sensitiva Desechada.

19 Gestión del Almacenamiento.

20 Períodos de Retención y Plazos de Almacenamiento.

21 Sistema de Gestión de las Librerías de Medios de Almacenamiento.

22 Responsabilidades de la Gestión de las Librería de Medios de Almacenamiento.

23 Salvaguarda y Recuperación.

24 Trabajos de Salvaguarda.

25 Almacenamiento de las copias de Seguridad.

26 Archivo.

27 Protección de los Mensajes sensibles.

28 Autentificación e Integridad.

29 Integridad de las Transacciones Electrónicas.

30 Integridad continuada de los Datos Almacenados.

TANTO LOS OBJETIVOS DE CONTROL DETALLADOS COMO LOS DE ALTO NIVEL SON AUDITADOS MEDIANTE:

Obtención de un entendimiento a través de:

- **Entrevistas:**

  Administración de las operaciones de los servicios de información.

  Administración de las bases de datos de los servicios de información.

  Administración del desarrollo de las aplicaciones de los servicios de información.

  Administración de formación y recursos humanos de los servicios de información.

  Administración del soporte de los sistemas de los servicios de información.

  Administración de la seguridad de las copias de seguridad.

  Administraciones de los usuarios para aplicaciones críticas.

- **Obteniendo:**

Políticas y procedimientos de la organización relacionados con la naturaleza y administración de los datos, incluyendo:

- Flujo de datos dentro de los servicios de información y entre los usuarios de los datos.
- Puntos en la organización donde se originan los datos, concentrados en grupos o tandas (“batched”), editados, capturados, procesados, extraídos, revisados, corregidos y remitidos, y distribuidos a los usuarios.
- Proceso de autorización de los documentos fuente.
- Procesos de recolección, seguimiento y transmisión de los datos.
- Procedimientos para asegurar la suficiencia, precisión, registro y transmisión de los documentos fuente completos.
- Procedimientos utilizados para identificar y corregir errores durante la creación de los datos.
- Procedimientos para asegurar la integridad, confidencialidad y aceptación de los mensajes delicados transmitidos por Internet o cualquier otra red pública.

- Métodos utilizados por la organización para retener documentos fuente (archivo, imagen, etc.), para definir qué documentos deben ser retenidos, los requerimientos de retención legales y regulatorios, etc.
- Sistemas de interface que proporcionan y utilizan datos para los servicios de información.
- Contratos de los proveedores para llevar a cabo las tareas de administración de datos.
- Informes administrativos utilizados para realizar un seguimiento de las actividades e inventarios.

Una lista de todas las principales aplicaciones, así como de la documentación para el usuario relacionada con:

- Módulos que llevan a cabo revisiones de precisión, suficiencia y autorización de obtención de datos.
- Funciones que llevan a cabo entradas de datos para cada aplicación.
- Funciones que llevan a cabo rutinas de corrección de errores de la entrada de datos.
- Métodos utilizados para prevenir (por medios manuales y programados), detectar y corregir errores.
- Control de la integridad de los procesos de datos emitidos.
- Edición y autentificación de la validación del procesamiento de los datos tan cerca del punto de origen como sea posible.
- Gestión y retención de las salidas creadas por aplicaciones.
- Salidas, distribución de salidas y sistemas de interface que utilizan salidas.
- Procedimientos de obtención de salidas para el control de los totales y conciliación de las variaciones.
- Revisión de la precisión de los informes de salida y de la información.
- Seguridad en los informes de procesamiento de salidas.
- Seguridad de los datos transmitidos y entre aplicaciones.
- Disposición de documentación sensible de entrada, proceso y salida.
- Procedimientos de control de los proveedores como terceros con respecto a la preparación, entrada, procesamiento y salida.

Políticas y procedimientos relacionados con cualquier depósito de las bases de datos de la organización, incluyendo:

- Organización de la base de datos y diccionario de datos.
- Procedimientos de mantenimiento y seguridad de las bases de datos.
- Determinación y mantenimiento de la propiedad de las bases de datos.
- Procedimientos de control de los cambios sobre el diseño y contenido de las bases de datos.

- Informes administrativos y seguimientos de auditoría que definen actividades de las bases de datos.

Políticas y procedimientos relacionados con la librería de medios y con el almacenamiento de datos fuera del sitio, incluyendo:

- Administración de la librería de medios y del sistema de administración de la librería.
- Requerir la identificación externa de todos los medios.
- Requerir el inventario actual de todos los contenidos y procesos para las actividades de control.
- Procesos de la administración para proteger los recursos de datos.
- Procedimientos de conciliación entre los registros reales y de datos.
- Reciclaje de los datos y rotación de los datos medios.
- Datos de pruebas pasadas de las pruebas de inventario y recuperaciones llevadas a cabo.
- Funciones del personal en los planes de gestión de desastres y recuperación del negocio.

Evaluación de los controles:

- **Considerando si:**

  Para la preparación de los datos:

- Los procedimientos de preparación de datos aseguran suficiencia, precisión y validez.
- Existen procedimientos de autorización para todos los documentos fuente.
- Existe una separación de las funciones entre el origen, la aprobación y la conversión de los documentos fuente a datos.
- Los datos autorizados permanecen completos, precisos y válidos a través de la creación original de los documentos fuente.
- Los datos se transmiten de manera oportuna.
- Se lleva a cabo una revisión periódica de los documentos fuente en cuanto a su suficiencia y aprobaciones apropiadas.
- Se lleva a cabo una gestión apropiada de los documentos fuente erróneos.
- Existe un control adecuado de la información sensible en los documentos fuente en cuanto a protección contra transgresiones.
- Los procedimientos aseguran suficiencia y precisión de los documentos fuente, contabilidad apropiada y conversión oportuna.
- La retención de los documentos fuente es lo suficientemente larga para permitir: la reconstrucción en caso de pérdida, la disponibilidad para

revisiones y auditoría, las averiguaciones de litigación o los requerimientos regulatorios.

Para la entrada de datos:

- Los documentos fuente siguen un proceso de aprobación apropiada antes de su obtención.
- Existe una separación apropiada de las funciones entre las actividades de envío, aprobación, autorización y entrada de datos.
- Existen códigos únicos para el terminal o estación e identificaciones seguras de los operadores.
- Existen procesos de uso, mantenimiento y control de los códigos de estación e identificadores de operador.
- Se lleva a cabo un seguimiento de la auditoría para identificar la fuente de entrada.
- Existen verificaciones de rutina o revisiones de la edición de los datos obtenidos tan cerca del punto de origen como sea posible.
- Existen procesos apropiados de gestión de los datos erróneos de entrada.
- Se asignan claramente las responsabilidades para cumplir con la autorización apropiada de los datos.

Para el procesamiento de datos:

- Los programas contienen rutinas de prevención, detección y corrección de errores.
- Los programas deben probar las entradas en cuanto a errores (por ejemplo, validación y edición).
- Los programas deben validar todas las transacciones con respecto a una lista maestra.
- Los programas deben rechazar la anulación de las condiciones de error.

Los procesos de gestión de errores incluyen:

- La aprobación de la corrección y del reenvío de errores.
- La definición de las responsabilidades individuales para archivos suspendidos.
- La generación de informes de errores no resueltos por parte de los archivos en suspenso.
- La disponibilidad del esquema de priorización de archivos suspendidos tomando como base la edad y el tipo.

Existen logs de los programas ejecutados y las transacciones procesadas y rechazadas para los propósitos de auditoría.

Existe un grupo de control para realizar un seguimiento de las actividades de entrada e investigar los eventos no estándar, así como realizar un control de las cuentas de los registros y los totales de control para todos los datos procesados.

Todos los campos son editados apropiadamente, aunque uno de los campos contenga algún error.

Las tablas utilizadas en la validación son revisadas frecuentemente.

Existen procedimientos por escrito para la corrección y reenvío de datos con errores incluyendo una solución no descriptiva para volver a procesarlos.

Las transacciones reenviadas son procesadas exactamente como fueron procesadas originalmente.

La responsabilidad de la corrección de los errores reside dentro de la función de envío original.

Los sistemas de Inteligencia Artificial están colocados en un Marco de Referencia de control interactivo con los operadores que aseguran que las decisiones importantes se aprueban.

Para las salidas, interfaces y distribución:

El acceso a las salidas está restringido física y lógicamente al personal autorizado.

Se lleva a cabo una revisión continua de las necesidades de salidas.

Las salidas son comparadas rutinariamente con respecto a los totales de control.

Existen seguimientos de auditoría para facilitar el seguimiento del procesamiento de las transacciones y la conciliación de datos confusos.

La precisión de los informes de salida se revisa y los errores existentes en las salidas se revisan por personal capacitado.

Existe una definición clara de los problemas de seguridad durante las salidas, interfaces y distribución.

Las violaciones de la seguridad durante cualquier fase se comunican a la administración, se llevan a cabo acciones correctivas sobre ellas y se reflejan apropiadamente en nuevos procedimientos.

El proceso y la responsabilidad de la disposición de las salidas está claramente definida.

La destrucción de los materiales utilizados pero no solicitados después de ser procesados es presenciada por alguien.

Todos los medios de entrada y salida se almacenan fuera en caso de requerirse en un futuro.

La información marcada como eliminada cambia de tal forma que no se puede recuperar.

Para la librería de medios:

El contenido de la librería de medios es inventariada sistemáticamente.

Las discrepancias descubiertas por el inventario se solucionan oportunamente.

Se toman medidas para mantener la integridad de los medios magnéticos almacenados en la librería.

Existen procesos de administración para proteger el contenido de la librería de medios.

Las responsabilidades de la administración de la librería de medios se asignan a miembros específicos del personal de los servicios de información.

Existen estrategias de copias de seguridad y restauración de medios.

Las copias de seguridad de medios se llevan a cabo de acuerdo con la estrategia de copias de seguridad y la utilidad de las mismas se verifica regularmente.

Las copias de seguridad de medios se almacenan con seguridad y el almacén se revisa periódicamente en cuanto a la seguridad de su acceso físico y a la seguridad de los archivos de datos y otros elementos.

Los periodos de mantenimiento y almacenamiento se definen con documentos, datos, programas, informes y mensajes (de entrada y salida) así como los datos (claves, certificados) utilizados para su encriptación y autentificación.

Los procedimientos adecuados están activos en relación con el archivo de información (datos y programas) en línea con los requerimientos legales y del negocio y reforzando la capacidad de respuesta y reproducción.

Para la autentificación e integridad de la información:

La integridad de los archivos de datos se verifica periódicamente.

Las solicitudes externas a la organización recibidas por vía telefónica o correo de voz se verifican confirmando por teléfono o algún otro medio de autentificación.

Un método preestablecido se utiliza independiente de la verificación de la autentificación de la fuente y el contenido de las solicitudes de transacción recibidas vía fax o sistema de imágenes.

La firma electrónica o la certificación se utiliza para verificar la integridad y autenticidad de los documentos electrónicos que entran.

Evaluación de la suficiencia:

- **Probando que:**

La preparación de datos:

Para una muestra seleccionada de documentos fuente, existe consistencia evidente con respecto a los procedimientos establecidos relacionados con la autorización, aprobación, precisión, suficiencia y recepción de la entrada de datos y si la entrada de datos es oportuna.

El personal de las fuentes, entradas y conversión tiene conciencia y comprende los requerimientos de control en la preparación de datos.

La entrada de datos:

Se envían datos de prueba (tanto transacciones correctas como erróneas) para asegurar que se llevan a cabo revisiones de precisión, suficiencia y autorización.

Para transacciones seleccionadas se comparan los archivos maestros antes y después de la captura.

Existe una apropiada revisión de retención, solución e integridad en la gestión de errores.

Los procedimientos y acciones de gestión de errores cumplen con las políticas y controles establecidos.

El procesamiento de datos:

Se utilizan efectivamente tanto el control de iniciación del sistema como los controles de actualización de los archivos maestros.

Se envían datos de prueba (tanto transacciones correctas como erróneas) para asegurar que se llevan a cabo la validación, autentificación y edición del procesamiento de datos tan cerca del punto de origen como sea posible.

El proceso de gestión de los errores se lleva a cabo de acuerdo con los procedimientos y controles establecidos.

Se llevan a cabo la retención, solución y revisión apropiada de la integridad en el control de errores y éstas funcionan adecuadamente.

Los procedimientos y acciones de gestión de errores cumplen con los procedimientos y controles establecidos.

La Salida, Interface y Distribución de los Datos:

La salida se compara rutinariamente con totales de control relevantes.

Los seguimientos de auditoría se proporcionan para facilitar el seguimiento del procesamiento de las transacciones en la conciliación de datos confusos o erróneos.

Los informes de salida se revisan en cuanto a su precisión por parte del proveedor y los usuarios relevantes.

Existe la retención, solución y revisión apropiada de la integridad en la gestión de los errores y éstas funcionan adecuadamente.

Los procedimientos y acciones de la gestión de los errores cumplen con las políticas y controles establecidos.

Los informes de salidas son asegurados al esperar ser distribuidos, así como aquéllos ya distribuidos a los usuarios de acuerdo con los procedimientos y controles establecidos.

Existe la protección adecuada para la información sensible durante la transmisión y transporte contra los accesos no autorizados y las modificaciones.

Existe una protección adecuada de la información sensible durante la transmisión y transporte en cuanto a accesos y modificaciones no autorizadas.

Los procedimientos y las acciones de información sensible dispuesta cumplen con los procedimientos y controles establecidos.

La Librería de Medios:

El contenido de la librería de medios es inventariado sistemáticamente, todas las discrepancias encontradas son solucionadas oportunamente y se toman medidas para mantener la integridad de los medios almacenados en la librería.

Los procedimientos de la administración diseñados para proteger el contenido de la librería de medios existen y funcionan adecuadamente.

Las responsabilidades de la administración de la librería de medios son asignadas apropiadamente.

La librería de medios es independiente de las funciones de preparación, entrada, procesamiento y salida.

La estrategia de copias de seguridad y restauración de los medios es apropiada.

Los copias de seguridad de medios se llevan a cabo apropiadamente de acuerdo con la estrategia de copias de seguridad definida.

Los almacenes de medios son seguros físicamente y su inventario está actualizado.

El almacenamiento de datos considera los requerimientos de recuperación y la economía o efectividad de los costes.

Los períodos de retención y los términos de almacenamiento son apropiados para documentos, datos, programas e informes.

El riesgo de enviar mensajes a direcciones incorrectas (por carta, fax o e-mail) se reduce con los procedimientos adecuados.

Los controles normalmente se aplican a un proceso de transacción específico, como faxes o contestadores telefónicos automáticos, también se aplica a los

sistemas informáticos que soportan la transacción o proceso (ej., software de fax en los ordenadores personales).

Evaluación del riesgo de que no se cumplan los objetivos de control:

- **Llevando a cabo:**

Mediciones ("Benchmarking") de la administración de los datos con respecto a organizaciones similares o estándares internacionales y buenas prácticas reconocidas en la industria del sector.

Para una selección de transacciones, la confirmación de la propiedad del procesamiento durante:

- La preparación de los datos.
- El procesamiento de las entradas.
- El procesamiento de los datos.
- La salida, distribución o integración.

- La gestión de los errores en todas las fases del proceso.
- La integridad de los datos a través de la gestión de errores en todas las fases del procesamiento.
- Retención y destrucción.

Pruebas específicas para lo siguiente:

- Suficiencia, precisión y validez durante cada fase del procesamiento.
- Aprobaciones y autorizaciones aprobadas.
- Existencia de controles preventivos, detectivos y correctivos dentro del procesamiento o vía funciones manuales y procedimientos de los grupos de control.
- Retención de los documentos fuente para la revisión posterior de la consistencia con respecto a los requerimientos de retención.
- Recuperación de una selección de los documentos fuente y medios de transacción para confirmar la existencia y la precisión.
- Análisis de la disponibilidad del seguimiento de la auditoría: existencia, identificación de la fuente y operador, y asegurar que cualquier sistema de interface cuenta con niveles iguales de control sobre las transacciones.

Edición de las funciones de los programas de entrada y procesamiento, incluyendo, pero sin limitarse a:

- Blancos en los campos deseados.

- Validación de los códigos de las transacciones.
- Importes negativos.
- Cualquier otra condición apropiada.
- Suficiencia de las pruebas de validación internas del procesamiento.

Archivos suspendidos con transacciones defectuosas, incluyendo los siguientes controles:

- Identificación inmediata del operador que comete el error y aviso.
- Todas las transacciones de error son transferidas a estos archivos suspendidos.
- El registro se mantiene hasta que la transacción sea resuelta y eliminada.
- Las transacciones muestran un código de error, fecha y hora de captura, operador y máquina.
- Los archivos de suspenso crean informes de seguimiento para la revisión administrativa, el análisis de las tendencias y formación para realizar las correcciones.
- Separación de las funciones de origen, entrada, procesamiento, verificación y distribución.

Para una selección de transacciones de salida:

- Revisar una muestra de las listas de las transacciones procesadas en cuanto a su suficiencia y precisión.
- Revisar una muestra de los informes de las salida en cuanto a la precisión y suficiencia.
- Revisar los calendarios de retención de salidas en cuanto a su adecuación y cumplimiento de los procedimientos.
- Confirmar que la distribución real de una muestra de salida se lleva a cabo con precisión.
- Confirmar el procesamiento integrado confirmando la salida de un log de procesamiento de transacciones de un sistema con la entrada de un log de otro sistema.
- Revisar los procedimientos de control para todas las entradas, salidas de procesamiento y otras transacciones del uso de los sistemas.
- Confirmar que únicamente el personal autorizado tiene acceso a informes sensibles.
- Confirmar la destrucción o relocalización de almacenamientos fuera para todos los medios de datos, políticas y procedimientos de retención.
- Confirmar los períodos reales de retención contra los procedimientos de retención.

- Atestiguar la entrega o transmisión real de las salidas sensibles y el cumplimiento con los procedimientos de procesamiento, distribución y seguridad.
- Confirmar la creación e integridad de las copias de seguridad en asociación con el procesamiento normal, así como para los requerimientos del plan de recuperación en caso de desastre.

Para la librería de medios:

Revisar el acceso de los usuarios a los servicios sensibles: determinar que el acceso es apropiado.

Seleccionar una muestra de los medios para destruir y observar el proceso completo; verificar el cumplimiento de los procedimientos aprobados.

Determinar la adecuación de los controles para los datos en almacenamientos fuera del sitio y mientras los datos están en tránsito.

Obtener resultados del inventario de la librería de medios más reciente; confirmar su precisión.

Confirmar que los procesadores de los registros son suficientes para acceder a los medios necesarios.

Revisar los controles en cuanto a las desviaciones o “bypass” restringidos de reglas de etiquetado internas y externas.

Probar el cumplimiento de los controles internos y externos vía revisión de los medios seleccionados.

Revisar los procedimientos para generar copias de seguridad para asegurar la existencia de datos suficientes en caso de desastre.

Confirmar las inspecciones de la librería de medios por requerimientos del calendario.

- **Identificando:**

- Cuando se accede a los archivos de producción directamente por los operadores que “antes” y “después” no crean ni mantienen imágenes de archivos.
- Formas de entrada y salida sensibles (por ejemplo, certificados de reservas) no protegidas.

- Logs no llevados y mantenidos para totales batch y de control para todas las fases del procesamiento.
- Informes de salidas que no son útiles a los usuarios: datos relevantes y útiles, informes necesarios, distribución apropiada, formato y frecuencia adecuados, acceso en línea a los informes considerados.
- Datos transmitidos sin controles adicionales, incluyendo:

- Accesos de envío y recepción de transmisiones limitados.
- Autorización e identificación apropiadas del emisor y del receptor.
- Medios seguros de transmisión.
- Encriptación de los datos transmitidos y algoritmos de decodificación apropiados.
- Pruebas de integridad de la transmisión en cuanto a su suficiencia.
- Procedimientos de retransmisión.

- Contratos de proveedores con controles inexistentes como servicios de destrucción.
- Deficiencias fuera del sitio con respecto a las amenazas tales como fuego, agua, fallos eléctricos y accesos no autorizados.

DS 12 Administrar las Infraestructuras

OBJETIVOS DE CONTROL:

1 Seguridad Física.

2 Perfil difuso del lugar de las TI.

3 Vigilancia al Visitante.

4 Salud y Seguridad del Personal.

5 Protección frente a los Factores Ambientales.

6 Suministro Ininterrumpido de Energía.

TANTO LOS OBJETIVOS DE CONTROL DETALLADOS COMO LOS DE ALTO NIVEL SON AUDITADOS MEDIANTE:

Obtención de un entendimiento a través de:

- **Entrevistas:**

Administrador de las Instalaciones.

Responsable de Seguridad.

Administrador de Riesgos.

Administración de operaciones de los servicios de información.

Administrador de la seguridad de los servicios de información.

- **Obteniendo:**

Políticas y procedimientos de la organización relacionados con la administración, disposición , seguridad, inventario de activos fijos e inventario de las instalaciones, así como adquisición y arrendamiento del capital.

Políticas y procedimientos de los servicios de información relacionados con la disposición o plano de las instalaciones, la seguridad física y lógica, acceso, mantenimiento, salud, seguridad y requerimientos del entorno, mecanismos de entrada y salida, informe de seguridad, contratos de seguridad y mantenimiento, inventario de equipo, procedimientos de vigilancia, y requerimientos regulatorios.

Una lista de los individuos que tienen acceso a las instalaciones y la disposición o plano de las instalaciones.

Una lista de los acuerdos de resultado, capacidad y nivel de servicios con respecto a las expectativas de resultado de los recursos de los sistemas de información (equipo e instalaciones), incluyendo estándares industriales.

Copia del documento de planificación de recuperación y contingencia en caso de desastre.

Evaluación de los controles:

- **Considerando si:**

La localización de las instalaciones no es obviamente externa, se encuentra en el área u organización menos accesible, y si el acceso es limitado al menor número de personas.

Los procedimientos de acceso lógico y físico son suficientes, incluyendo perfiles de seguridad de acceso para empleados, proveedores, equipo y personal de mantenimiento de las instalaciones.

Los procedimientos y prácticas de administración de llave ("Key") y lectora de tarjetas ("card reader") son adecuados, incluyendo la actualización y revisión continuas tomando como base una “menor necesidad de acceso”.

Las políticas de acceso y autorización de entrada y salida, escolta, registro, pases temporales requeridos, cámaras de vigilancia son apropiadas para todas las áreas y especialmente para las áreas más sensibles.

Se llevan a cabo revisiones periódicas de los perfiles de acceso, incluyendo revisiones administrativas.

Existen y se llevan a cabo los procesos de revocación, respuesta y priorización en caso de violaciones a la seguridad.

Existe el proceso de “signage” con respecto a la no identificación de las áreas sensibles, y si es consistente con los requerimientos de seguro, código de construcción local y regulatorios.

Las medidas de control de seguridad y acceso incluyen los dispositivos de información portátiles utilizados fuera del sitio.

Se lleva a cabo una revisión de los registros de los visitantes, asignación de pases, escolta, persona responsable del visitante, log para asegurar tanto los registros de entradas como de salidas y el conocimiento de la recepcionista con respecto a los procedimientos de seguridad.

Se lleva a cabo una revisión de los procedimientos de aviso contra incendio, cambios de clima, problemas eléctricos y procedimientos de alarma, así como las respuestas esperadas en los distintos escenarios para los diferentes niveles de emergencias ambientales.

Se lleva a cabo una revisión de los procedimientos de control del aire acondicionado, ventilación, humedad y las respuestas esperadas en los distintos escenarios de pérdida o extremos no anticipados.

Existe una revisión del proceso de alarma al ocurrir una violación de la seguridad, que incluye:

- Definición de la prioridad de la alarma (por ejemplo, apertura de la puerta por parte de una persona armada que ha entrado en las instalaciones).
- Escenarios de respuesta para cada alarma.

- Responsabilidades del personal interno y personal de seguridad local o proveedores.
- Interacción con las autoridades locales.
- Revisión del simulacro de alarma más reciente.

La organización es responsable del acceso físico dentro de los servicios de información, incluyendo:

- Desarrollo, mantenimiento y revisiones continuas de las políticas y procedimientos de seguridad.
- Establecimiento de las relaciones con proveedores relacionados con la seguridad.
- Contacto con la administración de las instalaciones en cuanto a los problemas de tecnología relacionados con la seguridad.
- Coordinación de la formación y concienciación sobre la seguridad para la organización.
- Coordinación de las actividades que afectan al control de acceso lógico vía aplicaciones centralizadas y software del sistema operativo.
- Proporcionar formación y crear conciencia de seguridad no sólo dentro de los servicios de información, sino para los servicios de usuarios.

Se llevan a cabo prácticas de distribuidores automáticos y servicios de conserjería para investigación del personal en las instalaciones de la organización.

Se llevan a cabo la actualización y negociación del contenido de los contratos de servicio.

Los procedimientos de las pruebas de penetración y los resultados.

- Coordinan los escenarios de la prueba de penetración física.
- Coordinan la prueba de penetración física con los proveedores y autoridades locales.

Se cumple con las regulaciones de salud, seguridad y entorno.

La seguridad física se toma en cuenta en el plan de recuperación y contingencia en caso de desastre y abarca una seguridad física similar en las instalaciones aprovisionadas.

Existen elementos de infraestructura específicos alternativos necesarios para implementar seguridad:

- Fuente de poder ininterrumpida (UPS).
- Alternativas o cambio de las rutas de las líneas de telecomunicaciones.
- Recursos alternativos de agua, gas, aire acondicionado y humedad.

Evaluación de la suficiencia:

- **Probando que:**

El personal tiene conciencia y comprende la necesidad de la seguridad y controles.

Los armarios cableados están físicamente protegidos con el acceso posible autorizado y el cableado se encuentra bajo tierra o conductos protegidos tanto como sea posible.

El proceso de “signage” identifica rutas de emergencia y qué hacer en caso de una emergencia o violación de la seguridad.

Los directorios de teléfono en otra partes de la instalación no identifican localidades sensibles.

El log de visitantes sigue apropiadamente los procedimientos de seguridad.

Existen los procedimientos de identificación requeridos para cualquier acceso dentro o fuera vía observación.

Las puertas, ventanas, ascensores, ventiladores y conductos o cualquier otro modo de acceso están identificados.

La sala de servidores está separada, cerrada y asegurada y se accede únicamente por el personal de operaciones y personal de mantenimiento tomando como base un “acceso necesario”.

El personal de las instalaciones rota por turnos y toma vacaciones y descansos apropiados.

Existen los procedimientos de mantenimiento y registro para un oportuno resultado de trabajo.

Se informa sobre las variaciones de las políticas y procedimientos en las operaciones del segundo y tercer turno.

Los planes físicos son actualizados a medida que cambia la configuración, el entorno y las instalaciones.

Los registros y el equipo de seguimiento de seguridad - debajo, en, sobre, y alrededor – se mantienen.

No se almacenan útiles peligrosos.

Existe el seguimiento de la auditoría de control de acceso sobre el software de seguridad o informes clave de administración.

Se ha realizado un seguimiento sobre cualquier emergencia ocurrida en el pasado o sobre su documentación.

El personal con acceso son empleados reales.

Se llevan a cabo verificaciones de suficiencia de la clave de acceso de la administración.

Se ofrece una educación en seguridad física y concienciación sobre seguridad.

Existe una cobertura y experiencia de seguros para los gastos asociados con algún evento de seguridad, pérdida de negocio y gastos para recuperar la instalación.

El proceso para la implementación de cambios de acceso para llaves y controles de los procesos lógicos es continuo y conocido.

El entorno cumple con los requerimientos reguladores establecidos.

Los logs de mantenimiento de las alarmas no se pueden modificar inapropiadamente.

La frecuencia de los cambios de los códigos de acceso y las revisiones del perfil – involucramiento de usuario e instalaciones – está documentada.

Evaluación del riesgo de que no se cumplan los objetivos de control:

- **Llevando a cabo:**

Mediciones (“Benchmarking”) de la administración de las instalaciones con respecto a organizaciones similares o estándares internacionales y buenas prácticas reconocidas en la industria.

Comparaciones del plano físico con el crecimiento del edificio y los dispositivos de seguridad.

Determinaciones sobre:

- La no aparición de la instalación en sí como una localidad de los servicios de sistemas, ni siquiera sugerida indirectamente vía direcciones, señalización de estacionamiento, etc.
- La limitación del número de puertas por códigos locales de construcción y seguro.
- La suficiente protección de las instalaciones a través de barreras físicas para evitar el acceso inapropiado de vehículos y personas.
- Patrones de tránsito para asegurar que el flujo no dirige a las personas hacia las áreas de seguridad.
- La suficiencia del seguimiento con videos y la revisión de cintas.

- La existencia de espacio apropiado para la sala de servidores en cuanto a acceso, temperatura y mantenimiento.
- La suficiencia y disponibilidad de las cubiertas para el equipo contra agua o elementos externos en caso de emergencia.
- La revisión de los logs de mantenimiento de alarmas y la información sobre el último informe de simulacro.

Pruebas sobre temperatura, humedad, electricidad – sobre y debajo de los suelos; si se han producido anomalías, cuáles fueron las actividades de investigación y las soluciones resultantes.

Revisiones de todos los seguros y bisagras (bisagras dentro de la habitación).

Una visita de las instalaciones para determinar si se llevan a cabo detenciones e interrogatorios sobre el hecho de no llevar tarjeta identificativa.

Revisiones de la cobertura del guardia o recepcionista cuando un visitante es escoltado a través de las instalaciones.

Pruebas de seguridad de penetración en las instalaciones.

- **Identificando:**

Suficiencia de “signage”, extinguidores de incendios, sistemas de aspersión, UPS, drenaje, cableado y mantenimiento regular.

Para las ventanas: asegurar que ningún recurso es visible desde el exterior, que no existen “aparadores” en el centro de datos.

Determinación de las pruebas de seguridad de penetración.

Pruebas de visitantes, incluyendo registro, tarjeta identificativa, escolta, inspección, salida.

Discrepancias en los log de los visitantes y en las tarjetas identificativas de los mismos.

Evaluación de los perfiles e historia de acceso tomando como base el informe clave de la administración incluyendo el reemplazo de la tarjeta identificativa y tarjetas maestras, y artículos perdidos inactivos.

Revisión de las estadísticas sobre desastres locales.

Desarrollo de los escenarios de penetración en caso de desastre.

Contratos de los proveedores para asegurar que se lleva a cabo una investigación del personal y el cumplimiento con los requerimientos de salud y seguridad.

Pruebas de UPS y verificar que los resultados cumplen con los requerimientos operacionales y la capacidad para sostener las actividades críticas del procesamiento de datos.

Pruebas de acceso de información (logs, cintas, registros) para asegurar que éstos se revisan por los usuarios y la administración en cuando a su propiedad.

Pruebas de procedimientos de seguimiento de la entrada a la instalación cerca del área.

DS 13 Administrar las Operaciones

OBJETIVOS DE CONTROL:

1 Procedimientos de Procesos de Operaciones y Manual de Instrucciones.

2 Proceso de Arranque y Otras Documentaciones de Operaciones.

3 Planificación del Trabajo.

4 Salidas desde Programas de Trabajo Estándar.

5 Continuidad de Procesamiento.

6 Registros de Operaciones.

7 Salvaguardia de formularios especiales y dispositivos de salida.

8 Operaciones Remotas.

TANTO LOS OBJETIVOS DE CONTROL DETALLADOS COMO LOS DE ALTO NIVEL SON AUDITADOS MEDIANTE:

Obtención de un entendimiento a través de:

- **Entrevistas:**

  Administración de operaciones de los servicios de información.

  Administración de la planificación de recuperación y contingencia en caso de desastre de los servicios de información.

  Dirección de los servicios de información.

  Usuarios seleccionados como recursos de los servicios de información.

  Proveedores seleccionados que proporcionan servicios o productos de software.

- **Obteniendo:**

Políticas y procedimientos de la organización relacionados con la administración de operaciones y el rol de los sistemas de información en el cumplimiento de los objetivos del negocio.

Políticas y procedimientos de los servicios de información relacionados con el rol operacional, las expectativas de resultado, el calendario de trabajos, los acuerdos del nivel de servicio, las instrucciones para el operador, la rotación del personal, la planificación de recuperación y contingencias en caso de desastre, y las operaciones de las instalaciones remotas.

Instrucciones operacionales para la función general de inicio, término, calendario de la carga de trabajo, estándares, acuerdos del nivel de servicio, procedimientos fijos de emergencia, respuestas de procesamiento anormal, logs de consola, seguridad física y lógica, separación de librerías de desarrollo y producción, y procedimientos de problemas de priorización.

Una muestra seleccionada de instrucciones operacionales para aplicaciones clave incluyendo, calendario, entradas, tiempo de procesamiento, mensajes de error, instrucciones de fin anormal, reinicio, procedimientos de priorización de problemas, trabajos antes y después y archivos fuera del sitio.

Evaluación de los controles:

- **Considerando si:**

  Existe evidencia sobre:

- La suficiencia de todos los procesamientos llevados a cabo, reinicios y recuperaciones.
- La suficiencia de la carga del programa inicial (IPL) y del procedimiento de finalización.
- Estadísticas de suficiencia del calendario para confirmar la finalización completa y con éxito de todos los requerimientos.
- La separación física y lógica de las librerías fuente y objeto, de pruebas, desarrollo y producción, y los procedimientos del control de cambios para trasladar programas de una librería a otra.
- Estadísticas de resultados para actividades operacionales, incluyendo, aunque sin limitarse a:

- Capacidad, utilización y resultado del hardware y periféricos.
- Utilización y resultado de la memoria.
- Utilización y resultado de las telecomunicaciones.

- Prueba de que el resultado alcanza las normas sobre el resultado del producto, los estándares de resultado definidos internamente y los compromisos de acuerdo del nivel de servicio de los usuarios.
- El mantenimiento, retención y revisión periódicos de los logs de operación.
- La oportunidad de mantenimiento realizado sobre todo el equipo.
- La rotación de turnos, disfrute de vacaciones y mantenimiento de competencia de los operadores.

Evaluación de la suficiencia:

- **Probando que:**

  Los miembros del personal de operaciones tienen conciencia y comprenden:

- Los procedimientos de operaciones de los que son responsables.

- Las expectativas de resultado dentro de las instalaciones – normas de los proveedores, estándares de la organización y acuerdos de nivel de servicio con los usuarios.
- El programa fijo de emergencia, así como los procedimientos de reinicio y recuperación.
- Los requerimientos y la revisión administrativa de los logs de operaciones.
- Los procedimientos de priorización de problemas.
- La comunicación de los cambios de turno y las responsabilidades entre turnos.
- Procedimientos de cambio o rotación para trasladar los programas de desarrollo a producción.
- Interacción con las instalaciones remotas del procesamiento y las instalaciones centrales.
- Las responsabilidades de comunicar las oportunidades de mejoras a la administración.

Evaluación del riesgo de que no se cumplan los objetivos de control:

- **Llevando a cabo:**

Una revisión de las estadísticas de resultado operacional (equipo y personal) para asegurar la adecuación de su utilización; compararlas con organizaciones similares, normas de proveedores y estándares internacionales y buenas prácticas reconocidas en la industria.

Una revisión de una muestra limitada de manuales de operaciones de los servicios de información y determinar si cumplen con los requerimientos de las políticas y procedimientos.

Un examen de la documentación de los procesos de inicio y término, y confirmar que los procedimientos se prueban y actualizan regularmente.

Un examen del calendario de procesamiento para asegurar lo adecuado y la suficiencia del resultado comparado con el plan o calendario.

- **Identificando:**

Usuarios seleccionados y asegurando la suficiencia del resultado operacional relacionado con actividades continuas y acuerdos del nivel de servicio.

Una muestra de los términos anormales (ABENDS) para trabajos y determinando la solución a los problemas acaecidos.

Las experiencias sobre formación, rotación de turnos y vacaciones de los operadores.

Una muestra de los logs de consola para revisar la precisión, las tendencias en el resultado y la revisión administrativa de la solución de los problemas – evaluar la priorización de problemas.

A usuarios para determinar la satisfacción con el compromiso de acuerdo del nivel de servicio.

Procedimientos de mantenimiento preventivo completados en todo el equipo por sugerencia del proveedor.

Seguimiento

M 1 Supervisar los Procesos

OBJETIVOS DE CONTROL:

1 Recogida de Datos de la Supervisión.

2 Evaluación del Rendimiento.

3 Evaluación de la Satisfacción del Cliente.

4 informe de la Dirección.

TANTO LOS OBJETIVOS DE CONTROL DETALLADOS COMO LOS DE ALTO NIVEL SON AUDITADOS MEDIANTE:

Obtención de un entendimiento a través de:

- **Entrevistas:**

  Director Ejecutivo.

  Director de Información

  Director de auditoría interna.

  Director de los servicios de información y administración del control de calidad.

  Gerente de auditoría externa.

Usuarios seleccionados como recursos de los servicios de información.

Miembros del comité de auditoría.

- **Obteniendo:**

Políticas y procedimientos de la organización relacionadas con la planificación, administración, seguimiento e informe sobre el resultado.

Políticas y procedimientos de los servicios de información relacionadas con el seguimiento y el informe sobre el resultado, estableciendo iniciativas para mejorar el resultado y la frecuencia de las revisiones.

Informes sobre las actividades de los servicios de información incluyendo, pero no limitados a: informes internos, informes de auditorías internas, informes de auditorías externas, informes de usuarios, encuestas de satisfacción de los usuarios, planes de desarrollo de los sistemas e informes de avance, actas del comité de auditoría y cualquier otro tipo de evaluación sobre el uso de los recursos de los servicios de información de la organización.

Documentos de planificación de los servicios de información con los objetivos para cada grupo de recursos y el resultado real en comparación con dichos planes.

Evaluación de los controles:

- **Considerando si:**

Los datos identificados para realizar un seguimiento de los recursos de los servicios de información son apropiados.

Se usan indicadores clave de rendimiento y factores críticos de éxito para medir el resultado de los servicios de información en comparación con los niveles deseables.

Los informes internos sobre la utilización de los recursos de los servicios de información (gente, instalaciones, aplicaciones, tecnología y datos) son adecuados.

Existe una revisión administrativa de los informes de resultado de los recursos de los servicios de información.

Considerar si, continúa.

Existen controles de seguimiento para proporcionar una retroalimentación fiable y útil de forma oportuna.

La respuesta de la organización a las recomendaciones para mejorar el control de calidad, auditoría interna y auditoría externa es apropiada.

Existen iniciativas y resultados de mejoras del resultado deseado.

Se está dando el resultado de la organización en comparación con las metas establecidas dentro de la organización.

La confiabilidad y utilidad de los informes de resultado para los no usuarios es suficiente, tales como auditor externo, comité de auditoría y alta administración de la organización.

La oportunidad de los informes permite una respuesta rápida ante las excepciones o incumplimientos identificados del resultado.

Los informes son suficientes en comparación con las políticas y procedimientos establecidos para el resultado de las actividades (por ejemplo, informes de resultado).

Evaluación de la suficiencia:

- **Probando que:**

Existen informes de seguimiento del resultado de la información.

Existe revisión administrativa de los informes de seguimiento del resultado e iniciativas de acciones correctivas.

Los empleados son conscientes y comprenden las políticas y procedimientos relativos al seguimiento del resultado.

La calidad y el contenido de los informes internos se relacionan con:

- La recolección de datos de seguimiento del resultado.
- El análisis de los datos de seguimiento del resultado.
- El análisis de los datos del resultado de los recursos.
- Las acciones administrativas sobre los problemas del resultado.
- El análisis de las encuestas de satisfacción de los usuarios.

La alta administración está satisfecha con los informes sobre el seguimiento del resultado.

Evaluación del riesgo de que no se cumplan los objetivos de control:

- **Llevando a cabo:**

Referencia del seguimiento del resultado respecto a organizaciones similares o estándares internacionales y prácticas industriales reconocidas.

Revisión de la relevancia de los datos dentro de los procesos que se están revisando.

Revisión del resultado real con respecto a lo planificado en todas las áreas de los servicios de información.

Satisfacción real con respecto a lo anticipado de los usuarios de todas las áreas de los servicios de información.

Análisis del grado de cumplimiento de las metas e iniciativas para realizar mejoras.

Análisis del nivel de implantación de las recomendaciones de la administración.

- **Identificando:**

La responsabilidad, autoridad e independencia del personal de seguimiento dentro de la organización de los sistemas de información.

M 2 Evaluar la Adecuación del Control Interno

OBJETIVOS DE CONTROL:

1 Supervisión del Control Interno.

2 Operación Oportuna de los Controles Internos.

3 Informe de Nivel de Control Interno.

4 Seguridad Operativa y Aseguramiento del Control Interno.

TANTO LOS OBJETIVOS DE CONTROL DETALLADOS COMO LOS DE ALTO NIVEL SON AUDITADOS MEDIANTE:

Obtención de un entendimiento a través de:

- **Entrevistas:**

  Director Ejecutivo.

  Director de la Información.

  Director de auditoría interna.

  Director de los servicios de información y administración del control de calidad.

  Gerente de auditoría externa.

  Administración de usuarios seleccionados como recursos de los servicios de información.

  Miembros del comité de auditoría.

- **Obteniendo:**

Políticas y procedimientos de la organización relacionados con la planificación, administración, seguimiento e informe sobre los controles internos.

Políticas y procedimientos de los servicios de información relacionadas con el seguimiento y el informe sobre los controles internos y la frecuencia de las revisiones.

Informes sobre las actividades de los servicios de información incluyendo, pero no limitados a: informes internos, informes de auditorías internas, informes de auditorías externas, informes de usuarios, encuestas de satisfacción de los usuarios, planes de desarrollo de los sistemas e informes de avance, actas del comité de auditoría y cualquier otro tipo de evaluación de los controles internos de los servicios de información.

Políticas y procedimientos específicos de los servicios de información relacionados con asegurar la seguridad operacional y el control interno.

Evaluación de los controles:

- **Considerando si:**

Los datos identificados para el seguimiento de los controles internos de los servicios de información son apropiados.

Los informes internos de los datos del control interno de los servicios de información son adecuados.

Existe una revisión administrativa de los controles internos de los servicios de información.

Existen controles de seguimiento para proporcionar retroalimentación fiable y útil de manera oportuna.

La respuesta de la organización a las recomendaciones sobre mejora del control de calidad, auditoría interna y auditoría externa es apropiada.

Existen iniciativas y resultados de mejora del control interno deseable.

Se está dando el resultado de la organización en comparación con las metas establecidas dentro de la organización.

La información concerniente a errores, inconsistencias y excepciones del control interno se mantiene de manera sistemática y se informa a la administración.

La confiabilidad y utilidad de los informes de control interno para no usuarios, tales como auditor externo, comité de auditoría y alta administración de la organización, es suficiente.

La oportunidad de los informes permite una respuesta rápida ante las excepciones o incumplimientos identificados del control interno.

Los informes sobre control interno son suficientes en comparación con las políticas y procedimientos establecidos para el desarrollo de las actividades (por ejemplo, informes de control interno).

Evaluación de la suficiencia:

- **Probando que:**

Existen informes de seguimiento del control interno.

Está habiendo revisión administrativa de los informes de control interno e iniciativas de acciones correctivas.

Los empleados son conscientes y comprenden las políticas y procedimientos relativos al seguimiento del control interno.

La calidad y el contenido de los informes internos se relacionan con:

- La recolección de datos de seguimiento del control interno.
- El resultado del cumplimiento del control interno.
- Las acciones administrativas sobre problemas del control interno.
- Asegurar la seguridad operacional y el control interno.

La alta administración está satisfecha con los informes sobre la seguridad y el control interno.

Evaluación del riesgo de que no se cumplan los objetivos de control:

- **Llevando a cabo:**

Referencia de la evaluación del control interno respecto a organizaciones similares o estándares internacionales y prácticas industriales reconocidas.

Revisión de la relevancia de los datos dentro de los procesos que se están siguiendo e informar sobre los controles internos.

Marco de referencia para la revisión de los controles internos de toda la organización y en particular de los servicios de información para asegurar la suficiencia de la cobertura y de los diversos niveles de detalle para los responsables del proceso.

Revisión del control interno real en comparación con lo planificado en todas las áreas de los servicios de información.

Análisis del grado de cumplimiento de las metas del control interno e iniciativas de mejora.

Revisión de la satisfacción del comité de auditoría con los informes sobre los controles internos.

Análisis del nivel de implantación de las recomendaciones de la administración.

- **Identificando:**

Las áreas adicionales para el probable informe de control interno, en consistencia con los requerimientos de los servicios de información, auditoría, administración, auditores externos y regulaciones.

La responsabilidad, autoridad e independencia del personal de revisión del control interno dentro de la organización de los sistemas de información.

M 3 Obtener Certificaciones Independientes

OBJETIVOS DE CONTROL:

1 Seguridad independiente y certificación/acreditación del control interno de los servicios de las TI.

2 Seguridad independiente y certificación/acreditación del control interno de los proveedores de servicios de terceras partes.

3 Evaluación independiente de la eficacia de los servicios de las TI.

4 Evaluación independiente de la eficacia de los proveedores de servicios de terceras partes.

5 Aseguramiento independiente del cumplimiento con las leyes y requerimiento regulatorios y compromisos contractuales.

6 Aseguramiento independiente del cumplimiento con las leyes y requerimiento legales y compromisos contractuales por proveedores de servicios de terceras partes.

7 Competencia de la función de aseguramiento independiente.

8 Implicación preactiva de la auditoría.

TANTO LOS OBJETIVOS DE CONTROL DETALLADOS COMO LOS DE ALTO NIVEL SON AUDITADOS MEDIANTE:

Obtención de un entendimiento a través de:

- **Entrevistas:**

  Director Ejecutivo

  Director de Información

  Director de auditoría interna

Director de los servicios de información

Gerente de auditoría externa

Gerente de la entidad emisora de certificaciones independientes

- **Obteniendo:**

Organigrama a nivel de toda la organización y manual de las políticas y procedimientos.

Políticas y procedimientos relativos al proceso de obtención de certificaciones independientes.

Contratos y Acuerdos de servicio con el proveedor del servicio de tecnología de la información.

Requerimientos legales y regulaciones pertinentes y compromisos contractuales.

Contratos, presupuestos, informes previos e historial de resultados de la entidad emisora de certificaciones independientes.

Historial de experiencia y educación continua del personal de dicha entidad independiente.

Informes de auditorías previas.

Evaluación de los controles:

- **Considerando si:**

Los contratos celebrados con la entidad independiente están debidamente establecidos y ejecutados para asegurar la cobertura de revisión adecuada (por ejemplo, certificación y acreditación, evaluación de eficacia y evaluaciones de cumplimiento).

La acreditación y certificación independiente se obtiene antes de implantar los servicios nuevos e importantes de la tecnología de la información.

La recertificación y reacreditación independiente de los servicios de la tecnología de la información se obtiene en un ciclo rutinario después de la implantación.

La certificación y acreditación independiente se obtiene antes de utilizar a los proveedores de servicios de la tecnología de la información.

La recertificación y reacreditación se obtiene en un ciclo rutinario.

La evaluación independiente de la eficacia de los servicios de la tecnología de la información se obtiene en un ciclo rutinario.

La evaluación independiente de la eficacia de los proveedores de los servicios de tecnología de la información se obtiene en un ciclo rutinario.

Las revisiones independientes del cumplimiento de los servicios de información con los requerimientos legales y regulaciones, y los compromisos contractuales se obtiene en un ciclo rutinario.

Las revisiones independientes del cumplimiento de los proveedores externos de servicios con los requerimientos legales y regulaciones y los compromisos contractuales se obtiene en un ciclo rutinario.

El personal que estudia la certificación independiente es competente y realiza su tarea de acuerdo con los estándares profesionales apropiados.

El programa de educación profesional continuada ayuda para proporcionar la capacitación técnica al personal independiente.

La administración busca el involucramiento de la auditoría antes de decidir sobre las soluciones del servicio de la tecnología de la información.

Evaluación de la suficiencia:

- **Probando que:**

La alta administración aprueba el resultado de la entidad independiente.

La certificación o acreditación independiente antes de la implantación de los nuevos servicios importantes de la tecnología de la información es global, completa y oportuna.

La recertificación o reacreditación independiente de los servicios de la tecnología de la información se realiza en un ciclo rutinario después de la implantación, global, completa y oportuna.

La certificación o acreditación independiente antes de utilizar proveedores de servicios de la tecnología de la información es global, completa y oportuna.

La recertificación o reacreditación independiente se realiza en un ciclo rutinario y es global, completa y oportuna.

La evaluación independiente de la eficacia de los servicios de la tecnología de la información se realiza en un ciclo rutinario y es global, completa y oportuna.

La evaluación independiente de la eficacia de los proveedores de los servicios de la tecnología de la información se realiza en un ciclo rutinario y es global, completa y oportuna.

Las revisiones independientes del cumplimiento de los servicios de información con los requerimientos legales y regulaciones y los compromisos contractuales se realizan en ciclos rutinarios y son globales, completas y oportunas.

Las revisiones independientes del cumplimiento de los proveedores externos de servicios con los requerimientos legales y regulaciones, y los compromisos contractuales se realizan en ciclos rutinarios y son globales, completas y oportunas.

Los informes de la entidad independiente son relevantes en cuanto a hallazgos, conclusiones y recomendaciones.

La función de certificación independiente posee las habilidades y el conocimiento necesario para realizar un trabajo competente.

Existe un involucramiento proactivo, antes de decidir sobre las soluciones del servicio de la tecnología de la información.

Evaluación del riesgo de que no se cumplan los objetivos de control:

- **Llevando a cabo:**

Referencia de las actividades de revisión de la entidad independiente respecto a otras organizaciones similares o estándares internacionales y prácticas industriales reconocidas.

Una revisión detallada que:

- Verifique los contratos de certificación independiente respecto a las actividades de revisión realizadas.
- Determine la suficiencia y oportunidad de las certificaciones o acreditaciones.
- Determine la suficiencia y oportunidad de las recertificaciones o reacreditaciones.

- Determine la suficiencia y oportunidad de las evaluaciones de eficacia.
- Determine la suficiencia y oportunidad de las revisiones del cumplimiento de requerimientos legales y regulaciones, y de compromisos contractuales.
- Verifique la capacidad del personal de certificación independiente.
- Verifique el involucramiento proactivo de la auditoría.

- **Identificando:**

El valor agregado de las actividades de revisión independiente.

El resultado real con respecto a lo planificado con relación a los planes y presupuestos de certificación independiente.

El grado y la oportunidad del involucramiento proactivo de la auditoría.

M 4 Realizar Auditorías Independientes

OBJETIVOS DE CONTROL:

1 Diagrama de la Auditoría.

2 Independencia.

3 Ética Profesional y Estándares.

4 Competencia.

5 Planificación.

6 Realización del Trabajo de Auditoría.

7 Informe.

8 Actividades de Aseguramiento.

TANTO LOS OBJETIVOS DE CONTROL DETALLADOS COMO LOS DE ALTO NIVEL SON AUDITADOS MEDIANTE:

Obtención de un entendimiento a través de:

- **Entrevistas:**

  Director Ejecutivo.

  Director de Información.

Director de auditoría interna.

Director de los servicios de información y administración del control de calidad.

Gerente de auditoría externa.

Miembros del comité de auditoría.

- **Obteniendo:**

Organigrama de toda la organización y manual de las políticas y procedimientos.

Código de conducta de la organización.

Políticas y procedimientos relativos al proceso de auditoría independiente.

Contratación de la auditoría, misión, políticas, procedimientos y estándares, informes previos y planes de auditoría.

Opiniones de la auditoría externa, revisiones y planes de auditoría.

Historial sobre la experiencia y formación continua del personal de auditoría independiente.

Evaluación del riesgo de la auditoría, presupuesto e historial de resultados.

Actas de las reuniones del comité de auditoría.

Evaluación de los controles:

- **Considerando si:**

El comité de auditoría está debidamente establecido y se reúne con regularidad.

La organización de auditoría interna está debidamente establecida.

Las auditorías externas contribuyen a la consecución del plan de auditoría.

La adherencia de la auditoría a los códigos profesionales aplicables es suficiente.

Considerar si, continúa.

La independencia del auditor está confirmada mediante declaraciones firmadas de conflicto de intereses.

El plan de auditoría se basa en la metodología de evaluación de los riesgos y en las necesidades generales del plan.

Las auditorías se planifican y supervisan de forma adecuada.

El programa de educación profesional continuada ayuda a la capacitación técnica de los auditores.

El personal de auditoría es competente y realiza sus tareas de acuerdo con los estándares profesionales de auditoría.

Existe un proceso adecuado de información sobre los hallazgos de la auditoría dirigidos a la dirección.

El seguimiento de todos los problemas de control se está realizando de forma oportuna.

La cobertura de la auditoría incluye todo el rango de auditoría de los sistemas de información (por ejemplo, controles generales y de aplicaciones, ciclo de desarrollo del sistema, rentabilidad, economía, eficiencia, eficacia, enfoque proactivo de la auditoría, etc.).

Evaluación de la suficiencia:

- **Probando que:**

La alta administración aprueba el resultado de la auditoría independiente.

Las actitudes de la alta administración son consistentes con la contratación de la auditoría.

Referencias de la auditoría interna respecto a los estándares profesionales.

La designación de auditores asegura la independencia y las habilidades necesarias.

Existe una mejora continua de la experiencia profesional del personal de auditoría.

El contenido del informe de auditoría es relevante respecto a las recomendaciones.

Existen informes de seguimiento que resumen la oportunidad de la implantación.

Evaluación del riesgo de que no se cumplan los objetivos de control:

- **Llevando a cabo:**

Referencia de la auditoría respecto a otras organizaciones similares o estándares internacionales y prácticas industriales reconocidas.

Una revisión detallada que:

- Verifique que el plan de auditoría representa una revisión cíclica y continua.
- La auditoría está contribuyendo al éxito del negocio y a los planes de la Tecnología de la Información.
- La evidencia de la auditoría apoya las conclusiones y recomendaciones.
- Los hallazgos de la auditoría se transmiten y se toma ventaja de los mismos o se reducen riesgos.
- Las recomendaciones de la auditoría están siendo implantadas de forma consciente respecto al beneficio que representan.

- **Identificando:**

El coste y beneficio de las recomendaciones de la auditoría.

El resultado real con respecto a lo planificado con relación al plan y presupuesto de auditoría.

Anexo 2

Resumen Dominios y Procesos de COBIT

PLANEACIÓN Y ORGANIZACIÓN

1.0 Definir un Plan Estratégico de TI

2.0 Definir la Arquitectura de la Información

3.0 Determinar el Rumbo Tecnológico

4.0 Definir la Organización y las Relaciones de TI

5.0 Administrar la Inversión de TI

6.0 Comunicar los Objetivos y el Rumbo Administrativo

7.0 Administrar los Recursos Humanos

8.0 Asegurar el Cumplimiento de los Requerimientos Externos

9.0 Evaluar los Riesgos

10.0 Administrar los Proyectos

11.0 Administrar la Calidad

ADQUISICIÓN E IMPLANTACIÓN

1.0 Identificar las Soluciones

2.0 Adquirir y Dar Mantenimiento al Software de Aplicación

3.0 Adquirir y Dar Mantenimiento a la Arquitectura Tecnológica

4.0 Desarrollar y Mantener Procedimientos de TI

5.0 Instalar y Acreditar los Sistemas

6.0 Manejar los Cambios

SUMINISTRO Y SOPORTE

1.0 Definir los Niveles de Servicio

2.0 Manejar los Servicios de Terceros

3.0 Administrar el Desempeño y la Capacidad

4.0 Asegurar el Servicio Continuo

5.0 Asegurar la Seguridad de los Sistemas

6.0 Identificar y Atribuir los Costos

7.0 Educar y Capacitar a los Usuarios

8.0 Ayudar y Aconsejar a los Clientes de TI

9.0 Manejar la Configuración

10.0 Manejar los Problemas e Incidentes

11.0 Manejar los Datos

12.0 Manejar las Instalaciones

13.0 Manejar las Operaciones

MONITOREO

1.0 Monitorear las Operaciones

2.0 Evaluar la Suficiencia del Control Interno

3.0 Obtener Aseguramiento Independiente

4.0 Preparar Auditorías Independientes

Anexo 3

Cuestionarios

De la extracción de conocimientos se detectaron los siguientes cuestionarios.

1. Organización, gestión y base jurídica principalmente organismos públicos

- La gestión informática se lleva a cabo:
    - En forma unificada, por la gerencia o área de Sistemas
    - En forma compartida, por 2 o mas áreas independientes entre si
    - Por un servicio tercerizado a través de una contratación a una empresa especializada en sistemas
    - Por personal especializado dependiente de las áreas usuarias

- Indique el nombre completo del área de sistema

- El área de sistemas reviste el carácter de:
    - Gerencia o dirección
    - Departamento, Jefatura, coordinación
    - Grupo de trabajo
    - Otro

- La ubicación del área de sistemas en el organigrama es la siguiente
    - Depende de la máxima autoridad del organismo
    - Depende de otro área o Gerencia
    - Otras

- El área de sistemas cuenta con una estructura
    - Formalmente definida
    - Definida pero aun no aprobada formalmente
    - Definida informalmente dentro del área

- El área de sistemas dispone de
    - Planes de corto y largo plazo aprobados formalmente, que se ajustan al plan estratégico del organismo

  - Un plan general no formalizado, para las actividades del sector
  - No dispone de planificación documentada

- El cumplimiento de los objetivos planificados para el área de sistemas, se controla mediante
  - Un tablero de comandos utilizado por el organismo para monitorear las actividades de las distintas áreas.
  - Informes de avance periódicos elevados a las autoridades del organismo
  - Reportes de carácter informal
  - Supervisión no documentada

- Los planes de sistemas están integrados a los planes estratégicos de la organización
  - Si
  - No

- La estructura del área de sistemas contempla los siguientes sectores y funciones asignados a responsables independientes
  - Desarrollo y producción / procesamiento independiente
  - Administración de base de datos
  - Control de calidad
  - Administración de redes / telecomunicaciones

- El área de sistemas dispone de políticas, procedimientos y estándares documentados y aprobados formalmente para las siguientes tareas
  - Desarrollo y mantenimiento de sistemas
  - Administración de la seguridad
  - Tratamiento de contingencias
  - Administración de copias de backup
  - Actividades de soporte
  - Gestión y control de licencias de software
  - Otros

- La incorporación de sistemas en el organismo es realizado por
    - Desarrollos realizados por el área de sistemas
    - Desarrollos realizados por un grupo externo contratado y supervisado por el área de sistemas
    - Desarrollos realizados por analistas/programadores contratados por el área usuarios
    - Adquisición de sistemas aplicativos estándares del mercado
    - Provisión de sistemas por parte de otros organismos del estado
    - Otro

- Existe un comité de informática
    - Si
    - No

- Si existe un comité de informática quien lo integra y cuales son sus objetivos

- Las tareas de procesamiento de los sistemas de aplicación son realizados por
    - Las áreas usuarias
    - El área de sistemas
    - Especialistas en sistemas dependientes de las áreas usuarias
    - Terceros contratados para esta área
    - Otros

- El soporte técnico informático a los usuarios es realizado por
    - El personal de desarrollo de sistemas
    - El área de capacitación
    - Una mesa de ayuda dedicada a la atención de problemas de usuarios
    - Los usuarios
    - Terceros contratados para esta tarea

  - Otros

- La tarea de Auditoría interna de sistemas es realizada por
  - Auditores especializados en sistemas dependientes de la Unidad de Auditoría interna
  - Auditores no especializados en sistemas dependientes de la Unidad de Auditoría Interna
  - No se realizan auditorias internas de sistemas
  - Otros

- La plataforma tecnológica del organismo cuenta con
  - Mainframe
  - Servidores de tecnología Intel con sistema operativos tipo Novell, Windows NT, Linux, Unix, etc.
  - Servidores de tecnología Risc con sistemas operativos Unís
  - Otros servidores (AS 400, VAX, etc.)

- El organismo dispone de
  - Hasta 50 computadoras personales
  - Entre 51 y 100 PC
  - Entre 101 y 500 PC
  - Entre 500 y 1000 PC
  - Mas de 1000 PC

- El organismo dispone de
  - Base de datos
  - Sitio Web
  - Correo electrónico
  - Firewall
  - Intranet

- El sitio Web del organismo es utilizado para
  - Difusión de información y/o servicios de carácter publico

  - Recepción de información que reviste carácter de Declaración Jurada
  - Recepción de denuncias u otra información de carácter critico.
  - Recepción de información de carácter oficial.
  - Recaudación o manejo de fondos

- Las bases de datos del organismo cuentan con información
  - De carácter general
  - Administrativa y/o presupuestaria interna del organismo
  - De personas físicas o jurídicas con carácter confidencial o privada y / o podría estar alcanzada por la ley de Habeas Data
  - Económica y/o presupuestaria de carácter confidencial

- El presupuesto para las actividades informáticas del presente ejercicio ascienden a
  - Hasta $500.000.-
  - Entre $500.001 y 2.000.000.-
  - Entre $2.000.001 y $5.000.000
  - Entre $5.000.001 y $20.000.000
  - Mas de $20.000.001

- El presupuesto para actividades informáticas representa el siguiente porcentaje del presupuesto total del organismo
  - Hasta 2%
  - Entre 2% y el 5%
  - Entre el 5% y el 10%
  - Mas de 10%

- La cantidad de sistemas de aplicación de Misión Crítica utilizados en el organismo es
  - Hasta 5
  - Entre 6 y 15
  - Entre 16 y 30
  - Mas de 30

- La cantidad de sistemas de aplicación que no son de Misión Crítica utilizados en el organismo es
    - Hasta 20
    - Entre 21 y 50
    - Entre 51 y 100
    - Mas de 100

- Se ajusta la estructura orgánica actual a las disposiciones jurídicas vigentes
    - Si
    - No

- Permiten los niveles jerárquicos actuales que se desarrolle adecuadamente la
    - Operación
    - Supervisión
    - Control

- Permiten los actuales niveles jerárquicos que se tenga una ágil
    - Comunicación ascendente
    - Comunicación descendente
    - Toma de decisiones

- Considera que algunas áreas deberían tener
    - Mayor jerarquía
    - Menor jerarquía

- Se consideran adecuados los departamentos, áreas y oficinas en que esta actualmente dividida actualmente la estructura de la dirección.
    - Si
    - No

- El numero de empleados que trabaja actualmente es adecuado para cumplir con las funciones encomendadas

  - Si
  - No

- Se han establecido funciones del área
  - Si
  - No

- Conocen las otras áreas las funciones del área de sistemas
  - Si
  - No

- Existe duplicidad de funciones en el mismo área
  - Si
  - No

- Se han establecido objetivos del área de sistemas
  - Si
  - No

- Participo el área de sistemas en el establecimiento de objetivos
  - Si
  - No

- Se han dado a conocer los objetivos del área
  - Si
  - No

- Existen mecanismos para conocer el grado de cumplimiento de los objetivos
  - Si
  - No

- Se revisan los objetivos
  - Si

- No

- Se tiene conciencia en toda la organización de que la función informática es principalmente proporcionar un servicio estratégico a las áreas de negocios
  - Si
  - No

- Se tienen problemas económicos organizacionales y de otro tipo por el uso actual de informática
  - Si
  - No

- Cual es la participación de las áreas usuarias en la definición y ejecución de las políticas informáticas.

2. Recursos Humanos

- Es suficiente el número de personal para el desarrollo de las funciones del área
  - Si
  - No

- Se deja de realizar alguna actividad por falta de personal
  - Si
  - No

- Esta capacitado el personal para realizar con eficiencia sus funciones
  - Si
  - No

- Es eficiente el personal en el cumplimiento de sus funciones
  - Si

  - No

- Es frecuente la repetición de trabajos encomendados
  - Si
  - No

- El personal es discreto en el manejo de información confidencial
  - Si
  - No

- En general responde el personal a las políticas y procedimientos establecidos
  - Si
  - No

- Respeta el personal la autoridad establecida
  - Si
  - No

- Existe colaboración del personal para la realización del trabajo
  - Si
  - No

- El personal tiene afán de superación
  - Si
  - No

- Presenta el personal sugerencias para mejorar el actual desempeño
  - Si
  - No

- Los programas de capacitación incluyen al personal de
  - Dirección

  - Análisis
  - Programación
  - Operación
  - Administración
  - Dba
  - Redes
  - Otros

- Se han identificado las necesidades actuales y futuras de capacitación
  - Si
  - No

- Se desarrollan actualmente programas de capacitación
  - Si
  - No

- Apoya la dirección los planes de capacitación
  - Si
  - No

- Cual es el índice de rotación promedio del personal
  - De 1 a 6 meses
  - De 6 meses a un año
  - De una año a dos años
  - Mas de dos años

- En general se adapta el personal al mejoramiento administrativo
  - Si
  - No

- En promedio cual es el grado de asistencia y puntualidad del personal
  - Bueno
  - Malo

  - Regular

- Existe una política de sanción disciplinaria del personal
  - Si
  - No

- Esta el personal adecuadamente remunerado
  - Si
  - No

- El personal esta integrado como grupo de trabajo
  - Si
  - No

- Existe un proceso formal de comunicación interna entre el personal informático
  - Cual es el sistema
  - Cuales son los obstáculos principales de comunicación entre el personal informático

- Son adecuadas las condiciones ambientales con respecto a
  - Espacio del área
  - Iluminación
  - Ventilación
  - Mobiliario
  - Ruido
  - Limpieza y aseo
  - Instalación sanitaria
  - Instalación de comunicaciones

- Esta prevista la sustitución del personal clave
  - Si
  - No

- Existen oportunidades de ascenso y promociones
    - Si
    - No

- Se ha evaluado el nivel de capacitación del personal en el ultimo año
    - Si
    - No

3. Sistemas en desarrollo

- Cuales son los sistemas que actualmente están en desarrollo
    - Nombre de cada uno
    - Breve descripción funcional
    - Etapa del desarrollo

- Existe un plan maestro de sistemas
    - Si
    - No

- Esta relacionado el plan de desarrollo de sistemas con el plan general de desarrollo de la dependencia
    - Si
    - No

- Ofrece el plan maestro la atención de solicitudes urgentes de los usuarios
    - Si
    - No

- Quien autoriza los proyectos

- Como se asignan los recursos

- Como se estiman los tiempos de duración de los proyectos
- Quien interviene en la evaluación de proyectos
- Como se calcula el presupuesto de cada proyecto
- Que técnicas se usan en el control de los proyectos
- Quien asigna las prioridades
- Como se controla el avance de los proyectos
- Con que periodicidad se revisa el avance de los proyectos
- Que acciones correctivas se toman en caso de desviaciones en los proyectos
- Se llevan a cabo revisiones periódicas de los sistemas en desarrollo para determinar si cumplen los objetivos.
    - De análisis
    - De programación
    - Otros
- Quien interviene al diseñar un sistema
    - Usuario
    - Analista
    - Gerente
    - Dba
    - Personal de comunicaciones
    - Auditores internos
    - Asesores
    - Otros

- Que lenguaje de programación conoce el equipos de desarrollo

- Que metodología de desarrollo de sistemas se utiliza

- Existe un procedimiento formal para realizar las pruebas
    - Si
    - No

- Participan los usuarios en el proceso de testing
    - Si
    - No

- Existe un procedimiento formal para realizar la conversión de datos de un sistema en retiro a un nuevo sistema
    - Si
    - No

- Existe un procedimiento formal para realizar la implantación de los nuevos sistemas
    - Si
    - No

- Que documentación acompaña al programa cuando se entrega

- El software utilizado para el desarrollo de sistemas es legal

    - Si
    - No
    - Open source

- El motor de base de datos es legal
    - SI

  - NO
  - Open source

- Cuales son las herramientas que se utilizan en el desarrollo de sistemas.

- Cual es el proceso de Gestión de configuración en el desarrollo de sistemas.

- La función de aseguramiento de la calidad en el desarrollo de sistemas contempla
  - Puntos de revisión en el análisis
  - Puntos de revisión en el diseño
  - Puntos de revisión en la construcción
  - Puntos de revisión en las pruebas
  - Puntos de revisión en la implementación

4. Operación y soporte

- Cuales son los sistemas que se operan actualmente
  - Nombre
  - Breve descripción funcional
  - Lenguaje
  - Motor de base de datos
  - Fecha de desarrollo
  - Desarrollador
  - Ultima actualización
  - Ubicación

- La arquitectura del procesamiento es
  - Centralizada
  - Descentralizada
  - Mixta

- Existen normas que definan el contenido de los instructivos de captación de datos
    - Si
    - No

- Quien controla la entrada del documento fuente
    - Quien carga
    - Otra persona
    - No se controla

- Cuando la carga de trabajo supera la capacidad instalada se requiere
    - Tiempo extra
    - Se subcontrata

- Se verifica la calidad de la información recibida para su captura
    - SI
    - No

- Cual es el procedimiento para solicitar un servicio de informática

- Como se asegura el cumplimiento oportuno de los servicios solicitados

- Existe un procedimiento escrito que indique como tratar la información invalida
    - Si
    - No

- Los documentos fuentes de entrada se guardan en lugar seguro
    - Si
    - No

- Existe un registro de anomalías de la información de entrada a los sistemas que no se encuentra de acuerdo a los procedimientos establecidos

- Si
- No

- Existe una relación completa de distribución de listados, en la cual indiquen personas, secuencias y sistemas a los que pertenecen
  - Si
  - No

- Se hace una relación de cuando y a quien fueron distribuidos los listados
  - Si
  - No

- Se controlan separadamente los documentos confidenciales
  - Si
  - No

- Se aprovecha adecuadamente el papel de los listados inservibles
  - Si
  - No

- Existen procedimientos formales para lo operación de los sistemas
  - Si
  - No

- Los retrasos o incumplimientos del programa de operación diaria, se revisa y analiza.
  - Si
  - No

- Existe un procedimiento formal para la recuperación del sistema en caso de fallas
  - Si
  - No

- Opera el personal del área de informática los sistemas en producción.
    - Si
    - No

- Tienen los operadores una bitácora con los incidentes que se producen en la operación de los sistemas
    - Si
    - No

- Existe un procedimiento para evitar la ejecución no autorizada de sistemas
    - Si
    - No

- Los equipos que se utilizan en la operación de los sistemas tienen seguro
    - Si
    - No

- Cada cuanto se cambian las claves de acceso a los sistema
    - De 1 a 7 días
    - De 7 días a 30 días
    - De 30 días a 90 días
    - De 90 días a 180 días
    - De 180 días a 360 días
    - Mas de un año
    - Nunca

- Existe copia de las bases de datos en otros locales
    - Si
    - No

- Cual es la política de backup

- Los locales asignados a almacenamiento magnético tienen
    - Aire acondicionado
    - Protección contra fuego
    - Cerradora especial
    - Otros

- Existe un procedimiento formal que permita reconstruir un archivo dañado
    - Si
    - No

- Cual es el impacto de una hora de interrupción en el centro de cómputos

- Cual es la actitud del personal informático en caso de desastres
    - Organizados
    - Poco organizados
    - Desorganizados

- Se tiene documentación formal actualizada de los sistemas en producción.
    - Manual de usuario
    - Manual de operación
    - Manuales técnicos
    - Procedimientos de contingencias
    - Otros

5. Ambiente físico

- Cual es la periodicidad con que se realiza la limpieza del área de sistemas
    - Semanalmente
    - Diariamente
    - Otro

- Existe un lugar asignado para almacenar dispositivos externos de almacenamiento
    - Si
    - No

- Son funcionales los muebles del área de sistemas
    - Si
    - No
- Existe prohibición de fumar y comer en el área de servidores
    - Si
    - No

- El acceso al área de servidores tiene acceso restringido a su personal
    - Si
    - No

- La sala de servidores se encuentra a salvo de
    - Inundaciones
    - Terremotos
    - Fuego
    - Sabotaje
    - Motines

- El centro de cómputos da al exterior
    - Si
    - No

- El área de sistemas esta en un lugar de alto trafico de personas
    - Si
    - No

- El área de sistemas tiene suficiente lugar para las computadoras y personas.
    - Si

  - No

- El área de sistemas tiene lugar previsto para
  - Almacenar backups
  - Guardar papel
  - Mesas de trabajo
  - Equipos de telecomunicaciones
  - área de programación
  - área de análisis
  - área de atención a usuarios
  - Sala de reuniones
  - Bóvedas de seguridad

- La temperatura en que trabajan los equipos es la recomendada por los proveedores
  - Si
  - No

- Los equipos de aire acondicionado son suficientes
  - Si
  - No

- La instalación eléctrica cuenta con tierra física
  - Si
  - No

- El cableado eléctrico se encuentra debidamente instalado
  - Si
  - No

- Hay alarma contra inundación
  - Si
  - No

- Hay alarma contra incendios
    - Si
    - No

- Existe personal responsable de la seguridad
    - Personal externo
    - Interno
    - No existe

- La seguridad es durante las 24 hs
    - Si
    - No

- Existen matafuegos
    - Si
    - No

6. Hardware

- Cuantas computadoras, servidores, y periféricos se tienen conectados a la red
    - Cantidad
    - Tipo

- Existe un comité para la compra de hardware
    - Si
    - No

- Existen políticas formales de adquisición de equipos
    - Si
    - No

- Como se determinan los proveedores de hardware

- El mantenimiento del hardware es
    - Propio
    - Tercerizado
    - Mixto

- Existe un listado formal de parque de hardware
    - Si
    - No

- Se cuenta con manuales técnicos del hardware instalado
    - Servidores
    - Estaciones de trabajo
    - Otros

- Existe un procedimiento formal para el mantenimiento del hardware
    - Si
    - No

7. Software

- Hay una lista del software existente en la organización
    - Si
    - No

- Se cuenta con manuales del software
    - Si
    - No

- Existe un procedimiento formal para actualizar el software instalado en las estaciones de trabajo
    - Si

- No

- Esta identificado el software original y las copias
  - Si
  - No

- Cual es el procedimiento para la instalación de software en las estaciones de trabajo

- Hay una lista actualizada del software instalado en cada estación de trabajo
  - Si
  - No

8. Seguridad lógica y física

- Cuales son los perfiles de usuarios que se establecen en cada sistema

- El control de acceso a los sistemas esta dada por
  - Seguridad del sistema operativo
  - Seguridad del sistema
  - Ldap
  - Ambas
  - Otras

- La validación de acceso a los sistemas esta dada por
  - Claves de acceso
  - Credencial
  - Huella dactilar
  - Retina
  - Voz
  - Retina
  - Otros

- Cada cuanto se cambian las claves de acceso a los sistemas
    - Semanalmente
    - Mensualmente
    - Semestralmente
    - Anualmente
    - Otros

- Cada cuanto se cambian las claves de administradores de los sistemas
    - Semanalmente
    - Mensualmente
    - Semestralmente
    - Anualmente
    - Otros

- Cada cuanto se cambian las claves de dba
    - Semanalmente
    - Mensualmente
    - Semestralmente
    - Anualmente
    - Otros

- Las claves de acceso a los sistemas se encuentran almacenadas en algún lugar
    - Si
    - No

- Las claves de acceso de los administradores de los sistemas se encuentran almacenadas en algún lugar
    - Si
    - No

- Las claves de acceso de los dba se encuentran almacenadas en algún lugar
    - Si
    - No

- Existe acceso a Internet
    - Desde los servidores
    - Desde las estaciones de trabajo

- Se encriptan las bases de datos
    - Si
    - No

- Si se encriptan las bases de datos describa que datos y que metodología de encriptamiento se utiliza.

- Existe un plan de contingencias
    - Si
    - No

- En caso de existir un plan de contingencias describa su contenido

- Existe una política de prevención contra virus
    - Si
    - No

- En el caso de existir una política de prevención de virus descríbala

9. Parámetros de medición

- Se tiene un procedimiento formal de seguimiento al desempeño del personal informático, Indique si dicho procedimiento contempla los siguientes puntos

  - Parámetros de medición por puesto
  - Parámetros de medición por función
  - Objetivos y alcances de cada puesto
  - Resultados esperados de cada puesto
  - Tiempo esperado para la ejecución de cada función
  - Responsables de dar seguimiento a cada puesto
  - Encuestas a usuarios al final de cada proyecto

- Existen fechas predefinidas para la aplicación de parámetros de medición durante el desarrollo de cada proyecto

- Las funciones de controlar y ejecutar están divididas

- El personal informático participa del proceso de evaluación o solo se le notifica de los resultados

- Existe un análisis costo beneficio de la función informática

- La dirección considera que el apoyo informático es pobre. Porque

- Desde su punto de vista hay descontento en la organización por los servicios que brinda informática

- La función informática ha difundido los servicios y productos que ofrece a los usuarios

Anexo 4

CHECKLIST

PREGUNTA
• La gestión informática se lleva a cabo: o En forma unificada, por la gerencia o área de Sistemas o En forma compartida, por 2 o mas áreas independientes entre si o Por un servicio tercerizado a través de una contratación a una empresa especializada en sistemas o Por personal especializado dependiente de las áreas usuarias
• Organización, GESTION Y base jurídica
• Planeación y organización
• Definir la organización y las relaciones de TI

PREGUNTA
• Indique el nombre completo del área de sistema
• Organización, GESTION Y base jurídica
DOMINIO
• Planeación y organización
• Definir la organización y las relaciones de TI

PREGUNTA
• El área de sistemas reviste el carácter de: o Gerencia o dirección o Departamento, Jefatura, coordinación o Grupo de trabajo o Otro
TIPO DE AUDITORÍA
• Organización, GESTION Y base jurídica
• Planeación y organización
PROCESO
• Definir la organización y las relaciones de TI

PREGUNTA
•
TIPO DE AUDITORÍA
• Organización, GESTION Y base jurídica

• Planeación y organización
PROCESO
• Definir la organización y las relaciones de TI

PREGUNTA
• La ubicación del área de sistemas en el organigrama es la siguiente o Depende de la máxima autoridad del organismo o Depende de otra área o Gerencia o Otras
TIPO DE AUDITORÍA
• Organización, GESTION Y base jurídica
DOMINIO
• Planeación y organización
• Definir la organización y las relaciones de TI

PREGUNTA
• El área de sistemas cuenta con una estructura o Formalmente definida o Definida pero aun no aprobada formalmente o Definida informalmente dentro del área
TIPO DE AUDITORÍA
• Organización, GESTION Y base jurídica
DOMINIO
• Planeación y organización
• Definir la organización y las relaciones de TI

PREGUNTA
• El área de sistemas dispone de o Planes de corto y largo plazo aprobados formalmente, que se ajustan al plan estratégico del organismo o Un plan general no formalizado, para las actividades del sector o No dispone de planificación documentada
TIPO DE AUDITORÍA
• Organización, GESTION Y base jurídica
• Planeación y organización
PROCESO
• Definir un plan estratégico de TI

PREGUNTA
• El cumplimiento de los objetivos planificados para el área de sistemas, se controla mediante

○ Un tablero de comandos utilizado por el organismo para monitorear las actividades de las distintas áreas. ○ Informes de avance periódicos elevados a las autoridades del organismo ○ Reportes de carácter informal ○ Supervisión no documentada
TIPO DE AUDITORÍA
• Organización, GESTION Y base jurídica
• Comunicar los objetivos y el rumbo administrativo
PROCESO
• Definir un plan estratégico de TI

PREGUNTA
• Los planes de sistemas están integrados a los planes estratégicos de la organización ○ Si ○ No
TIPO DE AUDITORÍA
• Organización, GESTION Y base jurídica
• Planeación y organización
• Definir un plan estratégico de TI

PREGUNTA
• La estructura del área de sistemas contempla los siguientes sectores y funciones asignados a responsables independientes ○ Desarrollo y producción / procesamiento independiente ○ Administración de base de datos ○ Control de calidad ○ Administración de redes / telecomunicaciones
TIPO DE AUDITORÍA
• Organización, GESTION Y base jurídica
• Planeación y organización
PROCESO
• Definir definir la organización y las relaciones de TI

PREGUNTA
• El área de sistemas dispone de políticas, procedimientos y estándares documentados y aprobados formalmente para las siguientes tareas ○ Desarrollo y mantenimiento de sistemas ○ Administración de la seguridad ○ Tratamiento de contingencias

○ Administración de copias de backup ○ Actividades de soporte ○ Gestión y control de licencias de software ○ Otros
TIPO DE AUDITORÍA
• Organización, GESTION Y base jurídica
• Planeación y organización
PROCESO
• Comunicar los objetivos y el rumbo tecnológico

PREGUNTA
• La incorporación de sistemas en el organismo es realizado por ○ Desarrollos realizados por el área de sistemas ○ Desarrollos realizados por un grupo externo contratado y supervisado por el área de sistemas ○ Desarrollos realizados por analistas/programadores contratados por el área usuarios ○ Adquisición de sistemas aplicativos estándares del mercado ○ Provisión de sistemas por parte de otros organismos del estado ○ Otro
TIPO DE AUDITORÍA
• Organización, GESTION Y base jurídica
• Planeación y organización
• Definir la organización y las relaciones de TI

PREGUNTA
• Existe un comité de informática ○ Si ○ No
TIPO DE AUDITORÍA
• Organización, GESTION Y base jurídica
• Planeación y organización
• Definir la organización y las relaciones de TI

PREGUNTA
• Si existe un comité de informática quien lo integra y cuales son sus objetivos
TIPO DE AUDITORÍA
• Organización, GESTION Y base jurídica

DOMINIO
• Planeación y organización
• Definir la organización y las relaciones de TI

PREGUNTA
• Las tareas de procesamiento de los sistemas de aplicación son realizados por o Las áreas usuarias o El área de sistemas o Especialistas en sistemas dependientes de las áreas usuarias o Terceros contratados para esta área o Otros
• Organización, GESTION Y base jurídica
• Planeación y organización
• Definir la organización y las relaciones de TI

PREGUNTA
• El soporte técnico informático a los usuarios es realizado por o El personal de desarrollo de sistemas o El área de capacitación o Una mesa de ayuda dedicada a la atención de problemas de usuarios o Los usuarios o Terceros contratados para esta tarea o Otros
TIPO DE AUDITORÍA
• Organización, GESTION Y base jurídica
• Planeación y organización
• Definir la Organización y las relaciones de TI

PREGUNTA
• La tarea de Auditoría interna de sistemas es realizada por o Auditores especializados en sistemas dependientes de la Unidad de Auditoría interna o Auditores no especializados en sistemas dependientes de la Unidad de Auditoría Interna o No se realizan auditorias internas de sistemas o Otros
TIPO DE AUDITORÍA
• Organización, GESTION Y base jurídica

DOMINIO
• Monitoreo
• Preparación de auditorías independientes

PREGUNTA
• La plataforma tecnológica del organismo cuenta con o Mainframe o Servidores de tecnología Intel con sistema operativos tipo Novell, Windows NT, Linux, Unix, etc. o Servidores de tecnología Risc con sistemas operativos Unís o Otros servidores (AS 400, VAX, etc.)
TIPO DE AUDITORÍA
• Organización, GESTION Y base jurídica
• Planeación y organización
• Determinar el rumbo tecnológico

PREGUNTA
• El organismo dispone de o Hasta 50 computadoras personales o Entre 51 y 100 PC o Entre 101 y 500 PC o Entre 500 y 1000 PC o Mas de 1000 PC
TIPO DE AUDITORÍA
• Organización, GESTION Y base jurídica
• Planeación y organización
• Determinar el rumbo tecnológico

PREGUNTA
• El organismo dispone de o Base de datos o Sitio Web o Correo electrónico o Firewall o Intranet
TIPO DE AUDITORÍA
• Organización, GESTION Y base jurídica
• Planeación y organización

• Determinar el rumbo Tecnológico

PREGUNTA
• El sitio Web del organismo es utilizado para o Difusión de información y/o servicios de carácter publico o Recepción de información que reviste carácter de Declaración Jurada o Recepción de denuncias u otra información de carácter critico. o Recepción de información de carácter oficial. o Recaudación o manejo de fondos
TIPO DE AUDITORÍA
• Organización, GESTION Y base jurídica
• Planeación y organización
• Definir la arquitectura de la información

PREGUNTA
• Las bases de datos del organismo cuentan con información o De carácter general o Administrativa y/o presupuestaria interna del organismo o De personas físicas o jurídicas con carácter confidencial o privada y / o podría estar alcanzada por la ley de Habeas Data o Económica y/o presupuestaria de carácter confidencial
TIPO DE AUDITORÍA
• Organización, GESTION Y base jurídica
• Planeación y organización
• Definir la arquitectura de la información

PREGUNTA
• El presupuesto para las actividades informáticas del presente ejercicio ascienden a o Hasta $500.000.- o Entre $500.001 y 2.000.000.- o Entre $2.000.001 y $5.000.000 o Entre $5.000.001 y $20.000.000 o Mas de $20.000.001
TIPO DE AUDITORÍA
• Organización, GESTION Y base jurídica
• Planeación y organización
• Administrar la inversión de TI

PREGUNTA
• El presupuesto para actividades informáticas representa el siguiente porcentaje del presupuesto total del organismo o Hasta 2% o Entre 2% y el 5% o Entre el 5% y el 10% o Mas de 10%
• Organización, GESTION Y base jurídica
• Planeación y organización
• Administrar la inversión de tecnología de la información

PREGUNTA
• La cantidad de sistemas de aplicación de Misión Crítica utilizados en el organismo es o Hasta 5 o Entre 6 y 15 o Entre 16 y 30 o Mas de 30 •
• Organización, GESTION Y base jurídica
• Planeación y organización
PROCESO
• Definir la arquitectura de la información

PREGUNTA
• La cantidad de sistemas de aplicación que no son de Misión Crítica utilizados en el organismo es o Hasta 20 o Entre 21 y 50 o Entre 51 y 100 o Mas de 100
TIPO DE AUDITORÍA
• Organización, GESTION Y base jurídica
• Planeación y organización

PROCESO
• Definir la arquitectura de la información

PREGUNTA
• Se ajusta la estructura orgánica actual a las disposiciones jurídicas vigentes o Si o No
TIPO DE AUDITORÍA
• Organización, GESTION Y base jurídica
• Planeación y organización
• Asegurar el cumplimiento de requerimientos externos

PREGUNTA
• Permiten los niveles jerárquicos actuales que se desarrolle adecuadamente la o Operación o Supervisión o Control
TIPO DE AUDITORÍA
• Organización, GESTION Y base jurídica
• Planeación y organización
• Definir la Organización y las relaciones de TI

PREGUNTA
• Permiten los actuales niveles jerárquicos que se tenga una ágil o Comunicación ascendente o Comunicación descendente o Toma de decisiones •
TIPO DE AUDITORÍA
• Organización, GESTION Y base jurídica
• Planeación y organización
• Definir la Organización y las relaciones de TI

PREGUNTA
• Considera que algunas áreas deberían tener o Mayor jerarquía o Menor jerarquía •

TIPO DE AUDITORÍA
• Organización, GESTION Y base jurídica
DOMINIO
• Planeación y organización
PROCESO
• Definir la organización y las relaciones de TI

PREGUNTA
• Se consideran adecuados los departamentos, áreas y oficinas en que esta actualmente dividida actualmente la estructura de la dirección. o Si o No
TIPO DE AUDITORÍA
• Organización, GESTION Y base jurídica
• Planeación y organización
• Definir la organización y las relaciones de TI

PREGUNTA
El numero de empleados que trabaja actualmente es adecuado para cumplir con las funciones encomendadas o Si o No
TIPO DE AUDITORÍA
• Organización, GESTION Y base jurídica
• Planeación y organización
• Definir la organización y las relaciones de TI

PREGUNTA
Se han establecido funciones del área o Si o No
TIPO DE AUDITORÍA
• Organización, GESTION Y base jurídica
DOMINIO
• Planeación y organización
PROCESO
• Definir la organización y las relaciones de TI

PREGUNTA
• Conocen las otras áreas las funciones del área de sistemas o Si

○ No
TIPO DE AUDITORÍA
• Organización, GESTION Y base jurídica
DOMINIO
• Planeación y organización
PROCESO
• Definir la organización y las relaciones de TI

PREGUNTA
• Existe duplicidad de funciones en el mismo área ○ Si ○ No •
TIPO DE AUDITORÍA
• Organización, GESTION Y base jurídica
DOMINIO
• Planeación y organización
• Definir la organización y las relaciones de TI

PREGUNTA
Se han establecido objetivos del área de sistemas ○ Si ○ No •
• Organización, GESTION Y base jurídica
• Planeación y organización
• Definir la organización y las relaciones de TI

PREGUNTA
Participo el área de sistemas en el establecimiento de objetivos ○ Si ○ No
TIPO DE AUDITORÍA
• Organización, GESTION Y base jurídica
• Planeación y organización
• Definir la organización y las relaciones de TI

PREGUNTA
Se han dado a conocer los objetivos del área ○ Si

○ No
TIPO DE AUDITORÍA
• Organización, GESTION Y base jurídica
• Planeación y organización
• Definir la organización y las relaciones de TI

PREGUNTA
Existen mecanismos para conocer el grado de cumplimiento de los objetivos ○ Si ○ No •
• Organización, GESTION Y base jurídica
• Planeación y organización
• Administrar la calidad

PREGUNTA
Se revisan los objetivos ○ Si ○ No
TIPO DE AUDITORÍA
• Organización, GESTION Y base jurídica
• Planeación y organización
• Administrar la calidad

PREGUNTA
Se tiene conciencia en toda la organización de que la función informática es principalmente proporcionar un servicio estratégico a las áreas de negocios ○ Si ○ No
TIPO DE AUDITORÍA
• Organización, GESTION Y base jurídica
• Planeación y organización
• Administrar la calidad

PREGUNTA

Se tienen problemas económicos organizacionales y de otro tipo por el uso actual de informática o Si o No
TIPO DE AUDITORÍA
• Organización, GESTION Y base jurídica
• Planeación y organización
• Administrar la inversión de TI

PREGUNTA
• Cual es la participación de las áreas usuarias en la definición y ejecución de las políticas informáticas.
TIPO DE AUDITORÍA
• Organización, GESTION Y base jurídica
• Planeación y organización
• Administrar la calidad

PREGUNTA
Es suficiente el número de personal para el desarrollo de las funciones del área o Si o No
• Recursos Humanos
• Planeación y organización
• Administrar los recursos Humanos

PREGUNTA
Se deja de realizar alguna actividad por falta de personal o Si o No
TIPO DE AUDITORÍA
• Recursos Humanos
• Planeación y organización
• Administrar los recursos Humanos

PREGUNTA

Esta capacitado el personal para realizar con eficiencia sus funciones o Si o No
TIPO DE AUDITORÍA
• Recursos Humanos
• Planeación y organización
• Administrar los recursos Humanos

PREGUNTA
Es eficiente el personal en el cumplimiento de sus funciones o Si o No
TIPO DE AUDITORÍA
• Recursos Humanos
• Planeación y organización
• Administrar los recursos Humanos

PREGUNTA
Es frecuente la repetición de trabajos encomendados o Si o No
TIPO DE AUDITORÍA
• Recursos Humanos
• Planeación y organización
• Definir la organización y las relaciones de TI

PREGUNTA
El personal es discreto en el manejo de información confidencial o Si o No
TIPO DE AUDITORÍA
• Recursos Humanos
• Planeación y organización
• Evaluar los riesgos

PREGUNTA

En general responde el personal a las políticas y procedimientos establecidos o Si o No
TIPO DE AUDITORÍA
• Recursos Humanos
• Planeación y organización
• Definir la organización y las relaciones de TI

PREGUNTA
Respeta el personal la autoridad establecida o Si o No
TIPO DE AUDITORÍA
• Recursos Humanos
• Planeación y organización
• Definir la organización y las relaciones de TI

PREGUNTA
Existe colaboración del personal para la realización del trabajo o Si o No
TIPO DE AUDITORÍA
• Recursos Humanos
• Planeación y organización
PROCESO
• Definir la organización y las relaciones de TI
El personal tiene afán de superación o Si o No
TIPO DE AUDITORÍA
• Recursos Humanos
• Planeación y organización
• Administrar los recursos humanos

PREGUNTA
Presenta el personal sugerencias para mejorar el actual desempeño o Si

○ No
TIPO DE AUDITORÍA
• Recursos Humanos
• Planeación y organización
• Administrar los recursos humanos

PREGUNTA
• Los programas de capacitación incluyen al personal de ○ Dirección ○ Análisis ○ Programación ○ Operación ○ Administración ○ Dba ○ Redes ○ Otros
TIPO DE AUDITORÍA
• Recursos Humanos
• Planeación y organización
• Administrar los recursos humanos

PREGUNTA
•
• Recursos Humanos
• Planeación y organización
• Administrar los recursos humanos

PREGUNTA
Se han identificado las necesidades actuales y futuras de capacitación ○ Si ○ No
TIPO DE AUDITORÍA
• Recursos Humanos
• Planeación y organización

• Administrar los recursos humanos

PREGUNTA
Se desarrollan actualmente programas de capacitación o Si o No
TIPO DE AUDITORÍA
• Recursos Humanos
• Planeación y organización
• Administrar los recursos humanos

PREGUNTA
Apoya la dirección los planes de capacitación o Si o No
TIPO DE AUDITORÍA
• Recursos Humanos
• Planeación y organización
• Administrar los recursos humanos

PREGUNTA
Cual es el índice de rotación promedio del personal o De 1 a 6 meses o De 6 meses a un año o De una año a dos años o Mas de dos años
TIPO DE AUDITORÍA
• Recursos Humanos
• Planeación y organización
• Administrar los recursos humanos

PREGUNTA
En general se adapta el personal al mejoramiento administrativo o Si o No
TIPO DE AUDITORÍA
• Recursos Humanos
• Planeación y organización

PROCESO
• Comunicar los objetivos y rumbos administrativos

PREGUNTA
En promedio cual es el grado de asistencia y puntualidad del personal o Bueno o Malo o Regular
• Recursos Humanos
• Planeación y organización
• Administrar los recursos humanos

PREGUNTA
• Existe una política de sanción disciplinaria del personal o Si o No •
• Recursos Humanos
• Planeación y organización
• Administrar los recursos humanos

PREGUNTA
• Esta el personal adecuadamente remunerado o Si o No
TIPO DE AUDITORÍA
• Recursos Humanos
• Planeación y organización
• Administrar los recursos humanos

PREGUNTA
• El personal esta integrado como grupo de trabajo o Si o No
TIPO DE AUDITORÍA
• Recursos Humanos
• Planeación y organización

PROCESO
• Definir la organización y las relaciones de TI

PREGUNTA
• Existe un proceso formal de comunicación interna entre el personal informático o Cual es el sistema o Cuales son los obstáculos principales de comunicación entre el personal informático
TIPO DE AUDITORÍA
• Recursos Humanos
• Planeación y organización
PROCESO
• Definir la organización y las relaciones de TI

PREGUNTA
• Son adecuadas las condiciones ambientales con respecto a o Espacio del área o Iluminación o Ventilación o Mobiliario o Ruido o Limpieza y aseo o Instalación sanitaria o Instalación de comunicaciones
TIPO DE AUDITORÍA
• Recursos Humanos
• Suministro y soporte
PROCESO
• Manejo de las instalaciones

PREGUNTA
• Esta prevista la sustitución del personal clave o Si o No
TIPO DE AUDITORÍA
• Recursos Humanos
• Planeación y organización
• Administrar los recursos humanos

PREGUNTA

• Existen oportunidades de ascenso y promociones
  ○ Si
  ○ No

TIPO DE AUDITORÍA
• Recursos Humanos
• Planeación y organización
• Administrar los recursos humanos

PREGUNTA

• Se ha evaluado el nivel de capacitación del personal en el ultimo año
  ○ Si
  ○ No
•

TIPO DE AUDITORÍA
• Recursos Humanos
• Planeación y organización
• Administrar los recursos humanos

PREGUNTA

• Cuales son los sistemas que actualmente están en desarrollo
  ○ Nombre de cada uno
  ○ Breve descripción funcional
  ○ Etapa del desarrollo

TIPO DE AUDITORÍA
• Sistemas en desarrollo
• Adquisición e implementación
PROCESO
• Identificar las soluciones

PREGUNTA

• Existe un plan maestro de sistemas
  ○ Si
  ○ No

TIPO DE AUDITORÍA
• Sistemas en desarrollo
• Planeación y organización
• Administrar los proyectos

PREGUNTA
• Esta relacionado el plan de desarrollo de sistemas con el plan general de desarrollo de la dependencia o Si o No
TIPO DE AUDITORÍA
• Sistemas en desarrollo
• Planeación y organización
• Administrar los proyectos

PREGUNTA
• Ofrece el plan maestro la atención de solicitudes urgentes de los usuarios o Si o No
TIPO DE AUDITORÍA
• Sistemas en desarrollo
• Planeación y organización
• Administrar los proyectos

PREGUNTA
• Quien autoriza los proyectos
TIPO DE AUDITORÍA
• Sistemas en desarrollo
• Planeación y organización
• Administrar los proyectos

PREGUNTA
• Como se asignan los recursos
TIPO DE AUDITORÍA
• Sistemas en desarrollo
• Planeación y organización
• Administrar los proyectos

PREGUNTA
• Como se estiman los tiempos de duración de los proyectos

TIPO DE AUDITORÍA
• Sistemas en desarrollo
• Planeación y organización
• Administrar los proyectos

PREGUNTA
• Quien interviene en la evaluación de proyectos
TIPO DE AUDITORÍA
• Sistemas en desarrollo
DOMINIO
• Planeación y organización
PROCESO
• Administrar los proyectos

PREGUNTA
• Como se calcula el presupuesto de cada proyecto
TIPO DE AUDITORÍA
• Sistemas en desarrollo
• Adquisición e implementación
• Identificar las soluciones

PREGUNTA
• Que técnicas se usan en el control de los proyectos
TIPO DE AUDITORÍA
• Sistemas en desarrollo
• Planeación y organización
• Administrar la calidad

PREGUNTA
• Quien asigna las prioridades
TIPO DE AUDITORÍA
• Sistemas en desarrollo
• Adquisición e implementación
• Identificar las soluciones

PREGUNTA
•
TIPO DE AUDITORÍA
• Sistemas en desarrollo
DOMINIO
• Planeación y organización
PROCESO
• Administrar la calidad

PREGUNTA
• Como se controla el avance de los proyectos
TIPO DE AUDITORÍA
• Sistemas en desarrollo
DOMINIO
• Planeación y organización
PROCESO
• Administrar la calidad

PREGUNTA
• Con que periodicidad se revisa el avance de los proyectos
TIPO DE AUDITORÍA
• Sistemas en desarrollo
DOMINIO
• Planeación y organización
PROCESO
• Administrar la calidad

PREGUNTA
• Que acciones correctivas se toman en caso de desviaciones en los proyectos
TIPO DE AUDITORÍA
• Sistemas en desarrollo
DOMINIO
• Planeación y organización
PROCESO
• Administrar la calidad

PREGUNTA
• Se llevan a cabo revisiones periódicas de los sistemas en desarrollo para determinar si cumplen los objetivos. o De análisis o De programación o Otros

TIPO DE AUDITORÍA
• Sistemas en desarrollo
DOMINIO
• Adquisición e implementación
PROCESO
• Manejar los cambios

PREGUNTA
• Quien interviene al diseñar un sistema o Usuario o Analista o Gerente o Dba o Personal de comunicaciones o Auditores internos o Asesores o Otros
TIPO DE AUDITORÍA
• Sistemas en desarrollo
DOMINIO
• Adquisición e implementación
PROCESO
• Adquirir y dar mantenimiento al software de aplicación

PREGUNTA
• Que lenguaje de programación conoce el equipos de desarrollo
TIPO DE AUDITORÍA
• Sistemas en desarrollo
DOMINIO
• Planeación y organización
PROCESO
• Administrar los recursos humanos

PREGUNTA
• Que metodología de desarrollo de sistemas se utiliza
TIPO DE AUDITORÍA
• Sistemas en desarrollo
DOMINIO
• Adquisición e implementación
PROCESO
• Adquirir y dar mantenimiento al software de aplicación

PREGUNTA
• Existe un procedimiento formal para realizar las pruebas o Si

○ No
TIPO DE AUDITORÍA
• Sistemas en desarrollo
DOMINIO
• Adquisición e implementación
PROCESO
• Instalar y acreditar los sistemas

PREGUNTA
• Participan los usuarios en el proceso de testing ○ Si ○ No
TIPO DE AUDITORÍA
• Sistemas en desarrollo
DOMINIO
• Adquisición e implementación
PROCESO
• Instalar y acreditar los sistemas

PREGUNTA
• Existe un procedimiento formal para realizar la conversión de datos de un sistema en retiro a un nuevo sistema ○ Si ○ No
TIPO DE AUDITORÍA
• Sistemas en desarrollo
DOMINIO
• Adquisición e implementación
PROCESO
• Instalar y acreditar los sistemas

PREGUNTA
• Existe un procedimiento formal para realizar la implantación de los nuevos sistemas ○ Si ○ No
TIPO DE AUDITORÍA
• Sistemas en desarrollo
DOMINIO
• Adquisición e implementación
PROCESO
• Instalar y acreditar los sistemas

PREGUNTA

• Que documentación acompaña al programa cuando se entrega
TIPO DE AUDITORÍA
• Sistemas en desarrollo
DOMINIO
• Adquisición e implementación
• Desarrollar y mantener procedimientos de TI (Manuales)

PREGUNTA
• El software utilizado para el desarrollo de sistemas es legal o Si o No o Open source
TIPO DE AUDITORÍA
• Sistemas en desarrollo
• Adquisición e implementación
• Adquirir y dar mantenimiento a la arquitectura tecnológica

PREGUNTA
• El motor de base de datos es legal o SI o NO o Open source
TIPO DE AUDITORÍA
• Sistemas en desarrollo
• Adquisición e implementación
• Adquirir y dar mantenimiento a la arquitectura tecnológica

PREGUNTA
• Cuales son las herramientas que se utilizan en el desarrollo de sistemas.
TIPO DE AUDITORÍA
• Sistemas en desarrollo
• Adquisición e implementación
• Adquirir y dar mantenimiento a la arquitectura tecnológica

PREGUNTA
• Cual es el proceso de Gestión de configuración en el desarrollo de sistemas.

TIPO DE AUDITORÍA
• Sistemas en desarrollo
• Adquisición e implementación
• Manejar los cambios

PREGUNTA
• La función de aseguramiento de la calidad en el desarrollo de sistemas contempla o Puntos de revisión en el análisis o Puntos de revisión en el diseño o Puntos de revisión en la construcción o Puntos de revisión en las pruebas o Puntos de revisión en la implementación
TIPO DE AUDITORÍA
• Sistemas en desarrollo
• Planeación y organización
• Administrar la calidad

PREGUNTA
• Cuales son los sistemas que se operan actualmente o Nombre o Breve descripción funcional o Lenguaje o Motor de base de datos o Fecha de desarrollo o Desarrollador o Ultima actualización o Ubicación
TIPO DE AUDITORÍA
• Operación y soporte
• Suministro y soporte
• Definir los niveles de servicios

PREGUNTA
• La arquitectura del procesamiento es o Centralizada o Descentralizada o Mixta

TIPO DE AUDITORÍA
• Sistemas en desarrollo
• Planeación y organización
• Definir la arquitectura de la información

PREGUNTA

• Existen normas que definan el contenido de los instructivos de captación de datos
  ○ Si
  ○ No

TIPO DE AUDITORÍA
• Operación y soporte
• Suministro y soporte
• Manejar los datos

PREGUNTA

• Quien controla la entrada del documento fuente
  ○ Quien carga
  ○ Otra persona
  ○ No se controla

TIPO DE AUDITORÍA
• Operación y soporte
• Suministro y soporte
• Manejar los datos

PREGUNTA

• Cuando la carga de trabajo supera la capacidad instalada se requiere
  ○ Tiempo extra
  ○ Se subcontrata

TIPO DE AUDITORÍA
• Operación y soporte
• Suministro y soporte
• Manejar los problemas e incidentes

PREGUNTA
• Se verifica la calidad de la información recibida para su captura   ○ SI

○ No
TIPO DE AUDITORÍA
• Operación y soporte
• Suministro y soporte
• Manejar los datos

PREGUNTA
• Cual es el procedimiento para solicitar un servicio de informática
TIPO DE AUDITORÍA
• Operación y soporte
• Suministro y soporte
• Definir los niveles de servicios

PREGUNTA
• Como se asegura el cumplimiento oportuno de los servicios solicitados
TIPO DE AUDITORÍA
• Operación y soporte
• Suministro y soporte
• Definir los niveles de servicios

PREGUNTA
• Existe un procedimiento escrito que indique como tratar la información invalida ○ Si ○ No
• Operación y soporte
• Suministro y soporte
• Manejar los datos

PREGUNTA
• Los documentos fuentes de entrada se guardan en lugar seguro ○ Si ○ No
TIPO DE AUDITORÍA

• Operación y soporte
DOMINIO
• Suministro y soporte
• Manejar los datos

PREGUNTA
• Existe un registro de anomalías de la información de entrada a los sistemas que no se encuentra de acuerdo a los procedimientos establecidos o Si o No
TIPO DE AUDITORÍA
• Operación y soporte
• Suministro y soporte
• Asegurar la seguridad de los sistemas

PREGUNTA
• Existe una relación completa de distribución de listados, en la cual indiquen personas, secuencias y sistemas a los que pertenecen o Si o No
TIPO DE AUDITORÍA
• Operación y soporte
• Suministro y soporte
• Manejar las operaciones

PREGUNTA
• Se hace una relación de cuando y a quien fueron distribuidos los listados o Si o No
TIPO DE AUDITORÍA
• Operación y soporte
• Suministro y soporte
• Manejar las operaciones

PREGUNTA
• Se controlan separadamente los documentos confidenciales o Si o No

TIPO DE AUDITORÍA
• Operación y soporte
• Suministro y soporte
• Manejar los datos

PREGUNTA
• Se aprovecha adecuadamente el papel de los listados inservibles o Si o No
TIPO DE AUDITORÍA
• Operación y soporte
• Suministro y soporte
• Asegurar la seguridad de los sistemas

PREGUNTA
• Existen procedimientos formales para lo operación de los sistemas o Si o No
TIPO DE AUDITORÍA
• Operación y soporte
• Suministro y soporte
• Manejar las operaciones

PREGUNTA
• Los retrasos o incumplimientos del programa de operación diaria, se revisa y analiza. o Si o No
TIPO DE AUDITORÍA
• Operación y soporte
• Suministro y soporte
• Manejar las operaciones

PREGUNTA
• Existe un procedimiento formal para la recuperación del sistema en caso de fallas

○ Si ○ No
TIPO DE AUDITORÍA
• Operación y soporte
• Suministro y soporte
• Manejar los problemas e incidentes

PREGUNTA
• Opera el personal del área de informática los sistemas en producción. ○ Si ○ No
TIPO DE AUDITORÍA
• Operación y soporte
• Suministro y soporte
• Asegurar la seguridad de los sistemas

PREGUNTA
• Tienen los operadores una bitácora con los incidentes que se producen en la operación de los sistemas ○ Si ○ No
TIPO DE AUDITORÍA
• Operación y soporte
• Suministro y soporte
• Manejar los problemas e incidentes

PREGUNTA
• Existe un procedimiento para evitar la ejecución no autorizada de sistemas ○ Si ○ No
TIPO DE AUDITORÍA
• Operación y soporte
• Suministro y soporte
• Asegurar la seguridad de los sistemas

PREGUNTA

• Los equipos que se utilizan en la operación de los sistemas tienen seguro o Si o No
TIPO DE AUDITORÍA
• Operación y soporte
• Suministro y soporte
• Asegurar la seguridad de los sistemas

PREGUNTA
• Cada cuanto se cambian las claves de acceso a los sistema o De 1 a 7 días o De 7 días a 30 días o De 30 días a 90 días o De 90 días a 180 días o De 180 días a 360 días o Mas de un año o Nunca
TIPO DE AUDITORÍA
• Operación y soporte
• Suministro y soporte
• Asegurar la seguridad de los sistemas

PREGUNTA
• Existe copia de las bases de datos en otros locales o Si o No
TIPO DE AUDITORÍA
• Operación y soporte
• Suministro y soporte
• Asegurar el servicio continuo

PREGUNTA
• Cual es la política de backup
TIPO DE AUDITORÍA
• Operación y soporte
• Suministro y soporte

• Asegurar el servicio continuo

PREGUNTA
• Los locales asignados a almacenamiento magnético tienen o Aire acondicionado o Protección contra fuego o Cerradora especial o Otros
TIPO DE AUDITORÍA
• Operación y soporte
• Suministro y soporte
• Manejar las instalaciones

PREGUNTA
• Existe un procedimiento formal que permita reconstruir un archivo dañado o Si o No
TIPO DE AUDITORÍA
• Operación y soporte
• Suministro y soporte
• Asegurar el servicio continuo

PREGUNTA
• Cual es el impacto de una hora de interrupción en el centro de cómputos
TIPO DE AUDITORÍA
• Operación y soporte
• Suministro y soporte
• Manejar los problemas e incidentes

PREGUNTA
• Cual es la actitud del personal informático en caso de desastres o Organizados o Poco organizados o Desorganizados
• Operación y soporte
• Suministro y soporte

PROCESO
• Manejar los problemas e incidentes

PREGUNTA
• Se tiene documentación formal actualizada de los sistemas en producción. o Manual de usuario o Manual de operación o Manuales técnicos o Procedimientos de contingencias o Otros
TIPO DE AUDITORÍA
• Operación y soporte
• Adquisición e implementación
• Desarrollar y mantener procedimientos de TI (manuales)

PREGUNTA
TIPO DE AUDITORÍA
• Ambiente físico
DOMINIO
• Suministro y soporte
• Manejar las instalaciones

PREGUNTA
• Cual es la periodicidad con que se realiza la limpieza del área de sistemas o Semanalmente o Diariamente o Otro
TIPO DE AUDITORÍA
• Ambiente físico
• Suministro y soporte
PROCESO
• Manejar las instalaciones

PREGUNTA
• Existe un lugar asignado para almacenar dispositivos externos de almacenamiento o Si o No
TIPO DE AUDITORÍA
• Ambiente físico

DOMINIO
• Suministro y soporte
• Manejar los datos

PREGUNTA
• Son funcionales los muebles del área de sistemas o Si o No
• Ambiente físico
DOMINIO
• Suministro y soporte
• Manejar las instalaciones

PREGUNTA
• Existe prohibición de fumar y comer en el área de servidores o Si o No
TIPO DE AUDITORÍA
• Ambiente físico
• Suministro y soporte
• Manejar las instalaciones

PREGUNTA
• El acceso al área de servidores tiene acceso restringido a su personal o Si o No
• Ambiente físico
• Suministro y soporte
PROCESO
• Manejar las instalaciones

PREGUNTA
• La sala de servidores se encuentra a salvo de o Inundaciones o Terremotos o Fuego o Sabotaje o Motines

TIPO DE AUDITORÍA
• Ambiente físico
• Suministro y soporte
PROCESO
• Manejar las instalaciones

PREGUNTA
• El centro de cómputos da al exterior o Si o No
TIPO DE AUDITORÍA
• Ambiente físico
• Suministro y soporte
• Manejar las instalaciones

PREGUNTA
• El área de sistemas esta en un lugar de alto trafico de personas o Si o No
TIPO DE AUDITORÍA
• Ambiente físico
• Suministro y soporte
• Manejar las instalaciones

PREGUNTA
• El área de sistemas tiene suficiente lugar para las computadoras y personas. o Si o No
TIPO DE AUDITORÍA
• Ambiente físico
• Suministro y soporte
• Manejar las instalaciones

PREGUNTA
• El área de sistemas tiene lugar previsto para o Almacenar backups

○ Guardar papel ○ Mesas de trabajo ○ Equipos de telecomunicaciones ○ área de programación ○ área de análisis ○ área de atención a usuarios ○ Sala de reuniones ○ Bóvedas de seguridad
TIPO DE AUDITORÍA
• Ambiente físico
• Suministro y soporte
• Manejar los datos

PREGUNTA
• La temperatura en que trabajan los equipos es la recomendada por los proveedores ○ Si ○ No
TIPO DE AUDITORÍA
• Ambiente físico
• Suministro y soporte
PROCESO
• Manejar las instalaciones

PREGUNTA
• Los equipos de aire acondicionado son suficientes ○ Si ○ No
TIPO DE AUDITORÍA
• Ambiente físico
• Suministro y soporte
PROCESO
• Manejar las instalaciones

PREGUNTA
• La instalación eléctrica cuenta con tierra física ○ Si ○ No
TIPO DE AUDITORÍA
• Ambiente físico

DOMINIO
• Suministro y soporte
• Manejar las instalaciones

PREGUNTA
• El cableado eléctrico se encuentra debidamente instalado o Si o No
TIPO DE AUDITORÍA
• Ambiente físico
DOMINIO
• Suministro y soporte
PROCESO
• Manejar las instalaciones

PREGUNTA
• Hay alarma contra inundación o Si o No
TIPO DE AUDITORÍA
• Ambiente físico
• Suministro y soporte
• Manejar las instalaciones

PREGUNTA
• Hay alarma contra incendios o Si o No
• Ambiente físico
• Suministro y soporte
• Manejar las instalaciones

PREGUNTA
• Existe personal responsable de la seguridad o Personal externo o Interno o No existe
TIPO DE AUDITORÍA

• Ambiente físico
DOMINIO
• Suministro y soporte
• Manejar las instalaciones

PREGUNTA
• La seguridad es durante las 24 hs o Si o No
TIPO DE AUDITORÍA
• Ambiente físico
• Suministro y soporte
• Manejar las instalaciones

PREGUNTA
• Existen matafuegos o Si o No
TIPO DE AUDITORÍA
• Ambiente físico
• Suministro y soporte
• Manejar las instalaciones

PREGUNTA
• Cuantas computadoras, servidores, y periféricos se tienen conectados a la red o Cantidad o Tipo
TIPO DE AUDITORÍA
• Hardware
• Planeación y organización
• Determinar el rumbo tecnológico

PREGUNTA
• Existe un comité para la compra de hardware o Si o No

TIPO DE AUDITORÍA
• Hardware
• Planeación y organización
• Determinar el rumbo tecnológico

PREGUNTA
• Existen políticas formales de adquisición de equipos o Si o No • Como se determinan los proveedores de hardware
TIPO DE AUDITORÍA
• Hardware
DOMINIO
• Suministro y soporte
• Manejar los servicios de terceros

PREGUNTA
TIPO DE AUDITORÍA
• Hardware
• Planeación y organización
PROCESO
• Determinar el rumbo tecnológico

PREGUNTA
• El mantenimiento del hardware es o Propio o Tercerizado o Mixto
TIPO DE AUDITORÍA
• Hardware
• Planeación y organización
• Determinar el rumbo tecnológico

PREGUNTA
• Existe un listado formal de parque de hardware o Si o No
TIPO DE AUDITORÍA

• Hardware
DOMINIO
• Planeación y organización
PROCESO
• Determinar el rumbo tecnológico

PREGUNTA
• Se cuenta con manuales técnicos del hardware instalado o Servidores o Estaciones de trabajo o Otros
TIPO DE AUDITORÍA
• Hardware
• Planeación y organización
• Determinar el rumbo tecnológico

PREGUNTA
• Existe un procedimiento formal para el mantenimiento del hardware o Si o No
TIPO DE AUDITORÍA
• Hardware
DOMINIO
• Planeación y organización
• Determinar el rumbo tecnológico

PREGUNTA
• Hay una lista del software existente en la organización o Si o No
TIPO DE AUDITORÍA
• Software
DOMINIO
• Adquisición e implementación
• Adquirir y dar mantenimiento a la arquitectura tecnológica

PREGUNTA
• Se cuenta con manuales del software o Si o No

TIPO DE AUDITORÍA
• Software
DOMINIO
• Adquisición e implementación
• Adquirir y dar mantenimiento a la arquitectura tecnológica

PREGUNTA
• Existe un procedimiento formal para actualizar el software instalado en las estaciones de trabajo o Si o No
TIPO DE AUDITORÍA
• Software
• Adquisición e implementación
• Adquirir y dar mantenimiento a la arquitectura tecnológica

PREGUNTA
• Esta identificado el software original y las copias o Si o No
TIPO DE AUDITORÍA
• Software
• Suministro y soporte
• Manejar la configuración

PREGUNTA
• Cual es el procedimiento para la instalación de software en las estaciones de trabajo
TIPO DE AUDITORÍA
• Software
• Adquisición e implementación
• Adquirir y dar mantenimiento a la arquitectura tecnológica

PREGUNTA
• Hay una lista actualizada del software instalado en cada estación de trabajo o Si o No

TIPO DE AUDITORÍA
• Software
• Adquisición e implementación
• Adquirir y dar mantenimiento a la arquitectura tecnológica

PREGUNTA
TIPO DE AUDITORÍA
• Seguridad lógica y física
• Suministro y soporte
• Asegurar la seguridad de los sistemas

PREGUNTA
• Cuales son los perfiles de usuarios que se establecen en cada sistema
TIPO DE AUDITORÍA
• Seguridad lógica y física
• Suministro y soporte
• Asegurar la seguridad de los sistemas

PREGUNTA

• El control de acceso a los sistemas esta dada por
  ○ Seguridad del sistema operativo
  ○ Seguridad del sistema
  ○ Ldap
  ○ Ambas
  ○ Otras

TIPO DE AUDITORÍA
• Seguridad lógica y física
• Suministro y soporte
• Asegurar la seguridad de los sistemas

PREGUNTA

• La validación de acceso a los sistemas esta dada por
  ○ Claves de acceso
  ○ Credencial
  ○ Huella dactilar

○ Retina ○ Voz ○ Retina ○ Otros
TIPO DE AUDITORÍA
• Seguridad lógica y física
• Suministro y soporte
• Asegurar la seguridad de los sistemas

PREGUNTA
• Cada cuanto se cambian las claves de acceso a los sistemas ○ Semanalmente ○ Mensualmente ○ Semestralmente ○ Anualmente ○ Otros
TIPO DE AUDITORÍA
• Seguridad lógica y física
• Suministro y soporte
• Asegurar la seguridad de los sistemas

PREGUNTA
• Cada cuanto se cambian las claves de administradores de los sistemas ○ Semanalmente ○ Mensualmente ○ Semestralmente ○ Anualmente ○ Otros
TIPO DE AUDITORÍA
• Seguridad lógica y física
• Suministro y soporte
• Asegurar la seguridad de los sistemas

PREGUNTA
• Cada cuanto se cambian las claves de dba ○ Semanalmente ○ Mensualmente ○ Semestralmente ○ Anualmente

○ Otros
TIPO DE AUDITORÍA
• Seguridad lógica y física
• Suministro y soporte
• Asegurar la seguridad de los sistemas

PREGUNTA
• Las claves de acceso a los sistemas se encuentran almacenadas en algún lugar ○ Si ○ No
TIPO DE AUDITORÍA
• Seguridad lógica y física
• Suministro y soporte
• Asegurar la seguridad de los sistemas

PREGUNTA
• Las claves de acceso de los administradores de los sistemas se encuentran almacenadas en algún lugar ○ Si ○ No
TIPO DE AUDITORÍA
• Seguridad lógica y física
• Suministro y soporte
• Asegurar la seguridad de los sistemas

PREGUNTA
• Las claves de acceso de los dba se encuentran almacenadas en algún lugar ○ Si ○ No
TIPO DE AUDITORÍA
• Seguridad lógica y física
• Suministro y soporte
• Asegurar la seguridad de los sistemas

PREGUNTA

• Existe acceso a Internet
  ○ Desde los servidores
  ○ Desde las estaciones de trabajo

TIPO DE AUDITORÍA
• Seguridad lógica y física
• Planeación y organización
• Determinar el rumbo tecnológico

PREGUNTA

• Se encriptan las bases de datos
  ○ Si
  ○ No

TIPO DE AUDITORÍA
• Seguridad lógica y física
• Suministro y soporte
• Asegurar la seguridad de los sistemas

PREGUNTA
• Si se encriptan las bases de datos describa que datos y que metodología de encriptamiento se utiliza.
TIPO DE AUDITORÍA
• Seguridad lógica y física
• Suministro y soporte
• Asegurar la seguridad de los sistemas

PREGUNTA

• Existe un plan de contingencias
  ○ si
  ○ No

TIPO DE AUDITORÍA
• Seguridad lógica y física
• Suministro y soporte
• Asegurar la seguridad de los sistemas

PREGUNTA
• En caso de existir un plan de contingencias describa su contenido

TIPO DE AUDITORÍA
• Seguridad lógica y física
• Suministro y soporte
• Asegurar la seguridad de los sistemas

PREGUNTA
• Existe una política de prevención contra virus o Si o No
TIPO DE AUDITORÍA
• Seguridad lógica y física
• Suministro y soporte
• Asegurar la seguridad de los sistemas

PREGUNTA
• En el caso de existir una política de prevención de virus descríbala
TIPO DE AUDITORÍA
• Seguridad lógica y física
• Suministro y soporte
• Asegurar la seguridad de los sistemas

PREGUNTA
• Se tiene un procedimiento formal de seguimiento al desempeño del personal informático, Indique si dicho procedimiento contempla los siguientes puntos o Parámetros de medición por puesto o Parámetros de medición por función o Objetivos y alcances de cada puesto o Resultados esperados de cada puesto o Tiempo esperado para la ejecución de cada función o Responsables de dar seguimiento a cada puesto o Encuestas a usuarios al final de cada proyecto
TIPO DE AUDITORÍA
• Parámetros de medición
• Planeación y organización

• Administrar los recursos humanos

PREGUNTA
• Existen fechas predefinidas para la aplicación de parámetros de medición durante el desarrollo de cada proyecto
TIPO DE AUDITORÍA
• Parámetros de medición
• Monitoreo
• Monitorear las operaciones

PREGUNTA
• Las funciones de controlar y ejecutar están divididas
TIPO DE AUDITORÍA
• Parámetros de medición
• Monitoreo
• Evaluar la suficiencia del control interno

PREGUNTA
• El personal informático participa del proceso de evaluación o solo se le notifica de los resultados
TIPO DE AUDITORÍA
• Parámetros de medición
• Monitoreo
• Evaluar la suficiencia del control interno

PREGUNTA
• Existe un análisis costo beneficio de la función informática
TIPO DE AUDITORÍA
• Parámetros de medición
• Planeación y organización
• Administrar la inversión de TI

PREGUNTA
• La dirección considera que el apoyo informático es pobre. Porque
TIPO DE AUDITORÍA

• Parámetros de medición
DOMINIO
• Monitoreo
• Monitorear las operaciones

PREGUNTA
• Desde su punto de vista hay descontento en la organización por los servicios que brinda informática
TIPO DE AUDITORÍA
• Parámetros de medición
• Monitoreo
• Monitorear las operaciones

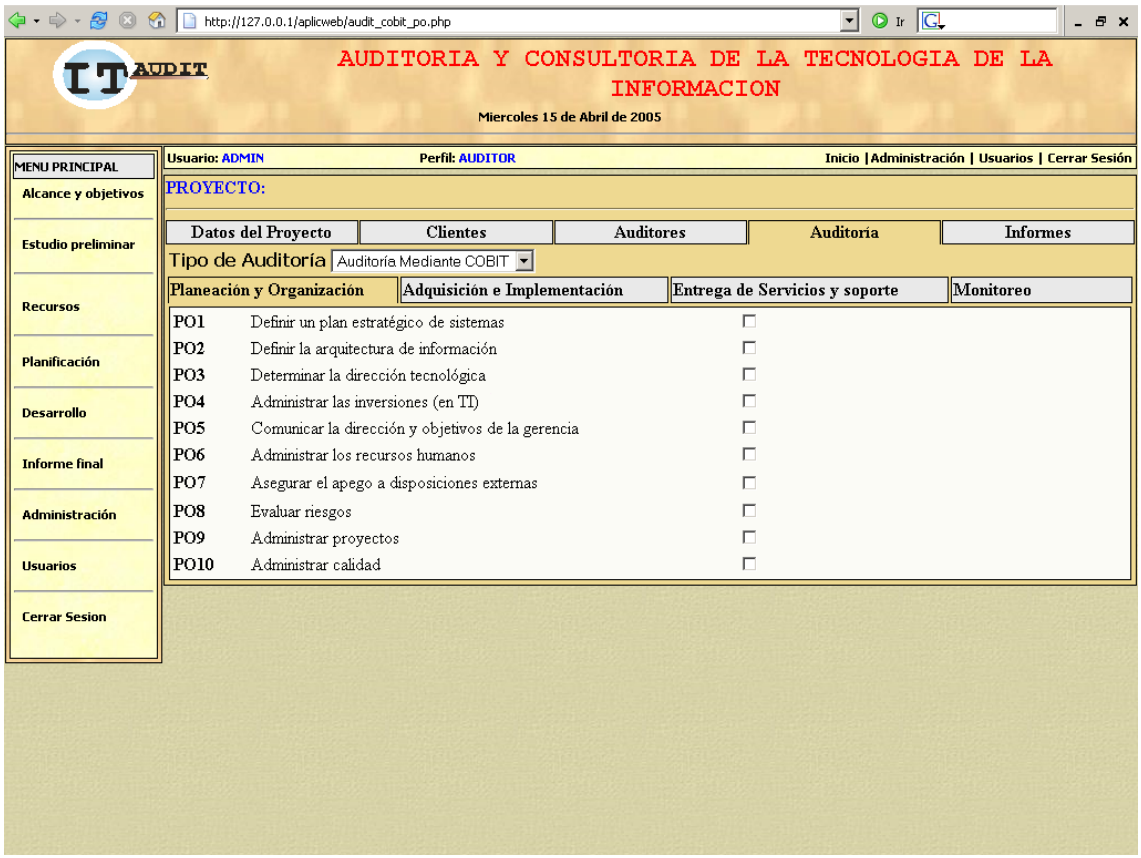
PREGUNTA
• La función informática ha difundido los servicios y productos que ofrece a los usuarios
TIPO DE AUDITORÍA
• Parámetros de medición
• Monitoreo
• Monitorear las operaciones

Anexo 5

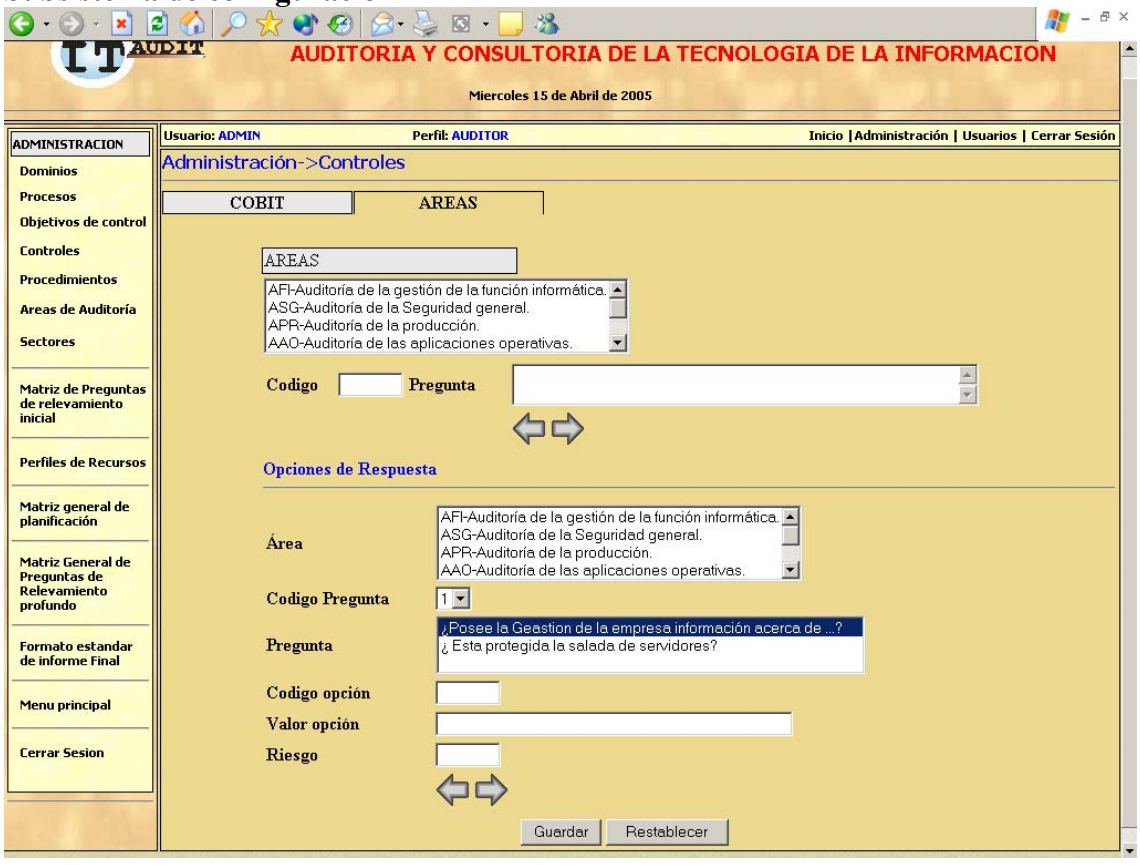
Interfaces

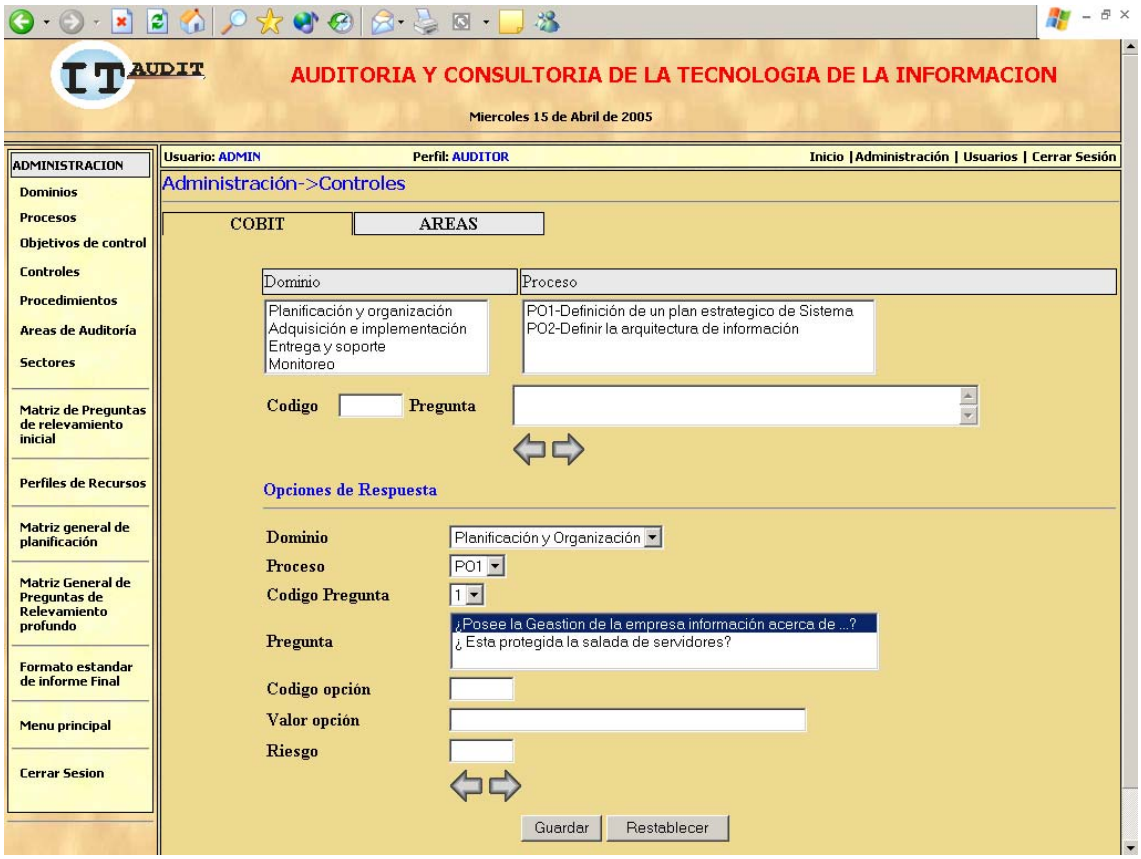
Subsistema de inicio

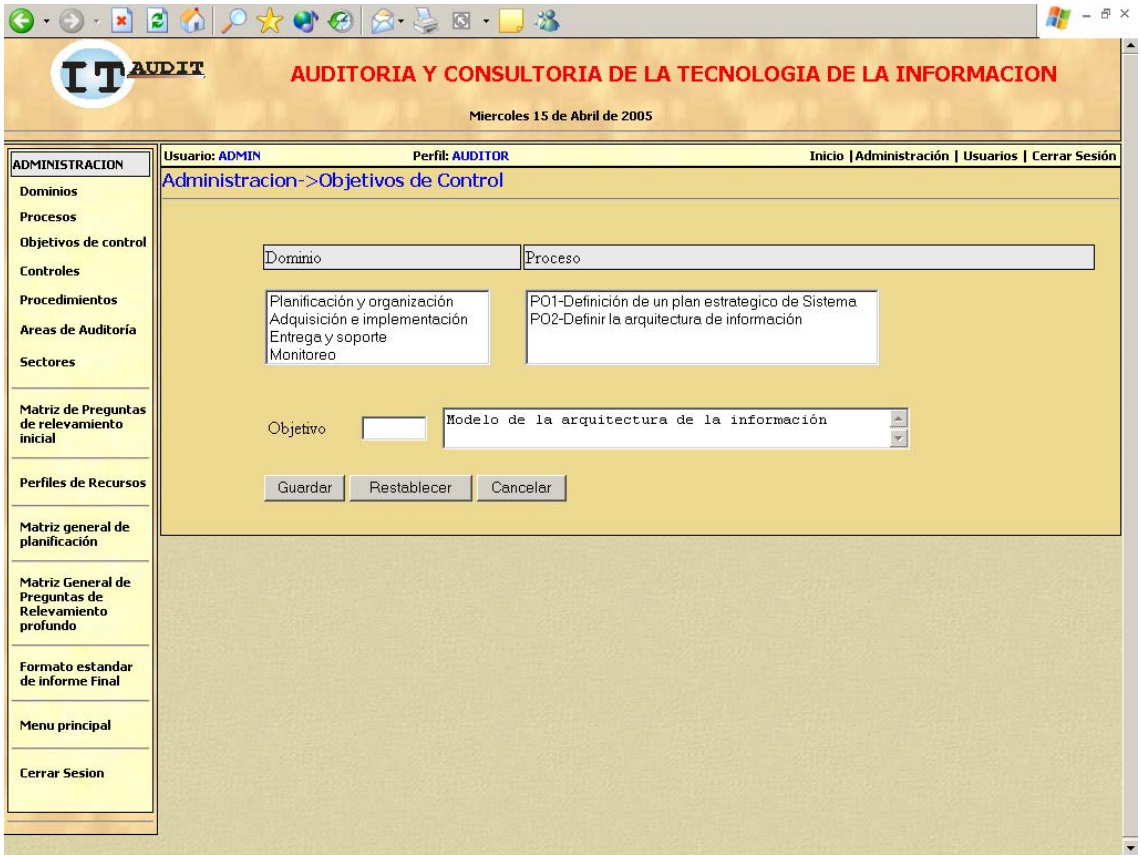

http://127.0.0.1/aplicweb/personal.php
AUDITORIA Y CONSULTORIA DE LA TECNOLOGIA DE LA INFORMACION
Miercoles 15 de Abril de 2005
MENU PRINCIPAL
Alcance y objetivos
Estudio preliminar
Recursos
Planificación
Desarrollo
Informe final
Administración
Usuarios
Cerrar Sesion
Usuario: ADMIN
Perfil: AUDITOR
Inicio | Administración | Usuarios | Cerrar Sesión
PROYECTO:
Datos del Proyecto
Clientes
Auditores
Auditoría
Informes
Nombre
Apellido
Título
Direccion
Cargo
Categoría
Seleccione
Especialidad
Especialista en Cobit
Especialista en seguridad
Especialista en Gestión de Sistemas
Telefono
Correo electrónico
Guardar
Restablecer
Cancelar
Busqueda
Seleccionar Criterio
Buscar
Auditores Existentes
Codigo
Nombre y apellido
Cargo
Email
Primero | Anterior | Siguiente | Último

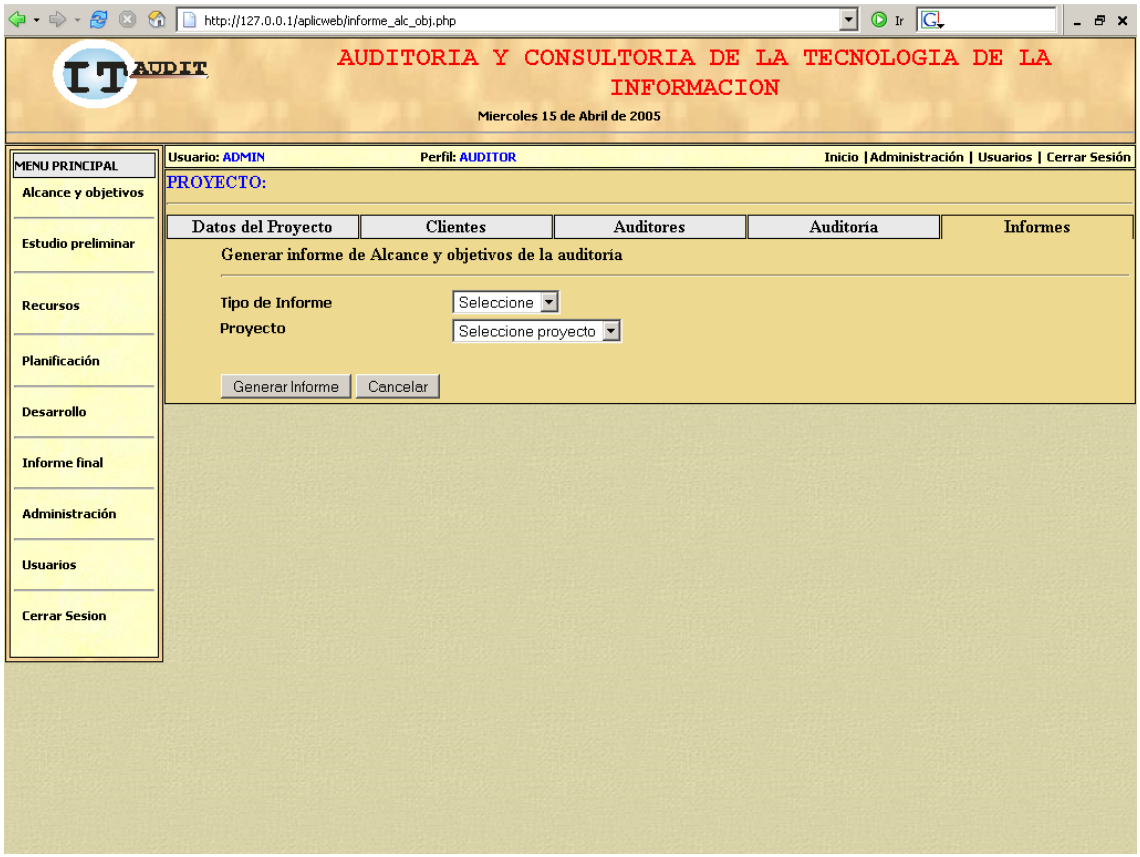

http://127.0.0.1/aplicweb/audit_cobit_po.php
AUDITORIA Y CONSULTORIA DE LA TECNOLOGIA DE LA INFORMACION
Miercoles 15 de Abril de 2005
MENU PRINCIPAL
Alcance y objetivos
Estudio preliminar
Recursos
Planificación
Desarrollo
Informe final
Administración
Usuarios
Cerrar Sesion
Usuario: ADMIN
Perfil: AUDITOR
Inicio | Administración | Usuarios | Cerrar Sesión
PROYECTO:
Datos del Proyecto
Clientes
Auditores
Auditoría
Informes
Tipo de Auditoría
Auditoría Mediante COBIT
Planeación y Organización
Adquisición e Implementación
Entrega de Servicios y soporte
Monitoreo
PO1 Definir un plan estratégico de sistemas
PO2 Definir la arquitectura de información
PO3 Determinar la dirección tecnológica
PO4 Administrar las inversiones (en TI)
PO5 Comunicar la dirección y objetivos de la gerencia
PO6 Administrar los recursos humanos
PO7 Asegurar el apego a disposiciones externas
PO8 Evaluar riesgos
PO9 Administrar proyectos
PO10 Administrar calidad

Subsistema de configuración

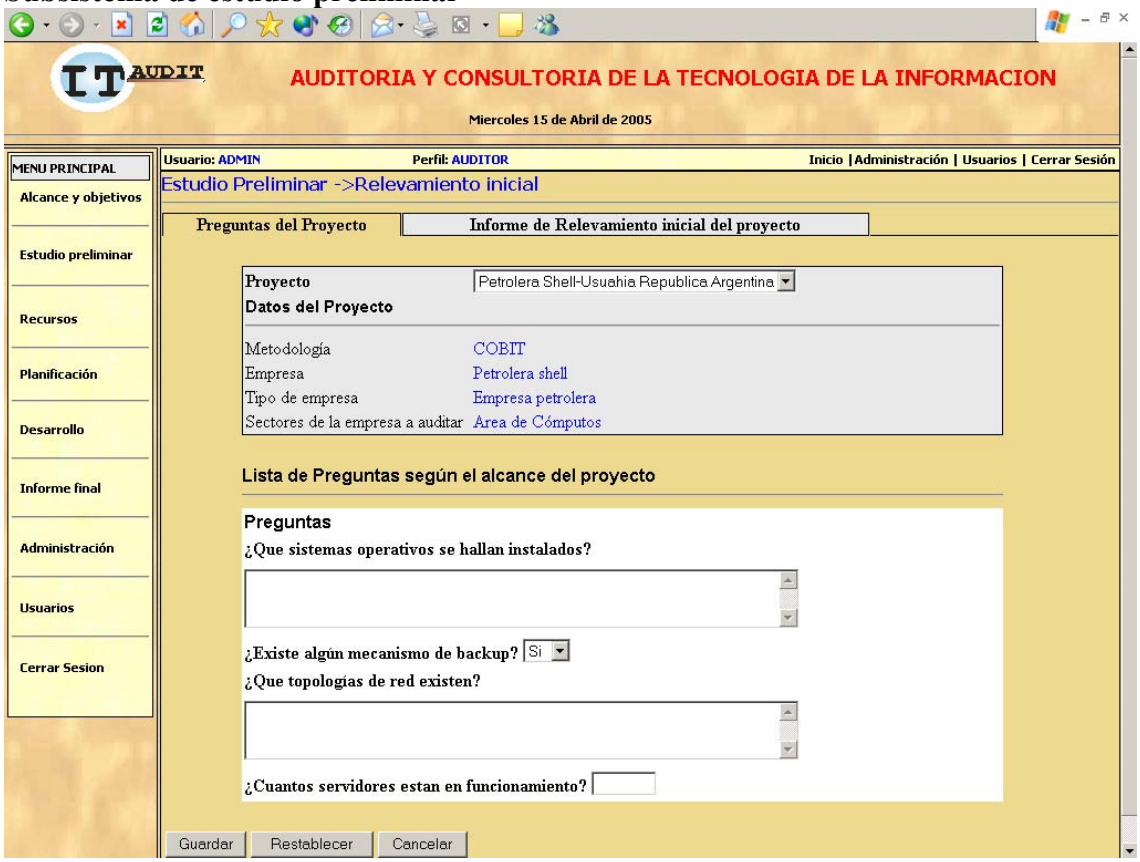



AUDITORIA Y CONSULTORIA DE LA TECNOLOGIA DE LA INFORMACION
Miercoles 15 de Abril de 2005
ADMINISTRACION
Dominios
Procesos
Objetivos de control
Controles
Procedimientos
Areas de Auditoría
Sectores
Matriz de Preguntas de relevamiento inicial
Perfiles de Recursos
Matriz general de planificación
Matriz General de Preguntas de Relevamiento profundo
Formato estandar de informe Final
Menu principal
Cerrar Sesion
Usuario: ADMIN
Perfil: AUDITOR
Inicio | Administración | Usuarios | Cerrar Sesión
Administración->Controles
COBIT
AREAS
Dominio
Proceso
Planificación y organización
Adquisición e implementación
Entrega y soporte
Monitoreo
PO1-Definición de un plan estrategico de Sistema
PO2-Definir la arquitectura de información
Codigo
Pregunta
Opciones de Respuesta
Dominio
Planificación y Organización
Proceso
PO1
Codigo Pregunta
1
Pregunta
¿Posee la Geastion de la empresa información acerca de ...?
¿ Esta protegida la salada de servidores?
Codigo opción
Valor opción
Riesgo
Guardar
Restablecer


AUDITORIA Y CONSULTORIA DE LA TECNOLOGIA DE LA INFORMACION
Miercoles 15 de Abril de 2005
ADMINISTRACION
Dominios
Procesos
Objetivos de control
Controles
Procedimientos
Areas de Auditoría
Sectores
Matriz de Preguntas de relevamiento inicial
Perfiles de Recursos
Matriz general de planificación
Matriz General de Preguntas de Relevamiento profundo
Formato estandar de informe Final
Menu principal
Cerrar Sesion
Usuario: ADMIN
Perfil: AUDITOR
Inicio | Administración | Usuarios | Cerrar Sesión
Administracion->Objetivos de Control
Dominio
Proceso
Planificación y organización
Adquisición e implementación
Entrega y soporte
Monitoreo
PO1-Definición de un plan estrategico de Sistema
PO2-Definir la arquitectura de información
Objetivo
Modelo de la arquitectura de la información
Guardar
Restablecer
Cancelar



Subsistema de estudio preliminar



Subsistema de recursos:

Subsistema de planificación

Subsistema de inicio