TESIS DE MAGISTER

ANÁLISIS DE EVENTOS DE SEGURIDAD EN SERVIDORES, USANDO TÉCNICAS DE MINERÍA DE DATOS

Tesista: Lic. Javier Crosa

Directores: M.Ing. María Alejandra Ochoa

Dr. Ramón García-Martínez

2008

ÍNDICE DE CONTENIDO

ÍNDICE DE CONTENIDO 2

ÍNDICE DE TABLAS 6

ÍNDICE DE FIGURAS 11

1 INTRODUCCIÓN 17

1.1 Algunas Consideraciones 17

1.2 Estructura del Documento 18

2 ESTADO DE LA CUESTIÓN 19

2.1 Estado de la Tecnología Actual 19

2.2 Discusión 24

3 PROBLEMA 27

3.1 Objetivo de la Tesis 27

3.2 Descripción del Problema 27

3.2.1 Definición de Conceptos 27

3.2.2 El Problema 28

4 SOLUCIÓN 30

4.1 Proyecto de Explotación de Información (Crisp-DM) 30

4.1.1 Entendimiento del Negocio 30

4.1.1.1 Objetivos del negocio 30

4.1.1.1.1 Escenario Actual 30

4.1.1.1.2 Objetivos del negocio 35

4.1.1.1.3 Factores Críticos de Éxito 36

4.1.1.2 Evaluar la situación 36

4.1.1.2.1 Inventario de Recursos 36

4.1.1.2.2 Requisitos, Supuestos y Requerimientos 37

4.1.1.2.3 Riesgos y Contingencias 38

4.1.1.2.4 Terminologías 38

4.1.1.2.5 Glosario 39
4.1.1.2.6 Costos y Beneficios 46
4.1.1.3 Determinar Objetivos del Proceso de Exploración de Información 47
4.1.1.3.1 Objetivos del Proceso de Exploración de Información 47
4.1.1.3.2 Criterios de Éxito del Proceso de Exploración de Información 48
4.1.1.4 Realizar el Plan del Proyecto 48
4.1.1.4.1 Plan de Proyecto 48
4.1.1.4.2 Validación Inicial de Técnicas y Herramientas 49
4.1.2 Entendimiento de los Datos 50
4.1.2.1 Recolectar los Datos Iniciales 50
4.1.2.2 Descripción de los Datos 50
4.1.2.3 Exploración de los Datos 51
4.1.2.3.1 Hipótesis 51
4.1.2.4 Verificación de la Calidad de los Datos 52
4.1.3 Preparación de los datos 53
4.1.3.1 Seleccionar los datos 53
4.1.3.2 Limpiar los datos 55
4.1.3.3 Construcción de datos 55
4.1.3.4 Integrar los datos 57
4.1.3.5 Formato de los datos 58
4.1.4 Modelado 58
4.1.4.1 Seleccionar la Técnica de Modelado 58
4.1.4.1.1 Técnicas de Modelado 58
4.1.4.1.2 Supuestos de Modelado 58
4.1.4.2 Generar Diseño de Pruebas 59
4.1.4.3 Construir el Modelo 60
4.1.4.3.1 Parámetros de las Herramientas 60
4.1.4.3.2 Modelos Obtenidos 65
4.1.4.4 Evaluar el Modelo 71
4.1.4.4.1 Análisis de los Modelos 71
4.1.5 Evaluación 73
4.1.5.1 Evaluar el modelo 73
4.1.5.1.1 Red Neuronal de Mapas Autoorganizados 73
4.1.5.1.2 Árbol de Decisión con Algoritmo de Inducción C4.5 74
4.1.5.2 Proceso de revisión 75
4.1.5.3 Determinar los próximos pasos 77
4.1.6 Implementación 78

4.1.6.1 Plan de Implementación 78
4.1.6.2 Plan de Monitoreo y Mantenimiento 78
4.1.6.3 Armando del Informe Final 80
4.1.6.4 Revisión del Proyecto 81
4.2 Desarrollo de la Solución (Métrica III) 82
4.2.1 Planificación de Sistemas de Información (PSI) 83
4.2.1.1 Documento Entregable 83
4.2.1.2 Control de Actividades 96
4.2.2 Desarrollo de Sistemas de Información 98
4.2.2.1 Estudio de Viabilidad del Sistema (EVS) 98
4.2.2.1.1 Documento Entregable 98
4.2.2.1.2 Control de Actividades 104
4.2.2.2 Análisis del Sistema de Información (ASI) 105
4.2.2.2.1 Documento Entregable 105
4.2.2.2.2 Control de Actividades 140
4.2.2.3 Diseño del Sistema de Información (DSI) 142
4.2.2.3.1 Documento Entregable 142
4.2.2.3.2 Control de Actividades 172
4.2.2.4 Construcción del Sistema de Información (CSI) 175
4.2.2.4.1 Documento Entregable 175
4.2.2.4.2 Control de Actividades 185
4.2.2.5 Implantación y Aceptación del Sistema (IAS) 187
4.2.2.5.1 Documento Entregable 187
4.2.2.5.2 Control de Actividades 194
4.2.2.6 Mantenimiento de Sistema de Información (MSI) 196
4.2.2.6.1 Documento Entregable 196
4.2.2.6.2 Control de Actividades 202
4.2.3 Aseguramiento de la Calidad 203
4.2.3.1 Documento Entregable 203
4.2.3.2 Control de Actividades 207
4.2.4 Interfaz de Seguridad 210
4.2.4.1 Documento Entregable 210
4.2.4.2 Control de Actividades 214
4.2.5 Gestión del Proyecto 218
4.2.5.1 Documento Entregable 218
4.2.5.2 Control de Actividades 226
4.2.6 Gestión de la Configuración 229

4.2.6.1 Documento Entregable 229
4.2.6.2 Control de Actividades 236

5 ESTUDIO DE CASOS 237

5.1 Producción de las Reglas de Decisión 237
5.2 Caso 1 245
5.3 Caso 2 252
5.4 Caso 3 259
5.5 Caso 4 264
5.6 Conclusiones del Estudio de Casos 269

6 CONCLUSIONES 274

6.1 Aportes 274
6.2 Futuras líneas de investigación 275

7 ANEXO 277

7.1 Las redes neuronales 277
7.2 Árboles de Decisión 278
7.2.1 Transformación a Reglas de Decisión 278
7.3 Sistema de desarrollo Kappa-PC 279
7.3.1 Razonamiento Basado en Reglas versus Programación Convencional 279
7.3.2 ¿Cuando deben Usarse las Reglas? 280

8 REFERENCIAS 281

ÍNDICE DE TABLAS

Tabla 2-1. Ejemplo 1 Precio Producto de Mercado. 21

Tabla 2-2. Ejemplo 2 Precio Producto de Mercado. 24

Tabla 4-1. Riegos y Contingencias. 38

Tabla 4-2. Acrónimos y Abreviaturas. 39

Tabla 4-3. Costos de la Estimación de Datos. 46

Tabla 4-4. Costos de Desarrollo y Ejecución de la Solución. 47

Tabla 4-5. Costos de Operación y Mantenimiento. 47

Tabla 4-6. Plan de Proyecto. 49

Tabla 4-7. Descripción de Datos. 51

Tabla 4-8. Campos de Datos. 53

Tabla 4-9. Ejemplo de Información de Campos de Datos. 54

Tabla 4-10. Ejemplo Datos sin Transformar. 56

Tabla 4-11. Ejemplo Datos Transformados. 56

Tabla 4-12. Información de Regla. 70

Tabla 4-13. Control de Actividades PSI. 97

Tabla 4-14. Control de Actividades EVS. 104

Tabla 4-15. Estimación de horas del plan. 109

Tabla 4-16. Especificación de Caso de Uso RF1, Ingreso al Sistema. 114

Tabla 4-17. Especificación de Caso de Uso RF2, Crear Usuario. 115

Tabla 4-18. Especificación de Caso de Uso RF3, Cambio de Contraseña. 115

Tabla 4-19. Especificación de Caso de Uso RF4, Consulta de Reportes. 116

Tabla 4-20. Especificación de Caso de Uso RF5, Consulta Estadísticas Históricas. 116

Tabla 4-21. Especificación de Caso de Uso RF6, Configurar Vistas y Reportes. 117
Tabla 4-22. Especificación de Caso de Uso RF7, Selección Archivo de Entrada. 117
Tabla 4-23. Especificación de Caso de Uso RF8, Selección Archivos de Salida. 118
Tabla 4-24. Especificación de Caso de Uso RF9, Análisis de Registros. 119
Tabla 4-25. Especificación de Caso de Uso RF10, Visualizar Monitor Registro en Proceso. 120
Tabla 4-26. Especificación de Caso de Uso RF11, Visualizar Monitor Cantidad de Observaciones Procesadas. 120
Tabla 4-27. Especificación de Caso de Uso RF12, Visualizar Gráfico de Secciones. 121
Tabla 4-28. Especificación de Caso de Uso RF13, Visualizar Estadísticas de Reglas. 121
Tabla 4-29. Especificación de Caso de Uso RF14, Visualizar Estadísticas de Usuario. 122
Tabla 4-30. Especificación de Caso de Uso RF15, Visualizar Reportes. 123
Tabla 4-31. Especificación de Caso de Uso RF16, Salir del Sistema. 123
Tabla 4-32. Modelo de Clases. 124
Tabla 4-33. Descripción de Clases. 131
Tabla 4-34. Diseño de Interfaz de Pantalla. 133
Tabla 4-35. Análisis de Consistencia de los Modelos de la Fase de Análisis. 138
Tabla 4-36. Modelo para Registro de Casos de Pruebas. 139
Tabla 4-37. Control de Actividades ASI. 141

Tabla 4-38. Catálogo de Excepciones. 146

Tabla 4-39. Diseño de los casos de Uso. 150

Tabla 4-40. Información de la clase de interfaz. 158

Tabla 4-41. Descripción de los Atributos de las clases. 159

Tabla 4-42. Descripción de los métodos de las clases. 160

Tabla 4-43. Diseño Caso 1 de Prueba Unitaria. 167

Tabla 4-44. Diseño Caso 2 de Prueba Unitaria. 168

Tabla 4-45. Diseño Caso 3 de Prueba Unitaria. 168

Tabla 4-46. Diseño Caso 1 de Prueba de Integración. 169

Tabla 4-47. Diseño Caso 2 de Prueba de Integración. 169

Tabla 4-48. Diseño Caso 1 de Prueba de Sistema. 169

Tabla 4-49. Diseño Caso 1 de Prueba de Implantación. 170

Tabla 4-50. Diseño Caso 1 de Prueba de Aceptación. 170

Tabla 4-51. Control de Actividades DSI. 174

Tabla 4-52. Ejecución Caso 1 de Prueba Unitaria. 177

Tabla 4-53. Ejecución Caso 2 de Prueba Unitaria. 178

Tabla 4-54. Ejecución Caso 3 de Prueba Unitaria. 178

Tabla 4-55. Resultados de Ejecución de Pruebas Unitarias. 178

Tabla 4-56. Ejecución Caso 1 de Prueba de Integración. 179

Tabla 4-57. Ejecución Caso 2 de Prueba de Integración. 179

Tabla 4-58. Ejecución Caso 2 de Prueba de Integración. 179

Tabla 4-59. Resultados de Ejecución de Pruebas de Integración. 180

Tabla 4-60. Ejecución Caso 1 de Prueba de Sistema. 181

Tabla 4-61. Resultados de Ejecución de Pruebas de Sistema. 181

Tabla 4-62. Control de Actividades CSI. 186

Tabla 4-63. Caso 1 de Prueba de Aceptación 189

Tabla 4-64. Caso 1 de Prueba de Aceptación 189

Tabla 4-65. Ejecución Caso 1 de Prueba de Aceptación 191

Tabla 4-66. Resultados de Ejecución de Pruebas. 191

Tabla 4-67. Ejecución Caso 1 de Prueba de Aceptación 191

Tabla 4-68. Resultados de Ejecución de Pruebas. 192

Tabla 4-69. Control de Actividades IAS. 195

Tabla 4-70. Registro estadístico de la petición. 201

Tabla 4-71. Control de Actividades MSI. 202

Tabla 4-72. Aseguramiento de Calidad. Análisis del Sistema. 205

Tabla 4-73. Aseguramiento de Calidad. Diseño del Sistema..... 205

Tabla 4-74. Aseguramiento de Calidad. Construcción del Sistema. 205

Tabla 4-75. Aseguramiento de Calidad. Implantación del Sistema. 206

Tabla 4-76. Control de Actividades Aseguramiento de la Calidad. 209

Tabla 4-77. Interfaz de Seguridad. 217

Tabla 4-78. Gestión de Proyectos. Catalogo de Clases. 220

Tabla 4-79. Gestión de Proyectos. Estimación de Esfuerzo. 221

Tabla 4-80. Gestión del Proyecto. Hitos 223

Tabla 4-81. Gestión del Proyecto. Impacto sobre incidencias. 224

Tabla 4-82. Gestión del Proyecto. Informe de Seguimiento. 225

Tabla 4-83. Gestión de Proyectos. Esfuerzo Real Insumido. 225

Tabla 4-84. Control de Actividades Gestión del Proyecto. 228

Tabla 4-85. Elementos de Configuración. 231

Tabla 4-86. Identificación y Registro de Cambios de Productos. 235

Tabla 4-87. Control de Actividades Gestión de la Configuración..... 236

Tabla 5-1. Codificación de eventos. 239

Tabla 5-2. Codificación de Usuarios. 240

Tabla 5-3. Codificación de Días y Horarios. 240

Tabla 5-4. Distribución de las observaciones en los clusters. 241

Tabla 5-5. Clasificación de los Cluster generados por SOM. 242

Tabla 5-6. Reglas de Decisión. 244

Tabla 5-7. Caso de Estudio 1: Operaciones que pueden realizar los administradores de redes. 250

Tabla 5-8. Análisis de Error de las Reglas de Decisión. 273

ÍNDICE DE FIGURAS

Figura 4-1. Organigrama del sector en estudio. 31

Figura 4-2. Eventos de un servidor..... 50

Figura 4-3. Propiedades de un Evento vista en el servidor. 54

Figura 4-4. Ventana de Configuración de la Red Neuronal. 61

Figura 4-5. Ventana de Configuración del Árbol de Decisión. 65

Figura 4-6. Distribución de las observaciones en los Clusters. 65

Figura 4-7. Información estadística de cada Cluster. 65

Figura 4-8. Gráfico de tipo radar..... 66

Figura 4-9. Información estadística de cada Regla de Decisión..... 69

Figura 4-10. Modelo de Información..... 89

Figura 4-11. Nuevo modelo del sistema de información..... 91

Figura 4-12. Módulos del Sistema Software a Desarrollar. 102

Figura 4-13. Caso de Uso RF1. Ingreso al Sistema. 110

Figura 4-14. Caso de Uso RF2. Crear Usuario..... 110

Figura 4-15. Caso de Uso RF3. Cambio de Contraseña. 110

Figura 4-16. Caso de Uso RF4. Consulta de Reportes. 110

Figura 4-17. Caso de Uso RF5. Consulta de Estadísticas Históricas..... 111

Figura 4-18. Caso de Uso RF6. Configurar Vistas y Reportes. 111

Figura 4-19. Caso de Uso RF7. Selección Archivo de Entrada. 111

Figura 4-20. Caso de Uso RF8. Selección Archivos de Salida..... 111

Figura 4-21. Caso de Uso RF9. Análisis de Registros. 112

Figura 4-22. Caso de Uso RF10. Visualizar Monitor Registro en Proceso. 112

Figura 4-23. Caso de Uso RF11. Visualizar Monitor Cantidad de Observaciones Procesadas..... 112

Figura 4-24. Caso de Uso RF12. Visualizar Gráfico de Secciones. 112

Figura 4-25. Caso de Uso RF13. Visualizar Estadísticas de Reglas. 113

Figura 4-26. Caso de Uso RF14. Visualizar Estadísticas de Usuario. 113

Figura 4-27. Caso de Uso RF15. Visualizar Reportes. 113

Figura 4-28. Caso de Uso RF16. Salir del Sistema. 113

Figura 4-29. Diagrama de Secuencia RF1. Ingreso al Sistema. 125

Figura 4-30. Diagrama de Secuencia RF2. Crear Usuario. 125

Figura 4-31. Diagrama de Secuencia RF3. Cambio de Contraseña. 125

Figura 4-32. Diagrama de Secuencia RF4. Consulta de Reportes. 126

Figura 4-33. Diagrama de Secuencia RF5. Consulta de Estadísticas Históricas. 126

Figura 4-34. Diagrama de Secuencia RF6. Configurar Vistas y Reportes. 126

Figura 4-35. Diagrama de Secuencia RF7. Selección Archivo de Entrada. ... 127

Figura 4-36. Diagrama de Secuencia RF8. Selección Archivos de Salida. 127

Figura 4-37. Diagrama de Secuencia RF9. Análisis de Registros. 127

Figura 4-38. Diagrama de Secuencia RF10. Visualizar Monitor Registro en Proceso. 128

Figura 4-39. Diagrama de Secuencia RF11. Visualizar Monitor Cantidad de Observaciones Procesadas. 128

Figura 4-40. Diagrama de Secuencia RF12. Visualizar Gráfico de Secciones. 128

Figura 4-41. Diagrama de Secuencia RF13. Visualizar Estadísticas de Reglas. 129

Figura 4-42. Diagrama de Secuencia RF14. Visualizar Estadísticas de Usuario. 129

Figura 4-43. Diagrama de Secuencia RF15. Visualizar Reportes. 129

Figura 4-44. Diagrama de Secuencia RF16. Salir del Sistema..... 130

Figura 4-45. Modelo Interfaz de Pantalla..... 134

Figura 4-46. Descomposición física del sistema..... 143

Figura 4-47. Ventana de Bienvenida al Sistema..... 151

Figura 4-48. Ventana de Ingreso al Sistema. 151

Figura 4-49. Ventana del Módulo de Inicio. 152

Figura 4-50. Ventana de Configuración de Vistas y Reportes. 152

Figura 4-51. Ventana del Módulo de Análisis de Eventos. 153

Figura 4-52. Ventana de Evento en Análisis..... 153

Figura 4-53. Ventana del Módulo de Estadísticas. 154

Figura 4-54. Ventana del Gráfico de Secciones. 154

Figura 4-55. Ventana de Información de Reglas. 155

Figura 4-56. Ventana de Información de Usuarios. 155

Figura 4-57. Ventana del Informe de Salida. 156

Figura 4-58. Ventana del Módulo de Estadísticas Históricas. 156

Figura 4-59. Ventana del Módulo de Seguridad. 157

Figura 4-60. Formato de Impresión de un Archivo de Salida. 157

Figura 4-61. Arquitectura de Módulos del sistema. 162

Figura 4-62. Asignación de subsistemas de construcción a nodos. 165

Figura 4-63. Representación de los componentes de construcción. 165

Figura 4-64. Componentes del subsistema de construcción Seguridad y Control de Acceso..... 166

Figura 4-65. Componentes del subsistema de construcción Análisis de Sucesos..... 166

Figura 4-66. Componentes del subsistema de construcción Gestor de Datos. 166

Figura 4-67. Componentes del subsistema de construcción Generador de Reportes. 166

Figura 5-1. Archivo exportado del Visor de Eventos de Seguridad. 238

Figura 5-2. Eliminación de registros irrelevantes. 238

Figura 5-3. Eliminación de atributos irrelevantes. 239

Figura 5-4. Extracto del Archivo de entrada de la red neuronal con los Eventos Normalizados. 240

Figura 5-5. Clasificación de cada Observación. 242

Figura 5-6. Configuración de las reglas de decisión en Kappa-PC. 245

Figura 5-7. Caso de Estudio 1: Archivo de entrada con los datos a procesar. 246

Figura 5-8. Caso de Estudio 1: Selección del Archivo de entrada. 246

Figura 5-9. Caso de Estudio 1: Cantidad de Observaciones Analizadas por tipo. 247

Figura 5-10. Caso de Estudio 1: Gráfico de Secciones. 247

Figura 5-11. Caso de Estudio 1: Información de Observaciones Analizadas por Usuario y Tipo. 248

Figura 5-12. Caso de Estudio 1: Archivo de Salida de Observaciones Analizadas. 248

Figura 5-13. Caso de Estudio 1: Extracto del archivo de Salida de Observaciones Rojas. 251

Figura 5-14. Caso de Estudio 2: Archivo de entrada con los datos a procesar. 253

Figura 5-15. Caso de Estudio 2: Selección del Archivo de entrada. 253

Figura 5-16. Caso de Estudio 2: Cantidad de Observaciones Analizadas por tipo. 254
Figura 5-17. Caso de Estudio 2: Gráfico de Secciones. 254
Figura 5-18. Caso de Estudio 2: Información de Observaciones Analizadas por Usuario y Tipo. 255
Figura 5-19. Caso de Estudio 2: Archivo de Salida de Observaciones Analizadas. 255
Figura 5-20. Caso de Estudio 2: Extracto del archivo de Salida de Observaciones Rojas. 256
Figura 5-21. Caso de Estudio 2: Extracto del archivo de Salida de Observaciones Amarillas. 257
Figura 5-22. Caso de Estudio 2: Extracto del archivo de Salida de Observaciones Verdes. 258
Figura 5-23. Caso de Estudio 3: Archivo de entrada con los datos a procesar. 259
Figura 5-24. Caso de Estudio 3: Selección del Archivo de entrada. 260
Figura 5-25. Caso de Estudio 3: Cantidad de Observaciones Analizadas por tipo. 260
Figura 5-26. Caso de Estudio 3: Archivo de Salida de Observaciones Analizadas. 261
Figura 5-27. Caso de Estudio 3: Extracto del archivo de Salida de Observaciones Rojas. 262
Figura 5-28. Caso de Estudio 3: Extracto del archivo de Salida de Observaciones Amarillas. 262

Figura 5-29. Caso de Estudio 3: Extracto del archivo de Salida de Observaciones Verdes. 264

Figura 5-30. Caso de Estudio 4: Archivo de entrada con los datos a procesar. 265

Figura 5-31. Caso de Estudio 4: Selección del Archivo de entrada. 265

Figura 5-32. Caso de Estudio 4: Cantidad de Observaciones Analizadas por tipo. 266

Figura 5-33. Caso de Estudio 4: Gráfico de Secciones. 266

Figura 5-34. Caso de Estudio 4: Archivo de Salida de Observaciones Analizadas. 267

Figura 5-35. Caso de Estudio 4: Extracto del archivo de Salida de Observaciones Rojas. 268

Figura 5-36. Caso de Estudio 4: Extracto del archivo de Salida de Observaciones Amarillas. 268

Figura 5-37. Caso de Estudio 4: Extracto del archivo de Salida de Observaciones Verdes. 269

Figura 7-1. Esquema de una Red Neuronal. 277

1 INTRODUCCIÓN

1.1 Algunas Consideraciones

La administración de los eventos de servidores – monitoreo, recolección, consolidación y análisis de los archivos de sucesos – se ha convertido en una necesaria y creciente preocupación para los profesionales de seguridad de redes y los administradores de las Tecnologías de Información.

En los archivos de sucesos siempre se registran los problemas con suficiente anterioridad a la falla total de los sistemas. Ellos mantienen potencial y valiosa evidencia forense. Ante la presencia de una anomalía y/o problema en un sistema de información, los archivos de eventos poseen toda la información de las razones del mismo, cómo, cuando sucedió y finalmente la llave para prevenir futuros.

Toda red de datos empresarial, posee múltiples servidores en ejecución, con distintos tipos de archivos de sucesos, cada máquina genera una elevada cantidad de información de eventos. De hecho, un único servidor Microsoft Windows, es capaz de generar varios gigabytes de datos de sucesos en un solo día. Multiplicando este número por la cantidad de equipos en la organización, luego por la cantidad de archivos de sucesos que deben ser almacenados, la tarea de mantenimiento de los mismos es inmanejable.

Adicionalmente, cuando un administrador investiga porqué ha ocurrido o está ocurriendo un problema, debe lidiar con miles de eventos sin importancia y sin relación, dilatando la resolución.

Afortunadamente en la actualidad, las empresas están descubriendo que la información contenida en los archivos de eventos puede usarse como soporte a las decisiones, ya sea de mejora, resolución de problemas, detección de tareas fraudulentas, anticipación a fallas, satisfacción de los acuerdos de niveles de servicios.

Las organizaciones que deben cumplir con determinadas regulaciones, por ejemplo Sarbanes-Oxley (SOX) del año 2002 [SOX, 2002], deben guardar evidencias de las tareas o acciones realizadas por los empleados. La mayoría de éstas se encuentran en los archivos de sucesos. Ante una auditoria será necesario recuperarlas y demostrar la legitimidad de las tareas realizadas.

1.2 Estructura del Documento

El formato de la tesis consta de seis Capítulos y un Anexo que se describen a continuación.

Capítulo "Introducción". Se brinda una descripción del problema y la importancia de resolverlo.

Capítulo "Problema". Se describe el Objetivo de la tesis y la Descripción del problema que se pretenden resolver.

Capítulo "Solución". Cubre todos los pasos que se siguen para aplicar la tecnología propuesta a la resolución del problema. El capítulo se divide en dos secciones. La primera se desarrolla según un Proyecto de Explotación de información, siguiendo la metodología Crisp-DM [Chapman *et al*, 2000]. La segunda consiste en el desarrollo del Sistema y se estructura según Métrica versión 3 [Métrica, 2008].

Capítulo "Estudio de casos". Consiste de una serie de casos de pruebas donde se ensayan experiencias de aplicación práctica del estudio realizado.

Capítulo "Conclusiones". Se plantean los aportes de la tesis y futuras líneas de trabajo e investigación.

Capítulo "Referencias". Se describe la bibliografía consultada durante la elaboración de la tesis.

Anexo A. Se detalla información técnica acerca de las técnicas y herramientas utilizadas.

2 ESTADO DE LA CUESTIÓN

2.1 Estado de la Tecnología Actual

Para realizar el análisis de sucesos de seguridad, se utiliza algún aplicativo para leer los eventos y almacenarlos en una base de datos o en su defecto, y menos deseable por su ineficiencia, en una planilla de cálculo. Luego personal del sector de Seguridad Informática, en forma manual, realiza consultas y búsquedas específicas.

El mercado ofrece herramientas donde se configuran reglas y acciones. Ante la detección de un evento específico, se puede activar una alerta que es enviada al personal de sistemas encargado de la aplicación. Esta metodología presenta el problema que requiere el conocimiento previo de los potenciales errores. Además es necesario programar las series de reglas que se aplicarán a los sucesos lo cual al término de un tiempo la cantidad de las mismas es tan grande que es muy complicado administrarlas y entender su lógica.

A continuación se detallan las características importantes de los productos más relevantes que se analizaron.

ManageEngine™ EventLog Analyzer [ManageEngine, 2007]

Es una solución de administración de archivos de eventos. No utiliza agentes en el servidor a analizar y tiene una interfase Web. Su funcionamiento consiste en recolectar, analizar, archivar y reportar archivos de sucesos de distintos dispositivos informáticos.

Consta de distintos módulos:

- Log Management: Recolecta, analiza, archiva y reporta acerca de eventos de sucesos de distintos dispositivos informáticos.
- Log Reporting: Realiza reportes bajo demanda y en tiempo real.
- Cumplimiento de Regulaciones: permite cumplir con los requerimientos de regulaciones tales como SOX, HIPAA, etc.
- Alertas y Tareas: Se pueden definir alertas para eventos específicos y programar la generación de reportes y enviarlos automáticamente por correo electrónico.

Cuando un evento de seguridad importante es generado en un dispositivo de la red, es mostrado instantáneamente sobre la consola del producto.

Se pueden definir reglas que activen alertas cuando son generados eventos específicos. Por ejemplo, se puede definir una alerta para notificar al administrador cuando un evento de error es generado en un servidor. Las alertas pueden ser enviadas por correo electrónico.

Los eventos archivados contienen información relevante para conocer el rendimiento de un sistema de información por eso la aplicación automáticamente archiva los eventos de cada dispositivo en un almacenamiento central y permite a los ingenieros de sistemas accederlos en cualquier momento.

El producto no requiere la instalación de ningún agente o software en los dispositivos de red. El software de recolección es parte del producto por lo tanto no se genera carga adicional en los equipos a controlar.

GFI EventsManager [GFI, 2007]

Centraliza los sucesos generados por distintos dispositivos de la red. Posee las siguientes características:

- Configuración por asistentes que simplifican la operación y mantenimiento del usuario final
- Escaneo de sucesos de hasta 6 millones por hora
- Reglas preconfiguradas de procesamiento de sucesos para una eficaz clasificación y administración de sucesos.
- Monitoreo y alertas automatizadas de la actividad de los sucesos
- Generación de informes para el monitoreo eficaz de la actividad de red y para un inmediato ROI.

El funcionamiento operativo se divide en 2 etapas:

Etapa 1: Recolección de eventos

Durante la fase de Recolección de Eventos, GFI EventsManager colecta los logs de las fuentes de evento específicas. Esto se logra a través del uso de 2 motores de colección de eventos: El Motor de Recuperación de Evento y el Motor Receptor de Evento.

El Motor de Recuperación de Evento: se usa para recolectar eventos a intervalos de tiempo específicos. Durante el proceso este motor realizará los siguientes:

- Se autenticará en la fuente de eventos
- Recolectará los eventos
- Enviará los eventos recolectados al servidor del producto
- Liberará la fuente de eventos

El Motor Receptor de Evento: escucha y colecciona eventos y mensajes de Sistema, enviados por las fuentes de eventos de Sistema que se encuentran en la red. Se reciben los mensajes directamente de la fuente del evento; por consiguiente no requiere autenticarse remotamente a las fuentes de eventos para la colección de los mismos. Adicionalmente, los eventos y mensajes de Sistema son reunidos en tiempo real y por consecuentemente ningún intervalo de tiempo de colección necesita ser configurado.

Etapa2: Procesamiento de eventos

Durante esta fase, el producto ejecutará un juego de reglas de procesamiento de Eventos contra los sucesos reunidos. Las reglas de procesamiento de Eventos son instrucciones que:

- Analizan los logs reunidos y los clasifican como Crítico, Alto, Medio, Bajo o Ruido (no deseado o eventos repetidos).
- Filtra eventos que se corresponden a condiciones específicas.
- Dispara correos electrónicos, SMS y alertas para los eventos importantes.
- Dispara acciones de remediación tal como la ejecución de scripts para los eventos importantes.
- Opcionalmente los eventos se pueden almacenar en bases de datos.

Precio (en dólares estadounidenses) para 5 nodos o servidores:

Descripción	Código	Monto
Precio	ESM5	$ 1125
Acuerdo de Mantenimiento de Software (Precio por año)	ESMMC	$ 225
Actualización de Versión	ESMVU5	$ 675
TOTAL		**$ 2025**

Tabla 2-1. Ejemplo 1 Precio Producto de Mercado.

Event Log Analyzer Pro [ELAP, 2007]

La fuente de los datos puede leerse de la computadora local o cualquier otra computadora visible a través de la red (la aplicación ofrece una lista de servidores disponibles).

Esta aplicación permite leer la descripción de los eventos, esta característica es optativa ya que genera lentitud en la lectura de los eventos.

El usuario puede configurar las opciones de lectura de los archivos, y así, acortar el tiempo de lectura. La selección puede hacerse por distintos criterios tales como tipo de evento, tiempo y/o Evento ID. Adicionalmente, los datos leídos desde el archivo de sucesos pueden ser filtrados por Tipo, Fecha, Tiempo, Fuente, Categoría, ID, Usuario y Computadora.

Los datos pueden desplegarse ordenados en base a índices predefinidos. Toda la información de configuración es guardada para usos posteriores.

Es Freeware.

Prism Microsystems,Inc. EventTracker [PRISM, 2007]

El software de EventTracker™ proporciona consolidación automática y desatendida de eventos, en un ambiente seguro y en tiempo real, de diversos dispositivos de Red.

Una consola central reúne el administrador de seguridad, el monitor de eventos y el motor de reportes. En tiempo real, los eventos (filtrados con reglas) de todos los sistemas son mostrados en una consola centralizada a través de vistas personalizas.

Consolidación de eventos:

- Soporta sistemas pertenecientes y no pertenecientes al dominio
- Soporta múltiples dispositivos informáticos
- Soporta una Arquitectura multicapa - vista por empresa, vista departamental, etc.
- Interfase de administración basada en Web.
- El único punto de colección puede recibir 30.000 eventos por minuto en tiempo real. Aunque soporta múltiples puntos de colección.
- Autenticación del usuario basada en roles.

- Almacena los eventos comprimidos.
- La arquitectura permite colectar eventos con o sin agente en los dispositivos.

Pueden configurarse en correlación, eventos de múltiples servidores para proporcionar mayor seguridad y capacidad de decisión.

Por ejemplo: Generar una condición de alerta cuando se reciben 100 fracasos del logon en cinco minutos en todos los servidores controladores del Dominio.

El módulo de Análisis de eventos, tiene la habilidad para buscar y examinar eventos dentro de la descripción de los mismos, basándose en un string simple o múltiple. Posee más de 500 reglas predefinidas para investigar las condiciones más comunes.

La instalación tanto del Producto principal como de los agentes en los servidores a monitorear es rápida y sencilla. Monitorea los eventos al instante luego de la instalación.

NetIQ Security Manager [NETIQ, 2007]

El producto entrega información de seguridad y de administración de eventos del entorno de red de cualquier organización y ambiente multi-plataforma. El producto detecta intrusión en tiempo real, posee administración de información de seguridad y correlación, análisis de incidentes, administración y archivado de logs, herramientas de tendencia, análisis forense y reportes de seguridad.

Presenta información de seguridad en tiempo real, que representa el verdadero estado de la seguridad de los dispositivos de la red, además diferencia los eventos reales de los de ruido y alarmas falsas, facilitando las búsquedas. Estas capacidades manejan el flujo de información en una infraestructura central que colecta, correlaciona y analiza los eventos.

El ruido y los falsos positivos son reducidos a través de un motor de correlación que minimiza la información irrelevante lo cual permite analizar y hacer foco en los incidentes reales. Un asistente de Correlación permite la creación de nuevas reglas que pueden crearse fácilmente y usarse inmediatamente.

Posee un modulo de seguimiento de problemas que permite a los administradores de Tecnología de la Información, monitorear y analizar los eventos de problemas.

El módulo administrador de archivos de sucesos, realiza los procesos de archivado y análisis. Ésto permite colectar, consolidad y archivar la información

de actividad de los dispositivos. Mantener esta información en forma correcta es fundamental para las organizaciones que se ven afectadas por reglamentaciones y leyes que requieren el uso de estos datos por tema legales.

De acuerdo a las consultas realizadas a una empresa que lo implementó, el producto presenta problemas en el funcionamiento, en la consola del producto los dispositivos usados aparecen como no disponibles en forma intermitente.

Precios expresados en Dólares Estadounidenses con un Año de Mantenimiento.

Producto	Precio
NetIQ SM v5.1 Console	$ 3.000,00
NetIQ SM Universal Adapter Bundle - for IIS	$ 480,00
NetIQ SM Universal Adapter Bundle	$ 480,00
NetIQ SM for Firewalls Bundle	$ 1.800,00
NetIQ SM for Network IDS Bundle	$ 1.800,00
NetIQ SM for Windows Bundle	$ 1.440,00
NetIQ SM for Unix Bundle	$ 1.440,00

Tabla 2-2. Ejemplo 2 Precio Producto de Mercado.

2.2 Discusión

Como se comentó anteriormente, el mercado ofrece una gran variedad de herramientas para la administración de los archivos de sucesos, algunas de ellas se describieron en la sección previa, pero las mismas no logran satisfacer integralmente las necesidades de las gerencias de Tecnología de la Información.

La operatoria principal de los productos comerciales analizados y relevados, consiste en el uso de condiciones y acciones. La aplicación lee y aplica a cada registro todas las condiciones que tiene configuradas. Cuando una determinada condición se cumple, entonces se activa la acción correspondiente.

Esta metodología presenta las siguientes desventajas:

- Requiere el conocimiento previo de los potenciales errores del sistema operativo o productos que generan los eventos, para construir las duplas condiciones / acciones.

- Ciertos productos poseen condiciones de procesamiento de sucesos preestablecidas. Éstas están organizadas en “Conjuntos de Condiciones”,

y cada conjunto puede contener una o más condiciones especializadas que pueden ser ejecutadas contra los registros recogidos. Los conjuntos de Condiciones están a su vez organizados en "Carpetas de Conjuntos de Condiciones".

Además la mencionada organización puede ser personalizada para ajustarse a los requerimientos de procesamiento de sucesos.

Evidentemente la administración de toda la estructura de "condiciones", "conjuntos de condiciones" y "carpetas de conjuntos de condiciones" puede convertirse en una tarea difícil, laboriosa e inmanejable.

- Se debe prestar atención y elegir la "condición" correcta para el trabajo. Los conjuntos de condiciones pre-configurados aplican para registros específicos, por lo tanto es imperativo que se elijan los conjuntos de condiciones que puedan procesar efectivamente los sucesos.

- Ciertos conjuntos de condiciones, contienen condiciones especializadas que son específicas del suceso. Por lo tanto esas condiciones solo serán efectivas cuando se usen para procesar tales sucesos específicos, omitir hacerlo resultará en el procesamiento erróneo de sucesos, pérdida de datos y resultados no significativos.

- Para recoger y procesar los registros, algunas aplicaciones deben tener privilegios administrativos sobre los equipos objetivos. Este hecho implica un riesgo de seguridad ya que las cuentas de servicios que utilizan las herramientas deben tener derechos administrativos sobre todos los equipos involucrados.

- Ciertos productos realizan un análisis y una catalogación de los eventos, pero utilizan tecnologías y herramientas de terceras partes, por ejemplo Microsoft SQL Server Analysis Services. La desventaja es que estos paquetes son costosos y complejos de implementar.

En consecuencia, la mayoría de las aplicaciones del mercado, se basan en condiciones predefinidas (basada en los potenciales eventos que podrían suceder) que se encargan de realizar determinadas acciones si se cumplen las mencionadas condiciones.

En cambio, el objetivo del presente trabajo de tesis de magíster, consiste en detectar anomalías de manera proactiva pero analizando Patrones de Comportamientos.

La conveniencia de la tecnología propuesta se fundamenta en que las redes neuronales pueden agrupar los eventos convenientemente y, los árboles de decisión generar las reglas de decisión. Usando esta particularidad, se podrán construir patrones de comportamientos.

Aplicando esta tecnología al entorno de estudio, se podrán construir los patrones de las tareas, acciones y operaciones que realizan los usuarios administradores de red sobre los equipos informáticos.

Luego clasificando los nuevos eventos, se podrá predecir al patrón que pertenece, y dependiendo de cual sea el mismo, se lograrán detectar acciones deshonestas o no permitidas de los administradores.

Además se acotará el número de eventos que el personal del sector de Seguridad Informática debe analizar al realizar la inspección de las labores de los administradores. Adicionalmente se disminuye el tiempo que requiere esta ocupación y a la vez se incrementa la efectividad de la misma.

3 PROBLEMA

3.1 Objetivo de la Tesis

El objetivo principal de esta Tesis es detectar patrones de comportamiento irregulares en las operaciones de los administradores de redes, para reducir la cantidad de eventos que el sector de Seguridad Informática debe analizar, comparar y controlar, para detectar acciones fraudulentas realizadas por los administradores. El proyecto de Exploración de Datos está basado en la metodología CRISP-DM [Chapman *et al*, 2000].

Como meta secundaria se propuso el desarrollo de una versión "Beta" de un software simple que permita aplicar y analizar el conocimiento descubierto. El principal objetivo del mismo, será verificar y plasmar prácticamente si el análisis realizado en la fase de Minería de Datos es efectivo. El desarrollo se apoya en la metodología Métrica Versión 3 [Métrica, 2008].

3.2 Descripción del Problema

3.2.1 Definición de Conceptos

Con el fin de introducir el problema se detalla a continuación la definición de términos importante acerca del tema en estudio. [RAE, 2007].

Delito

(De delicto).

- 1. m. Culpa, quebrantamiento de la ley.
- 2. m. Acción o cosa reprobable. Comer tanto es un delito. Es un delito gastar tanto en un traje.
- 3. m. Der. Acción u omisión voluntaria o imprudente penada por la ley.

Fraude

(Del lat. fraus, fraudis).

- 1. m. Acción contraria a la verdad y a la rectitud, que perjudica a la persona contra quien se comete.
- 2. m. Acto tendente a eludir una disposición legal en perjuicio del Estado o de terceros.

- 3. m. Der. Delito que comete el encargado de vigilar la ejecución de contratos públicos, o de algunos privados, confabulándose con la representación de los intereses opuestos.

Informática

(Del fr. informatique).

- 1. f. Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores.

Delitos Informáticos

- La Organización para la Cooperación y el Desarrollo Económico (OCDE) publicó un estudio sobre delitos informáticos y el análisis de la normativa jurídica en donde se reseñan las normas legislativas vigentes y se define Delito Informático como "*cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos.*" [OCDE, 2007]

3.2.2 El Problema

Para presentar el problema con una situación de nuestro país, transcribo dos párrafos de una publicación del Señor Rubén Schilliró, Director de Consist Teleinformática, quien relata lo siguiente:

"*En diciembre de 2006, el Banco Central de la República Argentina emitió la Comunicación "A" 4609 sobre Registros de seguridad y pistas de auditoria. Esta comunicación se refiere específicamente a las "normas sobre requisitos mínimos de gestión, implementación y control de los riegos relacionados con tecnología informática y sistemas de información", y en el punto 8.2 señala concretamente: "todos los sistemas aplicativos deben generar registros de auditoria que contengan mínimamente las actividades de los usuarios, las tareas realizadas, las funciones monetarias y no monetarias utilizadas…".*

Sin embargo, más allá de las regulaciones públicas, es sorprendente la escasa concientización sobre la necesidad de implementar medidas de seguridad anti fraude. En 2006, la filial local de la consultora Ernst & Young realizó la 1º Encuesta Nacional sobre Fraude. Entre otras cosas, determinó que el 51 por ciento de las compañías combate el fraude a través de la auditoria interna. Esto implica que NO lo hace un 49 por ciento de las empresas (¡casi la mitad!)." [Schilliró, 2006]

Adicionalmente, en base a una encuesta de Global 2000, el 72% de los encuestados mantiene sus archivos de eventos menos de un año y el 33% los

mantiene menos de una semana o no tiene planes de guardarlos. Dos tercios no están conformes con su actual administración de archivos de sucesos. Dentro de esta proporción de participantes, 66,7% están planeando cambiarla, otros están pensando delegarla a terceros, o programar sus propias aplicaciones. El resto simplemente se encuentra frustrado por la falta de personal y presupuesto. [Northcutt *et at*, 2005.]

Por lo tanto se puede afirmar que, a pesar de que en los registros de seguridad que se generan en los dispositivos informáticos, hay información y datos relevantes del estado del entorno de sistemas, y por diversas razones, las empresas no los tienen en cuenta o no utilizan o subestiman.

A las realidades descriptas anteriormente, se suma el hecho que el mercado ofrece una gran variedad de herramientas para la administración de los archivos de sucesos pero las mismas no logran satisfacer integralmente las necesidades de las gerencias de Tecnología de la Información.

4 SOLUCIÓN

4.1 Proyecto de Explotación de Información (Crisp-DM)

4.1.1 Entendimiento del Negocio

4.1.1.1 Objetivos del negocio

4.1.1.1.1 Escenario Actual

Organización

Se trata de una empresa de sistemas de información que brinda principalmente servicios de Operaciones, Tecnología y Soporte. Los clientes son, en su mayoría, empresas distribuidas en los cinco continentes, que se desempeñan en el sector siderúrgico. Todas las sociedades pertenecen al mismo grupo empresario.

El rol principal es aplicar y adaptar las tecnologías de la información en valores agregados valiosos para los clientes, a través de soluciones y servicios profesionales, simplificando el acceso a tecnologías emergentes para así lograr los objetivos de negocio planteados y asegurar los beneficios de las inversiones realizadas.

Siendo una empresa de sistemas que trabaja exclusivamente pensando en sus clientes siderúrgicos, la sinergia lograda, facilita la toma de decisiones aprovechando las tecnologías disponibles, disminuyendo el tiempo y costos asociados a los sistemas y tecnologías de información; aumentando así, el valor aportado por las inversiones realizadas.

Misión

Brindar servicios profesionales con valor agregado para los clientes realizando un continuo análisis de las tecnologías de la información y aplicarlas para mejorar el negocio.

Visión

Ser una empresa líder de servicios de sistemas y tecnologías de información, con una participación activa en los proyectos innovadores de los clientes.

Valores

Respeto. Compromiso. Libertad. Lealtad. Honestidad.

Compromiso

Proveer el valor aportado a las empresas.

Mejorar la calidad de sistemas con Metodologías y Procesos.

Mantener siempre conciencia de rentabilidad.

Sector en Estudio

El sector de la Empresa que compete al presente estudio es **Seguridad y Control** y el Organigrama del mencionado sector es el siguiente (figura 4-1):

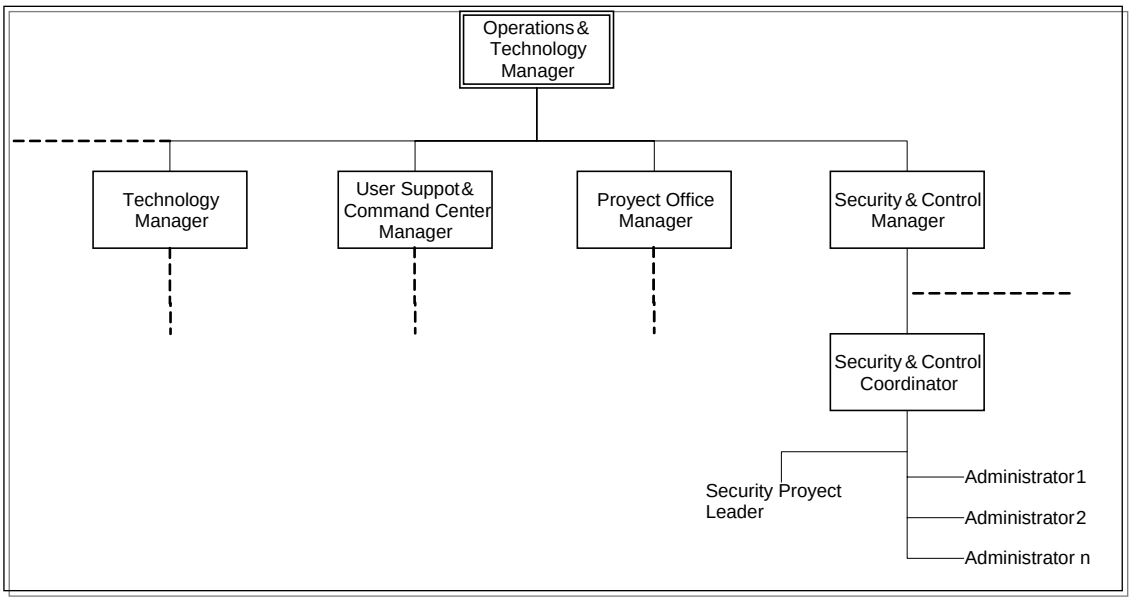


Figura 4-1. Organigrama del sector en estudio.

Las responsabilidades y roles de las personas del departamento en estudio son las siguientes:

Posición: Gerente de seguridad y Control (Security & Control Manager)

Rol:

Definir el plan de Seguridad de la Tecnología de Información para la infraestructura de información de la empresa, asegurando una base confiable para la Tecnología de Información y la disponibilidad de información, autorizando accesos y realizando controles periódicos para proporcionar a las compañías una base adecuada para el desarrollo y funcionamiento de sus Tecnologías de Información y sistemas de comunicación.

Responsabilidades con respecto a:

- Políticas y Procedimientos de Seguridad: Definir las Políticas y Procedimientos de Seguridad
- La Infraestructura tecnológica: Asegurar la disponibilidad, integridad y confidencialidad de los recursos
- La Seguridad de información: Asegurar la disponibilidad, integridad y confidencialidad de información
- Proyectos: Supervisar el logro de metas de los proyectos
- Plan de Recuperación de Desastre: Asegurar la continuidad del proceso
- Presupuesto: Asegurar que se respete el plan propuesto
- Recursos humanos: Desarrollo del personal

Posición: Coordinador de seguridad y Control (Security & Control Manager Coordinator)

Rol:

Coordinar el análisis, definición, implementación y soporte de los asuntos de seguridad de las Tecnologías de Información para proporcionar la infraestructura tecnológica con un nivel adecuado de seguridad en términos de la confidencialidad, integridad y disponibilidad de información para el desarrollo y funcionamiento de las Tecnologías de Información y sistemas de comunicación

Responsabilidades con respecto a:

- Políticas y Procedimientos de Seguridad: Asegure la obediencia con las Políticas y Procedimientos de Seguridad definidos.
- Infraestructura Tecnológica: Asegurar la protección de los recursos.
- La Seguridad de información: Salvaguardar la disponibilidad, integridad y confidencialidad de la Infraestructura Tecnológica.
- Al Plan de Recuperación de Desastre: Asegure la continuidad del proceso.
- Al soporte: Mantener un nivel adecuado de seguridad en las soluciones tecnológicas.
- Los proyectos: Asegurar que los proyectos se completen a tiempo.

- La Innovación tecnológica: Garantizar la minimización de ataques contra los recursos de la empresa.

Posición: Líder de Proyectos de Seguridad (Security Proyect Leader)

Rol:

Asegurar en términos de disponibilidad, integridad y confidencialidad una base tecnológica fiable para el desarrollo y funcionamiento de los sistemas de información y comunicación, analizando, definiendo e implementando la arquitectura de la plataforma tecnológica, obedeciendo a las estrategias de los sistemas, normas y procedimientos.

Responsabilidades con respecto a:

- Políticas y Procedimientos de Seguridad: Asegure la obediencia con las Políticas y Procedimientos de Seguridad definidos
- La Infraestructura tecnológica: Asegurar una infraestructura de seguridad adecuada.
- La Seguridad de información: Cumplir con las buenas prácticas de la Seguridad de la Información, normas internacionales, procedimientos y certificaciones.
- Al Plan de Recuperación de Desastre: Asegurar la continuidad del proceso.
- Los proyectos: Asegurar la complacencia con las estrategias de sistemas de la empresa.
- La Innovación tecnológica: Colaborar en la actualización de las herramientas y plataformas usadas.
- SOX 404: Asegurar la complacencia de las regulaciones en las áreas bajo su responsabilidad
- Los Recursos humanos: Desarrollo del personal.

El coordinador de Seguridad y Control es seleccionado como Representante Interno o Sponsor.

La unidad de negocio que es afectada por el proyecto de minería es el Departamento de Seguridad Informática.

Problema

El problema se encuentra circunscrito al proceso de control de las tareas de los administradores de redes que realiza el área de Seguridad Informática.

Toda red de datos empresarial, posee múltiples servidores en ejecución, con distintos tipos de archivos de sucesos, donde cada máquina genera una elevada cantidad de información de eventos. De hecho, un único servidor, es capaz de generar varios gigabytes de datos de sucesos en un solo día. Multiplicando este número por la cantidad de equipos en la organización, luego por la cantidad de archivos de sucesos que deben ser almacenados, la tarea de mantenimiento de los mismos es inmanejable.

En los archivos de sucesos siempre se registran los problemas con suficiente anterioridad a la falla total de los sistemas, como así también las tareas que realizan los administradores de redes. Ellos mantienen potencial y valiosa evidencia forense. Ante la presencia de una anomalía y/o problema en un sistema de información, los archivos de eventos poseen toda la información de las razones del mismo, cómo, cuando sucedió y finalmente la llave para prevenir futuros.

Particularmente las tareas que realizan los administradores de redes se registran en los archivos de eventos de Seguridad.

La motivación del presente trabajo radica en que la empresa están descubriendo que la información contenida en los archivos de eventos puede usarse como soporte a las decisiones, ya sea de mejora, resolución de problemas, detección de tareas fraudulentas, anticipación a fallas, satisfacción de los acuerdos de niveles de servicios.

Además la organización debe cumplir con determinadas regulaciones, por ejemplo Sarbanes-Oxley (SOX) del año 2002 [SOX, 2002], y debe guardar evidencias de las tareas o acciones realizadas por los empleados. La mayoría de éstas se encuentran en los archivos de sucesos. Ante una auditoria será necesario recuperarlas y demostrar la legitimidad de las tareas realizadas.

El resultado del proyecto va dirigido al gerente del departamento de Seguridad y Control y posteriormente al Gerente de Operaciones y Tecnología.

Las expectativas que posee el Sector Usuario de este estudio consisten en que se logue detectar anomalías analizando patrones de comportamiento de los administradores de redes, acotando así, el número de eventos que personal del sector de Seguridad Informática debe analizar al realizar el control de las tareas de los mismos.

Solución Actual

Actualmente hay diversas soluciones y productos para resolver el problema. Uno de los procedimientos que se realiza para el análisis de sucesos de seguridad, es utilizar algún aplicativo para leer los eventos y almacenarlos en una base de datos o en su defecto, y menos deseable por su ineficiencia, en una planilla de cálculo. Luego personal del sector de Seguridad Informática, en forma manual, realiza consultas y búsquedas específicas.

Este método es muy débil ya que debido a la existencia de una elevada cantidad de datos, será necesario producir manualmente filtros y consultas extremadamente eficaces para lograr descubrir eventos que indiquen alguna tarea dudosa. Evidentemente lograr este propósito conlleva un costo alto de tiempo y difícilmente sea efectivo.

El mercado ofrece una gran variedad de herramientas para la administración de los archivos de sucesos pero no logran satisfacer integralmente las necesidades de las gerencias de Tecnología de la Información. Estos productos se basan en configurar condiciones y acciones. Ante la detección de un evento específico, se puede activar una alerta que es enviada al personal de sistemas encargado de la aplicación. Esta metodología presenta el problema que requiere el conocimiento previo de los potenciales errores para construir las condiciones. Además es necesario programar las series de condiciones que se aplicarán a los sucesos lo cual al término de un tiempo la cantidad de las mismas es tan grande que es muy complicado administrarlas y entender su lógica.

4.1.1.1.2 Objetivos del negocio

El objetivo es reducir la cantidad de eventos a analizar, por parte del sector de Seguridad Informática, para detectar acciones fraudulentas realizadas por los administradores de red.

El problema que será solucionado con el proyecto de minería de datos es la gran cantidad de eventos que personal del sector de Seguridad Informática tiene que analizar para controlar las acciones que se realizan en la red informática. El objetivo es reducir drásticamente el número de sucesos y producir como salida un fichero con solo las acciones consideradas dudosas o fraudulentas. De esta manera el personal avocado al control hará foco en este grupo reducido de datos, optimizando el tiempo y esfuerzo.

Los requerimientos y beneficios esperados por el área usuaria son:

- Minimizar el tiempo y optimizar los recursos dedicados a las tareas de control de eventos de seguridad.

- Detectar las acciones fraudulentas realizadas en el entorno informático por personal dedicado a Tecnología de Información.
- Cumplir con los controles exigidos en las regulaciones.

4.1.1.1.3 Factores Críticos de Éxito

Los criterios de éxito consisten en:

- Lograr la recolección, consolidación y análisis de los archivos de sucesos.
- Lograr el agrupamiento de los eventos según su semejanza.
- Lograr generar Reglas de Decisión efectivas.

El gerente del Sector de Seguridad y Control será quien determina los criterios de éxito.

4.1.1.2 Evaluar la situación

4.1.1.2.1 Inventario de Recursos

Hardware

El hardware base a utilizar para el proyecto será un Servidor donde se ejecutará la aplicación desarrollada en este proyecto y los servidores controladores de dominio que son los que contienen los archivos de sucesos a analizar.

No habrá problemas de disponibilidad ni conflictos con el horario de mantenimiento del hardware base para el proyecto de exploración de la información ya que el servidor fue comprado por el proyecto.

Datos y Conocimiento

Las fuentes de datos serán los servidores controladores de dominio que se encuentran en línea y generan nuevos eventos constantemente.

La fuente de conocimiento será el Líder de Proyectos de Seguridad que es el experto en los que refiere a las tareas de control.

Las herramientas y técnicas a utilizar son:

- Técnicas de minería de datos para el procesamiento de los mismos.
    1. Redes neuronales para agrupamiento de datos.

2. Árboles de decisión para producción de las reglas de decisión.

Recursos Humanos

El analista/programador deberá Mantener actualizados los Compromisos, poseer Criterio común, Detectar áreas de oportunidad, poseer Fuerte Gestión en los Proyectos.

El experto del dominio es el Líder de Proyectos de Seguridad y no habrá inconvenientes con su disponibilidad. El mismo brindará toda la información necesaria en cuanto a metodología, controles, reglas y/o procedimiento que se utilizan en el proceso de control de sucesos.

El Especialista en Minería de Datos cuya responsabilidad es utilizar las técnicas que domina, como herramienta de análisis y descubrimiento de conocimiento, a partir de los datos.

No será necesario el contacto con personal técnico ya que inicialmente se trabajará en un entorno de laboratorio en el cual se tiene acceso total. Eventualmente ante algún problema de índole técnico se recurrirá al HelpDesk.

4.1.1.2.2 Requisitos, Supuestos y Requerimientos

Requerimientos

El proyecto debe ser comprensible para el área gerencial de Seguridad y Control.

El producto debe tener la propiedad de ser fácilmente soportable por terceras personas.

El proyecto y producto deben ser escalables desde el entorno de laboratorio al entorno de producción.

En cuanto a los datos, la cantidad de eventos, para realizar el tratamiento inicial, debe ser mayor a 5000. Se deben contemplar datos que cubran los siete días de la semana y preferentemente feriados.

Expectativas

Se espera que el tiempo dedicado al control de eventos se reduzca en un 30%.

Se pretende aumentar la cantidad de tareas fraudulentas detectadas en un 20%.

La confianza en el sector de sistemas y La seguridad de la información se incrementarán.

La disponibilidad de las fuentes de datos será del 99%. La confianza en que los mismos no estén inconsistentes ni haya faltantes es alta pero hay certeza de que posean un alto nivel de ruido.

En cuanto a los factores externos, debido a la rápida evolución del mercado tecnológico, hay perspectivas de que aparezcan nuevas versiones de productos para el tratamiento de eventos de servidores.

Restricciones

Durante el desarrollo del proyecto no se tendrá acceso a los datos de Producción de la empresa. Se manipularán datos del entorno de Desarrollo y Pruebas. En el entorno de Desarrollo y Pruebas se tendrá control total sobre los datos y servidor.

Se procesaran solo los archivos de sucesos de seguridad de los servidores controladores de dominio.

Se desarrollará una versión reducida y Beta del producto. La misma soportará hasta un máximo de 6 (seis) usuarios administradores y 21 (veintiuna) reglas de decisión.

4.1.1.2.3 Riesgos y Contingencias

Riegos	Contingencias
El sector para el cual se realiza el estudio no dispone de presupuesto para el mismo.	El estudio se realiza con financiamiento propio del equipo del trabajo.
Pérdida del soporte de los Consultores Seniors, debido a un cambio de personal.	Documentar todos los conocimientos en las fases iniciales del proyecto.
Habrá miembros del personal asignado al proyecto que trabajarán sólo a tiempo parcial en el proyecto.	Se programan las tareas y fases con un tiempo inicial holgado, para poder redistribuir el trabajo en caso de ser necesario.
La naturaleza de los datos no es adecuada para utilizar técnicas de minería de datos.	Se analizará la viabilidad de la solución en una instancia inicial del proyecto.
Pueden perderse eventos si no se programa la captura de los mismos convenientemente.	Se programarán los archivos de manera que solo puedan ser reciclados si y solo si se haya realizadazo un backup la captura de los eventos con el propósito de evitar la perdida de datos.

Tabla 4-1. Riegos y Contingencias.

4.1.1.2.4 Terminologías

Acrónimos y Abreviaturas

Concepto	Descripción
CIA	Acrónimo inglés de confidencialidad, integridad y disponibilidad, los parámetros básicos de la seguridad de la información.
CID	Acrónimo español de confidencialidad, integridad y disponibilidad, los parámetros básicos de la seguridad de la información.
CRISP-DM v1.0	CRoss Industry Standard Process for Data Mining versión 1
COCOMO	Modelo Constructivo de Costes (Constructive Cost Model)
GB	Gigabytes
ISO	Organización Internacional de Normalización
RN	Red Neuronal
RRHH	Recursos Humanos
S&C	Área de Seguridad y Control
SGSI	Sistema de Gestión de la Seguridad de la Información
SOM	Mapas Auto Organizados (Self Organizing Map)
SOX	Regulación Sarbaney & Oxley

Tabla 4-2. Acrónimos y Abreviaturas.

4.1.1.2.5 Glosario

[ISO 27000, 2007]

A

Acción correctiva

(Inglés: Corrective action). Medida de tipo reactivo orientada a eliminar la causa de una no-conformidad asociada a la implementación y operación del SGSI con el fin de prevenir su repetición.

Acción preventiva

(Inglés: Preventive action). Medida de tipo pro-activo orientada a prevenir potenciales no-conformidades asociadas a la implementación y operación del SGSI.

Activo

(Inglés: Asset). En relación con la seguridad de la información, se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización. Según (ISO/IEC 13335-1:2004): Cualquier cosa que tiene valor para la organización.

Alcance

(Inglés: Scope). Ámbito de la organización que queda sometido al SGSI. Debe incluir la identificación clara de las dependencias, interfaces y límites con el entorno, sobre todo si sólo incluye una parte de la organización.

Alerta

(Inglés: Alert). Una notificación formal de que se ha producido un incidente relacionado con la seguridad de la información que puede evolucionar hasta convertirse en desastre.

Amenaza

(Inglés: Threat). Según (ISO/IEC 13335-1:2004): causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Análisis de riesgos

(Inglés: Risk analysis). Según (ISO/IEC Guía 73:2002): Uso sistemático de la información para identificar fuentes y estimar el riesgo.

Auditor

(Inglés: Auditor). Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.

Auditoría

(Inglés: Audit). Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.

Autenticación

(Inglés: Authentication). Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

C

Checklist

Lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo. Este tipo de listas también se pueden utilizar durante la implantación del SGSI para facilitar su desarrollo.

Compromiso de la Dirección

(Inglés: Management commitment). Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI.

Confidencialidad

(Inglés: Confidenciality). Acceso a la información por parte únicamente de quienes estén autorizados. Según (ISO/IEC 13335-1:2004):" característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

Control

Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. (Nota: Control es también utilizado como sinónimo de salvaguarda o contramedida.

Control correctivo

(Inglés: Corrective control). Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas. Supone que la amenaza ya se ha materializado pero que se corrige.

Control detectivo

(Inglés: Detective control). Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.

Control disuasorio

(Inglés: Deterrent control). Control que reduce la posibilidad de materialización de una amenaza, p.ej., por medio de avisos disuasorios.

Control preventivo

(Inglés: Preventive control). Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

D

Desastre

(Inglés: Disaster). Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

Directiva

(Inglés: Guideline). Según (ISO/IEC 13335-1:2004): una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.

Disponibilidad

(Inglés: Availability). Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran. Según (ISO/IEC 13335-1:2004): característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

E

Evento

(Inglés: information security event). Según (ISO/IEC TR 18044:2004): Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardias, o una situación anterior desconocida que podría ser relevante para la seguridad.

Evidencia objetiva

(Inglés: Objective evidence). Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de seguridad de la información.

I

Impacto

(Inglés: Impact). El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc-.

Incidente

Según (ISO/IEC TR 18044:2004): Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad

(Inglés: Integrity). Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según (ISO/IEC 13335-1:2004): propiedad/característica de salvaguardar la exactitud y completitud de los activos.

ISO

Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.

ISO 27001

Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. Primera publicación en 2005

ISO 27002

Código de buenas prácticas en gestión de la seguridad de la información (transcripción de ISO 17799). No es certificable. Cambio de oficial de nomenclatura de ISO 17799:2005 a ISO 27002:2005 el 1 de Julio de 2007.

N

No conformidad

(Inglés: Nonconformity). Situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control

que permita dudar de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.

O

Objetivo

(Inglés: Objetive). Declaración del resultado o fin que se desea lograr mediante la implementación de procedimientos de control en una actividad de TI determinada.

P

Plan de continuidad del negocio

(Inglés: Bussines Continuity Plan). Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.

Plan de tratamiento de riesgos

(Inglés: Risk treatment plan). Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Política de seguridad

(Inglés: Security policy). Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. Según (ISO/IEC 27002:2005): intención y dirección general expresada formalmente por la Dirección.

R

Riesgo

(Inglés: Risk). Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Según (ISO Guía 73:2002): combinación de la probabilidad de un evento y sus consecuencias.

S

Sarbanes-Oxley

Ley de Reforma de la Contabilidad de Compañías Públicas y Protección de los Inversores aplicada en EEUU desde 2002. Crea un consejo de supervisión independiente para supervisar a los auditores de compañías públicas y le permite a este consejo establecer normas de contabilidad así como investigar y disciplinar a los contables. También obliga a los responsables de las empresas a garantizar la seguridad de la información financiera.

Segregación de tareas

(Inglés: Segregation of duties). Reparto de tareas sensibles entre distintos empleados para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

Seguridad de la información

Según (ISO/IEC 27002:2005): Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.

Selección de controles

Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

SGSI

(Inglés: ISMS). Sistema de Gestión de la Seguridad de la Información. Según (ISO/IEC 27001:2005): la parte de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.)

Sistema de Gestión de la Seguridad de la Información

(Inglés: Information Systems Management System). Ver SGSI.

T

Tratamiento de riesgos

(Inglés: Risk treatment). Según (ISO/IEC Guía 73:2002): Proceso de selección e implementación de medidas para modificar el riesgo.

V

Valoración de riesgos

(Inglés: Risk assessment). Según (ISO/IEC Guía 73:2002): Proceso completo de análisis y evaluación de riesgos.

Vulnerabilidad

(Inglés: Vulnerability). Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según (ISO/IEC 13335-1:2004): debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

4.1.1.2.6 Costos y Beneficios

Costos

Estimación de datos	Pesos por unidad	Cantidad de Horas	Total
Analista de Sistemas	$ 58	40	$ 2320
Programador	$ 39	10	$ 390
Líder de Proyectos de Seguridad y Control	$ 65	20	$ 1300
Gerente de Seguridad y Control	$ 110	2	$ 220
		Total	**$ 4230**

Tabla 4-3. Costos de la Estimación de Datos.

Desarrollo y Ejecución de la Solución	Pesos por unidad	Cantidad de Horas	Total
Servidor donde se ejecutará la Aplicación	$ 5000	-	$ 5000
Licencias de Software	$ 1000	-	$ 1000
Analista de Sistemas	$ 58	30	$ 1740
Programador	$ 39	70	$ 2730
Líder de Proyectos de Seguridad y Control	$ 65	20	$ 1300
Capacitación Usuarios, HelpDesk	$ 58	20	$ 1160

Desarrollo y Ejecución de la Solución	Pesos por unidad	Cantidad de Horas	Total
		Total	**$ 12930**

Tabla 4-4. Costos de Desarrollo y Ejecución de la Solución.

Costos de Operación y mantenimiento	Pesos por unidad	Cantidad de Horas	Total
Colocation en Centro de Cómputos	$ 2500	-	$ 2500
Capacitación Operadores	$ 58	4	$ 232
		Total	**$ 2732**

Tabla 4-5. Costos de Operación y Mantenimiento.

Beneficios

- Menor tiempo dedicado al control de las tareas.
- Incremento de la Efectividad y eficiencia para detectar tareas anormales.
- Incremento de la confianza, seguridad en la empresa.
- Mejora de la Imagen de la organización.
- Cumplir con las Regulaciones.

4.1.1.3 Determinar Objetivos del Proceso de Exploración de Información

4.1.1.3.1 Objetivos del Proceso de Exploración de Información

El objetivo del proceso de exploración de información es producir reglas decisión que permitan identificar eventos fraudulentos dentro de los registros de seguridad de los servidores controladores de dominio.

Se utilizarán como set de datos los ficheros que usa el sistema operativo de los equipos mencionados anteriormente, para registrar todas operaciones de seguridad realizadas, por parte de los administradores de red, sobre las cuentas del dominio.

4.1.1.3.2 Criterios de Éxito del Proceso de Exploración de Información

La cantidad de observaciones necesarias para entrenar la red neuronal debe ser mayor a 5000.

El error de detección de acciones anormales del proceso de minería debe ser menor a 30%.

El funcionamiento y mantenimiento del modelo debe ser simple, de manera que pueda realizarlo un tercero siguiendo solo la documentación.

Pruebas Patrones

Verificar la cantidad de observaciones relacionadas con las tareas de los administradores que se de los archivos de eventos.

Verificar, con la ayuda del sector de Seguridad Informática, si las acciones catalogadas como fraudulentas o anormales son realmente del mencionado tenor.

Verificar que la documentación del modelo sea simple, comprensible, completa.

4.1.1.4 Realizar el Plan del Proyecto

4.1.1.4.1 Plan de Proyecto

Actividad	Horas	RRHH	Entradas	Salidas
Entendimiento de los datos				
Recolectar Datos	5	Analista/Programador	Fichero de Observaciones	Informe de Recolección de datos
Descripción Datos	10	Analista/Programador Líder de Proyectos de S&C	Observaciones “crudas”	Informe de Descripción de datos
Exploración Datos	15	Analista/Programador Líder de Proyectos de S&C	Observaciones “crudas”	Informe de Exploración de datos
Verificación Datos	10	Analista/Programador Líder de Proyectos de S&C	Observaciones “crudas”	Informe de Calidad de datos
Preparación de los datos				
Seleccionar Datos	10	Analista/Programador Líder de Proyectos de S&C	Observaciones “crudas”	Datos excluidos/utilizados
Limpiar Datos	10	Analista/Programador	Observaciones Seleccionadas	Informe de limpieza de datos
Construcción Datos	10	Analista/Programador	Observaciones Depuradas	Informe de Registros
Integración Datos	10	Analista/Programador	Observaciones	Informe de Integración

			Depuradas	
Modelado				
Selección Técnica	15	Analista/Programador	Conjunto de técnicas Posibles	Supuestos de Modelado
Diseño de Pruebas	15	Analista/Programador Líder de Proyectos de S&C	Conjunto de Pruebas Posibles	Informe de Pruebas
Construir Modelo	15	Analista/Programador	Observaciones, Técnicas, Pruebas Seleccionadas	Descripción del Modelo
Evaluar Modelo	15	Analista/Programador Líder de Proyectos de S&C	Descripción del Modelo	Revisión del Modelo
Evaluación				
Evaluar Resultado Proceso	20	Analista/Programador Líder de Proyectos de S&C	Resultados Pruebas, Modelo	Informe del Resultado del Proceso
Revisión del Proceso	20	Analista/Programador Líder de Proyectos de S&C	Resultados Pruebas, Modelo	Informe de Revisión
Implementación				
Elaborar plan de monitoreo	10	Analista/Programador	Descripción Proceso, Modelo.	Plan de Monitoreo
Elaborar plan de mantenimiento	10	Analista/Programador	Descripción Proceso, Modelo.	Plan de Mantenimiento
Informe Final	10	Analista/Programador	Descripción Datos, Pruebas, Proceso, Modelo, Experiencias.	Informe Final

Tabla 4-6. Plan de Proyecto.

4.1.1.4.2 Validación Inicial de Técnicas y Herramientas

Para resolver el problema se propone utilizar distintas técnicas de detección de patrones, cambios y anomalías a partir de grandes cantidades de datos. Uno de los métodos de análisis de datos que se utilizará son las redes neuronales que son efectivas en el agrupamiento de datos. Una vez obtenidos los patrones, se aplicarán árboles de decisión.

La herramienta de Redes Neuronales a utilizar será NNClust. La misma usa Mapas Auto Organizados y es de uso libre.

La herramienta de Árboles de Decisión a utilizar será Ctree. La misma aplica el algoritmo de inducción C4.5 y es de uso libre.

En base a pruebas desarrolladas en un ambiente de laboratorio se pudo comprobar que las herramientas ofrecieron los resultados esperados.

4.1.2 Entendimiento de los Datos

4.1.2.1 Recolectar los Datos Iniciales

Como paso inicial será necesario recolectar los archivos de sucesos. Los datos de las distintas fuentes serán almacenados e integrados en un único almacenamiento.

La información requerida está disponible en todo momento. Hay que tener en consideración que la misma no se pierda al ser sobre escrita cuando se llega al tamaño máximo del log. Para evitar que se dilapiden los datos será necesario crean un mecanismo para leerlos y resguardarlos en un dispositivo de almacenamiento permanente de antemano.

Como el objetivo del presente estudio es analizar el comportamiento de las tareas que realizan los administradores de redes, se hará foco en los eventos de seguridad (figura 4-2) de los servidores controladores de dominio.

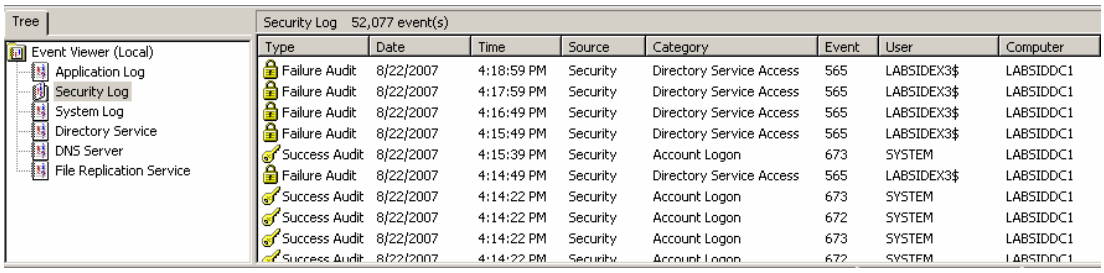


Figura 4-2. Eventos de un servidor.

No se utilizarán campos con entrada de texto libre. Los datos se extraerán utilizando un aplicativo que se ejecuta por líneas de comandos que descarga el archivo de sucesos de servidores a un archivo de tipo “separado por espacios”.

4.1.2.2 Descripción de los Datos

En la siguiente tabla se visualizan la información que contiene cada evento:

Event Type:	Tipo de Evento (Success, Failure, Error, Information)
Event Source:	Fuente, Proceso que genera el evento
Event Category:	Categoría del evento
Event ID:	Número Identificatorio del evento
Date:	Día que ocurre el evento
Time:	Hora que ocurre el evento
User:	Usuario que genera el evento

Event Type:	Tipo de Evento (Success, Failure, Error, Information)
Computer:	Computadora que genera el evento
Description:	Descripción del evento

Tabla 4-7. Descripción de Datos.

El método de captura de los eventos no es parte del presente estudio. Sin embargo, a continuación se describe una posible metodología.

- Una de las opciones es correr archivos ejecutables que se disparan en forma batch. El programa ejecutaría la aplicación dumpel.exe de Microsoft con ciertos parámetros para generar un archivo temporal con la recolección de los eventos logueados (Event Log – Security). En caso de existir varios dominios se utilizaría un ejecutable por cada uno de ellos.

No existen inconvenientes en el acceso de los datos a menos que haya problemas en la red o en el propio servidor. Cuando se reestablece el servicio se normaliza la captura.

En la presente experiencia no se vislumbra un volumen inmanejable de datos. Tampoco se esperan datos complejos, debido a la naturaleza de los mismos son todos de un mismo y simple formato.

4.1.2.3 Exploración de los Datos

Del conjunto de campos, el que contiene la descripción "Description", muestra un texto descriptivo del evento. Permite buscar eventos utilizando una porción del texto. En ocasiones puede presentarse el problema que no se encuentra accesible el archivo con la información de la descripción y ésta no pueda ser visualizada.

4.1.2.3.1 Hipótesis

Considerando que:

- En los archivos de sucesos se mantiene potencial y valiosa evidencia forense.
- Ante la presencia de una anomalía en un sistema de información, los repositorios de eventos poseen toda la información de las razones del mismo, cómo, cuando sucedió y finalmente la llave para prevenir futuros.
- Los archivos de sucesos son una importante fuente de información acerca de las tareas que realizan los administradores de redes.

- Los datos allí contenidos, pueden ayudar a los administradores de sistemas resolver y/o identificar problemas con la suficiente antelación para evitar que se vea afectada la operatoria del negocio.

- Otro aspecto substancial es la posibilidad de auditar la actividad de usuarios y administradores de sistemas.

Se define como hipótesis:

A partir del análisis de los archivos de sucesos, detectar patrones de comportamiento irregulares en las operaciones de los administradores de redes de la empresa y reducir la cantidad de eventos que el departamento de Seguridad Informática debe inspeccionar.

Las acciones para llevar a cabo la teoría formulada consisten en:

- Pre-procesar los datos de entrada. Ciertas tareas consisten en Limpiar, Integrar, Transformar, Reducir.

- Aplicar técnicas de minería de datos. Algunas de ellas son las Redes Neuronales, Árboles de Decisión, Reglas de Decisión.

El proceso básico gravita en:

- Descargar los sucesos desde las fuentes de datos.

- Aplicar los métodos de preparación de datos.

- Cargaron los datos en una Red Neuronal cuyo funcionamiento radica en congregar la información de entrada y obtener como salida una serie de clusters, es decir, los datos agrupados.

- Usando información brindada por la Red Neuronal, clasificar los grupos según las observaciones que contienen (Bueno, Dudoso, Malo).

- Ingresar, la salida de la Red Neuronal, como entrada de un Árbol de Decisión para obtener Reglas de Decisión.

- Aplicar la Reglas obtenidas a los nuevos eventos a analizar para su tipificación.

4.1.2.4 Verificación de la Calidad de los Datos

Se considera que la calidad de los datos es muy buena ya que no se presentan datos faltantes, ni con ruido. Además todos los datos están representados.

Podría darse el caso de encontrar datos corruptos si el sistema de almacenamiento o de generación de los mismos entra en falla. Se estima que el impacto es mínimo debido a que el problema se detectaría inmediatamente con el sistema de monitoreo y alarmas y actuaría en consecuencia. Al momento no se tiene registro de una falla de esta naturaleza.

Como se trata de una experiencia nueva y se trabaja en un entorno de laboratorio, se tiene acceso completo a los datos, sin restricciones.

Los valores de cada campo son similares. Pero los atributos se distinguen fácilmente entre ellos pues sus valores son muy distintos. Por ejemplo, evidentemente el campo "Fecha" será el mismo durante todo el día. El campo "hora" variará acorde al momento del día en que se produce el evento.

No se detectan atributos con datos en conflicto con el sentido común.

Durante la operación con los datos, los mismos se almacenarán en archivos planos. Como delimitador se utilizará un espacio en blanco. En el servidor cada evento reside y es manejado en el sistema de generación de sucesos que dispone el sistema operativo del equipo.

Al tomar datos de diversas fuentes, si bien puede darse el caso que la mayoría de los campos sean iguales, se utiliza uno de ellos para identificar el recurso.

4.1.3 Preparación de los datos

4.1.3.1 Seleccionar los datos

Se utilizarán los eventos relacionados con la Seguridad. Los mismos se encuentran en la sección Seguridad de la herramienta administrativa Visor de Eventos provista por el sistema operativo del equipo.

Adicionalmente, como consecuencia de analizar la información contenida en los eventos, se decidió trabajar con los siguientes campos y descartar el resto:

Event ID:	Número Identificatorio del evento
Date:	Día que ocurre el evento
Time:	Hora que ocurre el evento
User:	Usuario que genera el evento
Computer:	Computadora que genera el evento

Tabla 4-8. Campos de Datos.

En la siguiente tabla se muestra la información contenida en un evento:

Event ID:	565
Date:	17/08/2007
Time:	16:30
User:	Administrador
Computer:	Labsidex1

Tabla 4-9. Ejemplo de Información de Campos de Datos.

En la siguiente figura 4-3, se muestra los campos de un evento visto desde la consola de administración provista por el sistema operativo del dispositivo.

Figura 4-3. Propiedades de un Evento vista en el servidor.

La descripción de los campos, considerados relevantes para los objetivos del proyecto, son las siguientes:

- Event ID: muestra un número para identificar el evento específico. Ayuda a los administradores de sistema a rastrear las causas de problemas. Es de tipo numérico. Rango: 0 a 99999.
- Date: muestra el día en que fue generado el evento. Es de tipo Día.
- Time: muestra la hora que fue generado el evento. Es de tipo Hora.
- User: muestra el usuario que generó el evento. Es de tipo Texto.
- Computer: muestra el equipo donde fue generado el evento. Es de tipo Texto.

Los campos que se excluyen son los siguientes:

- Event Type: Tipo de Evento (Success, Failure, Error, Information)
- Event Source: Fuente, Proceso que genera el evento

- Event Category: Categoría del evento

El motivo de exclusión de los atributos anteriores se debe a que se consideran redundantes. El campo "Event ID" basta para identificar el tipo, fuente y categoría del suceso.

- Description: Descripción del evento

Se excluye porque la descripción no aporta información relevante para detectar patrones de comportamiento de los administradores que los ocasionan.

Adicionalmente, dada la naturaleza del archivo de suceso de seguridad de los servidores, los mismos contienen eventos de las acciones tanto de los administradores de redes como de los sistemas y procesos que son ejecutados en los dispositivos. Debido a esto, será necesario realizar un filtrado de los sucesos por el campo "User" para trabajar solo con los eventos de administradores.

4.1.3.2 Limpiar los datos

Como se mencionó en el apartado "Verificación de la calidad de datos", se considera que la calidad de los datos es muy buena por lo tanto la fase de "Limpieza de datos", si bien se tiene presente, no requiere mayor atención.

4.1.3.3 Construcción de datos

Como respuesta a los requerimientos de las herramientas de modelado, es necesario realizar la transformación de ciertos atributos.

En el presente trabajo, los datos se procesarán en una primera instancia con Redes Neuronales, puntualmente con el modelo Self Organizing Maps (SOM), para explotar la capacidad de agrupamiento de datos de las mismas. Debido a las características de los datos que requiere SOM como entrada, será necesario preparar la información contenida en cada evento de manera tal que la red pueda utilizarlos.

Todos los datos de entrada deben ser numéricos. Ninguno puede ser faltar o sea no puede ser un valor en "blanco".

Las transformaciones requeridas se detallan a continuación:

- Event ID: se ordenan los eventos de menor a mayor y se asignará a cada uno de ellos un número secuencial comenzando en uno. Esta secuencia será la que se usará y representará los eventos en las herramientas.

- Date: Se asignará el número uno a los días laborales y dos a los días no laborales. Se definen días laborales a los Lunes, Martes, Miércoles, Jueves y Viernes. Se definen días no laborales a los Sábados, Domingos y Feriados.

- Time: Se asignará el número uno al horario laboral y dos al horario no laboral. Se define horario laboral desde las 09:00 horas a las 18:00 horas. Se define horario no laboral desde las 18:01 horas a las 08:59 horas.

- User: se ordenan los valores del campo "User" de menor a mayor y se asignará a cada uno de ellos un número secuencial comenzando en uno.

- Computer: se ordenan los valores del campo "Computer" de menor a mayor y se asignará a cada uno de ellos un número secuencial comenzando en uno.

Ejemplo:

Datos generados en un Servidor:

Event ID:	673	565	565
Date:	17/08/2007	17/08/2007	18/08/2007
Time:	16:30	21:23	19:30
User:	Administrador	Manager	Administrador
Computer:	Labsiddc1	Labsiddc2	Labsiddc1

Tabla 4-10. Ejemplo Datos sin Transformar.

Datos luego de la transformación:

Event ID:	2	1	1
Date:	1	1	2
Time:	1	2	2
User:	1	2	1
Computer:	1	2	1

Tabla 4-11. Ejemplo Datos Transformados.

Posteriormente al agrupamiento de datos con la Red Neuronal, se procesarán los eventos con un Árbol de Decisión. En esta instancia será necesario construir un nuevo atributo que le llamaremos "Semáforo" y se usará como "Clase" en el Árbol de Decisión. La misma permitirá clasificar cada cluster de la Red Neuronal, según contenga eventos normales (afín con la luz verde del semáforo),

dudosos (afín con la luz amarilla del semáforo) o fraudulentos (afín con la luz roja del semáforo).

Este nuevo atributo no podrá tener ningún valor faltante y debe haber al menos dos valores para cada Clase.

La clasificación de los registros se estipulará según el siguiente razonamiento:

Se utilizará la cantidad de observaciones de cada cluster que arroja SOM en la solapa *Output* del archivo de salida. Se entiende que cuanto mayor sea el número de observaciones de un cluster mayor es la diversidad de tareas realizadas por los administradores lo que implica que son acciones habituales y normales. En cambio si SOM agrupa pocas observaciones en un grupo, la cantidad de tareas distintas es baja lo que da a suponer que puede tratarse de una acción dudosa.

Por lo tanto para definir la categoría de los clusters o grupos, se sigue la siguiente lógica:

- Si la cantidad de observaciones del grupo es menor al N_a% del total de observaciones procesadas por SOM se considera que el cluster tiene observaciones fraudulentas.
- Si la cantidad de observaciones del grupo varía entre N_b% y N_c% del total de observaciones procesadas por SOM se considera que el cluster tiene observaciones dudosas.
- Si la cantidad de observaciones del grupo es mayor a N_d% del total de observaciones procesadas por SOM se considera que el cluster tiene observaciones normales.

El valor N_i se definirá durante la ejecución práctica del modelo en base a cada muestra de datos en particular.

4.1.3.4 Integrar los datos

La integración consiste en congregar los archivos de eventos de seguridad de múltiples servidores controladores de dominios. Debido a la naturaleza de los datos contenidos en estas fuentes y a las características de las mismas (poseen los mismos atributos y tipos de datos), no se perciben problemas para la unión de los mismos en un único archivo.

El campo “Computer” podrá utilizarse para distinguir la fuente de datos de entrada. Este campo es opcional ya que depende del número de fuentes de datos.

4.1.3.5 Formato de los datos

Atendiendo los requerimientos del orden de los atributos de entrada de las herramientas de modelado, no se requieren modificaciones en los mismos, pueden ser ingresados indistintamente. Solo, para mayor comprensión se define ordenar los atributos de la siguiente manera:

Para la herramienta de Red Neuronal:

Date, Time, User, Event ID, Computer [opcional]

Para la herramienta de Árbol de Decisión:

Class, Date, Time, User, Event ID, Computer [opcional]

4.1.4 Modelado

4.1.4.1 Seleccionar la Técnica de Modelado

4.1.4.1.1 Técnicas de Modelado

Se utilizarán dos técnicas de modelado. La primera de ellas será una Red Neuronal de Mapas Autoorganizados (SOM – Self Organized Map) y la segunda será un Árbol de Decisión que aplica el algoritmo de inducción C4.5.

4.1.4.1.2 Supuestos de Modelado

Red Neuronal de Mapas Autoorganizados

- Todas las variables a usar en la clasificación deben estar en formato numérico. Las que no cumplan con este requisito serán consideradas valores perdidos. La aplicación podría reemplazarlas por algún dato de la misma columna.
- Mientras el mapa se entrena, los datos de las variables se actualizan de manera que cada valor de las variables se transforman en –1 y 1. Esto es los que se llama normalización de los datos. Este proceso puede ser muy largo, en especial en bases de datos con muchas observaciones y variables.
- No debe haber filas o columnas con datos en blanco. Las variables que se usan para clasificar deben estar en formato numérico.
- Los datos que no están en formato numérico serán considerados como datos perdidos y serán reemplazados por un valor de la misma columna.

Árbol de Decisión con Algoritmo de Inducción C4.5

- La variable de tipo "Class", no puede contener valores nulos.
- Cualquier dato de tipo no numérico en una columna de tipo "Cont", será considerado como un valor perdido; y la aplicación lo reemplazará por la media de la columna.
- Cualquier celda en blanco o con error de Excel, en una columna de tipo "Cat", será considerado como un valor perdido; la aplicación lo reemplazará por el valor de mayor frecuencia de ocurrencia en la misma columna.
- Debe haber como mínimo dos observaciones por cada columna tipo "Cat". Si hay sólo una se debe, o bien eliminar la observación o renombrar la categoría hacia otra de la misma columna.

4.1.4.2 Generar Diseño de Pruebas

Del Dataset disponible de datos se usarán el 60% para las pruebas y el 40% restante para la validación.

Las pruebas a realizar son las siguientes:

- Cargar los datos en la Red Neuronal. Entrenar la red y verificar si los clusters logran estabilizarse.
- Verificar si los datos de los clusters de la red entrenada son representativos de un patrón de comportamiento.
- Verificar si es coherente la clasificación de los cluster utilizando el número de observaciones que agrupa cada uno de ellos. La clasificación consiste en definir si el cluster contiene observaciones Normales, Sospechosas o Fraudulentas.
- Cargar los datos de salida de la Red Neuronal en el Árbol de Decisión y verificar la calidad de las Reglas de Decisión producidas.
- Procesar eventos con las Reglas de Decisión y verificar la tasa de error en la inferencia del tipo de observación.

En el documento de pruebas se asentarán las pruebas realizadas, los requisitos para cada prueba, los objetivos de la prueba, las salidas esperadas y las salidas reales de cada una de ellas.

4.1.4.3 Construir el Modelo

4.1.4.3.1 Parámetros de las Herramientas

Red Neuronal de Mapas Autoorganizados

Hoja "Input"

En esta hoja se ingresar los parámetros de configuración (figura 4-4) del funcionamiento del algoritmo. Estos datos deben ser consistentes con los ingresados en la hoja "Data".

- Número de observaciones/ registros: se definirá durante la ejecución práctica del modelo en base a cada muestra de datos en particular.
- Número de variables / columnas / campos: Valor entre 3 y 50. Se define el valor 4 para esta opción. Se podrá ajustar dependiendo de las necesidades prácticas.
- Las dimensiones del mapa: Valor, entre 2 y 100, que será elevado a la potencia 2 (dos) para obtener el total de neuronas del mapa. Se define el valor 4 para esta opción. Se podrá ajustar dependiendo de las necesidades prácticas.
- Número de ciclos de entrenamiento de la red: Entre 1 y 1000. Se define el valor 10 para esta opción.
- Parámetros de aprendizaje de la red: Valor inicial y final de aprendizaje, no debe ser mayor a 0 y menor que 1. Además se debe incorporar la forma del decrecimiento de la red (Exponencial o Lineal). Se definen los valores 0.9, 0.1 y Exponential para estas opciones.
- Valor de Sigma para la vecindad Gaussiana, como porcentaje del ancho del mapa: Valor inicial y final, además la forma de decrecimiento (Exponencial o Lineal). Se definen los valores 50%, 1% y Exponential para estas opciones.

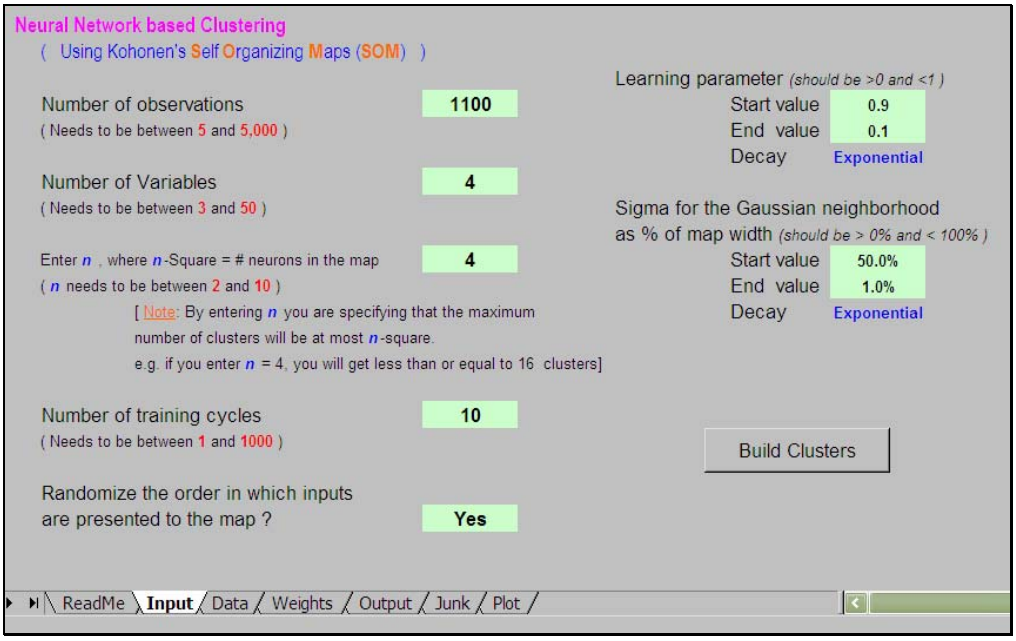


Figura 4-4. Ventana de Configuración de la Red Neuronal.

Hoja "Data"

En esta hoja se ingresan los datos de la base de datos.

Esta hoja contiene:

- Los datos deben ingresarse a partir de la celda C13.
- Las observaciones deben ubicarse en filas y las variables en columnas.
- Por cada columna se debe elegir el tipo apropiado: ("Use" u "Omit")
- Si se quiere que el proceso de clasificación excluya a alguna columna se debe selecciona la opción = "OMIT"
- Si se quiere incluir la columna en la clasificación, se debe elegir = "USE"
- Se pueden ingresar un máximo de 50 variables de clasificación. El aplicativo automáticamente tratará a todas las variables como continuas.
- Debe asegurarse que el número de variables ingresadas en la hoja "Input" sea la misma cantidad de columnas ingresadas en la hoja "Data" de tipo = "USE".
- Debe asegurarse que el número de observaciones ingresados en la hoja "Input" sea igual o menor a las filas ingresadas en la hoja "Data".
- No puede haber filas o columnas en blanco.

- Todas las variables a usar en la clasificación deben estar en formato numérico. Las que no cumplan con este requisito serán consideradas valores perdidos. La aplicación podría reemplazarlas por algún dato de la misma columna.

Árbol de Decisión con Algoritmo de Inducción C4.5

Hoja "Data"

En esta hoja se debe ingresar los datos a procesar.

- El ingreso datos se debe realizar en la hoja "Data", empezando por la celda L24. Los nombres de variables se deben ingresar en la fila 23. Los tipos de variables se especifican en la fila 21.

- Se pueden ingresar un total de filas entre 10 y 10.000.

- Las observaciones deben ubicarse en filas y las variables en columnas.

- Debe elegirse en cada columna el Tipo apropiado (Omit, Class, Cont, Cat). Si se quiere excluir la columna se debe seleccionar "Omit". Para que la columna funcione como categoría de predicción se debe seleccionar "Cat". Para que la columna funcione como predicción continua, se debe seleccionar "Cont". Para que la columna funcione como variable de clase, se debe seleccionar "Class". Se puede tener un máximo de 50 variables. Debe haber sólo una clase, veinte como máximo de tipo "Cat", incluida la de tipo "Class".

- No debe haber filas o columnas en blanco.

- La variable de tipo "Class", no puede contener valores nulos.

- Cualquier dato de tipo no numérico en una columna de tipo "Cont", será considerado como un valor perdido; y la aplicación lo reemplazará por la media de la columna.

- Cualquier celda en blanco o con error de Excel (aplicación usada para desarrollar el algoritmo), en una columna de tipo "Cat", será considerado como un valor perdido; la aplicación lo reemplazará por el valor de mayor frecuencia de ocurrencia en la misma columna.

- La aplicación es insensitivo a mayúsculas y minísculas en los nombres de las columnas. Todos serán tratados como misma categoría.

- Debe haber como mínimo dos observaciones por cada columna tipo "Cat". Si hay sólo una se debe, o bien eliminar la observación o renombrar la categoría hacia otra de la misma columna.

Hoja "User Input"

Las opciones de configuración se pueden apreciar en la figura 4-5.

- Criterios para partición de nodos:

    - Ajuste # categorías para un predictor de categorías: Cuando el nodo se divide, el algoritmo tiende a preferir predictores con más categorías. Esto puede ser activado, indicado el estado ON en la casilla correspondiente. Se selecciona OFF para esta opción.

- Criterios de ramificación: A medida que el árbol se va desarrollando, termine o no de ramificarse un nodo y se declare al nodo como un nodo hoja, puede ser determinado por los siguientes criterios. Se puede no elegir ningún criterio, uno o varios. Si no se elige ningún criterio, la aplicación usa los valores por defecto.

    - Tamaño mínimo del nodo (Valor por defecto = 5 registros). El nodo no se ramifica más si el número de registros en el nodo es = (porcentaje a ingresar) o menor al número total de registros. Se selecciona OFF para esta opción.

    - Nivel máximo de pureza (Valor por defecto = 100% de pureza). El nodo no se ramifica más si el valor de pureza es = (porcentaje a ingresar) o mayor. (Por ejemplo si la pureza es del 90 % significa que ese porcentaje de registros en el nodo pertenecen en un 90 % a la clase mayoritaria). Se selecciona OFF para esta opción.

    - Nivel máximo de profundidad (Valor por defecto = 20 es el máximo nivel de profundidad). El nodo no se ramifica más si el valor de la profundidad es = (valor a ingresar) o mayor. (El nodo raíz tiene profundidad 1. Cualquier nodo dependiente es igual a la profundidad de su nodo padre + 1). Se selecciona OFF para esta opción.

Si para algún predictor, los valores son idénticos para todos los registros del nodo, entonces ese predictor puede ser usado para ramificar el nodo. Aunque si esto sucede para todos los predictores del nodo, este nodo no podrá de ningún modo ser ramificado.

- Opciones de poda del árbol: Luego que el árbol se ha desarrollado, se puede seleccionar la posibilidad de realizar una poda (Si o No). Se selecciona YES para esta opción.

- Entrenamiento / Configuración de prueba: Se debe seleccionar si:

  - Se usan todos los datos para el entrenamiento, o se usa una parte de los datos: En el caso que se opte por usar una parte de los datos, se debe indicar la forma de seleccionar la configuración de la validación. Se puede elegir la opción 1 o la 2. La opción 1: Selecciona de manera aleatoria un porcentaje (valor a ingresar entre 1% y 50%) de datos como datos de prueba. La opción 2: Usa las últimas (valor a ingresar) filas de datos como datos de validación. Se selecciona Opción 1 y 20.

- Guardar el modelo en una hoja separada? (Ingresar Si o No). Se selecciona YES para esta opción.

- Opciones para generación de reglas. Ingresar si se desea generar reglas (Si o No). Se selecciona YES para esta opción.

- Opciones para limpieza de reglas:

  - Mínima confidencia (Valor por defecto = 50 %). No se genera reglas con confidencia = (porcentaje a ingresar) o menor. Se selecciona OFF para esta opción.

  - Máximo soporte (Valor por defecto = 0 %) No se genera reglas con soporte = (porcentaje a ingresar) o menor. Se selecciona OFF para esta opción.

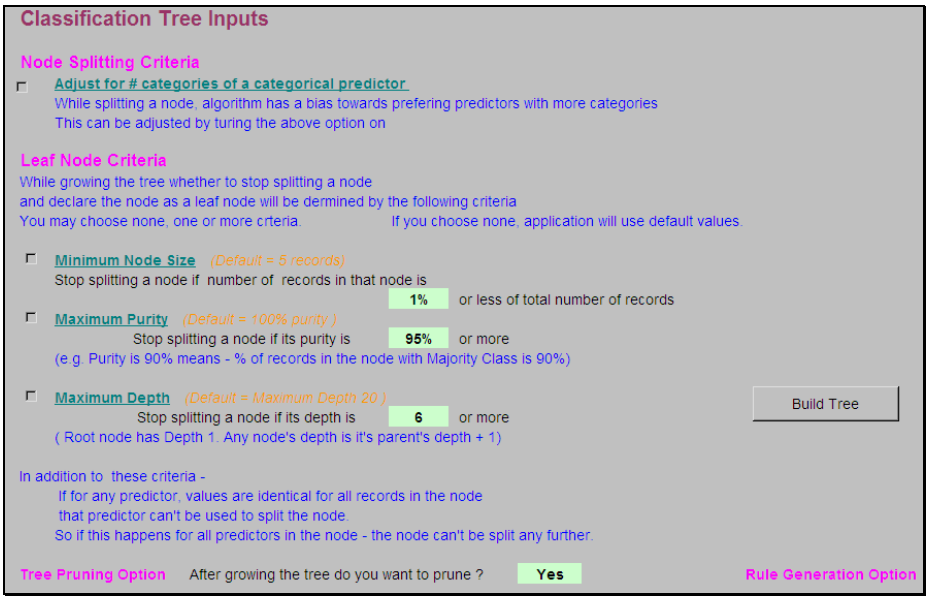


Figura 4-5. Ventana de Configuración del Árbol de Decisión.

4.1.4.3.2 Modelos Obtenidos

Red Neuronal de Mapas Autoorganizados

Al ejecutar la técnica sobre un dataset de entrada específico, se obtiene el modelo de la figura 4-6, la información estadística de la figura 4-7 y el mapa de radar, que representa el significado de las variables en función de los clusters obtenidos, de la figura 4-8.

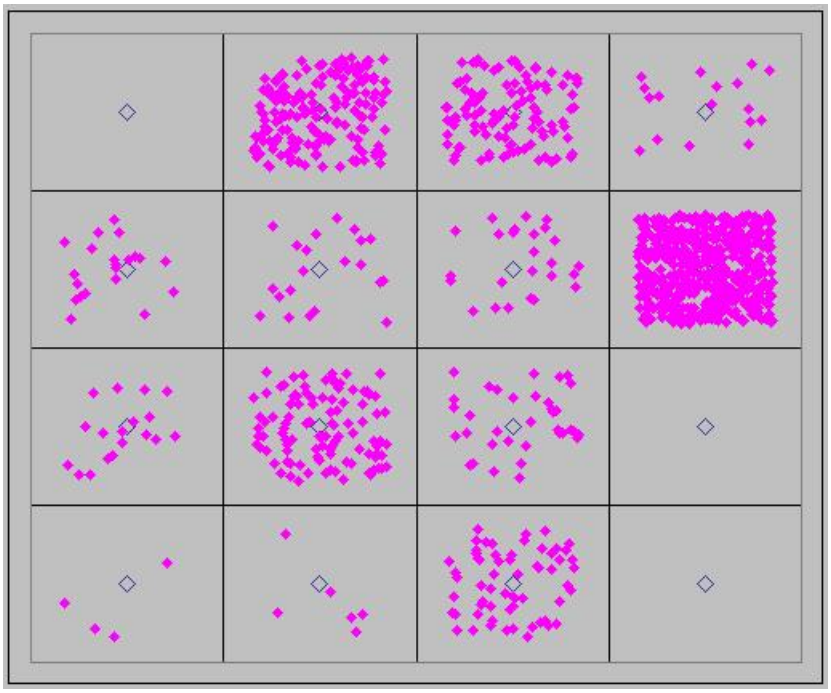


Figura 4-6. Distribución de las observaciones en los Clusters.

Cluster Sizes

	Cluster 1	Cluster 2	Cluster 3	Cluster 4	Cluster 5	Cluster 6	Cluster 7	Cluster 8	Cluster 9	Cluster 10	Cluster 11	Cluster 12	Cluster 13
	4	18	21	6	103	21	168	61	35	25	107	514	17

Cluster Position on the grid

	Cluster 1	Cluster 2	Cluster 3	Cluster 4	Cluster 5	Cluster 6	Cluster 7	Cluster 8	Cluster 9	Cluster 10	Cluster 11	Cluster 12	Cluster 13
Row	1	1	1	2	2	2	2	3	3	3	3	4	4
Column	1	2	3	1	2	3	4	1	2	3	4	3	4

Cluster Means

	Overall	Cluster 1	Cluster 2	Cluster 3	Cluster 4	Cluster 5	Cluster 6	Cluster 7	Cluster 8	Cluster 9	Cluster 10	Cluster 11	Cluster 12	Cluster 13
Dia	1.1	1.0	1.0	2.0	1.0	1.0	1.0	1.0	1.0	2.0	1.0	1.0	1.0	2.0
Horario	1.1	2.0	2.0	2.0	2.0	1.0	2.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
Usuario	8.3	2.5	9.4	10.7	5.8	2.5	11.8	11.2	9.8	10.1	12.7	2.6	8.9	6.4
Evento	2.1	3.0	1.1	2.0	3.5	3.6	2.2	3.2	4.0	3.2	1.3	1.6	1.2	1.0

Cluster Variances

	Overall	Cluster 1	Cluster 2	Cluster 3	Cluster 4	Cluster 5	Cluster 6	Cluster 7	Cluster 8	Cluster 9	Cluster 10	Cluster 11	Cluster 12	Cluster 13
Dia	0.1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Horario	0.1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Usuario	11.9	0.3	0.6	21.1	0.2	1.6	7.2	2.0	1.1	6.7	0.2	0.4	2.9	12.0
Evento	1.3	0.0	0.1	2.4	1.5	0.2	0.8	0.2	0.0	1.0	0.2	0.2	0.2	0.0

Figura 4-7. Información estadística de cada Cluster.

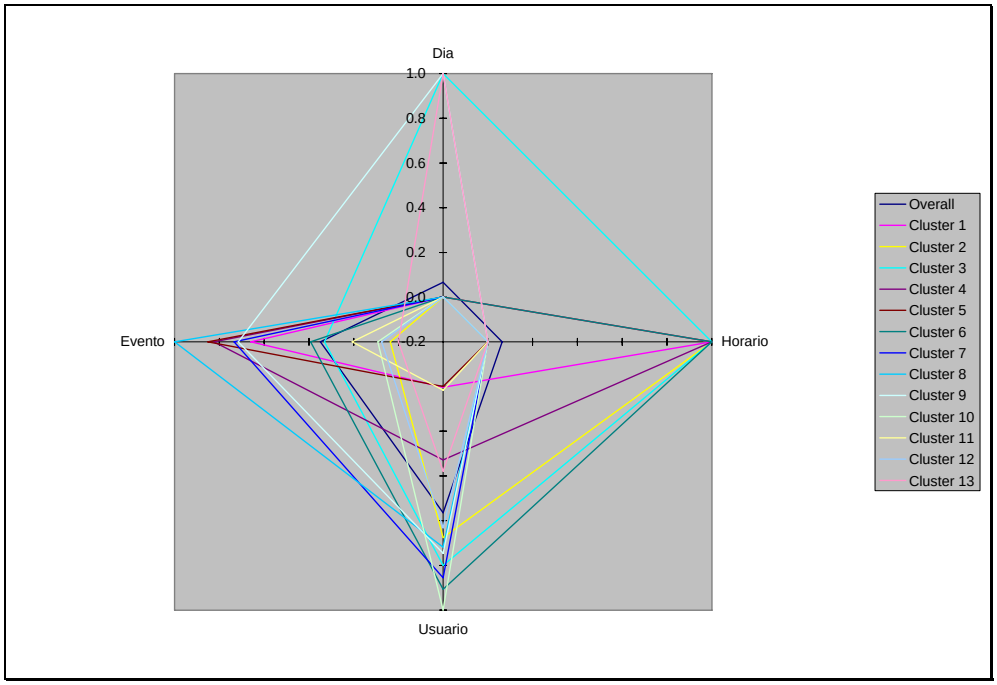


Figura 4-8. Gráfico de tipo radar.

Mientras el mapa se entrena, los datos de las variables se actualizan de manera que cada valor se transforma en –1 y 1. Esto es los que se llama normalización de los datos. Este proceso puede ser muy largo, en especial en bases de datos con muchas observaciones y variables.

Si se entrena la red con los mismos datos en dos veces sucesivas, se puede cancelar la normalización en la segunda vuelta. La aplicación preguntará si se quiere cancelar esta normalización o no. Cancelar esta tarea ahorra mucho tiempo. La aplicación siempre se ocupará de chequear el número de filas y columnas en los datos para determinar si ésta ha cambiado desde la última vez que se la ejecutó. No chequea los datos individuales de la hoja "Data". De manera que si se está seguro de que los datos han cambiado desde la última vez que se corrió el algoritmo, se debe nuevamente normalizar los datos.

Si se está entrenando la red con las mismas variables y con las mismas dimensiones de mapa, respecto de la última vez que se corrió, la aplicación preguntará si se quiere comenzar con los pesos obtenidos en el anterior procesamiento. El comenzar con los pesos obtenidos anteriormente aporta incrementos en el aprendizaje. Ésta opción permite resguardar los aprendizajes que se fueron acumulando. Si en cambio los datos se han cambiado, se debe volver a configurar las variables junto con su orden de procesamiento para poder reasignar valores a los pesos.

Los resultados pueden observarse en la hoja "Output". Los datos son de sólo lectura, ya que la planilla está protegida para evitar modificaciones.

La aplicación ofrece la posibilidad de guardar los resultados en una planilla aparte para que el usuario tenga la posibilidad de poder editar sus resultados.

En esta planilla se pueden guardan los datos procesaros por el algoritmo, el cluster asignado a cada observación, y los pesos. Además un gráfico será creado para permitir una comparación visual de los resultados de las variables que atraviesan los diferentes clusters.

En la hoja "Weights", un gráfico dará una representación visual de las observaciones que hay en cada porción del mapa.

Árbol de Decisión con Algoritmo de Inducción C4.5

Al ejecutar el Árbol sobre un dataset de entrada específico se obtienen las siguientes Reglas de Decisión:

```
Rule0          Clust. ID = verde

Rule1    IF    Evento = 5
         THEN  Clust. ID = verde

Rule2    IF    Evento = 6
         THEN  Clust. ID = verde

Rule3    IF    Evento = 7
         THEN  Clust. ID = verde

Rule4    IF    Evento = 9
         AND   Horario = 1
         THEN  Clust. ID = verde

Rule5    IF    Evento = 10
         AND   Horario = 1
         THEN  Clust. ID = verde

Rule6    IF    Evento = 11
         THEN  Clust. ID = verde

Rule7    IF    Evento = 13
         AND   Horario = 1
         THEN  Clust. ID = amarillo

Rule8    IF    Evento = 18
         THEN  Clust. ID = verde

Rule9    IF    Evento = 2
         AND   Horario = 2
         THEN  Clust. ID = rojo
```

```
Rule10   IF    Evento = 3
         AND   Horario = 2
         THEN  Clust. ID = rojo

Rule11   IF    Horario = 2
         THEN  Clust. ID = amarillo

Rule12   IF    Evento = 6
         AND   Horario = 2
         THEN  Clust. ID = rojo

Rule13   IF    Evento = 15
         THEN  Clust. ID = amarillo

Rule14   IF    Evento = 16
         THEN  Clust. ID = amarillo

Rule15   IF    Evento = 17
         THEN  Clust. ID = amarillo

Rule16   IF    Horario = 1
         THEN  Clust. ID = verde

Rule17   IF    Dia = 1
         THEN  Clust. ID = verde

Rule18   IF    Dia = 2
         AND   Evento = 4
         THEN  Clust. ID = amarillo

Rule19   IF    Evento = 12
         AND   Horario = 1
         AND   Usuario = 2
         THEN  Clust. ID = amarillo

Rule20   IF    Usuario = 3
         THEN  Clust. ID = verde

Rule21   IF    Evento = 12
         THEN  Clust. ID = verde
```

Rule Summary Table # Rules 21

Rule ID	Class	Length	Support	Confidence	Capture
0	verde	0	100.0%	90.6%	100.0%
1	verde	1	0.7%	87.5%	0.7%
2	verde	1	2.8%	83.3%	2.5%
3	verde	1	0.5%	80.0%	0.4%
4	verde	2	18.3%	100.0%	20.2%
5	verde	2	36.5%	100.0%	40.3%
6	verde	1	0.6%	83.3%	0.5%
7	amarillo	2	1.7%	100.0%	19.6%
8	verde	1	0.2%	100.0%	0.2%
9	rojo	2	0.2%	100.0%	20.0%
10	rojo	2	0.2%	100.0%	20.0%
11	amarillo	1	6.4%	85.7%	65.2%
12	rojo	2	0.5%	100.0%	50.0%
13	amarillo	1	0.2%	100.0%	2.2%
14	amarillo	1	0.2%	100.0%	2.2%
15	amarillo	1	0.4%	75.0%	3.3%
16	verde	1	93.6%	96.9%	100.0%
17	verde	1	94.2%	92.8%	96.5%
18	amarillo	2	0.6%	100.0%	6.5%
19	amarillo	3	0.6%	100.0%	7.6%
20	verde	1	19.2%	91.4%	19.3%
21	verde	1	9.8%	92.5%	10.0%

Figura 4-9. Información estadística de cada Regla de Decisión.

Las reglas se generan luego de que el árbol se desarrolló. La aplicación sólo genera reglas. La tabla que contiene la información estadística (figura 4-9) de las reglas informa acerca de la calidad individual de cada una. La calidad se mide según tres métricas que a continuación se explican.

- SOPORTE: es el porcentaje de datos de entrenamiento que justifican como verdadera la parte izquierda de la regla. Si para una determinada observación, la parte izquierda de la regla es verdadera, decimos que esta es la regla aplicable a dicha observación. La medida está dada por la cantidad de observaciones sobre las que se aplica la regla.

- CONFIDENCIALIDAD: fuera de los registros de entrenamiento para los cuales la parte izquierda de la regla es verdadera, existe un porcentaje de registros para los cuales la parte derecha de la regla también es verdadera. En otras palabras, representa el porcentaje de observaciones para la cual la regla es aplicable, es decir para la cual la regla es verdadera. La medida está dada por el alcance de la regla.

- REPRESENTATIVIDAD: es el porcentaje de registros de cada clase que fueron correctamente capturados por la regla. Esto lleva a una reflexión acerca de la estructura del problema. Si existe una regla que captura el 100% del total, esto significa que en el espacio de predicción, todas las observaciones de esta clase cierran entre sí y que la regla está habilitada para captar correctamente la parte el espacio de predicción.

A continuación se pueden observar los totales obtenidos y la interpretación de los resultados para una regla.

Clases	*Verde*	*Amarillo*	*Rojo*	*Total*
OBS	988	102	10	1090
Regla 4	200	0	0	200
	Verde	***Amarillo***	***Rojo***	***Total***
	Resultados	***Valores***	***Fórmulas***	
	Confianza	100%	200*100/200	
	Captura	20,2%	200*100/988	
	Soporte	18,3%	200*100/1090	

Tabla 4-12. Información de Regla.

La regla 4 afecta a un total de 200 observaciones de las 1090 que fueron procesadas. Las 200 afectan a la clase "Verde" y ninguna a las clases "Amarillo" o "Rojo". Con estos datos pueden evaluarse la confianza, el porcentaje de captura, y la cantidad de observaciones que soporta la regla respecto del total.

La confianza, esta dada por la relación que existe entre la totalidad de las observaciones que fueron afectados por la regla (200) y la cantidad de observaciones que fueron afectadas por la clase mayoritaria (200) con esta misma regla. Para este caso la confianza es del 100 %.

El porcentaje de captura, esta dado por la relación que existe entre la cantidad de observaciones de la clase mayoritaria que fueron afectadas por esta regla (200) y la cantidad total de observaciones procesadas pertenecientes a esta misma clase (988). Para este caso el resultado es del 20,2%.

La cantidad de observaciones que soporta la regla, esta dada por la relación que existe entre la totalidad de las observaciones que afecta la regla (200) y la totalidad de observaciones procesadas (1090). El resultado es del 18,3%.

4.1.4.4 Evaluar el Modelo

Durante la fase de evaluación de los modelos se tienen presente los siguientes criterios:

Red Neuronal

- Capacidad de la red para distribuir los eventos en los clusters.
- Velocidad de aprendizaje de la red neuronal.
- Posibilidad de categorizar los clusters acorde a las observaciones que contienen.

Árbol de Decisión

- Calidad de las reglas producidas.
- Velocidad del Árbol de Decisión para generar las reglas.
- Soporte y Confianza de cada regla de decisión.

4.1.4.4.1 Análisis de los Modelos

Red Neuronal de Mapas Autoorganizados

Se evaluó el modelo utilizando distinta cantidad de variables. Usando tres (Día, Hora, Usuario), cuatro (Día, Hora, Usuario, Evento) y cinco variables (Día, Hora, Usuario, Evento, Equipo). Finalmente se decidió trabajar con cuatro variables (Día, Hora, Usuario, Evento) descartando "Equipo" en el presente estudio porque los ensayos se realizan en el entorno de laboratorio donde se cuenta solo con un servidor controlador de dominio.

Para el caso del tamaño del mapa se utilizaron matrices cuadradas de dos por dos, tres por tres y cuatro por cuatro celdas. Se decidió utilizar mapas de cuatro por cuatro celdas debido a que la Red Neuronal realizó mejor la distribución de las observaciones. No se descarta realizar la experiencia con un mapa de cinco por cinco celdas, la desventaja es el mayor tiempo de ejecución y la cantidad de iteraciones que le lleva a Red estabilizarse.

El número de ciclos de entrenamiento se varío entre 10 y 100. No se observaron cambios significantes en la Red por lo tanto se definió en 10.

El orden en el cual las observaciones se presentan en la red se varío entre aleatorio y no aleatorio. No se observaron cambios significantes en la Red.

Para categorizar los clusters según las observaciones que contiene cada uno de ellos se utiliza la cantidad de observaciones de cada cluster que arroja SOM en la solapa *Output* del archivo de salida. Se entiende que cuanto mayor sea el número de observaciones de un cluster mayor es la diversidad de tareas realizadas por los administradores lo que implica que son acciones habituales y normales. En cambio si SOM agrupa pocas observaciones en un grupo, la cantidad de tareas distintas es baja lo que da a suponer que puede tratarse de una acción dudosa. No se usa la Varianza o la Media de cada grupo, que arroja SOM, porque estamos manejando datos categóricos y las anteriores medidas son continuas.

Por lo tanto para definir la categoría de los clusters o grupos, se sigue y ratifica la siguiente lógica:

- Si la cantidad de observaciones del grupo es menor al N_a% del total de observaciones procesadas por SOM se considera que el cluster tiene observaciones fraudulentas.

- Si la cantidad de observaciones del grupo varía entre N_b% y N_c% del total de observaciones procesadas por SOM se considera que el cluster tiene observaciones dudosas.

- Si la cantidad de observaciones del grupo es mayor a N_d% del total de observaciones procesadas por SOM se considera que el cluster tiene observaciones normales.

El valor N_i se define durante la ejecución práctica de cada muestra de datos.

Árbol de Decisión con Algoritmo de Inducción C4.5

Durante la producción de las reglas se decidió no filtrar las que poseían un soporte bajo (menor a un determinado porcentual). Justamente la particularidad de las observaciones que se pretenden detectar, poseen un soporte muy bajo.

La velocidad de construcción del Árbol y de las Reglas de Decisión fue considerablemente rápido.

4.1.5 Evaluación

4.1.5.1 Evaluar el modelo

4.1.5.1.1 Red Neuronal de Mapas Autoorganizados

En esta hoja "Weights" se puede visualizar los cluster (familias o grupos) obtenidos, luego de ejecutar la red. Las observaciones se van ubicando en cada cluster a medida que la aplicación se está ejecutando.

La hoja "Output" informa:

- El número de variables usadas para clasificar.
- El número de observaciones usadas para clasificar.
- Cantidad de grupos (clusters).
- Tabla "Cluster Assignment" (Asignación de clusters): Muestra por cada observación, (representada por una ID) el número de cluster asignado.
- Tabla "Clusters Size" (Tamaño de los clusters): Muestra la cantidad de observaciones encontradas en cada uno de los clusters o grupos.
- Tabla "Cluster Position on the grid" (Posición de cada cluster dentro de la grilla): Tabla de doble entrada donde se indica el número de fila y de columna que le corresponde a cada cluster.
- Tabla "Cluster Means" (Promedio de los clusters): Tabla de doble entrada donde se indica los valores promedio para la totalidad de los datos, y para cada uno de los clusters.
- Tabla "Cluster Variances" (Varianza de los clusters): Tabla de doble entrada donde se indica la varianza para la totalidad de los datos y para cada uno de los clusters.

En la hoja "RadarPlot" se presenta la imagen de un gráfico de radar que representa el significado de las variables en función de los clusters obtenidos. En los ejes del gráfico de radar, se reflejan las variables. La aproximación al centro del gráfico significa que esa variable tiene mayor peso que la variable que se aleja del centro.

Como se comentó anteriormente, se entiende que cuanto mayor sea el número de observaciones de un cluster mayor es la diversidad de tareas realizadas por los administradores lo que implica que son acciones habituales y normales. En

cambio si SOM agrupa pocas observaciones en un grupo, la cantidad de tareas distintas es baja lo que da a suponer que puede tratarse de una acción dudosa. Para este último caso, puede ocurrir que la tarea esté relacionada con una acción correcta pero se realice con poca frecuencia. Este asunto queda a juicio del personal encargado de la revisión.

Como conclusión de la evaluación se puede inferir que el modelo propuesto debe contener una elevada cantidad de observaciones como entrada en la Red Neuronal, cubriendo todos los días de la semana, fin de semana y feriados, observaciones de acciones correctas e incorrectas (no permitidas), de modo que la red tenga suficiente información para entrenarse.

4.1.5.1.2 Árbol de Decisión con Algoritmo de Inducción C4.5

En la hola "Result" se visualizan los resultados de árbol que generó el modelo:

- Número de observaciones para el entrenamiento
- Número de observaciones de prueba
- Número de predictores.
- Nombre de la clase variable.
- Número de clases
- Clase mayoritaria
- Porcentaje no clasificado, cuando la clase mayoritaria es usada como clase predictiva.
- Información del árbol
- Número total de nodos.
- Número total de nodos hoja.
- Cantidad de niveles
- Porcentaje no clasificado
- En los datos de entrenamiento
- En los datos de prueba
- Tiempo utilizado

- En el procesamiento de datos
- En el desarrollo del árbol
- En la poda del árbol
- En el diseño del árbol
- En la clasificación utilizando el árbol final
- En la generación de reglas.
- Tiempo Total
- Matriz de confusión
- Datos de entrenamiento: Tabla de doble entrada con los resultados obtenidos en el entrenamiento a partir de las clases predictivas.
- Datos de prueba: Tabla de doble entrada con los resultados obtenidos a partir de las clases predictivas en la prueba

La longitud de la regla representa la cantidad de clases que requiere la regla para generar un resultado.

Como conclusión de la evaluación se puede deducir que el modelo propuesto genera reglas que luego se aplican a las mismas observaciones. Esta situación puede presentarse porque hay reglas que tienen una longitud de regla pequeña y solo evalúan una sola variable, lo cual las convierte en muy genéricas.

4.1.5.2 Proceso de revisión

El proceso de exploración de información realizado es el siguiente:

- Descargar los eventos de seguridad de los dispositivos de red que se quieren analizar.
- Transformar los datos para que puedan ser usados en los modelos de minería de datos seleccionados.
- Cargar los datos convertidos en la Red Neuronal de Mapas Autoorganizados, definir su configuración y comenzar con el entrenamiento de la misma hasta que se considera que la red ha aprendido y está estabilizada (momento en el cual los cambios en los valores de los pesos son menores a un valor definido o se alcanza un

máximo predefinido de iteraciones). Al final esta fase obtenemos las observaciones agrupadas en clusters.

- Clasificar cada cluster según contenga eventos normales, dudosos o fraudulentos. Para realizar esta clasificación se utiliza la cantidad de observaciones de cada cluster que arroja SOM en la solapa *Output* del archivo de salida.

- En el archivo de salida de SOM, en la solapa Data, se reemplaza el Número de Cluster por la categoría asignada al mismo. Finalmente, la información contenida en esta solapa se utilizará como datos de entrada en un Árbol de Decisión para producir las reglas de decisión que evaluaran los nuevos eventos.

- Cargar los datos de salida de la Red Neuronal en el Árbol de Decisión, definir su configuración y ejecutar el algoritmo para generar las reglas de decisión. Al final esta fase obtenemos las reglas con el porcentual de Soporte y Confianza que le corresponde a cada de ellas. Al concluir el proceso de producción de las reglas de decisión, las mismas serán la base del mecanismo decisor principal que utilizará la herramienta Kappa-PC para analizar los nuevos eventos a monitorear.

Restricciones de la solución propuesta

La solución propuesta se orienta básicamente, en el análisis de las acciones que realizaron los administradores de redes, tomando patrones de comportamiento de los mismos y la frecuencia de repetición de las observaciones. Un caso que no sería detectado es aquel en el cual el administrador siempre realiza muchas acciones fraudulentas del mismo tipo, ya que su patrón de comportamiento tendría una alta frecuencia de repetición de las mismas tareas.

Otra restricción se presenta porque los patrones obtenidos de la red neuronal son estáticos, con lo que si la forma de proceder de los administradores de red de la empresa cambia drásticamente, será necesario volver a entrenar la red SOM para que produzca nuevos clusters de comportamiento.

Mejoras a la solución propuesta

Como se comentó en el apartado anterior, se detectaron ocasiones en que una misma observación es procesada por varias reglas de decisión. Esto sucede cuando las reglas tienen una corta longitud entonces cubren un amplio rango de sucesos.

Para mitigar estas situaciones, se consideraron dos soluciones.

La primera de ellas sería utilizar una matriz más grande para la red neuronal, durante el agrupamiento de las observaciones, las mismas podrán ser distribuidas en más grupos. Como resultado tendremos mayor precisión y familias con sucesos más análogos. Finalmente, obtendremos Reglas de Decisión menos globales y más exactas. La desventaja de ampliar el número de grillas de la SOM es la mayor cantidad de tiempo de procesamiento que requiere para entrenarla y producir su salida.

La segunda solución, es darle a cada regla un orden de prioridad. Las rojas tendrán mayor prioridad que las amarillas y éstas mayores que las verdes. Cuando una regla aplica a un registro entonces se pasará al siguiente evento evitando así que se aplique más de una regla a cada uno de ellos.

4.1.5.3 Determinar los próximos pasos

Considerando:

- La propuesta de mejora de la solución.
- Que los recursos de procesamiento disponibles en el equipo que se utiliza en el proyecto son suficientes.
- Que refinar el modelo aportará beneficios considerables.

Se recomienda:

- Desarrollar el procedimiento de minería de datos descrito en las secciones anteriores.
- Asignarle a cada regla un orden de prioridad. Las rojas tendrán mayor prioridad que las amarillas y éstas mayores que las verdes. Cuando una regla aplica a un registro entonces se pasará al siguiente evento evitando así, que múltiples reglas apliquen sobre un mismo evento.

4.1.6 Implementación

4.1.6.1 Plan de Implementación

Los resultados a implementar serán las Reglas de Decisión obtenidas a la salida del Árbol de Decisión utilizado. Los nuevos eventos serán procesados por estas Reglas.

Los conocimientos, resultados, experiencias del proyecto serán transferidas al sector usuario en un entregable impreso y además se expondrán en una reunión donde se explicarán los detalles de las conclusiones y se evacuarán las dudas y consultas que surjan.

El modelo resultante se implementará en primera instancia en el entorno de Laboratorio[1] (o pruebas) de nuevas aplicaciones y tecnologías. En la experiencia piloto, el departamento de Seguridad Informática será el encargado de registrar y medir las ventajas y desventajas de la solución. Para ello se tomará nota de la cantidad de eventos procesados, cantidad de falsos positivos, cantidad de falsos negativos, tiempos de ejecución y cantidad de aciertos.

Los problemas posibles que podrían presentarse al momento de implementar los resultados del proceso de Exploración de Información son los siguientes:

- Que el usuario final no interprete la salida del proceso.
- Que no haya una clara transferencia de conocimientos al área usuaria.
- Que debido a la elevada carga laboral por las tareas cotidianas, el área usuaria no dedique suficiente tiempo para el aprendizaje de la nueva funcionalidad.
- Que surjan inconvenientes o problemas causados por variables presentes en el régimen de funcionamiento de tiempo real que no se hayan tenido en cuenta.

4.1.6.2 Plan de Monitoreo y Mantenimiento

Monitoreo del Modelo

[1] Cabe aclarar que el entorno de desarrollo es intensamente utilizado por desarrolladores de nuevas aplicaciones a medida y por tecnólogo cuando se prueban y analizan nuevas tecnologías y productos de terceras partes. Si bien, este entorno no es de Producción, se considera muy importante por la cantidad de personas y actividades que se llevan a cabos en el mismo. Todas las aplicaciones, productos, procesos se prueban en este entorno antes que en Producción por lo tanto la experiencia del presente proyecto en el entorno de Laboratorio se considera habilitante para la futura implementación en el entorno Productivo.

Se llevará a cabo para mantener el óptimo funcionamiento del modelo.

Como parte del plan de monitoreo se implementarán las siguientes condiciones:

- Detectar si se agregan, eliminan o modifican servidores controladores de dominio.
- Detectar si cambia el formato de los eventos en nuevas versiones del producto que registran los mismos.
- Determinar si cambian radicalmente las funciones y tareas del personal siendo auditado.

Mantenimiento del Modelo

Se interesa por los errores, defectos, fallos, mejoras y cambios del modelo. El mantenimiento se centra en el cambio que va asociado a la corrección de errores, a las adaptaciones requeridas por la evolución del entorno y a las modificaciones debidas a los cambios de los requisitos del cliente dirigidos a reforzar o a ampliar el modelo.

Para lograr un nivel de facilidad en el mantenimiento del modelo se consideran los siguientes factores:

- Lograr una Estructura compresible del Proyecto.
- Facilidad de uso del modelo.
- Estructura de la documentación estandarizada.
- Disponibilidad de casos de prueba.
- Disponibilidad de un entorno apropiado para llevar a cabo el mantenimiento.
- Disponibilidad del grupo de personas que hayan participado originalmente del proyecto.
- Todas las peticiones de mantenimiento deben ser presentadas de una forma estandarizada.
- Si se encuentra un error, se debe incluir una completa descripción de las circunstancias que llevaron al error, incluyendo datos de entrada y otro material de soporte.

- Para peticiones de mantenimiento adaptativo o perfectivo, se ha de adjuntar una breve especificación de cambios que suponga una especificación de requisitos abreviada.

- Internamente, el equipo de desarrollo del modelo, debe confeccionar un informe de cambios indicando: la magnitud del esfuerzo requerido para satisfacer la petición de mantenimiento; la naturaleza de las modificaciones requeridas; la prioridad de la petición y otros datos sobre las modificaciones.

- El informe de cambios del modelo se envía a la autoridad de control de cambios antes de iniciar cualquier planificación del mantenimiento.

- Independientemente del tipo de mantenimiento, se siguen las mismas acciones técnicas. Estas acciones incluyen la modificación del diseño, la revisión, la prueba de unidad y de integración, incluyendo pruebas de regresión usando los casos de prueba ya existentes, la prueba de validación y la revisión.

- Se llevará un registro de las actividades de mantenimiento, para poder obtener medidas del rendimiento del mismo.

4.1.6.3 Armando del Informe Final

Serán necesarios los siguientes informes:

- Resumen, en diapositivas, de los resultados y beneficios a nivel general para la gerencia de Seguridad y Control.

- Informe de los modelos utilizados y de los resultados con alto nivel de detalles para el área de Tecnología de Seguridad y Control.

- Informe de uso, monitoreo y mantenimiento de los modelos para usuarios finales y personal técnico.

Los informes de resultados tendrán la siguiente estructura:

- Situación Actual.

- Requerimientos.

- Propuesta.

- Resultados y Beneficios

Los informes incluirán la siguiente información:

- Tipo de datos utilizados, Fuente de los datos.
- Modelos Utilizados para procesar los datos de entrada.
- Resultado obtenidos.
- Beneficios logrados.

Presentación Final

La presentación final se realizará a la Gerencia, Personal de Tecnología y Miembros del Departamento de Tecnología de Seguridad y Control. Como guía se utilizará el Resumen, en diapositivas, de los resultados y beneficios.

4.1.6.4 Revisión del Proyecto

Debido a que es el primer proyecto de Minería de datos llevado a cabo, en una primera instancia se determinó la factibilidad de cada modelo de minería de datos para solucionar el problema.

Fue una labor que demandó varios meses, donde se analizaron los datos disponibles, se transformaron los mismos para que los modelos los puedan procesar y finalmente se utilizaron distintos modelos y diversas configuraciones.

A continuación se describe el proceso de exploración de información y una propuesta de mejora del mismo para una futura etapa:

- Descargar los eventos de seguridad desde las fuentes de datos
- Transformar los datos para que puedan ser procesados por el modelo de minería de datos seleccionado. En la primera fase se usa una Red Neuronal de Mapas Auto-Organizados. La red se encarga en agrupar los sucesos en clusters o familias donde los miembros tienen características similares.
- Utilizando información estadística proporcionada por la red, se le da una categoría a cada grupo. Los mismos se dividirán según la cantidad de miembros y reflejaran colecciones de eventos que son normales, dudosos o malos.
- Los datos de salida de red se cargan como entrada en un Árbol de Inducción C4.5, el cual producirá las reglas de decisión que se utilizarán para evaluar los nuevos eventos.

4.2 Desarrollo de la Solución (Métrica III)

Para el desarrollo de esta sección se decidió realizar un documento de tipo entregable para cada etapa de Métrica de modo que el cliente pueda entender la evolución de la construcción del producto.

Al mismo tiempo, para no descuidar la forma de la metodología propuesta, se confeccionan Tablas de Control en forma paralela donde se valida el tratamiento de cada Actividad y Tarea de Métrica.

En consecuencia, cada fase está compuesta por el Documento Entregable y su respectiva Tabla de Control.

4.2.1 Planificación de Sistemas de Información (PSI)

4.2.1.1 Documento Entregable

DOCUMENTO DE PLANIFICACIÓN DE SISTEMAS DE INFORMACIÓN

Descripción general del PSI:

Aprobación de inicio del PSI

El área de "Seguridad y Control" de la compañía, la cual planteó el requerimiento, consideran que es necesario llevar a cabo el presente PSI.

La Gerencia General considerar que esta decisión es estratégica por lo tanto se tiene el respaldo de la misma.

Ámbito y objetivos del PSI

El ámbito del PSI se circunscribe en la Gerencia de Seguridad y Control, departamento de Seguridad Informática. Los usuarios y procesos afectados son los comisionados del control de las tareas administrativas de los administradores de redes.

El objetivo del PSI es:

- La instauración de un sistema de software que realice la producción de patrones de comportamiento de usuarios en los Servidores Controladores de Dominio.
- La mitigación, detección y registro de las acciones fraudulentas realizadas contra el negocio durante la operación de los permisos de acceso (a recursos informáticos, datos e información), cuentas y claves de usuarios.

Objetivos estratégicos relacionados con el PSI

El objetivo estratégico relacionado con el PSI es:

- Asegurar la continuidad de la producción.
- Incrementar la confiabilidad de los Sistemas de información.

Factores críticos de éxito

Los factores críticos de éxitos consisten en desarrollar un Sistema de Información capaz de producir mecanismos que detecten acciones de administración que no son correctas.

Responsables del PSI

El responsable del PSI (presente trabajo de magister) es el Licenciado en Sistemas Javier Crosa.

Descripción general de procesos de la organización afectados

Los procesos afectados son:

- La captura, procesamiento y almacenamiento de los eventos de seguridad de los servidores.
- El análisis de los sucesos de seguridad.
- El soporte de la toma de decisiones con respecto a la seguridad en la administración de las redes.

Catálogo de objetivos de PSI:

Objetivos generales

Los objetivos del PSI son:

- Generar un sistema software que permita:
  - Reducir el tiempo dedicado a las tareas de control de eventos de seguridad.
  - Tener información de soporte para la toma de decisiones cuando se detecta la ejecución de acciones fraudulentas realizadas en el entorno informático.

Catálogo de usuarios

Los usuarios involucrados en el proyecto son:

- El Coordinador de Seguridad y Control que es el Sponsor del Proyecto.
- El Líder de Proyectos de Seguridad y Control que es el área usuaria y quien dará el visto bueno al producto final.

- El Tecnólogo, Analista y Programador.

Plan de trabajo:

Aceptación del Plan de Trabajo por parte de los implicados

La estimación de horas del plan es la siguiente:

Actividad	Horas
Planificación del Sistema de Información	20
Estudio de Viabilidad del Sistema	20
Análisis del Sistema	50
Diseño del Sistema	50
Construcción del Sistema	50
Implantación y Aceptación del Sistema	20
Mantenimiento del Sistema	20
Gestión del Proyecto	50
Seguridad	20
Gestión de la Configuración	20
Aseguramiento de la Calidad	20
Total	340

Valoración de antecedentes

Actualmente, el sector de Seguridad y Control, para el análisis de sucesos de seguridad, utiliza un aplicativo para leer los eventos desde los servidores y almacenarlos en una base de datos. Luego personal del sector, en forma manual, realiza consultas y búsquedas específicas.

El área usuaria puede contratar a terceros (personal externo que trabaja en empresas consultoras) para realizar el control.

Catálogo de requisitos

La interfase del Sistema Software debe ser simple ya que al control lo debe poder realizar cualquier persona sin conocimientos previos en sistemas.

El sistema debe producir información de soporte a la toma de decisiones.

Los datos deben mostrarse por pantalla (salidas visuales) y en informes para impresión.

El proceso debe realizar la mayor cantidad de procesos en forma desatendida o automatizada.

Requisitos generales

Es necesario procesar todos los eventos de seguridad de los controladores de dominios.

Evitar la pérdida de sucesos. La misma puede producirse por no procesar con la frecuencia adecuada el log.

Producir Reglas de Decisión.

Resguardar la información procesada y los resultados

Registrar las ejecuciones

Modelo de procesos de la organización

Los procesos que comprende el presente plan son los siguientes:

Proceso 1: Análisis de los eventos de seguridad.

Los sucesos se encuentran almacenados en algún medio de almacenamiento. El personal a cargo realiza búsquedas y consultas con el objetivo de encontrar acciones dudosas, fraudulentas, no autorizadas que hayan realizado los administradores de redes.

Información Implicada: Eventos de seguridad de los servidores controladores de dominios.

Usuarios Implicados: Staff del sector de Seguridad y Control.

Proceso 2: Justificación, por parte de administradores de redes, de la realización de tareas no autorizadas.

Los administradores de Sistemas de Información solo pueden realizar sus tareas encomendadas si están respaldadas por un correo electrónico o en el sistema de control y seguimiento de cambios. No pueden realizar acciones que hayan sido requeridas por teléfono o en forma personal, para estos casos hay que requerir el respaldo mencionado correspondiente.

Cuando se detecta una o más acciones no autorizadas, que no sustentan la evidencia del pedido por parte del usuario final, la infracción se notifica al sector de Auditoria y Recursos Humanos para que tomen las acciones necesarias.

Información Implicada: Eventos de seguridad que muestran como evidencia la actividad realizada.

Usuarios Implicados: Administradores de Sistemas de Información, Staff del sector de Seguridad y Control.

Necesidades de información

Diariamente el área de Seguridad y Control tiene la labor controlar los eventos de seguridad de los servidores controladores de dominios. El objetivo es detectar la ejecución de tareas no autorizadas en los sistemas de información.

La base principal de información usada para este trabajo son los archivos de logs mencionados anteriormente.

Modelo de información

El modelo de información se muestra a continuación en la figura 4-10. El sistema propuesto resuelve los módulos "Consulta de Búsqueda", "¿Anormalidad?", "¿Otro Evento?", "Registro, Notificación".

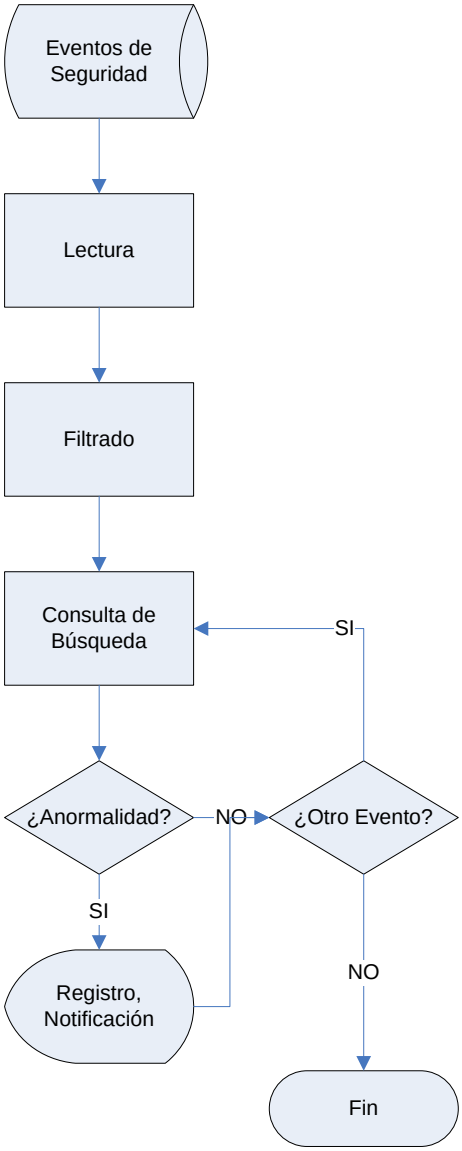


Figura 4-10. Modelo de Información.

Requisitos de los procesos afectados por el PSI

Interfase simple. Prioridad Media.

Producir información de soporte a la toma de decisiones. Prioridad Alta.

Mostrarse Información por pantalla (salidas visuales). Prioridad Alta.

Producir informes para impresión. Prioridad Alta.

Realizar procesos en forma desatendida o automatizada. Prioridad Media.

Fácil de Mantener. Prioridad Media.

Documentación de desarrollo Completa. Prioridad Media.

Objetivos del estudio de los Sistemas de Información actuales

El sistema de información actual persigue el objetivo de detectar acciones no autorizadas y fraudulentas en los sistemas y dispositivos informáticos.

No existe documentación alguna de su mantenimiento, uso, desarrollo.

Los usuarios no están satisfechos con él porque no cubre sus necesidades. Lo consideran obsoleto e ineficiente.

Identificación de los Sistemas de información actuales

El sistema de información actual es el proceso que comprende la detección de acciones no autorizadas y fraudulentas en los sistemas y dispositivos informáticos.

Valoración de la situación actual

El sistema actual se considera vulnerable y deficiente porque depende fuertemente de la experiencia del usuario que realice la búsqueda e investigación de las tareas administrativas. Además no permite reutilizar, enriquecer y transferir a terceros los métodos, juicios, antecedentes de las pesquisas llevadas a cabo anteriormente.

Adicionalmente, el proceso es lento y no llega a cubrir el crecimiento de la empresa.

Diagnóstico de la situación actual:

Relación de sistemas de información que se conservan y mejoras necesarias

El sistema de información actual se lleva a cabo íntegramente en forma manual por lo tanto no se conservará. Las mejoras que se realizarán al mismo deberán cubrir el procedimiento completo.

Modelo de sistemas de información

El nuevo modelo del sistema de información a elaborar se muestra en la figura 4-11.

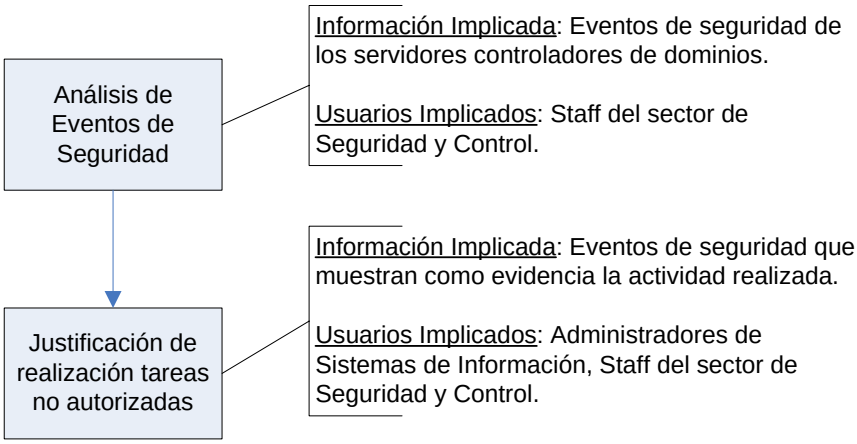


Figura 4-11. Nuevo modelo del sistema de información.

Alternativas de arquitectura tecnológica

Luego de un análisis inicial, se consideran que las opciones tecnológicas más relevantes son las siguientes:

Sistema Operativo:

- Windows XP
- UNIX

Lenguajes o Entornos de Programación:

- KAPPA-PC
- Visual Basic

Arquitectura tecnológica

Para la selección del Sistema Operativo se considera que los usuarios del aplicativo pueden ser terceros y que generalmente no tienen profundos conocimientos de sistemas. Por lo tanto, se utilizará el entorno Windows considerando que es el más conocido, amigable y cumple satisfactoriamente los requerimientos técnicos del desarrollo.

Como ambiente de programación se utilizará KAPPA-PC. El sistema de desarrollo de KAPPA-PC permite escribir aplicaciones en un ambiente gráfico de alto nivel y genera código estándar C y rutinas GUI. Además permite escoger la manera de desarrollar una aplicación, por ejemplo, Razonamiento Basado en Reglas, el cual es ideal para el presente caso de estudio.

Plan de proyectos:

Definición de proyectos

Se define que el proyecto a llevar a cabo es el denominado "Análisis de Eventos de Seguridad en Servidores".

Prioridad de proyectos

Para el presente ejercicio se ejecutará el proyecto "Análisis de Eventos de Seguridad en Servidores".

Se le asigna prioridad alta por considerarse que la seguridad y el prestigio de la sociedad están en riesgo.

Calendario de proyectos y acciones

El proyecto, incluyendo las acciones necesarias (planes de formación, gestión de configuración, gestión del cambio, gestión de la calidad), debe comenzar y terminar durante el transcurso del primer semestre del año 2008.

Plan de mantenimiento del PSI

El jefe del proyecto (analista/programador Lic. Javier Crosa) es el encargado de mantener actualizados los documentos del Plan de Sistemas.

Los documentos del Plan de Sistemas se almacenarán en dos copias de DVD y resguardarán, una, en el cofre de seguridad que posee el sector de Seguridad y Control y la otra, en el cofre ignífugo de la empresa.

Los documentos del Plan de Sistemas deberán ser revisados y actualizados, si corresponde, mensualmente por el analista/programador.

Plan de presentación

El jefe de proyecto enviará, el resumen del siguiente apartado con toda la información del Plan de Sistemas de Información, a la Gerencia de Seguridad y Control para su aprobación.

Presentación

A continuación se describe el resumen del Plan presentado a la Gerencia de Seguridad y Control.

Presentación Formal del Plan de Sistemas de Información

Identificación de Requisitos

Interfase simple. Prioridad Media.

Producir información de soporte a la toma de decisiones. Prioridad Alta.

Mostrarse Información por pantalla (salidas visuales). Prioridad Alta.

Producir informes para impresión. Prioridad Alta.

Realizar procesos en forma desatendida o automatizada. Prioridad Media.

Fácil de Mantener. Prioridad Media.

Documentación de desarrollo Completa. Prioridad Media.

Sistemas de Información Actuales

El sector de Seguridad y Control, para el análisis de sucesos de seguridad, utiliza un aplicativo para leer los eventos desde los servidores y almacenarlos en una base de datos. Luego personal del sector, en forma manual, realiza consultas y búsquedas específicas.

El área usuaria puede contratar a terceros (personal externo que trabaja en empresas consultoras) para realizar el control.

Diseño del Modelo de Sistemas de Información

Proceso 1: Análisis de los eventos de seguridad.

Proceso 2: Justificación, por parte de administradores de redes, de la realización de tareas no autorizadas.

Arquitectura Tecnológica

Para la selección del Sistema Operativo se considera que los usuarios del aplicativo pueden ser terceros y que generalmente no tienen profundos conocimientos de sistemas. Por lo tanto, se utilizará el entorno Windows

considerando que es el más conocido, amigable y cumple satisfactoriamente los requerimientos técnicos del desarrollo.

Como ambiente de programación se utilizará KAPPA-PC. El sistema de desarrollo de KAPPA-PC permite escribir aplicaciones en un ambiente gráfico de alto nivel y genera código estándar C y rutinas GUI. Además permite escoger la manera de desarrollar una aplicación, por ejemplo, Razonamiento Basado en Reglas, el cual es ideal para el presente caso de estudio.

Definición del Plan

Se define que el proyecto a llevar a cabo es el denominado "Análisis de Eventos de Seguridad en Servidores".

Para el presente ejercicio se ejecutará el proyecto "Análisis de Eventos de Seguridad en Servidores".

Se le asigna prioridad alta por considerarse que la seguridad y el prestigio de la sociedad están en riesgo.

El proyecto, incluyendo las acciones necesarias (planes de formación, gestión de configuración, gestión del cambio, gestión de la calidad), debe comenzar y terminar durante el transcurso del primer semestre del año 2008.

El jefe del proyecto (analista/programador Lic. Javier Crosa) es el encargado de mantener actualizados los documentos del Plan de Sistemas.

Los documentos del Plan de Sistemas se almacenarán en dos copias de DVD y resguardarán, una, en el cofre de seguridad que posee el sector de Seguridad y Control y la otra, en el cofre ignífugo de la empresa.

Los documentos del Plan de Sistemas deberán ser revisados y actualizados, si corresponde, mensualmente por el analista/programador.

Aprobación formal del PSI

La Gerencia de Operaciones y Tecnología junto con la Gerencia de Seguridad y Control deberán aprobar formalmente el Plan de Sistemas de Información.

Plan de comunicación del PSI

En una reunión mantenida entre el Tesista y la Directora del proyecto se dio por aprobada la fase.

El jefe del proyecto comunica formalmente a los participantes, afectados y usuarios del Plan los resultados del mismo. Se utiliza el siguiente anuncio.

Estimados Colaboradores,

Cumplo en informarles que el Plan de Sistema de Información que comprende el proyecto "Análisis de Eventos de Seguridad en Servidores" ha sido aprobado satisfactoriamente por la Gerencia de Operaciones y Tecnología y la Gerencia de Seguridad y Control.

Desde ya muchas gracias por su participación y compromiso.

4.2.1.2 Control de Actividades

Actividad / Tarea	Desarrollo	Justificación
ACTIVIDAD PSI 1: INICIO DEL PLAN DE SISTEMAS DE INFORMACIÓN		
Tarea PSI 1.1: Análisis de la Necesidad del PSI	SI	Se dispone de la información necesaria.
Tarea PSI 1.2: Identificación del Alcance del PSI	SI	Se dispone de la información necesaria.
Tarea PSI 1.3: Determinación de Responsables	SI	Se dispone de la información necesaria.
ACTIVIDAD PSI 2: DEFINICIÓN Y ORGANIZACIÓN DEL PSI		
Tarea PSI 2.1: Especificación del Ámbito y Alcance	SI	Se dispone de la información necesaria.
Tarea PSI 2.2: Organización del PSI	PARCIAL	No corresponde el desarrollo de: “Equipos de trabajo”.
Tarea PSI 2.3: Definición del Plan de Trabajo	SI	Se dispone de la información necesaria.
Tarea PSI 2.4: Comunicación del Plan de Trabajo	SI	Se dispone de la información necesaria.
ACTIVIDAD PSI 3: ESTUDIO DE LA INFORMACIÓN RELEVANTE		
Tarea PSI 3.1: Selección y Análisis de Antecedentes	SI	Se dispone de la información necesaria.
Tarea PSI 3.2: Valoración de Antecedentes	PARCIAL	No se dispone de un “Catálogo de Normas del PSI”
ACTIVIDAD PSI 4: IDENTIFICACIÓN DE REQUISITOS		
Tarea PSI 4.1: Estudio de los Procesos del PSI	SI	Se dispone de la información necesaria.
Tarea PSI 4.2: Análisis de las Necesidades de Información	SI	Se dispone de la información necesaria.
Tarea PSI 4.3: Catalogación de Requisitos	SI	Se dispone de la información necesaria.
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	SI	Se dispone de la información necesaria.
Tarea PSI 5.2: Análisis de los Sistemas de Información Actuales	NO	El proceso ya fue descrito en los puntos precedentes.
Tarea PSI 5.3: Valoración de los Sistemas de Información Actuales	SI	Se dispone de la información necesaria.
ACTIVIDAD PSI 6: DISEÑO DEL MODELO DE SISTEMAS DE INFORMACIÓN		
Tarea PSI 6.1: Diagnóstico de la Situación Actual	SI	Se dispone de la información necesaria.
Tarea PSI 6.2: Definición del Modelo de Sistemas de Información	SI	Se dispone de la información necesaria.
ACTIVIDAD PSI 7: DEFINICIÓN DE LA ARQUITECTURA TECNOLÓGICA		

Actividad / Tarea	Desarrollo	Justificación
Tarea PSI 7.1: Identificación de las Necesidades de Infraestructura Tecnológica	SI	Se dispone de la información necesaria.
Tarea PSI 7.2: Selección de la Arquitectura Tecnológica	SI	Se dispone de la información necesaria.
ACTIVIDAD PSI 8: DEFINICIÓN DEL PLAN DE ACCIÓN		
Tarea PSI 8.1: Definición de Proyectos a Realizar	SI	Se dispone de la información necesaria.
Tarea PSI 8.2: Elaboración del Plan de Mantenimiento del PSI	SI	Se dispone de la información necesaria.
ACTIVIDAD PSI 9: REVISIÓN Y APROBACIÓN DEL PSI		
Tarea PSI 9.1: Convocatoria de la Presentación	SI	Se dispone de la información necesaria.
Tarea PSI 9.2: Evaluación y Mejora de la Propuesta	SI	Se dispone de la información necesaria.
Tarea PSI 9.3: Aprobación del PSI	SI	Se dispone de la información necesaria.

Tabla 4-13. Control de Actividades PSI.

4.2.2 Desarrollo de Sistemas de Información

4.2.2.1 Estudio de Viabilidad del Sistema (EVS)

4.2.2.1.1 Documento Entregable

DOCUMENTO DE ESTUDIO DE VIABILIDAD DEL SISTEMA

Descripción General del Sistema

La necesidad planteada por el usuario consiste en disponer de un sistema software que permita detectar acciones fraudulentas o dudosas que realicen los administradores de sistemas de información.

El estudio de restricciones es el siguiente:

- Económicas: no se dispone de presupuesto para la compra o desarrollo de productos complejos y costosos.
- Técnicas: las pruebas iniciales utilizadas y analizadas fueron satisfactorias. Se plantea utilizar otras metodologías, procedimientos y técnicas en futuras líneas de investigación. Adicionalmente, como la implementación se realizará en el entorno de desarrollo, no causará inconvenientes en producción.
- Operativo: el alcance del presente estudio no restringe, inicialmente, a pruebas en el entorno de desarrollo de la compañía. No hay interferencias con otros proyectos.
- Legal: El sector de Legales apoya el presente proyecto por considerarlo de extrema importancia para la seguridad de los datos y reputación de la empresa.

Catálogo de Objetivos del EVS

Verificar restricciones Económicas, Técnicas, Operativas y Legales.

Verificar si se solapa con otros Proyectos.

Verificar disponibilidad de las personas involucradas.

Catálogo de Requisitos

Los Requisitos y su Importancia se listan a continuación.

- Ejecución en el entorno de Desarrollo. Media
- Riesgo técnico bajo. Alta

- Ninguna objeción legal. Alta
- Procesar todos los eventos de seguridad de los controladores de dominios. Alta
- Evitar la pérdida de sucesos. La misma puede producirse por no procesar con la frecuencia adecuada el log. Alta
- Producir Reglas de Decisión Alta

Catálogo de Usuarios

Los usuarios que intervendrán son:

- Analista / programador
- Responsable del sector de Seguridad y Control

Plan de Trabajo

No se considera necesario realizar el estudio detallado de la situación actual de los sistemas debido a que la tarea, que realizará el sistema software que genera el presente trabajo, se realiza en su mayor parte manualmente. No existe un procedimiento ni una metodología formal.

Descripción de la Situación Actual

Se utiliza un aplicativo para la leer los eventos y almacenarlos en una base de datos. Luego personal del sector de Seguridad Informática, en forma manual, realiza consultas y búsquedas específicas con el objetivo de detectar eventos sospechosos.

Alternativas de Solución a Estudiar

Descomposición inicial del sistema

El sistema en estudio se puede descomponer en los siguientes subsistemas:

- Lectura de los eventos desde los dispositivos informáticos.
- Análisis de los sucesos.

Alternativas de Solución

- Lectura de los eventos desde los dispositivos informáticos.

El mercado ofrece variadas alternativas de acceso libre por lo tanto se puede utilizar alguna de ellas. De todos modos, este análisis no corresponde al presente trabajo.

- Análisis de los sucesos.

  El mercado ofrece productos donde se configuran reglas y acciones. Antes la detección de un evento específico, se puede activar una alerta que es enviada al personal de sistemas encargado de la aplicación. Esta metodología presenta el problema que requiere el conocimiento previo de los potenciales errores. Además es necesario programar las series de reglas que se aplicarán a los sucesos lo cual al término de un tiempo la cantidad de las mismas es tan grande que es muy complicado administrarlas y entender su lógica.

  Los paquetes software que pueden cumplir con el requerimiento del cliente son costosos y exceden el presupuesto. Aquellos menos onerosos no cubren íntegramente las necesidades (en el apartado 5.1 Estado de la Tecnología Actual se describen las aplicaciones más importantes del mercado), en consecuencia se decide realizar un desarrollo propio en una versión beta para las pruebas en el entorno de desarrollo.

Catálogo de Requisitos

- Ejecución en el entorno de Desarrollo.
- Riesgo técnico bajo: la implementación se realizará en el entorno de desarrollo, lo cual no causará inconvenientes en producción.
- Procesar todos los eventos de seguridad de los controladores de dominios: la empresa cuenta con varios servidores de este tipo y los usuarios pueden conectarse a uno u otro.
- Evitar la pérdida de sucesos: la frecuencia de lectura y descarga de los sucesos debe ser alta.
- Producir Reglas de Decisión: las mismas darán soporte a la toma de decisiones.
- Resguardar la información procesada y los resultados: guardar las observaciones y su catalogación en archivos.

- Registrar las ejecuciones: al momento de procesar cada observación se debe agregar la fecha y hora en el archivo de salida.

Descripción conceptual de la Alternativa del Desarrollo Propio

La descripción conceptual de la alternativa del desarrollo propio se muestra en la parte recuadrada de la figura 4-12.

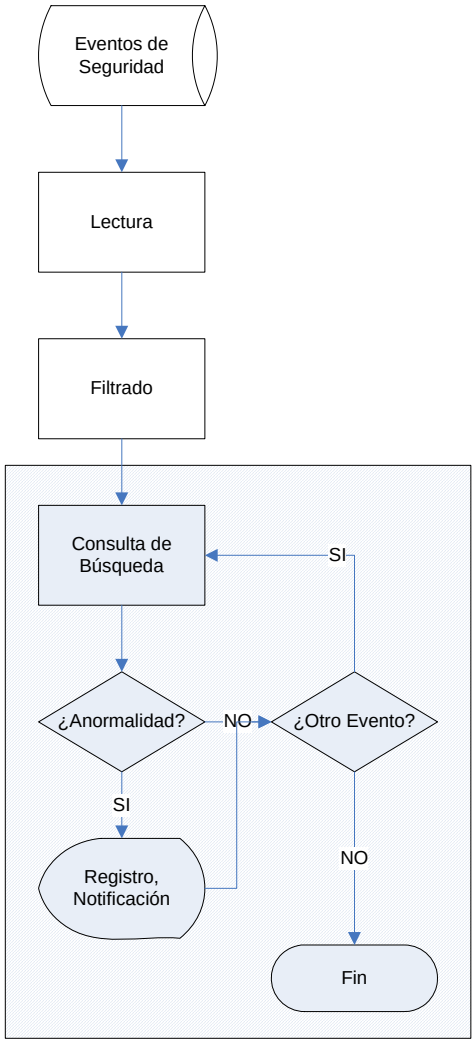


Figura 4-12. Módulos del Sistema Software a Desarrollar.

Valoración de Alternativas

Impacto en la Organización de Alternativas

Se considera que el impacto es ínfimo. El desarrollo es propio. No requiere contacto con proveedores y/o consultores externos.

Costos / Beneficios de Alternativas

Los beneficios consisten en comenzar a utilizar un procedimiento sistematizado y dejar de operar en forma manual. Logrando mejoras en la eficacia, efectividad, tiempos de ejecución de las tareas.

El detalle de los costos se describe en el apartado 4.1.1.2.6 Costos.

Valoración de Riesgos

No se detectan riesgos asociados porque las experiencias y pruebas iniciales se realizaran en el entorno de desarrollo.

Aprobación de la Solución

En reunión de seguimiento, control y aprobación entre las partes, Tesista y Directora del proyecto, se dio por aprobada esta fase.

El jefe del proyecto comunica formalmente a los participantes, afectados y usuarios los resultados de la fase. Se utiliza el siguiente anuncio.

Estimados Colaboradores, Cumplo en informarles que la fase del Estudio de Viabilidad del proyecto "Análisis de Eventos de Seguridad en Servidores" ha sido aprobada satisfactoriamente. Desde ya muchas gracias por su participación y compromiso.

4.2.2.1.2 Control de Actividades

Actividades / Tareas	Desarrollo	Justificación
ACTIVIDAD EVS 1: ESTABLECIMIENTO DEL ALCANCE DEL SISTEMA		
Tarea EVS 1.1: Estudio de la Solicitud	SI	Se dispone de la información necesaria.
Tarea EVS 1.2: Identificación del Alcance del Sistema	SI	Se dispone de la información necesaria.
Tarea EVS 1.3: Especificación del Alcance del EVS	SI	Se dispone de la información necesaria.
ACTIVIDAD EVS 2: ESTUDIO DE LA SITUACIÓN ACTUAL		
Tarea EVS 2.1: Valoración del Estudio de la Situación Actual	SI	Se dispone de la información necesaria.
Tarea EVS 2.2: Identificación de los Usuarios Participantes en el Estudio de la Situación Actual	NO	No requiere desarrollo por la naturaleza del sistema actual
Tarea EVS 2.3: Descripción de los Sistemas de Información Existentes	NO	No requiere desarrollo por la naturaleza del sistema actual
Tarea EVS 2.4: Realización del Diagnóstico de la Situación Actual	NO	No requiere desarrollo por la naturaleza del sistema actual
ACTIVIDAD EVS 3: DEFINICIÓN DE REQUISITOS DEL SISTEMA		
Tarea EVS 3.1: Identificación de las Directrices Técnicas y de Gestión	NO	No requiere desarrollo por la naturaleza del sistema nuevo
Tarea EVS 3.2: Identificación de Requisitos	SI	Se dispone de la información necesaria.
Tarea EVS 3.3: Catalogación de Requisitos	SI	Se dispone de la información necesaria.
ACTIVIDAD EVS 4: ESTUDIO DE ALTERNATIVAS DE SOLUCIÓN		
Tarea EVS 4.1: Preselección de Alternativas de Solución	SI	Se dispone de la información necesaria.
Tarea EVS 4.2: Descripción de las Alternativas de Solución	SI	Se dispone de la información necesaria.
ACTIVIDAD EVS 5: VALORACIÓN DE LAS ALTERNATIVAS		
Tarea EVS 5.1: Estudio de la Inversión	SI	Se dispone de la información necesaria.
Tarea EVS 5.2: Estudio de los Riesgos	SI	Se dispone de la información necesaria.
Tarea EVS 5.3: Planificación de Alternativas	SI	Se dispone de la información necesaria.
ACTIVIDAD EVS 6: SELECCIÓN DE LA SOLUCIÓN		
Tarea EVS 6.1: Convocatoria de la Presentación	NO	Las personas involucradas son pocas.
Tarea EVS 6.2: Evaluación de las Alternativas y Selección	SI	Se dispone de la información necesaria.
Tarea EVS 6.3: Aprobación de la Solución	SI	Se dispone de la información necesaria.

Tabla 4-14. Control de Actividades EVS.

4.2.2.2 Análisis del Sistema de Información (ASI)

4.2.2.2.1 Documento Entregable

DOCUMENTO DE

ANÁLISIS DEL SISTEMA DE INFORMACIÓN

Catálogo de Requisitos

Los requisitos que el sistema debe cumplir son los siguientes:

Requisitos Funcionales

- RF1. Ingreso al sistema con usuario y clave.
- RF2. Permitir la creación de credenciales de usuario para la validación del ingreso al sistema.
- RF3. Permitir el cambio de clave a los usuarios.
- RF4. Consultar reportes de salida.
- RF5. Consultar estadísticas históricas.
- RF6. Seleccionar vistas y reportes a desplegar durante análisis de registros.
- RF7. Seleccionar archivo de entrada.
- RF8. Seleccionar archivos de salida.
- RF9. Permitir ejecución de análisis de registros.
- RF10. Permitir la visualización del registro en análisis en el momento de ejecución.
- RF11. Permitir la visualización de la cantidad de registros por tipo, analizados en el momento de ejecución.
- RF12. Permitir la visualización de gráficos de secciones de la cantidad de registros por tipo.
- RF13. Permitir la visualización de estadísticas de las reglas utilizadas.
- RF14. Permitir la visualización de estadísticas por usuarios administradores de redes involucrados en los registros.

- RF15. Permitir la visualización de los archivos de salida generados con la información producida de los registros.
- RF16. Salir del sistema.

Requisitos de Negocio

- RN1. Ejecución en el entorno de Desarrollo.
- RN2. Riesgo técnico bajo.
- RN3. Procesar todos los eventos de seguridad de los controladores de dominios.
- RN4. Evitar la pérdida de sucesos.
- RN5. Producir Reglas de Decisión.
- RN6. Resguardar la información procesada y los resultados
- RN7. Registrar las ejecuciones

Glosario

Eventos de seguridad: cada dispositivo informático registra todas las tareas de seguridad que se realizan en el mismo. Accesos a recursos, Ingreso/egreso al dispositivo.

Servidores controladores de dominio: son los servidores que contienen toda la información de las cuentas y claves de todos los usuarios, recursos, dispositivos de la empresa.

Reglas de Decisión: permitirán clasificar las observaciones según sus características y ser el soporte para penalizar a los administradores que realicen tareas no autorizadas.

Descripción General del Entorno Tecnológico del Sistema

Durante el desarrollo del proyecto no se tendrá acceso a los datos de Producción de la empresa. Se manipularán datos del entorno de Desarrollo y Pruebas, en consecuencia se tendrá control total sobre los datos y servidores.

El entorno de desarrollo es intensamente utilizado por desarrolladores de nuevas aplicaciones y por tecnólogos, cuando se prueban y analizan nuevas tecnologías y productos de terceras partes. Si bien, este entorno no es de Producción, se considera muy importante por la cantidad de personas y actividades que se

llevan a cabos en el mismo. Todas las aplicaciones, productos, procesos se prueban en este entorno antes que en Producción por lo tanto la experiencia del presente proyecto en el entorno de Laboratorio se considera habilitante para la futura implementación en el entorno Productivo.

El hardware y software de ambos ambientes son análogos y tienen los mismos niveles de versiones y actualizaciones.

Catálogo de Normas

La seguridad de la información se establece con la implementación de un conjunto de controles a través de políticas, procedimientos y prácticas operativas con la preservación de:

- Confidencialidad: Garantizar que toda la información está protegida del uso no autorizado, violación de privacidad y otras acciones de accesos de terceros no permitidos.
- Integridad: referido a la exactitud y totalidad de la información y los métodos de procesamiento. Asegurar que sea procesada toda la información necesaria.
- Disponibilidad: garantizar acceso a la información y recursos relacionados con ella toda vez que se requiera. Garantizar que la información y la capacidad de procesamiento manual y automático sean resguardados y recuperados eventualmente cuando sea necesario.
- Autorización: que todos los accesos a datos y/o transacciones que los utilicen cumplan con los niveles de autorización correspondientes para su utilización y divulgación.

Cada usuario es responsable de la protección de los datos que tiene acceso y no se puede delegar. Principales responsabilidades:

- Identificar toda la información que corresponde a su área de responsabilidad cualquiera sea su forma y medio de conservación.
- Clasificar todos los datos de su propiedad de acuerdo con el grado de criticidad de los mismos.
- Autorizar el acceso a sus datos de acuerdo con sus respectivas funciones.
- Participar en la definición de los mecanismos de seguridad que considere necesario para la protección de su información.

Catálogo de Usuarios Participantes y Finales

Los usuarios involucrados:

- El Líder de Proyectos de Seguridad y Control que es el área usuaria y quien dará el visto bueno al producto final.
- El Tecnólogo y Analista quién será el encargado de recomendar analizar los lineamientos tecnológicos y de sistemas de información.

Planificación

La estimación de horas del plan es la siguiente:

Actividad	Horas
Definición del Sistema.	10
Establecimiento de Requisitos.	5
Identificación de Subsistemas de Análisis.	5
Análisis de los Casos de Uso.	20
Análisis de Clases.	10
Elaboración del Modelo de Datos.	5
Elaboración del Modelo de Procesos.	10
Definición de Interfaces de Usuario.	20
Análisis de Consistencia y Especificación de Requisitos.	5
Especificación del Plan de Pruebas.	10
Aprobación del Análisis del Sistema de Información.	5
Total	105

Tabla 4-15. Estimación de horas del plan.

Modelo de Casos de Uso

Los modelos de los Casos de Uso se muestran en las figuras 4-13 a 4-28.

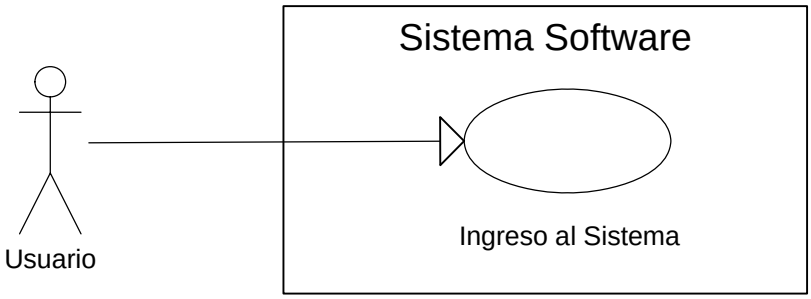


Figura 4-13. Caso de Uso RF1. Ingreso al Sistema.

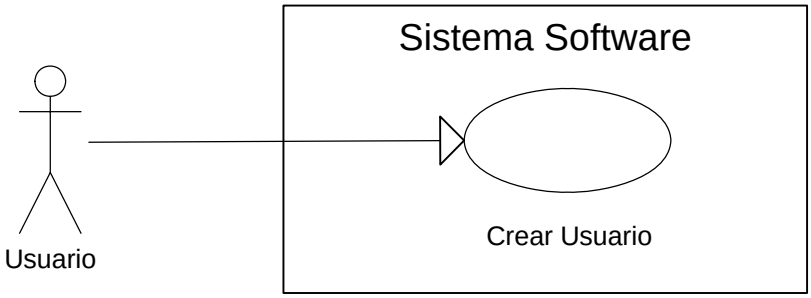


Figura 4-14. Caso de Uso RF2. Crear Usuario.

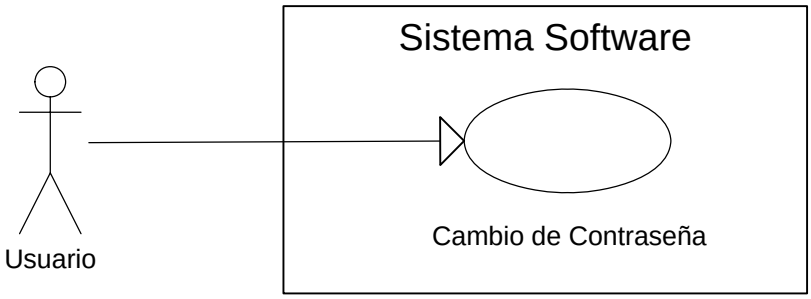


Figura 4-15. Caso de Uso RF3. Cambio de Contraseña.

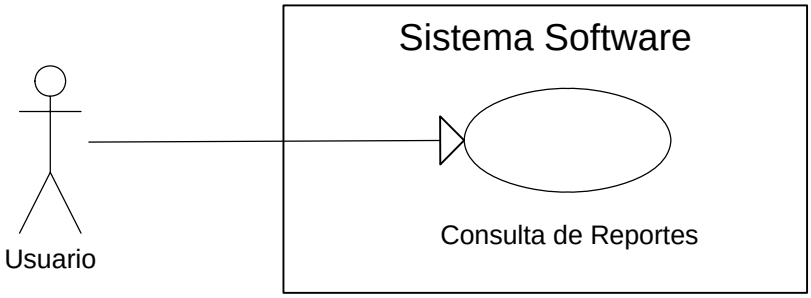


Figura 4-16. Caso de Uso RF4. Consulta de Reportes.

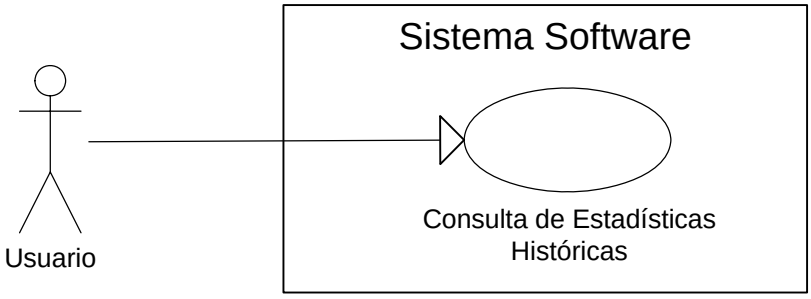


Figura 4-17. Caso de Uso RF5. Consulta de Estadísticas Históricas.

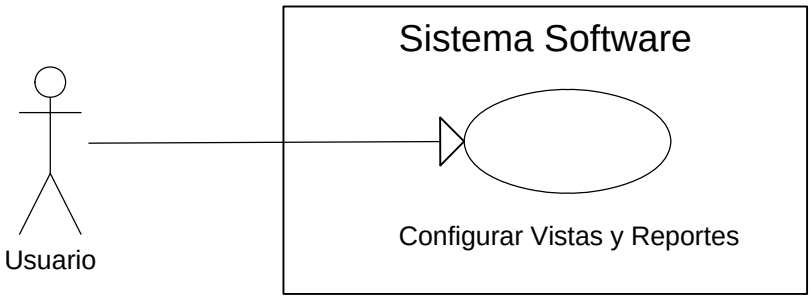


Figura 4-18. Caso de Uso RF6. Configurar Vistas y Reportes.

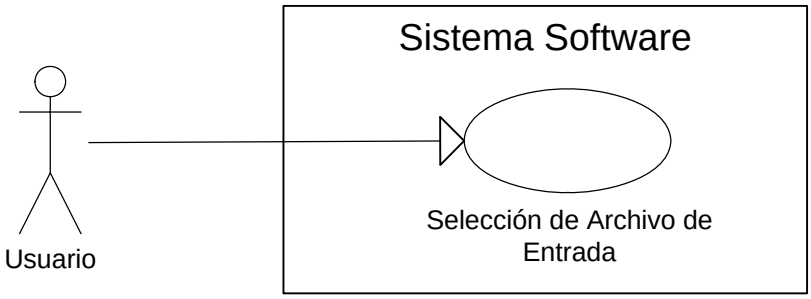


Figura 4-19. Caso de Uso RF7. Selección Archivo de Entrada.

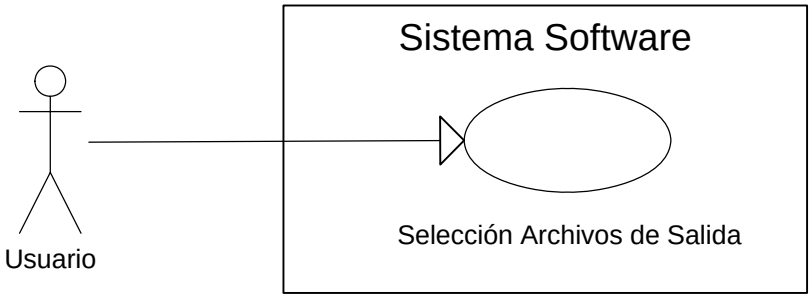


Figura 4-20. Caso de Uso RF8. Selección Archivos de Salida.

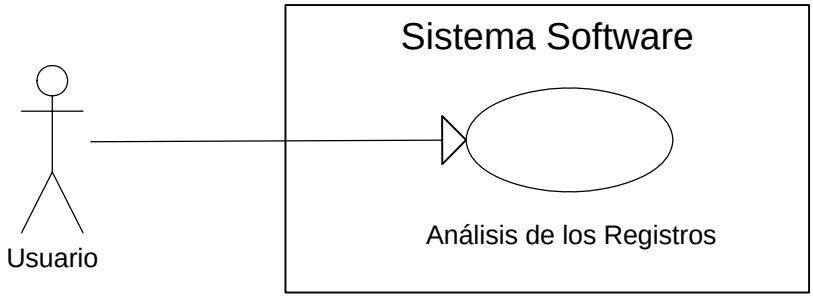


Figura 4-21. Caso de Uso RF9. Análisis de Registros.

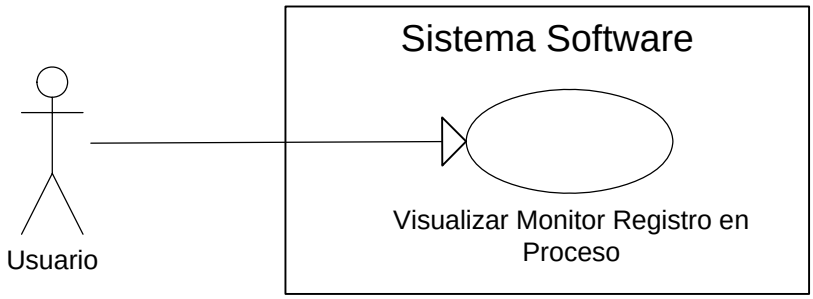


Figura 4-22. Caso de Uso RF10. Visualizar Monitor Registro en Proceso.

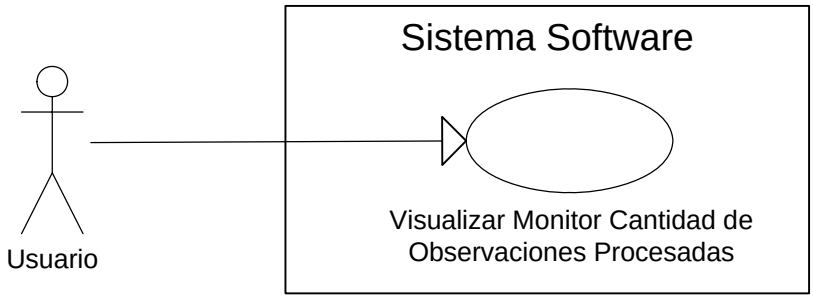


Figura 4-23. Caso de Uso RF11. Visualizar Monitor Cantidad de Observaciones Procesadas.

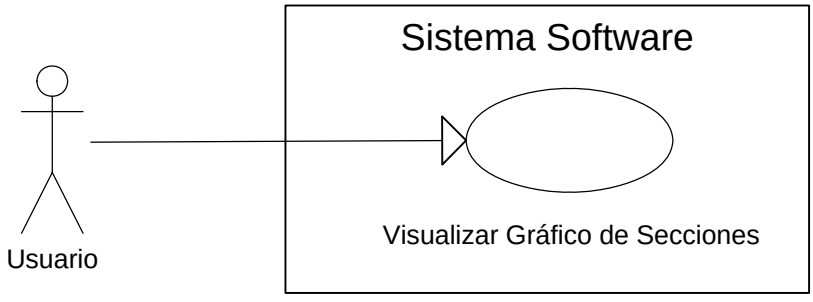


Figura 4-24. Caso de Uso RF12. Visualizar Gráfico de Secciones.

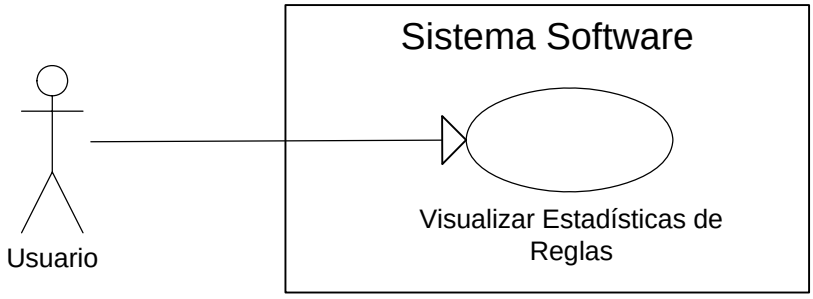


Figura 4-25. Caso de Uso RF13. Visualizar Estadísticas de Reglas.

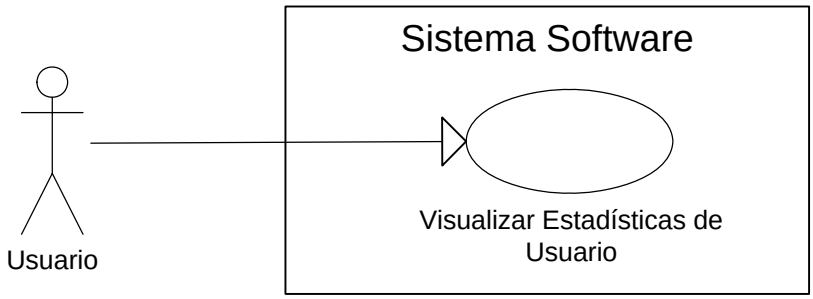


Figura 4-26. Caso de Uso RF14. Visualizar Estadísticas de Usuario.

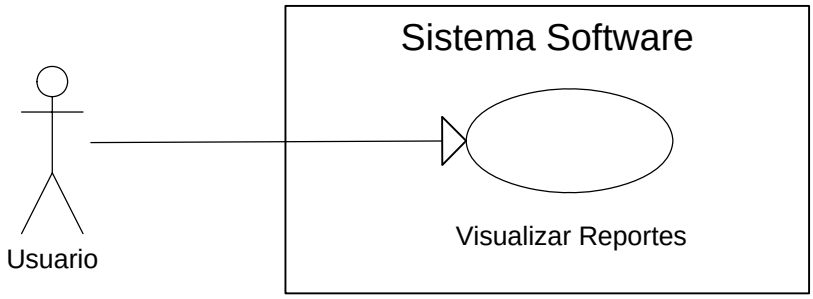


Figura 4-27. Caso de Uso RF15. Visualizar Reportes.

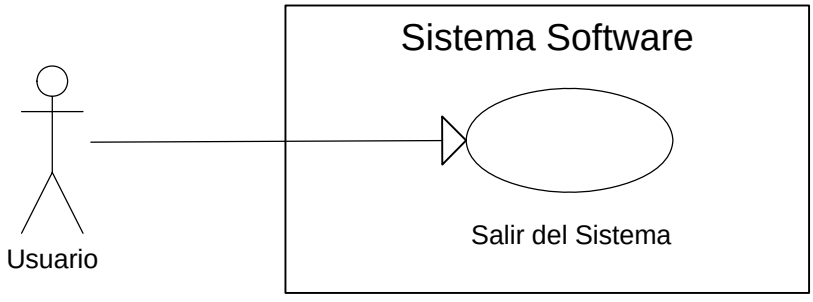


Figura 4-28. Caso de Uso RF16. Salir del Sistema.

Especificación de Casos de Uso

Las especificaciones de los Casos de Uso se muestran en las tablas 4-16 a 4-31.

Descripción del escenario	Para hacer uso del sistema los usuarios deben ingresar un usuario y contraseña. El usuario ejecuta el sistema y se presenta la pantalla para el ingreso de las credenciales de acceso.
Ejecución	Ventana Ingreso al Sistema
Procedimiento	1. El usuario ejecuta el sistema. 2. El sistema solicita el ingreso de las credenciales de acceso. 3. El usuario carga su usuario y clave. 4. El sistema valida que los datos ingresados sean correctos. 5. Si los datos ingresados son correctos, el usuario ingresa al sistema, si no, se solicita que se revisen que los datos ingresados sean correctos.
Precondiciones	El sistema debe estar instalado y configurado correctamente. El usuario que se ingresa debe estar dado de alta en el sistema previamente.
Poscondiciones	El operador del sistema puede crear una cuenta de usuario. El operador del sistema puede ingresar y utilizar el sistema.
Ejecución Alternativa	Cancelar el Ingreso de Credenciales de Acceso.
Identificación de Interfaces de usuario	Ventana Ingreso al Sistema
Condiciones de fallo	Usuario Incorrecto Contraseña Incorrecta

Tabla 4-16. Especificación de Caso de Uso RF1, Ingreso al Sistema.

Descripción del escenario	Para poder hacer uso del sistema el operador debe poseer un usuario y clave para acceder al mismo. El usuario Administrador del sistema debe crear una cuenta de usuario para cada operador del mismo.
Ejecución	1. Ventana Módulo de Seguridad. 2. Botón Crear Usuario.
Procedimiento	1. Seleccionar el botón Módulo de Seguridad. 2. Seleccionar el botón Crear Usuario. 3. Ingresar la nueva cuenta de usuario y su contraseña.
Precondiciones	El sistema debe estar instalado y configurado correctamente.
Poscondiciones	El usuario debe cambiar la contraseña inicial. El usuario puede ingresar y utilizar el sistema.
Ejecución Alternativa	Seleccionar el botón Finalizar y volver al Módulo de Inicio.
Identificación de Interfaces	Ventana Ingreso al Sistema.

de usuario	Ventana Módulo de Inicio. Ventana Módulo de Seguridad.
Condiciones de fallo	Ingreso erróneo de contraseña al crear la nueva cuenta de Usuario.

Tabla 4-17. Especificación de Caso de Uso RF2, Crear Usuario.

Descripción del escenario	El usuario debe cambiar la contraseña inicial que el Administrador del sistema define al crear la cuenta de usuario. Al ingresar por primera vez al sistema, el usuario debe ingresar con su contraseña inicial e inmediatamente cambiarla para evitar que el Administrador se impersone con sus credenciales.
Ejecución	1. Ventana Módulo de Seguridad. 2. Botón Cambiar Clave.
Procedimiento	1. En la ventana Módulo de Inicio, seleccionar el botón Módulo de Seguridad. 2. Ingresar la cuenta de usuario y la nueva contraseña (confirmar contraseña). 3. Seleccionar el botón Cambiar Clave.
Precondiciones	El usuario debe poseer una cuenta de usuario en el sistema.
Poscondiciones	El usuario puede ingresar y utilizar el sistema en forma segura.
Ejecución Alternativa	Seleccionar el botón Finalizar y volver al Módulo de Inicio.
Identificación de Interfaces de usuario	Ventana Ingreso al Sistema. Ventana Módulo de Inicio. Ventana Módulo de Seguridad.
Condiciones de fallo	Ingreso erróneo de contraseña al cambiarla.

Tabla 4-18. Especificación de Caso de Uso RF3, Cambio de Contraseña.

Descripción del escenario	El usuario debe seleccionar los reportes que desea visualizar.
Ejecución	1. Ventana Archivo de Salida. 2. Opciones: Mostrar Salida de Observaciones Verdes Mostrar Salida de Observaciones Amarillas Mostrar Salida de Observaciones Rojas
Procedimiento	1. En la ventana Módulo de Inicio, seleccionar el botón Módulo de Consulta de Reportes. 2. En la ventana Archivo de Salida, seleccionar las opciones de Reportes que se desean obtener. 3. Seleccionar el botón Finalizar.
Precondiciones	El usuario debe poseer una cuenta de usuario en el sistema.

	El usuario debe ingresar al sistema correctamente su usuario y clave. El usuario debe posee permisos de consultar Reportes.
Poscondiciones	No posee
Ejecución Alternativa	Seleccionar el botón Finalizar y volver al Módulo de Inicio.
Identificación de Interfaces de usuario	Ventana Módulo de Inicio. Ventana Archivo de Salida.
Condiciones de fallo	No posee

Tabla 4-19. Especificación de Caso de Uso RF4, Consulta de Reportes.

Descripción del escenario	El usuario puede visualizar Gráficos con Información Histórica donde se muestra la evolución de los eventos procesados.
Ejecución	1. Ventana Módulo de Estadísticas Históricas. 2. Opciones: Total de Eventos. Tipo de Eventos.
Procedimiento	1. En la ventana Módulo de Inicio, seleccionar el botón Módulo de Consulta de Estadísticas Históricas. 2. En la ventana Módulo de Estadísticas Históricas, seleccionar las opciones de gráficos que se desean visualiza. 3. Seleccionar el botón Finalizar.
Precondiciones	Ejecución del Proceso de Análisis de Eventos.
Poscondiciones	No posee.
Ejecución Alternativa	Seleccionar el botón Finalizar y volver al Módulo de Inicio.
Identificación de Interfaces de usuario	Ventana Módulo de Inicio. Ventana Módulo de Consulta de Estadísticas Históricas.
Condiciones de fallo	No se encuentra información histórica o el formato no es adecuado.

Tabla 4-20. Especificación de Caso de Uso RF5, Consulta Estadísticas Históricas.

Descripción del escenario	El usuario debe seleccionar la información de las estadísticas y los reportes que desea recibir del sistema.
Ejecución	1. Ventana Configuración Vistas y Reportes. 2. Opciones: Información Observaciones en Proceso. Gráfico de Secciones Mostrar Información de Reglas Mostrar Información de Usuarios

	Mostrar Reportes de Observaciones.
Procedimiento	1. En la ventana Módulo de Inicio, seleccionar el botón Módulo de Análisis. 2. En la ventana Configuración Vistas y Reportes, seleccionar las opciones de estadísticas que se desean visualizar. 3. En la ventana Configuración Vistas y Reportes, seleccionar las opciones de Reportes que se desean obtener. 4. Seleccionar el botón Continuar.
Precondiciones	El usuario debe poseer una cuenta de usuario en el sistema. El usuario debe ingresar al sistema correctamente su usuario y clave.
Poscondiciones	No posee
Ejecución Alternativa	Seleccionar el botón Cancelar y volver al Módulo de Inicio.
Identificación de Interfaces de usuario	Ventana Módulo de Inicio. Ventana Configuración Vistas y Reportes.
Condiciones de fallo	No posee

Tabla 4-21. Especificación de Caso de Uso RF6, Configurar Vistas y Reportes.

Descripción del escenario	El usuario debe seleccionar o verificar la ruta y nombre del archivo de entrada que contiene los registros a procesar y analizar.
Ejecución	1. Ventana Módulo de Análisis de Eventos. 2. Opción Archivo de Entrada.
Procedimiento	1. En la ventana Módulo de Inicio, seleccionar el botón Módulo de Análisis. 2. En la ventana Configuración Vistas y Reportes, seleccionar las opciones deseas y seleccionar el botón Continuar. 3. En la ventana Módulo de Análisis de Eventos, seleccionar la opción Archivo de Entrada. 4. Ingresar la ruta y el archivo de Entrada.
Precondiciones	La ruta del archivo seleccionado debe existir en el sistema de archivos del equipo. El archivo seleccionado debe existir.
Poscondiciones	No posee.
Ejecución Alternativa	Seleccionar el botón Cancelar y volver al Módulo de Inicio.
Identificación de Interfaces de usuario	Ventana Módulo de Inicio. Ventana Configuración Vistas y Reportes. Ventana Módulo de Análisis de Eventos.
Condiciones de fallo	La ruta de la carpeta seleccionada no existe en el sistema de archivos del equipo. El archivo seleccionado no existe.

Tabla 4-22. Especificación de Caso de Uso RF7, Selección Archivo de Entrada.

Descripción del escenario	El usuario debe seleccionar o verificar la ruta y nombres de los archivos de salida donde se almacenarán los resultados del análisis. Es mandatario ingresar tres archivos de salida, un archivo por cada tipo de observaciones.
Ejecución	1. Ventana Módulo de Análisis de Eventos. 2. Opciones: Archivo de Salida Verdes. Archivo de Salida Amarillas. Archivo de Salida Rojas.
Procedimiento	1. En la ventana Módulo de Inicio, seleccionar el botón Módulo de Análisis. 2. En la ventana Configuración Vistas y Reportes, seleccionar las opciones deseas y seleccionar el botón Continuar. 3. En la ventana de Análisis de Eventos: a. Seleccionar la opción Archivo de Salida Verdes, y luego ingresar o verificar la ruta y el nombre del archivo de Salida de las Observaciones Verdes. b. Seleccionar la opción Archivo de Salida Amarillas, y luego ingresar o verificar la ruta y el nombre del archivo de Salida de las Observaciones Amarillas. c. Seleccionar la opción Archivo de Salida Rojas, y luego ingresar o verificar la ruta y el nombre del archivo de Salida de las Observaciones Rojas.
Precondiciones	Las rutas de los archivos ingresados deben existir en el sistema de archivos del equipo. Los archivos ingresados deben existir previamente.
Poscondiciones	No posee.
Ejecución Alternativa	Seleccionar el botón Cancelar y volver al Módulo de Inicio.
Identificación de Interfaces de usuario	Ventana Módulo de Inicio. Ventana Configuración Vistas y Reportes. Ventana Módulo de Análisis de Eventos.
Condiciones de fallo	La ruta de las carpetas seleccionadas no existen en el sistema de archivos del equipo. Los archivos seleccionados no existen.

Tabla 4-23. Especificación de Caso de Uso RF8, Selección Archivos de Salida.

Descripción del escenario	Con la información suministrada al momento el sistema está en condiciones de comenzar el Análisis de Eventos. El usuario debe ejecutar la opción para que el sistema, comience la tarea.
Ejecución	1. Ventana Módulo de Análisis de Eventos.

	2. Botón Comenzar el Proceso de Análisis de Eventos.
Procedimiento	1. En la ventana Módulo de Inicio, seleccionar el botón Módulo de Análisis. 2. En la ventana Configuración Vistas y Reportes, seleccionar las opciones deseas y seleccionar el botón Continuar. 3. En la ventana de Análisis de Eventos, Seleccionar o verificar las rutas de los Archivo de trabajo. 4. Ejecutar el proceso de Análisis con el botón Comenzar el Proceso de Análisis de Eventos.
Precondiciones	Los archivos de entrada y salidas seleccionados deben existir y en la ruta especificada. Los archivos de entrada y salidas seleccionados deben poseer el formato adecuado.
Poscondiciones	No posee.
Ejecución Alternativa	Seleccionar el botón Cancelar y volver al Módulo de Inicio.
Identificación de Interfaces de usuario	Ventana Módulo de Inicio. Ventana Configuración Vistas y Reportes. Ventana Módulo de Análisis de Eventos.
Condiciones de fallo	Los archivos de entrada y/o salidas seleccionados no existen. Los archivos de entrada y/o salidas seleccionados poseen errores y/o están corruptos y/o no tienen el formato adecuado.

Tabla 4-24. Especificación de Caso de Uso RF9, Análisis de Registros.

Descripción del escenario	El usuario puede visualizar el Monitor del Registro en proceso durante la ejecución del análisis de los eventos.
Ejecución	Ventana Evento en Análisis.
Procedimiento	1. En la ventana Módulo de Inicio, seleccionar el botón Módulo de Análisis. 2. En la ventana Configuración Vistas y Reportes, seleccionar las opciones deseas y seleccionar el botón Continuar. 3. En la ventana de Análisis de Eventos, Seleccionar o verificar las rutas de los Archivo de trabajo. 4. Ejecutar el proceso de Análisis con el botón Comenzar el Proceso de Análisis de Eventos. 5. Visualizar la Ventana Evento en Análisis.
Precondiciones	Ejecución del Proceso de Análisis de Eventos.
Poscondiciones	No posee
Ejecución Alternativa	Seleccionar el botón Cancelar y volver al Módulo de Inicio.
Identificación de Interfaces de usuario	Ventana Módulo de Inicio. Ventana Configuración Vistas y Reportes. Ventana Módulo de Análisis de Eventos. Ventana Evento en Análisis.

Condiciones de fallo	El archivo de entrada no tiene el formato adecuado.

Tabla 4-25. Especificación de Caso de Uso RF10, Visualizar Monitor Registro en Proceso.

Descripción del escenario	El usuario puede visualizar la Cantidad de Observaciones Procesadas durante la ejecución del análisis de los eventos.
Ejecución	Ventana Módulo de Estadísticas.
Procedimiento	1. En la ventana Módulo de Inicio, seleccionar el botón Módulo de Análisis. 2. En la ventana Configuración Vistas y Reportes, seleccionar las opciones deseas y seleccionar el botón Continuar. 3. En la ventana de Análisis de Eventos, Seleccionar o verificar las rutas de los Archivo de trabajo. 4. Ejecutar el proceso de Análisis con el botón Comenzar el Proceso de Análisis de Eventos. 5. Visualizar la Ventana Módulo de Estadísticas.
Precondiciones	Ejecución del Proceso de Análisis de Eventos.
Poscondiciones	No posee.
Ejecución Alternativa	Seleccionar el botón Cancelar y volver al Módulo de Inicio.
Identificación de Interfaces de usuario	Ventana Módulo de Inicio. Ventana Configuración Vistas y Reportes. Ventana Módulo de Análisis de Eventos. Ventana Módulo de Estadísticas.
Condiciones de fallo	El archivo de entrada no tiene el formato adecuado.

Tabla 4-26. Especificación de Caso de Uso RF11, Visualizar Monitor Cantidad de Observaciones Procesadas.

Descripción del escenario	El usuario puede visualizar un Gráfico de Secciones donde se muestra la distribución de las observaciones por tipo (Verde, Amarilla, Roja).
Ejecución	1. Ventana Gráfico de Secciones. 2. Botón Ver Gráfico.
Procedimiento	1. En la ventana Módulo de Inicio, seleccionar el botón Módulo de Análisis. 2. En la ventana Configuración Vistas y Reportes, seleccionar las opciones deseas y seleccionar el botón Continuar. 3. En la ventana de Análisis de Eventos, Seleccionar o verificar las rutas de los Archivo de trabajo. 4. Ejecutar el proceso de Análisis con el botón Comenzar el Proceso de Análisis de Eventos. 5. En la ventana Gráfico de Secciones, seleccionar el botón Ver Gráfico.

	6. Visualizar Gráfico de Secciones generado.
Precondiciones	Ejecución del Proceso de Análisis de Eventos.
Poscondiciones	No posee.
Ejecución Alternativa	Seleccionar el botón Cancelar y volver al Módulo de Inicio.
Identificación de Interfaces de usuario	Ventana Módulo de Inicio. Ventana Configuración Vistas y Reportes. Ventana Módulo de Análisis de Eventos. Ventana Gráfico de Secciones.
Condiciones de fallo	El archivo de entrada no tiene el formato adecuado. Los datos de salida no son consistentes y el gráfico no puede generarse.

Tabla 4-27. Especificación de Caso de Uso RF12, Visualizar Gráfico de Secciones.

Descripción del escenario	El usuario puede visualizar información estadística de cada regla de decisión utilizada por el proceso.
Ejecución	1. Ventana Información de Reglas. 2. Botón Ver Información de Regla.
Procedimiento	1. En la ventana Módulo de Inicio, seleccionar el botón Módulo de Análisis. 2. En la ventana Configuración Vistas y Reportes, seleccionar las opciones deseas y seleccionar el botón Continuar. 3. En la ventana de Análisis de Eventos, Seleccionar o verificar las rutas de los Archivo de trabajo. 4. Ejecutar el proceso de Análisis con el botón Comenzar el Proceso de Análisis de Eventos. 5. En la ventana Información de Reglas, en la lista Seleccionar una Regla, seleccionar la regla que se desea analizar y luego presionar el Botón Ver Información de Regla. 6. Visualizar la ventana Información de Regla Individual.
Precondiciones	Ejecución del Proceso de Análisis de Eventos.
Poscondiciones	No posee.
Ejecución Alternativa	Seleccionar el botón Cancelar y volver al Módulo de Inicio.
Identificación de Interfaces de usuario	Ventana Módulo de Inicio. Ventana Configuración Vistas y Reportes. Ventana Módulo de Análisis de Eventos. Ventana Información de Reglas. Ventana Información de Regla Individual.
Condiciones de fallo	El archivo de entrada no tiene el formato adecuado.

Tabla 4-28. Especificación de Caso de Uso RF13, Visualizar Estadísticas de Reglas.

Descripción del escenario	El usuario puede visualizar información estadística de cada Usuario administrador afectado por las reglas de decisión. Por ejemplo cuantas reglas y de que tipo afectaron a cada usuario.
Ejecución	Ventana Información de Usuarios.
Procedimiento	1. En la ventana Módulo de Inicio, seleccionar el botón Módulo de Análisis. 2. En la ventana Configuración Vistas y Reportes, seleccionar las opciones deseas y seleccionar el botón Continuar. 3. En la ventana de Análisis de Eventos, Seleccionar o verificar las rutas de los Archivo de trabajo. 4. Ejecutar el proceso de Análisis con el botón Comenzar el Proceso de Análisis de Eventos. 5. Visualizar la ventana Información de Usuarios.
Precondiciones	Ejecución del Proceso de Análisis de Eventos.
Poscondiciones	No posee.
Ejecución Alternativa	Seleccionar el botón Cancelar y volver al Módulo de Inicio.
Identificación de Interfaces de usuario	Ventana Módulo de Inicio. Ventana Configuración Vistas y Reportes. Ventana Módulo de Análisis de Eventos. Ventana Información de Usuarios.
Condiciones de fallo	El archivo de entrada no tiene el formato adecuado.

Tabla 4-29. Especificación de Caso de Uso RF14, Visualizar Estadísticas de Usuario.

Descripción del escenario	El usuario puede visualizar y analizar la información de Salida en Reportes independientes, uno por cada tipo de Observación.
Ejecución	1. Ventana Archivo de Salida. 2. Opciones: a. Rojas b. Amarillas c. Verdes
Procedimiento	1. En la ventana Módulo de Inicio, seleccionar el botón Módulo de Análisis. 2. En la ventana Configuración Vistas y Reportes, seleccionar las opciones deseas y seleccionar el botón Continuar. 3. En la ventana de Análisis de Eventos, Seleccionar o verificar las rutas de los Archivo de trabajo. 4. Ejecutar el proceso de Análisis con el botón Comenzar el Proceso de Análisis de Eventos. 5. En la ventana Archivo de Salida, seleccionar las opciones Rojas, Amarillas o Verdes para visualizar el Reporte deseado.
Precondiciones	Ejecución del Proceso de Análisis de Eventos.
Poscondiciones	No posee.

Ejecución Alternativa	Seleccionar el botón Finalizar y volver al Módulo de Inicio.
Identificación de Interfaces de usuario	Ventana Módulo de Inicio. Ventana Configuración Vistas y Reportes. Ventana Módulo de Análisis de Eventos. Ventana Archivo de Salida.
Condiciones de fallo	El archivo de entrada no tiene el formato adecuado.

Tabla 4-30. Especificación de Caso de Uso RF15, Visualizar Reportes.

Descripción del escenario	Salir del sistema.
Ejecución	1. Ventana Módulo de Inicio. 2. Botón Salir.
Procedimiento	1. El usuario debe desplazarse a la ventana Módulo de Inicio 2. Seleccionar el botón Salir. 3. Se cierra el sistema.
Precondiciones	Ingresar al sistema.
Poscondiciones	No posee
Ejecución Alternativa	a. Seleccionar el botón Módulo de Análisis. b. Seleccionar el botón Módulo de Consulta de Reportes. c. Seleccionar el botón Módulo de Consulta de Estadísticas Históricas. d. Seleccionar el botón Módulo de Seguridad.
Identificación de Interfaces de usuario	Ventana Módulo de Inicio
Condiciones de fallo	No posee

Tabla 4-31. Especificación de Caso de Uso RF16, Salir del Sistema.

Descripción de Subsistemas de Análisis

El sistema se puede descomponer, para facilitar su análisis, en los siguientes subsistemas:

- Seguridad y Control de Acceso: validación del usuario que accede al sistema.
- Análisis de Registros: cuyo mecanismo principal son las Reglas de Decisión
- Gestor de datos: acceso al fichero que contiene los datos de entrada y escritura a disco de los archivos con la información relevante de cada observación.

- Generación de Reportes: permite acceder a la información histórica y reportes de salida.

Descripción de Interfaces entre Subsistemas

El subsistema de Seguridad y Control de Acceso permite el acceso al subsistema de Análisis de Registros.

El subsistema Análisis de los Registros interactúa fuertemente con los subsistemas Gestor de datos (se utiliza para obtener los datos de entrada y escribir la información de salida) y Generación de Reportes (por cada evento analizado, se invoca éste para efectuar el registro correspondiente).

El subsistema de Generación de Reportes llama al subsistema Gestor de datos para leer la información requerida.

Modelo de Clases

Las clases descubiertas en el sistema son las siguientes:

Nombre Clase	Descripción
OBSERVACIONES	Representa los eventos a evaluar.
USUARIOS	Representa los usuarios operadores del sistema
GRAFICOS	Representa los gráficos que se usarán en el sistema para dibujar las estadísticas de los registros y usuarios.
ARCHIVOS	Representa los contenedores de datos e información.

Tabla 4-32. Modelo de Clases.

Análisis de la Realización de los Casos de Uso

Representación Diagramas de Secuencia

Los diagramas de secuencia se muestran en las figuras 4-29 a 4-44.

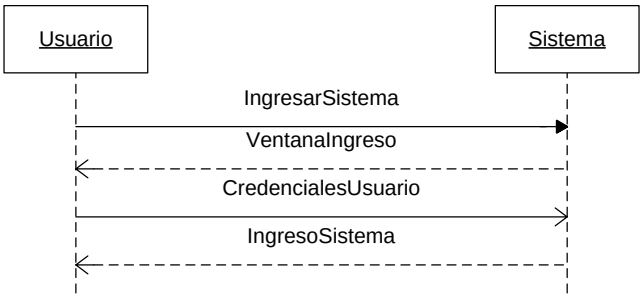


Figura 4-29. Diagrama de Secuencia RF1. Ingreso al Sistema.

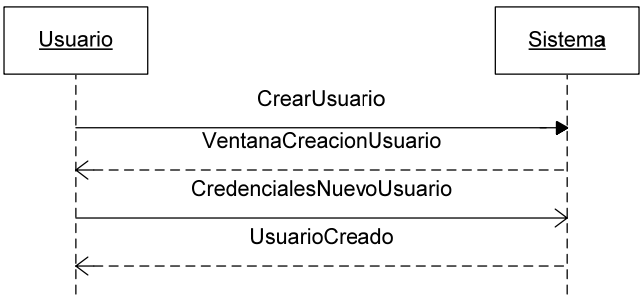


Figura 4-30. Diagrama de Secuencia RF2. Crear Usuario.

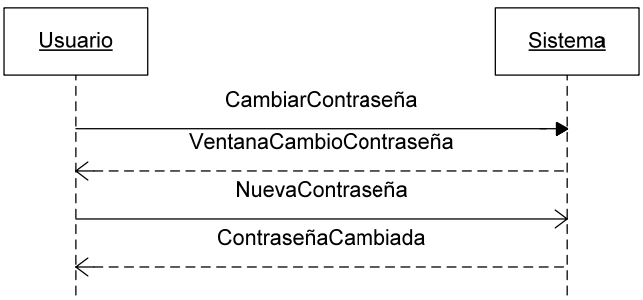


Figura 4-31. Diagrama de Secuencia RF3. Cambio de Contraseña.

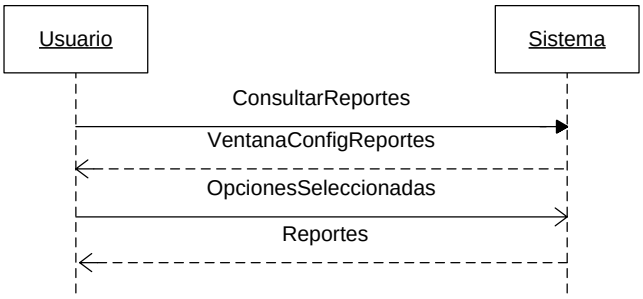


Figura 4-32. Diagrama de Secuencia RF4. Consulta de Reportes.

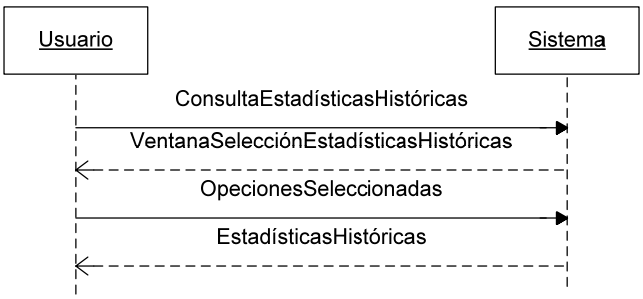


Figura 4-33. Diagrama de Secuencia RF5. Consulta de Estadísticas Históricas.

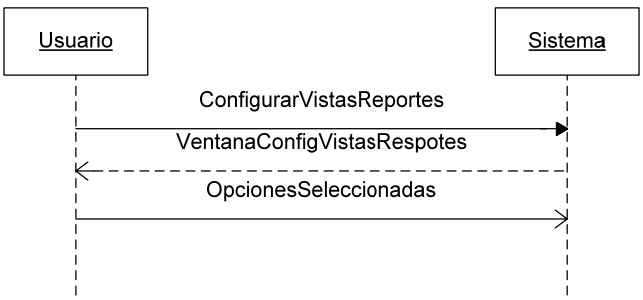


Figura 4-34. Diagrama de Secuencia RF6. Configurar Vistas y Reportes.

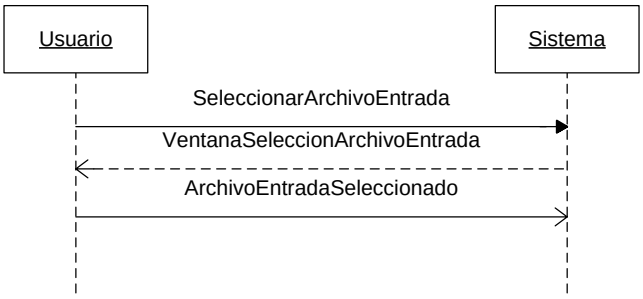


Figura 4-35. Diagrama de Secuencia RF7. Selección Archivo de Entrada.

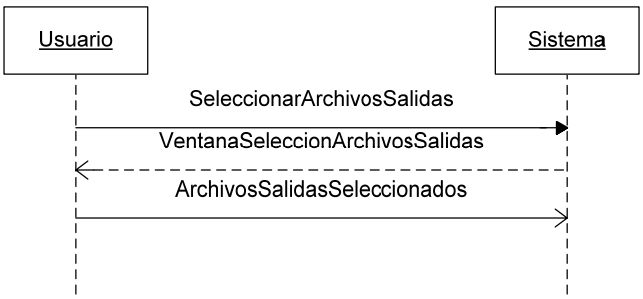


Figura 4-36. Diagrama de Secuencia RF8. Selección Archivos de Salida.

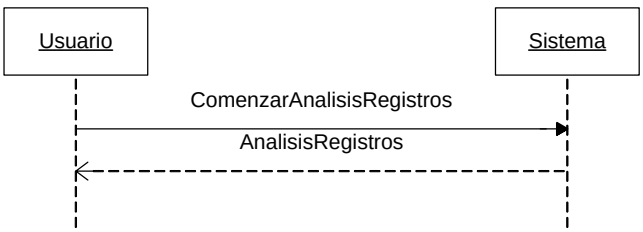


Figura 4-37. Diagrama de Secuencia RF9. Análisis de Registros.

Figura 4-38. Diagrama de Secuencia RF10. Visualizar Monitor Registro en Proceso.

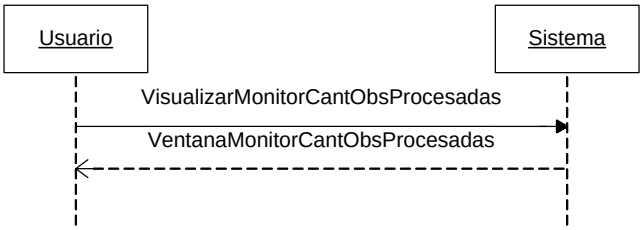


Figura 4-39. Diagrama de Secuencia RF11. Visualizar Monitor Cantidad de Observaciones Procesadas.

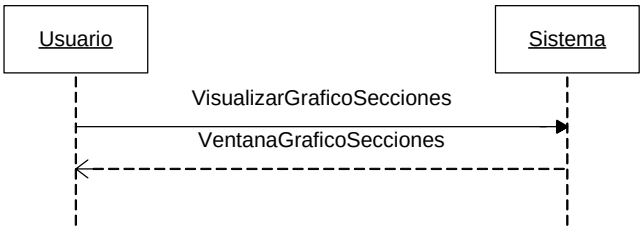


Figura 4-40. Diagrama de Secuencia RF12. Visualizar Gráfico de Secciones.

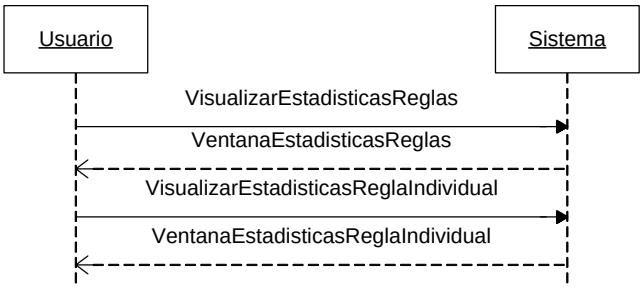


Figura 4-41. Diagrama de Secuencia RF13. Visualizar Estadísticas de Reglas.

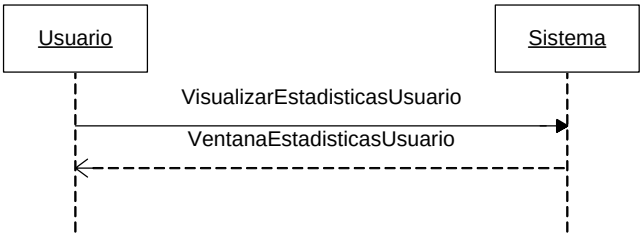


Figura 4-42. Diagrama de Secuencia RF14. Visualizar Estadísticas de Usuario.

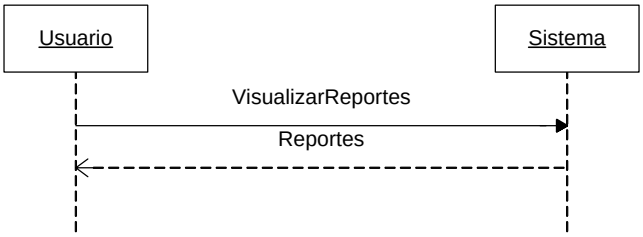


Figura 4-43. Diagrama de Secuencia RF15. Visualizar Reportes.

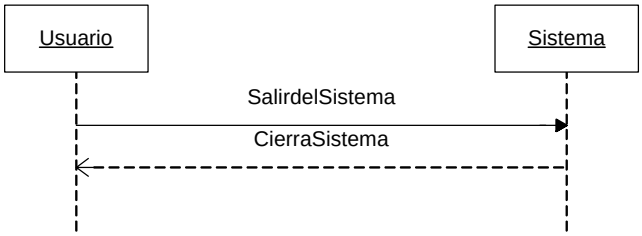


Figura 4-44. Diagrama de Secuencia RF16. Salir del Sistema.

Comportamiento de las Clases de Análisis

Las responsabilidades y atributos relevantes de las clases se muestran en la tabla 4-33.

Nombre Clase	Atributos	Métodos
OBSERVACIONES	ID DIA EVENTO HORA USUARIO CLASIFICACION REGLA HORA_EJECUCION	LEER() APLICAR_REGLAS() ESCRIBIR()
USUARIO	ID NOMBRE CLAVE PERMISOS	CREAR() CAMBIAR_CLAVE() VALIDAR()
GRAFICOS	EJE_X EJE_Y NOMBRE_EJE_X NOMBRE_EJE_Y ESCALA_EJE_X ESCALA_EJE_Y FUNCION	MOSTRAR() DIBUJAR() OCULTAR()
ARCHIVOS	NOMBRE RUTA PERMISOS BLOQUEO	ABRIR() ESCRIBIR() CERRAR()

Nombre Clase	Atributos	Métodos
	TAMAÑO FECHA_CREADO FECHA_MODIFICADO	

Tabla 4-33. Descripción de Clases.

Especificación de Interfaz de Usuario

Principios Generales de la Interfaz.

La interfaz del usuario será gráfica. La misma permitirá, a través de opciones de selección y botones, la elección de las estadísticas a mostrar y los reportes a generar.

Cada ventana mostrar información o datos relacionados o con las mismas características. Por ejemplo, una ventana mostrará información estadística de las observaciones, otra ventana mostrará el soporte, confianza de las reglas, etc.

Los mensajes de error se mostrarán en las ventanas emergentes propias de la herramienta de desarrollo.

La versión beta no contendrá ayuda en línea.

Catálogo de Perfiles de Usuarios.

En la presente versión beta permite tres perfiles de operadores del sistema:

- Perfil Administrador: será el único encargado de crear los usuarios en el sistema.
- Perfil Operador: tendrá acceso total al sistema software y podrán explotar plenamente las funcionalidades, [excepto la creación de nuevos usuarios].
- Perfil Auditor: podrá tener derechos solo para consultar reportes y archivos de salida.

Catálogo de Controles y Elementos de Diseño de Interfaz de Pantalla.

El catálogo se describe en la tabla 4-34.

Ventana	Posibilidad de cambio de tamaño / cambio de ubicación	Dispositivos de entrada para su ejecución	Datos que se usan y se generan luego de su ejecución	Controles y elementos inicialmente activos e inactivos
Análisis de Eventos de Seguridad	No / No	Teclado o Mouse.	No Posee	No Posee
Ingreso al Sistema	No / No	Teclado o Mouse.	Credenciales del Operador del sistema.	Validación de Cuenta y Clave del Operador.
Módulo de Inicio	Si / Si	Teclado o Mouse.	No Posee	- Menú de Opciones de Selección. - Validación de Cuenta y Clave del Operador.
Configuración Vistas y Reportes	Si / Si	Teclado o Mouse.	Tipo de Vistas y Reportes Seleccionados	Tipo de Vistas y Reportes para Selección.
Módulo de Análisis de Eventos	Si / Si	Teclado o Mouse.	Selección del Archivo de Entrada y los Archivos de Salida.	Validación que la ruta y los archivos seleccionados existan.
Evento en Análisis	Si / Si	Teclado o Mouse.	Archivo de Entrada y los Archivos de Salida.	Atributos del registro en análisis.
Módulo de Estadísticas	Si / Si	Teclado o Mouse.	Archivo de Entrada y los Archivos de Salida.	Cantidad de registros analizados.
Gráfico de Secciones	Si / Si	Teclado o Mouse.	Estadísticas de los registros analizados.	- Consistencia de Cantidades Totales de registros. - Gráfico de secciones.
Información de Reglas	Si / Si	Teclado o Mouse.	Estadísticas de los registros analizados.	Menú de selección de las Reglas utilizadas.
Información de Reglas Individuales	Si / Si	Teclado o Mouse.	Estadísticas de los registros analizados.	Información de las Reglas.
Información de Usuarios	Si / Si	Teclado o Mouse.	Estadísticas de los registros analizados.	Información de Tipo de eventos por Administrador.
Archivo de Salida	Si / Si	Teclado o Mouse.	Información contenida en los Archivos de Salida.	Selección del archivo de salida a usar.
Módulo de Estadísticas Históricas	Si / Si	Teclado o Mouse.	Información Histórica almacenada de los	- Validación de Cuenta y Clave del Operador.

Ventana	Posibilidad de cambio de tamaño / cambio de ubicación	Dispositivos de entrada para su ejecución	Datos que se usan y se generan luego de su ejecución	Controles y elementos inicialmente activos e inactivos
			análisis previos.	- Selección del gráfico a visualizar. - Gráficos de la Evolución de los registros analizados.
Módulo de Seguridad	Si / SI	Teclado o Mouse.	Información almacenada de Usuarios/Claves.	- Validación de Cuenta y Clave del Operador. - Opciones de Alta Modificación de Usuario/Clave.

Tabla 4-34. Diseño de Interfaz de Pantalla.

Modelo de Navegación de Interfaz de Pantalla.

En la siguiente figura 4-45 se muestra el modelo de navegación de interfaz de pantalla y como se vinculan entre ellas.

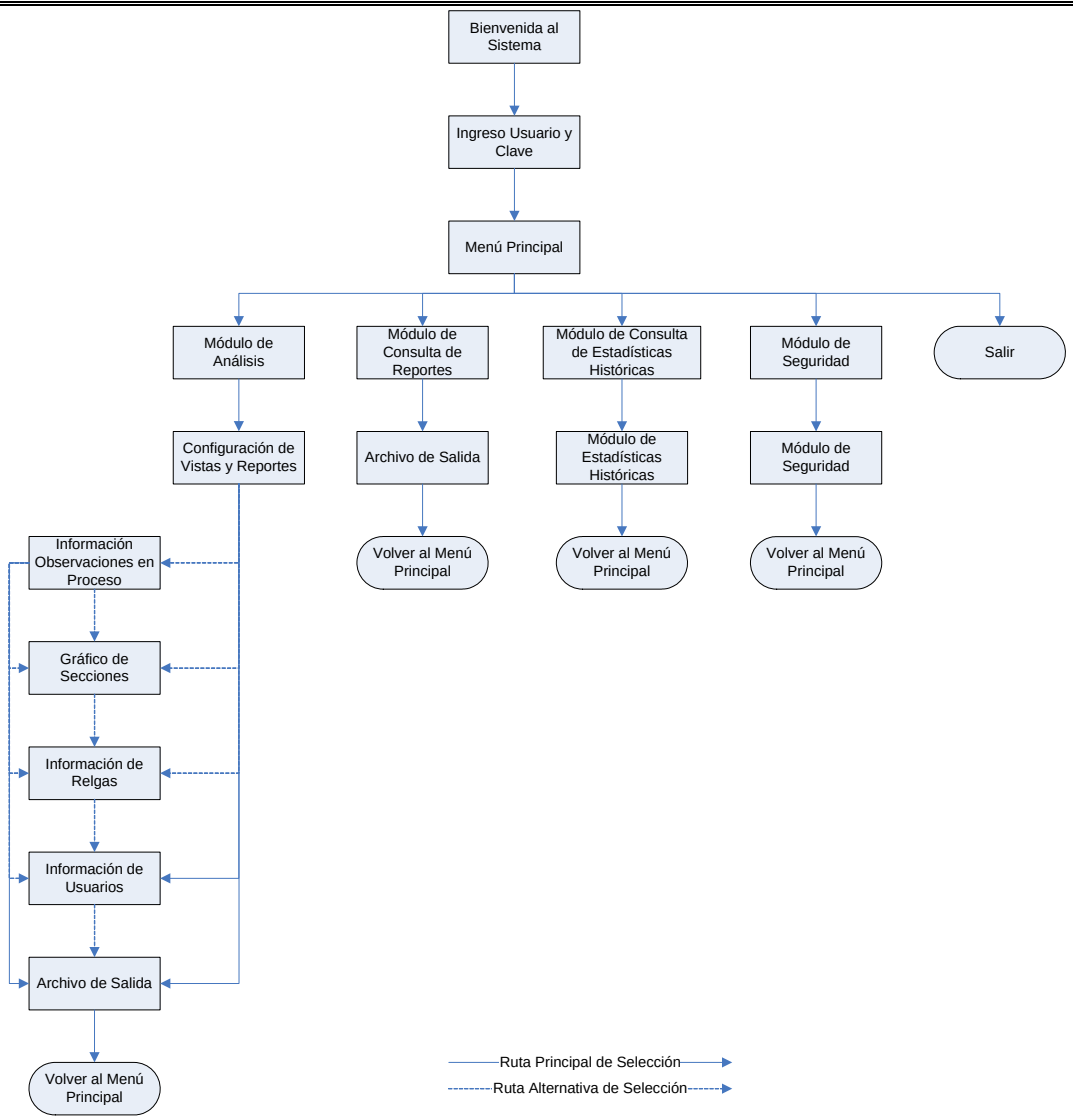


Figura 4-45. Modelo Interfaz de Pantalla.

Descripción de cada Interfaz.

El objetivo es realizar un análisis de los procesos del sistema en los que se requiere una interacción del usuario, con el fin de crear una interfaz que satisfaga todos los requisitos establecidos, teniendo en cuenta los diferentes perfiles a quiénes va dirigido.

A continuación se detalla la función y el objetivo de cada ventana.

Ventana de Bienvenida al Sistema.

Se utiliza para presentar formalmente el sistema al operador del mismo y mostrar su versión.

Ventana de Ingreso al Sistema.

El operador del Sistema debe ingresar sus credenciales de autenticación. Se distinguen tres perfiles de operadores (administración de credenciales de operadores, ejecución de análisis de eventos, consulta de reportes)

Ventana del Módulo de Inicio.

Se utiliza para ingresar a todas las funcionalidad del sistema. Antes de ingresar a un módulo, el sistema valida las credenciales del operador y verifica que tenga suficientes permisos para la ejecución del mismo.

Ventana de Configuración de Vistas y Reportes.

El operador del Sistema debe seleccionar las Estadísticas que desea visualizar durante y al finalizar el análisis de los eventos. Estas opciones no son obligatorias.

Ventana del Módulo de Análisis de Eventos.

El operador del Sistema debe seleccionar el Archivo de Entrada y los Archivos de Salidas que el sistema debe utilizar. El archivo de entrada contiene los nuevos registros para examinar. En los archivos de salidas se almacenarán los resultados de las inspecciones, lo cuales se dividirán por tipo (eventos correctos – "Verdes", dudosos – "Amarillos" e incorrectos – "Rojos"). Estas opciones son obligatorias y el sistema certificará que tanto la ruta como el nombre sean válidos.

Ventana de Evento en Análisis.

El operador podrá observar los atributos del evento que está siendo analizado en el momento.

Ventana del Módulo de Estadísticas.

El operador podrá observar la cantidad de eventos (u observaciones) que han sido procesadas hasta ese momento.

Ventana del Gráfico de Secciones.

El operador podrá observar la distribución por tipo (Verdes, Amarillos, Rojos), de los eventos (u observaciones) procesadas.

Ventana de Información de Reglas.

El operador podrá observar información estadística de cada regla utilizada por el sistema. Por ejemplo, cantidad de eventos afectados, soporte.

Ventana de Información de Usuarios.

El operador podrá observar la cantidad de eventos y por tipo, que realizó cada administrador de redes.

Ventana del Informe de Salida.

El operador podrá observar el resultado del análisis de cada registro. La información que contendrá es la siguiente: *Número de registro, Día, Hora, Usuario, Evento, Regla, Condición de Activación, Hora de Ejecución*.

Ventana del Módulo de Estadísticas Históricas.

El operador podrá obtener información histórica acerca de la cantidad de registro por tipo en cada ejecución.

Ventana del Módulo de Seguridad.

El administrador del sistema podrá:

- Crear nuevas credenciales para usuarios,
- Asignar los permisos a los módulos que correspondan y
- Cambiar la clave de las credenciales.

Formatos de Impresión.

Con respecto al formato de impresión, no se especifica ningún formateo especial. Si se desea imprimir el informe de salida generado por la aplicación, el mismo se puede abrir con un editor de archivos de texto y luego ejecutar la impresión.

Verificación de los Modelos

Se verificó la calidad de los modelos generados en el proceso de Análisis del Sistema de Información para garantizar la calidad de los mismos, y asegurar que los usuarios y el Analista tienen el mismo concepto del sistema.

Para cumplir dicho objetivo, se llevaron a cabo las siguientes acciones: Verificación de la calidad técnica de cada modelo, Aseguramiento de la

coherencia entre los distintos modelos, Validación del cumplimiento de los requisitos.

Resultado de Análisis de Consistencia de los Modelos.

El resultado del análisis de consistencia se muestra en la tabla 4-35.

Requisito	Caso de Uso	Especificación de los Casos de Uso	Modelos de Secuencia
RF1. Ingreso al sistema con usuario y clave.	Desarrollado	Desarrollado	Desarrollado
RF2. Permitir la creación de credenciales de usuario para la validación del ingreso al sistema.	Desarrollado	Desarrollado	Desarrollado
RF3. Permitir el cambio de clave a los usuarios.	Desarrollado	Desarrollado	Desarrollado
RF4. Consultar reportes de salida.	Desarrollado	Desarrollado	Desarrollado
RF5. Consultar estadísticas históricas.	Desarrollado	Desarrollado	Desarrollado
RF6. Seleccionar vistas y reportes a desplegar durante análisis de registros.	Desarrollado	Desarrollado	Desarrollado
RF7. Seleccionar archivo de entrada.	Desarrollado	Desarrollado	Desarrollado
RF8. Seleccionar archivos de salida.	Desarrollado	Desarrollado	Desarrollado
RF9. Permitir ejecución de análisis de registros.	Desarrollado	Desarrollado	Desarrollado
RF10. Permitir la visualización del registro en análisis en el momento de ejecución.	Desarrollado	Desarrollado	Desarrollado
RF11. Permitir la visualización de la cantidad de registros por tipo, analizados en el momento de ejecución.	Desarrollado	Desarrollado	Desarrollado
RF12. Permitir la visualización de gráficos de secciones de la cantidad de registros por tipo.	Desarrollado	Desarrollado	Desarrollado
RF13. Permitir la visualización de estadísticas de las reglas utilizadas.	Desarrollado	Desarrollado	Desarrollado
RF14. Permitir la visualización de estadísticas por usuarios administradores de redes involucrados en los	Desarrollado	Desarrollado	Desarrollado

Requisito	Caso de Uso	Especificación de los Casos de Uso	Modelos de Secuencia
registros.			
RF15. Permitir la visualización de los archivos de salida generados con la información producida de los registros.	Desarrollado	Desarrollado	Desarrollado
RF16. Salir del sistema.	Desarrollado	Desarrollado	Desarrollado

Tabla 4-35. Análisis de Consistencia de los Modelos de la Fase de Análisis.

Plan de Pruebas

El conjunto de pruebas a llevar a cabo, consistirán en:

- Realizar el análisis de no menos de 2000 observaciones.
- Los eventos deberán incluir tareas realizadas días laborables y no laborales.
- Generar todas las estadísticas disponibles.
- Generar todos los reportes disponibles.
- Verificar la eficacia, efectividad de los resultados.
- Verificar el porcentual de error obtenido.
- Analizar el tiempo insumido en la tarea y compararlo, si es posible, con la actividad realizada actualmente.

Las personas que participarán de las pruebas son:

- Staff del sector de Seguridad y Control.
- Analista / Desarrollador del proyecto.

Las pruebas serán documentadas según el formato de la tabla 4-36:

Número Prueba	
Objetivo	
Requisitos	
Caso de Prueba (pasos)	
Resultado Esperado	
Fecha Ejecución	

Resultado	
Notas	

Tabla 4-36. Modelo para Registro de Casos de Pruebas.

Para realizar las pruebas se utilizará el entorno de desarrollo, por cuanto los requisitos de hardware y software son los mismos que los planteados en fases anteriores.

Los criterios de aceptación del sistema son los siguientes:

- Tasa de error menor a 30%
- Reducir el tiempo que insume la tarea en 60%

Aprobación del Análisis del Sistema de Información

En reunión de seguimiento, control y aprobación entre las partes, Tesista y Directora del proyecto, se dio por aprobada esta fase.

El jefe del proyecto comunica formalmente a los participantes, afectados y usuarios los resultados del análisis. Se utiliza el siguiente anuncio.

Estimados Colaboradores,

Cumplo en informarles que la fase de Análisis del Sistema del proyecto "Análisis de Eventos de Seguridad en Servidores" ha sido aprobada satisfactoriamente.

Desde ya muchas gracias por su participación y compromiso.

4.2.2.2.2 Control de Actividades

Actividades / Tareas	Desarrollo	Justificación
ACTIVIDAD ASI 1: DEFINICIÓN DEL SISTEMA		
Tarea ASI 1.1: Determinación del Alcance del Sistema	SI	Se dispone de la información necesaria.
Tarea ASI 1.2: Identificación del Entorno Tecnológico	SI	Se dispone de la información necesaria.
Tarea ASI 1.3: Especificación de Estándares y Normas	SI	Se dispone de la información necesaria.
Tarea ASI 1.4: Identificación de los Usuarios Participantes y Finales	SI	Se dispone de la información necesaria.
ACTIVIDAD ASI 2: ESTABLECIMIENTO DE REQUISITOS		
Tarea ASI 2.1: Obtención de Requisitos	SI	Se dispone de la información necesaria.
Tarea ASI 2.2: Especificación de Casos de Uso	SI	Se dispone de la información necesaria.
Tarea ASI 2.3: Análisis de Requisitos	SI	Se dispone de la información necesaria.
Tarea ASI 2.4: Validación de Requisitos	SI	Se dispone de la información necesaria.
ACTIVIDAD ASI 3: IDENTIFICACIÓN DE SUBSISTEMAS DE ANÁLISIS		
Tarea ASI 3.1: Determinación de Subsistemas de Análisis	SI	Se dispone de la información necesaria.
Tarea ASI 3.2: Integración de Subsistemas de Análisis	SI	Se dispone de la información necesaria.
ACTIVIDAD ASI 4: ANÁLISIS DE LOS CASOS DE USO		
Tarea ASI 4.1: Identificación de Clases Asociadas a un Caso de Uso	SI	Se dispone de la información necesaria.
Tarea ASI 4.2: Descripción de la Interacción de Objetos	SI	Se dispone de la información necesaria.
ACTIVIDAD ASI 5: ANÁLISIS DE CLASES		
Tarea ASI 5.1: Identificación de Responsabilidades y Atributos	SI	Se dispone de la información necesaria.
Tarea ASI 5.2: Identificación de Asociaciones y Agregaciones	SI	Se dispone de la información necesaria.
Tarea ASI 5.3: Identificación de Generalizaciones	NO	El gestor del lenguaje utilizado realiza esta asignación internamente
ACTIVIDAD ASI 6: ELABORACIÓN DEL MODELO DE DATOS		
Tarea ASI 6.1: Elaboración del Modelo Conceptual de Datos	NO	Dada la naturaleza del sistema no aplica realizar esta tarea
Tarea ASI 6.2: Elaboración del Modelo Lógico de Datos	NO	Dada la naturaleza del sistema no aplica realizar esta tarea

Actividades / Tareas	Desarrollo	Justificación
Tarea ASI 6.3: Normalización del Modelo Lógico de Datos	NO	Dada la naturaleza del sistema no aplica realizar esta tarea
Tarea ASI 6.4: Especificación de Necesidades de Migración de Datos y Carga Inicial	NO	Dada la naturaleza del sistema no aplica realizar esta tarea
ACTIVIDAD ASI 7: ELABORACIÓN DEL MODELO DE PROCESOS		
Tarea ASI 7.1: Obtención del Modelo de Procesos del Sistema	NO	Dada la naturaleza del sistema no aplica realizar esta tarea
Tarea ASI 7.2: Especificación de Interfaces con otros Sistemas	NO	Dada la naturaleza del sistema no aplica realizar esta tarea
ACTIVIDAD ASI 8: DEFINICIÓN DE INTERFACES DE USUARIO		
Tarea ASI 8.1: Especificación de Principios Generales de la Interfaz	SI	Se dispone de la información necesaria.
Tarea ASI 8.2: Identificación de Perfiles y Diálogos	SI	Se dispone de la información necesaria.
Tarea ASI 8.3: Especificación de Formatos Individuales de la Interfaz de Pantalla	SI	Se dispone de la información necesaria.
Tarea ASI 8.4: Especificación del Comportamiento Dinámico de la Interfaz	SI	Se dispone de la información necesaria.
Tarea ASI 8.5: Especificación de Formatos de Impresión	SI	Se dispone de la información necesaria.
ACTIVIDAD ASI 9: ANÁLISIS DE CONSISTENCIA Y ESPECIFICACIÓN DE REQUISITOS		
Tarea ASI 9.1: Verificación de los Modelos	SI	Se dispone de la información necesaria.
Tarea ASI 9.2: Análisis de Consistencia entre Modelos	SI	Se dispone de la información necesaria.
Tarea ASI 9.3: Validación de los Modelos	SI	Se dispone de la información necesaria.
Tarea ASI 9.4: Elaboración de la Especificación de Requisitos Software (ERS)	NO	Se utiliza la información elaborada en las tareas precedentes.
ACTIVIDAD ASI 10: ESPECIFICACIÓN DEL PLAN DE PRUEBAS		
Tarea ASI 10.1: Definición del Alcance de las Pruebas	SI	Se dispone de la información necesaria.
Tarea ASI 10.2: Definición de Requisitos del Entorno de Pruebas	SI	Se dispone de la información necesaria.
Tarea ASI 10.3: Definición de las Pruebas de Aceptación del Sistema	SI	Se dispone de la información necesaria.
ACTIVIDAD ASI 11: APROBACIÓN DEL ANÁLISIS DEL SISTEMA DE INFORMACIÓN		
Tarea 11.1: Presentación y Aprobación del Análisis del Sistema de Información	SI	Se dispone de la información necesaria.

Tabla 4-37. Control de Actividades ASI.

4.2.2.3 Diseño del Sistema de Información (DSI)

4.2.2.3.1 Documento Entregable

DOCUMENTO DE DISEÑO DEL SISTEMA DE INFORMACIÓN

Diseño de la Arquitectura del Sistema

Descomposición Física del Sistema de Información

Los niveles de la arquitectura software se describen mediante la definición de las principales particiones físicas del sistema de información, representadas como nodos y comunicaciones entre nodos.

Se entiende por nodo cada partición física o parte significativa del sistema de información, con características propias de ejecución o función, e incluso de diseño y construcción.

La descomposición física del sistema de información en estudio se muestra en la figura 4-46.

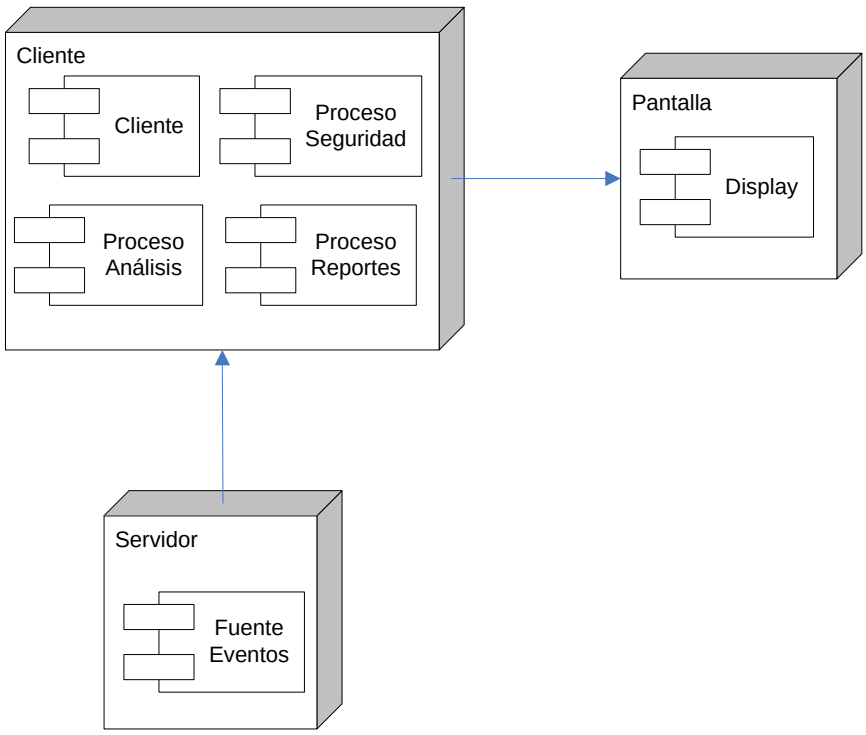


Figura 4-46. Descomposición física del sistema.

Nodos

El nodo *Cliente*, representa la terminal física desde la cual personal de Seguridad y Control ejecutará el sistema.

El nodo *Servidor*, representa el servidor controlar de dominio desde el donde se tomarán los datos de los eventos de seguridad.

El nodo *Pantalla*, representa el dispositivo de salida del sistema.

Componentes

La componente *Cliente*, representa la funcionalidad que puede realizar el personal de Seguridad y Control.

La componente *Proceso Análisis*, representa el proceso principal del sistema encargado de catalogar las observaciones.

La componente *Proceso Seguridad*, es el encargado de validar los permisos de acceso a los distintos procesos del sistema.

La componente *Proceso Reportes*, tiene la función de generar los informes y reportes solicitados por el operador del sistema.

La componente *Display*, es el encargado de mostrar los informes y reportes.

La componente *Fuente Eventos*, representa el sistema generador de eventos de seguridad del servidor controlador de dominio.

Consideraciones relevantes

Los usuarios accederán desde su posición física actual. En la versión Beta solo podrá acceder al sistema un usuario a la vez, para evitar corrupción de los archivos de salida y el procesamiento múltiple de las mismas observaciones.

Los datos tienen alta variabilidad y volumen. El repositorio usado en el dispositivo físico está configurado para sobrescribir los últimos sucesos cuando se llena el espacio asignado al mismo. Para evitar la pérdida de los eventos, se arbitrará un tamaño suficientemente alto al repositorio, como así también la lectura, descarga y resguardo frecuente del mismo.

El proceso principal se ejecutará en un sitio único y centralizado, pudiendo accederse en forma remota desde los puestos finales individuales de trabajo.

Catálogo de Requisitos

Los requisitos que el sistema debe cumplir son los siguientes:

Requisitos de Diseño

- RD1. El lenguaje a utilizar deberá soportar manejo de Reglas de Decisión.
- RD2. El módulo del proceso principal debe ejecutarse en un sitio centralizado.
- RD3. El módulo del proceso principal debe accederse en forma remota desde los puestos de trabajo.
- RD4. Los datos, para su posterior análisis, deben almacenarse en el nodo donde se ejecuta el módulo del proceso principal.

Catálogo de Excepciones

Las excepciones, que describen comportamientos no habituales en el sistema reflejando situaciones anómalas, se describen en la tabla 4-38.

Tipo y descripción de la excepción	Elemento afectado	Respuesta del sistema de información	Elemento asociado a la respuesta esperada del sistema
Tipo Validación. El cliente ingresa un usuario y/o clave errónea al ingresar al sistema	Componente Cliente	*El usuario o la clave es incorrecta*	Componente Proceso de Seguridad
Tipo Validación. El cliente ingresa un usuario y/o clave errónea al crear un usuario o al modificar una clave existente	Componente Cliente	*Las claves no Concuerdan* - *El usuario No existe*	Componente Proceso de Seguridad
Tipo Validación. El cliente ingresa a un módulo en el cual no tiene permisos suficientes	Componente Cliente	*Las credenciales de acceso son inválidas, vuelva a autenticarse al Sistema* - *Usted no tiene permisos suficientes para ingresar a este módulo*	Componente Proceso de Seguridad
Tipo Validación.	Componente	*El archivo de*	Componente

Tipo y descripción de la excepción	Elemento afectado	Respuesta del sistema de información	Elemento asociado a la respuesta esperada del sistema
El cliente ingresar una ruta o nombre del Archivo de Entrada que no existen	Cliente	*Entrada no Existe*	Proceso de Análisis
Tipo Validación. El cliente ingresar una ruta o nombres de los Archivos de Salidas que no existen	Componente Cliente	*El archivo de Salidas * no Existe*	Componente Proceso de Análisis
Tipo Validación. Los valores para representar los gráficos no son válidos	Componente Cliente	*Valores No Aptos para dibujar el Gráfico*	Componente Proceso de Reportes.
Tipo Validación. Para mostrar los Reportes de Salida, la ruta o nombres de los Archivos de Salidas no existen	Componente Cliente	*El archivo de Salidas * no Existe*	Componente Proceso de Reportes.
Tipo Validación. Para mostrar los Reportes de Estadísticas Históricas, la ruta o nombres del Archivo no existen	Componente Cliente	*El archivo Histórico no Existe*	Componente Proceso de Reportes.

Tabla 4-38. Catálogo de Excepciones.

Catálogo de Normas de Diseño y Construcción.

Se utilizará el Lenguaje de Modelado Unificado o UML (del inglés Unified Modeling Language) para especificar y documentar.

El Lenguaje UML v2 incluye más de una decena de diagramas. Con el fin de simplificar la especificación, solo se utilizarán las representaciones que aporten mayor información acerca del sistema.

Se utilizará Microsoft Visio como plataforma de desarrollo de los diagramas UML.

Se recomienda utilizar MAYUSCULAS para notación de los nombres de las clases, sus atributos y métodos.

Para cada caso de uso se deben describir las clases que intervienen y los subsistemas que participan en el mismo.

Para cada Clase se deben definir sus características (atributos, métodos, asociaciones, etc) según corresponda.

Como buena práctica se descompondrá el sistema de forma modular en subsistemas y los procesos que se van a implementar en cada uno de ellos.

Se define el uso de archivos planos y secuenciales para el repositorio de las observaciones a procesar para lograr simplicidad en la lectura de datos.

Se define el uso de archivos planos y secuenciales para el repositorio de las observaciones procesadas para lograr simplicidad en la salida de información.

Los procesos deben manejar un mismo formato de entrada de datos y salida de información.

La especificación del entorno de construcción debe cubrir los siguientes temas: Entorno Tecnológico, Generadores de Código, Restricciones Técnicas del entorno, Requisitos de Operación y Seguridad, Subsistemas de construcción, Componentes de Construcción.

Descripción de Subsistemas de Diseño

El sistema se puede descomponer, para reducir la complejidad y facilitar el mantenimiento, en los siguientes subsistemas:

Subsistema Específico

- Análisis de los Sucesos

Subsistemas de Soporte

- Seguridad y Control de Acceso
- Gestor de datos
- Generador de Reportes

Todos los subsistemas pertenecen al nodo *Cliente*.

Especificación del Entorno Tecnológico del Sistema

Se agrupan los elementos de la infraestructura en los siguientes conceptos.

- Hardware: Procesador de 2.5 Mhz o superior. 512 Mb de RAM. Placa de Red. Unidad de CD/DVD o Puerto USB. Espacio en disco de 1 Gb.
- Software: Sistema Operativo Microsoft Windows XP.
- Comunicaciones: Red de área local del tipo Ethernet de 100 Mbps.

Procedimientos de Seguridad y Control de Acceso

Los procedimientos de seguridad necesarios para no comprometer el correcto funcionamiento del sistema y garantizar el cumplimiento de los niveles de servicios son los siguientes:

- El acceso al sistema se realiza luego de ingresar correctamente el usuario y clave. El acceso es registrado en un archivo para posterior control en caso de necesidad.
- Mantenimiento de la integridad y confidencialidad de los datos se logra con el sistema provisto por el sistema operativo. Las carpetas de datos y información no podrán estar compartidas y se aplicarán permisos NTFS para el área de Auditoria y Seguridad y Control.
- El equipo donde se ejecutará el sistema software contará con un agente del sistema de backup que utiliza la empresa. Se arbitrarán las configuraciones necesarias para que diariamente se resguarden los datos, reportes y la aplicación. Ante la ocurrencia de un desastre, se recurrirán a estos backups para realizar la recuperación de información necesaria. La información que no haya sido resguarda por el sistema de backup, no podrá recuperarse.

Procedimientos de Operación y Administración del Sistema

La administración del sistema es simple, no requiere configuraciones ni ajustes iniciales por ende no es necesario proveer un procedimiento de administración. El tratamiento para los agentes de aplicaciones de monitoreo, backup y otros, son los estándares utilizados por la sociedad.

A continuación se incluye el Procedimiento de Operación para el equipo del centro de cómputos.

Procedimiento de Operación

1. Actividades remotas del Analista funcional

Miembros de las áreas de Auditoria y Seguridad y Control, pueden realizar conexiones remotas o locales sobre el equipo con fines de ejecución normal de la aplicación, revisión y control.

2. Actividades delegadas al Centro de Cómputos

Solo los miembros del área de Seguridad y Control están autorizados a solicitar actividades, sobre el equipo, por parte de operadores.

Ante problemas con la aplicación el operador podrá reiniciar el equipo.

3. Parada / Arranque

Pasos a seguir:

3.1. Logon de usuario.

===>>> Ejecutar ALT-CTRL-DEL

===>>> Ingresar Usuario, Clave y Dominio del usuario definido para Operaciones.

3.2. Inactivación

===>>> Ir a Start y luego seleccionar Shut down

===>>> En la opción What do you want the computer to do?, seleccionar Shut Down o Restart de acuerdo a lo solicitado.

===>>> En Comment, tipear el motivo de la operación

===>>> Presionar Ok

3.3. Activación

===>>> Arrancar el equipo con el botón de Power y verificar que no se presenten mensajes de error en pantalla.

Diseño de la Realización de los Casos de Uso

En la siguiente tabla 4-39 se describen:

- las clases que intervienen en cada caso de uso.
- cada caso de uso en términos de los subsistemas que participan en el mismo.

Caso de Uso	Clases	Subsistemas
RF1. Ingreso al Sistema.	USUARIOS	Cliente ProcesoSeguridad
RF2. Crear Usuario.	USUARIOS	Cliente ProcesoSeguridad
RF3. Cambio de Contraseña.	USUARIOS	Cliente ProcesoSeguridad
RF4. Consulta de Reportes.	USUARIOS ARCHIVOS	Cliente ProcesoSeguridad ProcesoReportes
RF5. Consulta de Estadísticas Históricas.	USUARIOS ARCHIVOS GRAFICOS	Cliente ProcesoSeguridad ProcesoReportes
RF6. Configurar Vistas y Reportes.	USUARIOS	Cliente ProcesoAnalisis
RF7. Selección Archivo de Entrada.	USUARIOS ARCHIVOS	Cliente ProcesoAnalisis
RF8. Selección Archivos de Salida.	USUARIOS ARCHIVOS	Cliente ProcesoAnalisis
RF9. Análisis de Registros.	USUARIOS OBSERVACIONES ARCHIVOS	Cliente ProcesoSeguridad ProcesoAnalisis
RF10. Visualizar Monitor Registro en Proceso.	USUARIOS OBSERVACIONES	Cliente ProcesoAnalisis
RF11. Visualizar Monitor Cantidad de Observaciones Procesadas.	USUARIOS OBSERVACIONES	Cliente ProcesoAnalisis
RF12. Visualizar Gráfico de Secciones.	USUARIOS OBSERVACIONES GRAFICOS	Cliente ProcesoAnalisis
RF13. Visualizar Estadísticas de Reglas.	USUARIOS OBSERVACIONES	Cliente ProcesoAnalisis
RF14. Visualizar Estadísticas de Usuario.	USUARIOS OBSERVACIONES	Cliente ProcesoAnalisis
RF15. Visualizar Reportes.	USUARIOS ARCHIVOS	Cliente ProcesoReportes
RF16. Salir del Sistema.	USUARIOS	Cliente ProcesoSeguridad

Tabla 4-39. Diseño de los casos de Uso.

Diseño de la Interfaz de Usuario.

Prototipo de Interfaz de Pantalla Gráfica

El formato y contenido de cada una de las interfaces de pantalla se muestra a continuación en las figuras 4-47 a 4-60.

Ventana de Bienvenida al Sistema.

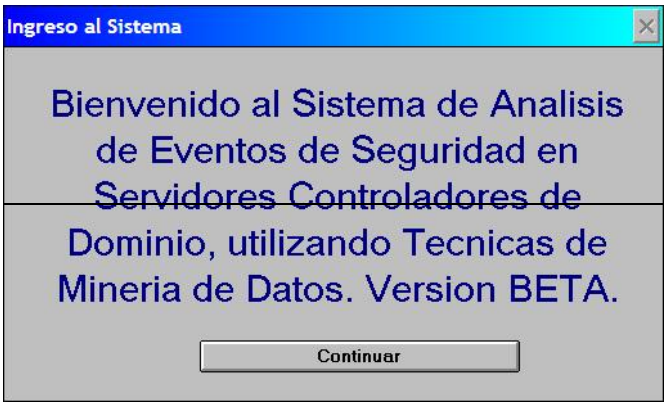


Figura 4-47. Ventana de Bienvenida al Sistema.

Ventana de Ingreso al Sistema.

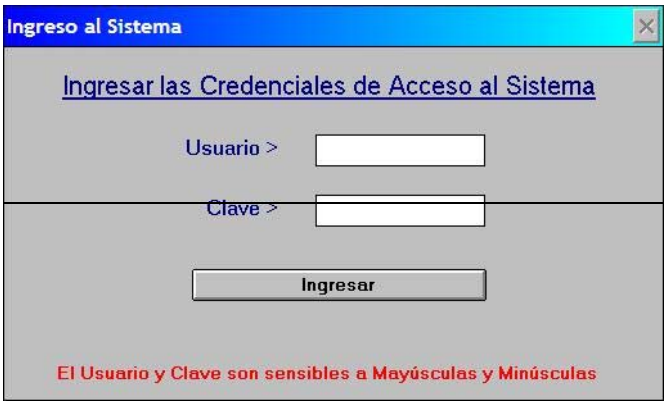


Figura 4-48. Ventana de Ingreso al Sistema.

Ventana del Módulo de Inicio.

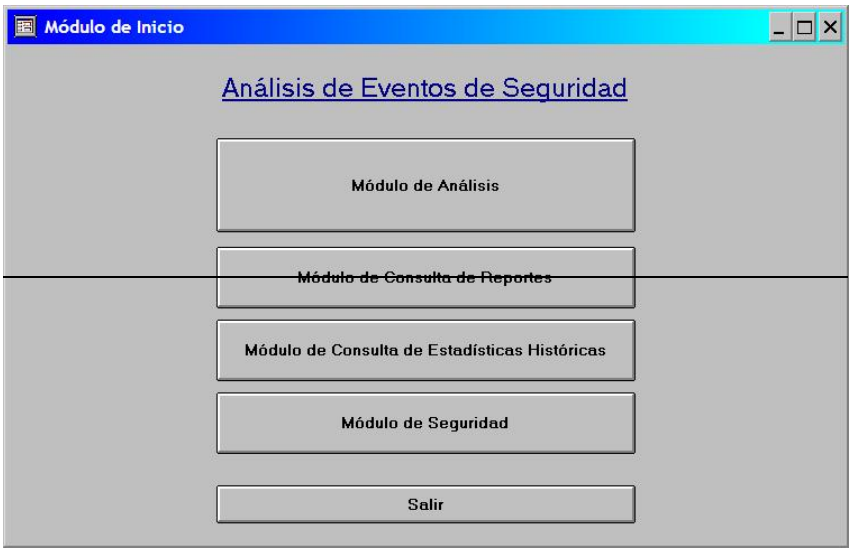


Figura 4-49. Ventana del Módulo de Inicio.

Ventana de Configuración de Vistas y Reportes.

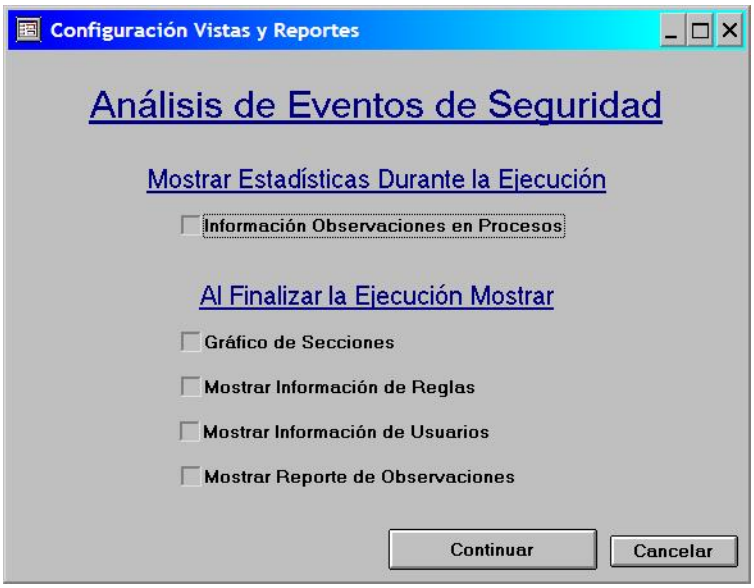


Figura 4-50. Ventana de Configuración de Vistas y Reportes.

Ventana del Módulo de Análisis de Eventos.

Figura 4-51. Ventana del Módulo de Análisis de Eventos.

Ventana de Evento en Análisis.

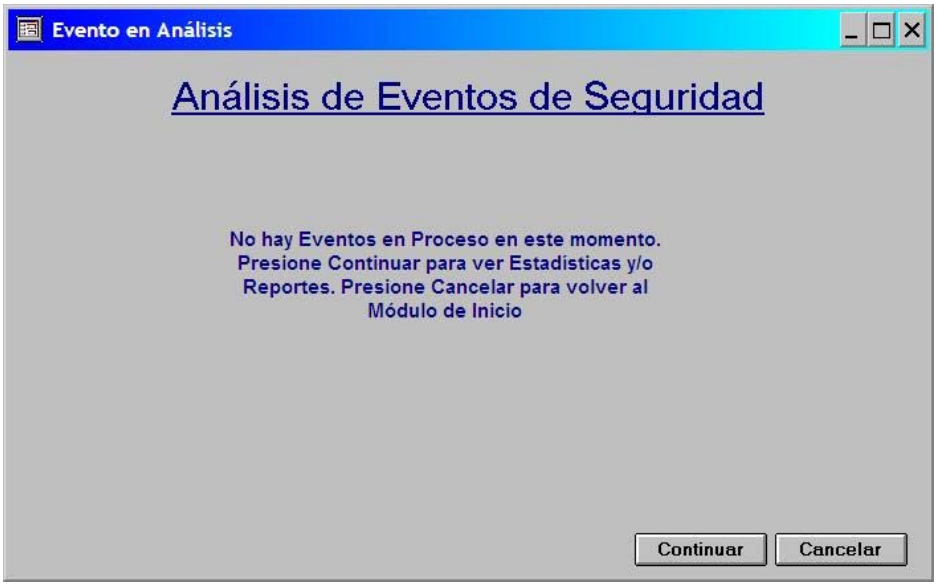


Figura 4-52. Ventana de Evento en Análisis.

Ventana del Módulo de Estadísticas.

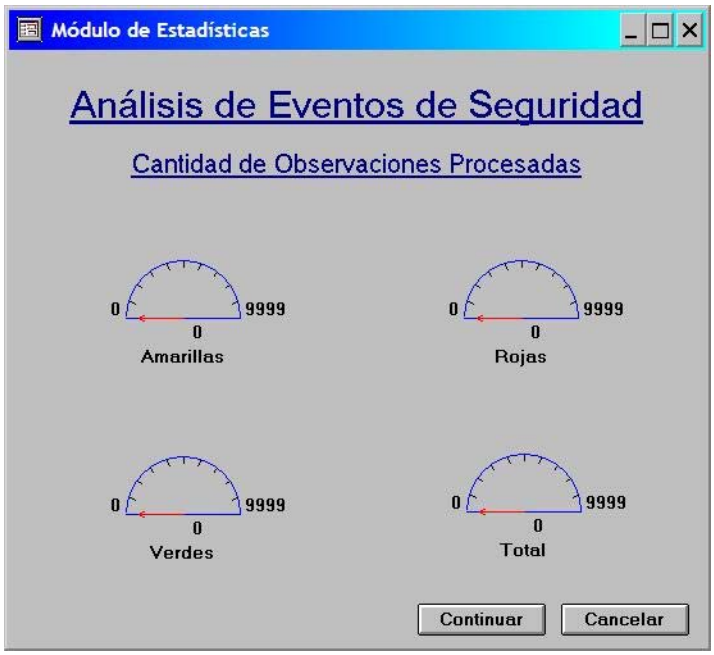


Figura 4-53. Ventana del Módulo de Estadísticas.

Ventana del Gráfico de Secciones.

Figura 4-54. Ventana del Gráfico de Secciones.

Ventana de Información de Reglas.

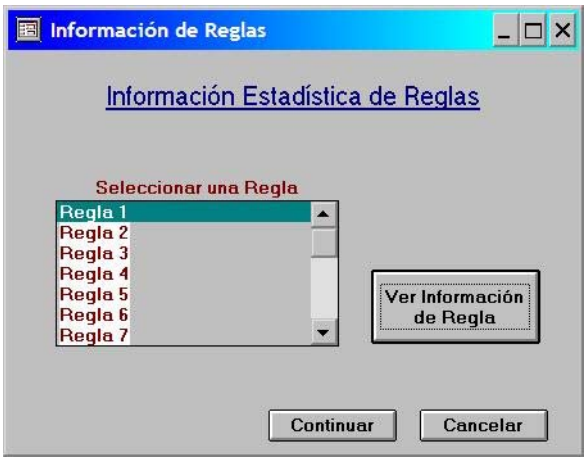


Figura 4-55. Ventana de Información de Reglas.

Ventana de Información de Usuarios.

Figura 4-56. Ventana de Información de Usuarios.

Ventana del Informe de Salida.

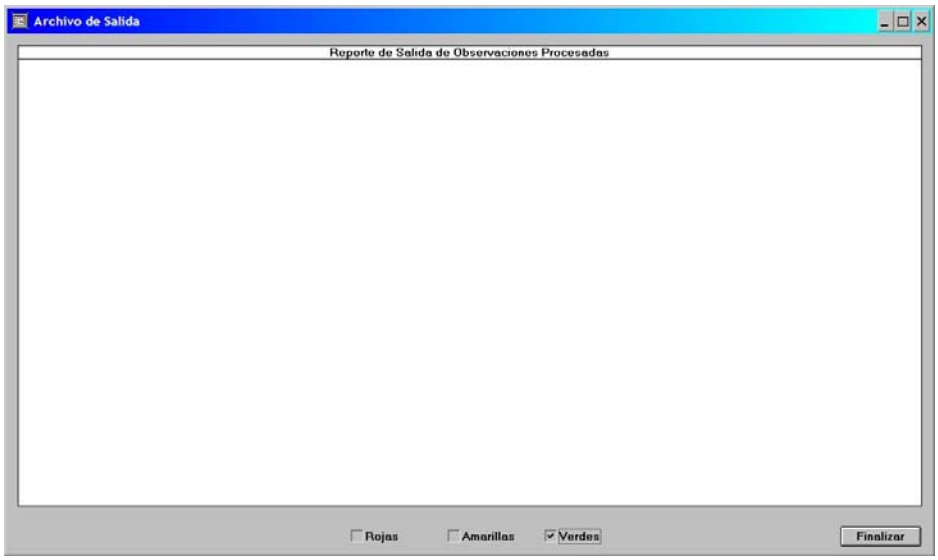


Figura 4-57. Ventana del Informe de Salida.

Ventana del Módulo de Estadísticas Históricas.

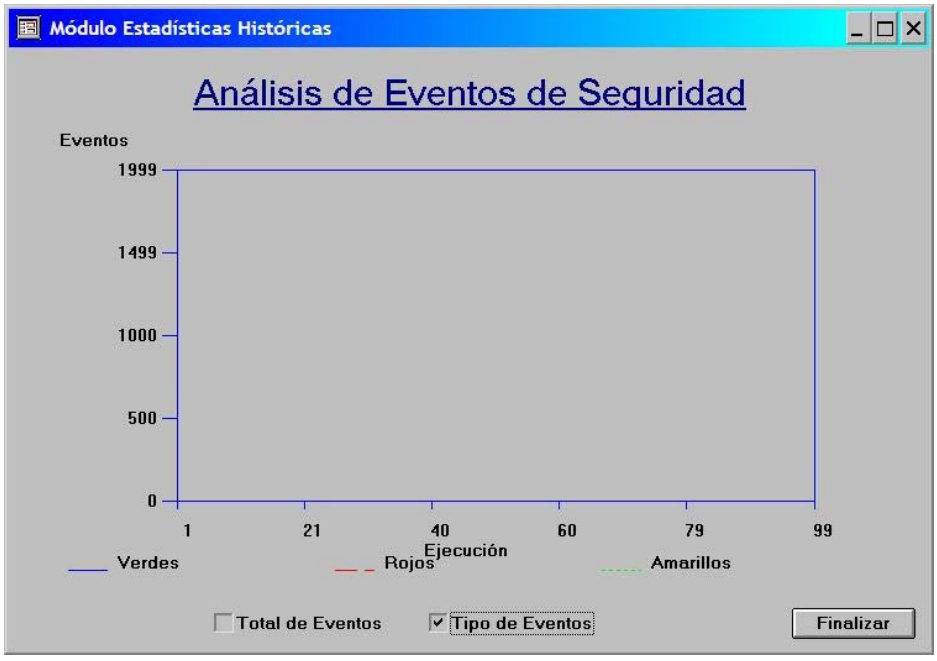


Figura 4-58. Ventana del Módulo de Estadísticas Históricas.

Ventana del Módulo de Seguridad.

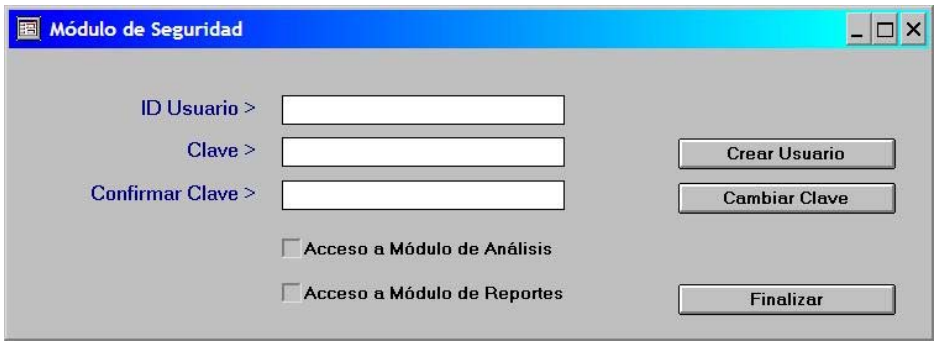


Figura 4-59. Ventana del Módulo de Seguridad.

Diseño del Formato de Impresión

En la siguiente figura se muestra el diseño de un archivo de salida.

Figura 4-60. Formato de Impresión de un Archivo de Salida.

Modelo de Clases de Diseño

El objetivo es identificar un conjunto de clases que completen el modelo de clases analizado en la fase de análisis teniendo en cuenta que cada interfaz identificada en el análisis se corresponde en el diseño con una clase que proporcione esa interfaz.

Tomando como base lo mencionado en el párrafo anterior, en la presente fase de diseño se identifica una nueva clase. Todas las interfaces del sistema utilizan la siguiente clase de interfaz, cuyos atributos y métodos se detallan a continuación en la tabla 4-40:

Clases de Interfaz	Atributos	Métodos
VENTANAS	NOMBRE POSICIÓN_X POSICIÓN_Y ALTURA	MOSTRAR() MOVER() MINIMIZAR() MAXIMIZAR()

Clases de Interfaz	Atributos	Métodos
	ANCHURA COLOR_FONDO MINIMIZA MAXIMIZA CIERRA MUEVE	CERRAR()

Tabla 4-40. Información de la clase de interfaz.

Identificación de Atributos de las Clases

En la siguiente tabla 4-41, se describen las características de los atributos de las clases identificadas.

Nombre Clase	Atributos	Tipo
OBSERVACIONES	ID DIA EVENTO HORA USUARIO CLASIFICACION REGLA HORA_EJECUCION	Integer String String String String String Integer Date
USUARIO	ID NOMBRE CLAVE PERMISOS	String String String String
GRAFICOS	EJE_X EJE_Y NOMBRE_EJE_X NOMBRE_EJE_Y ESCALA_EJE_X ESCALA_EJE_Y FUNCION	Integer Integer String String Integer Integer String
ARCHIVOS	NOMBRE RUTA PERMISOS BLOQUEO	String String String Bolean

Nombre Clase	Atributos	Tipo
	TAMAÑO	Integer
	FECHA_CREADO	Date
	FECHA_MODIFICADO	Date
VENTANAS	NOMBRE	String
	POSICIÓN_X	Integer
	POSICIÓN_Y	Integer
	ALTURA	Integer
	ANCHURA	Integer
	COLOR_FONDO	String
	MINIMIZA	Bolean
	MAXIMIZA	Bolean
	CIERRA	Bolean
	MUEVE	Bolean

Tabla 4-41. Descripción de los Atributos de las clases.

Comportamiento de Clases de Diseño

En la siguiente tabla 4-42, se describen las características (Operación, Parámetros y Visibilidad) de los métodos de las clases identificadas.

Nombre Clase	Métodos / Visibilidad	Operación	Parámetros
OBSERVACIONES	LEER() Visibilidad: Pública	Leer cada registro del archivo de entrada.	DIA EVENTO HORA USUARIO
	APLICAR_REGLAS() Visibilidad: Pública	Aplicar a cada registro las reglas de decisión, de modo de clasificarlo.	ID DIA EVENTO HORA USUARIO REGLA
	ESCRIBIR() Visibilidad: Pública	Registrar cada registro con su clasificación en los archivos de salidas.	ID DIA EVENTO HORA USUARIO CLASIFICACION REGLA HORA_EJECUCION
USUARIO	CREAR() Visibilidad: Pública	Crear nuevas credenciales para un operador.	ID CLAVE NOMBRE PERMISOS
	CAMBIAR_CLAVE() Visibilidad: Pública	Validar y llevar a cabo el cambio de claves del	ID CLAVE

Nombre Clase	Métodos / Visibilidad	Operación	Parámetros
		operador.	
	VALIDAR() Visibilidad: Pública	Validar las credenciales y permisos de un operador.	ID CLAVE PERMISOS
GRAFICOS	MOSTRAR() Visibilidad: Pública	Mostrar la ventana, etiquetas y coordenadas de un gráfico.	EJE_X EJE_Y NOMBRE_EJE_X NOMBRE_EJE_Y ESCALA_EJE_X ESCALA_EJE_Y
	DIBUJAR() Visibilidad: Protegida	Dibujar la función del gráfico con los valores actuales almacenados en el sistema.	EJE_X EJE_Y ESCALA_EJE_X ESCALA_EJE_Y FUNCION
	OCULTAR() Visibilidad: Pública	Ocultar la ventana de un gráfico.	No Requiere
ARCHIVOS	ABRIR() Visibilidad: Pública	Abrir un archivo y prepararlo para su posterior escritura.	NOMBRE RUTA PERMISOS BLOQUEO
	ESCRIBIR() Visibilidad: Pública	Escribir un archivo abierto.	NOMBRE RUTA PERMISOS
	CERRAR() Visibilidad: Pública	Cerrar un archivo abierto.	NOMBRE RUTA
VENTANAS	MOSTRAR() Visibilidad: Pública	Mostrar una ventana del sistema.	NOMBRE POSICIÓN_X POSICIÓN_Y ALTURA ANCHURA COLOR_FONDO
	MOVER() Visibilidad: Pública	Mover una ventana del sistema.	NOMBRE MUEVE
	MINIMIZAR() Visibilidad: Pública	Minimizar una ventana del sistema.	NOMBRE MINIMIZA
	MAXIMIZAR() Visibilidad: Pública	Maximizar una ventana del sistema.	NOMBRE MAXIMIZA
	CERRAR() Visibilidad: Pública	Cerrar una ventana del sistema.	NOMBRE CIERRA

Tabla 4-42. Descripción de los métodos de las clases.

Diseño de la Arquitectura Modular del Sistema

La descomposición modular de los subsistemas y los procesos que se van a implementar en cada uno de ellos es la siguiente y se muestra en la figura 4-61.

- Subsistema Análisis de los Sucesos.
    - Proceso análisis de los sucesos.

      Implementación: en línea.

      Iniciación: bajo petición.
- Subsistema Seguridad y Control de Acceso.
    - Proceso validación de usuario y clave de acceso.

      Implementación: en línea.

      Iniciación: bajo petición.
- Subsistema Gestor de datos.
    - Proceso de lectura de datos de entrada.

      Implementación: en línea.

      Iniciación: por el sistema.
    - Proceso de escritura de información de salida.

      Implementación: en línea.

      Iniciación: por el sistema.
- Subsistema Generador de reportes.
    - Proceso de generación de reportes.

      Implementación: en línea.

      Iniciación: bajo petición.

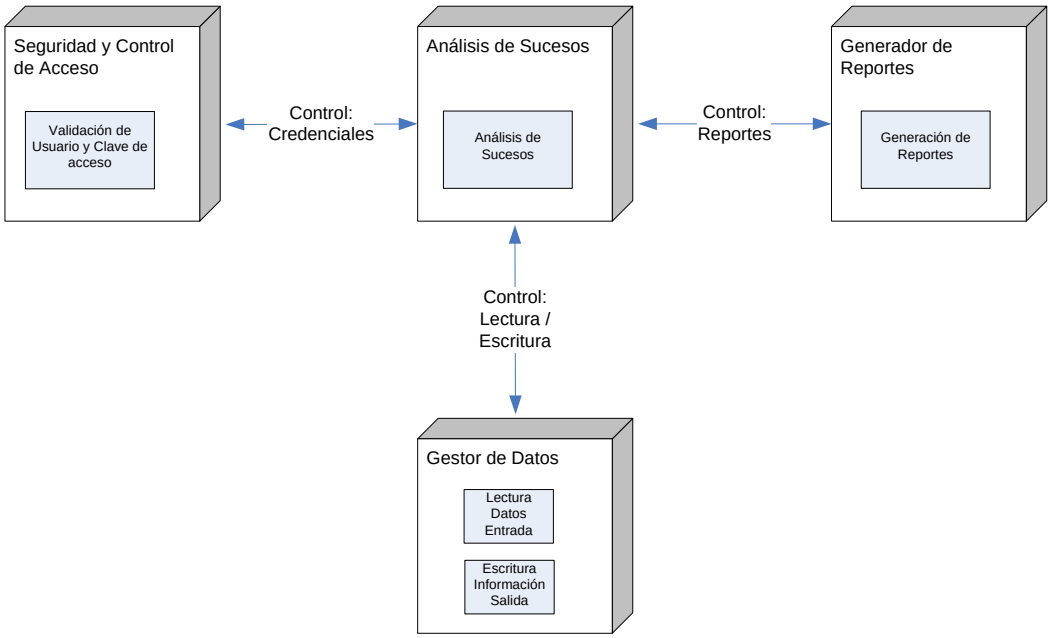


Figura 4-61. Arquitectura de Módulos del sistema.

Modelo Físico de Datos

El sistema en desarrollo trabajará con los siguientes tipos de archivos:

- Archivo para registrar el acceso al sistema

  El formato es el siguiente: *Fecha, Hora, Usuario*

- Archivo de lectura de datos de entrada

  El formato es el siguiente: *Identificación Observación, Día Evento, Hora Evento, Usuario, Identificación Evento*

- Archivos de escritura de información de salida

  El formato es el siguiente: "*Inicio de la Ejecución", Fecha y Hora Inicio Ejecución, Identificación Observación, Día Evento, Hora Evento, Usuario, Identificación Evento, Regla de Decisión Aplicada, Condición de Activación, Hora Ejecución, "Fin de la Ejecución", Fecha y Hora Fin Ejecución*

- Archivos de escritura de información histórica

  El formato es el siguiente: *Identificación Ejecución, Total de eventos Verdes, Total de eventos Amarillos, Total de eventos Rojos, Total de eventos de la ejecución*

Especificación de los Caminos de Acceso a los Datos

El acceso a los datos se realiza a través del sistema de acceso de archivos del sistema operativo del equipo donde se ejecuta la aplicación.

El subsistema *Gestor de Datos* es el que interviene en el acceso a los datos, a través de sus módulos *Proceso de lectura de datos de entrada* y *Proceso de escritura de Información*.

Esquemas Físicos de Datos

Los tres archivos, identificados anteriormente, utilizados por el sistema se alocarán en el equipo físico donde se ejecuta la aplicación.

Asignación esquemas Físicos de Datos a Nodos

La unidad física a utilizar para guardar los archivos se configurará con un sistema de redundancia y tolerancia a fallos del tipo RAID1. Esta configuración consta de dos discos iguales espejados, si uno de ellos falla, la información aun puede accederse con el disco bueno. Al reemplazar el disco dañado, los datos son replicados a éste desde el disco que había quedado funcionando).

Verificación de la Arquitectura del Sistema

En reunión de seguimiento y control entre las partes, Tesista y Directora del proyecto, se verificó que las especificaciones de diseño cumplen con el catálogo de normas especificado en el apartado "Catálogo de Normas de Diseño y Construcción".

Aceptación Técnica del Diseño

En reunión de seguimiento, control y aprobación entre las partes, Tesista y Directora del proyecto, se dio por aceptada la Arquitectura del Sistema.

Especificaciones de Construcción del Sistema de Información

Especificación del Entorno de Construcción

La especificación del entorno de construcción se realiza según los siguientes conceptos:

- Entorno tecnológico:

  Hardware: Se utilizará una PC con procesador de 2.5 Mhz o superior. 512 Mb de RAM. Placa de Red. Unidad de CD/DVD. Espacio en disco de 1 Gb.

Software: Sistema Operativo Microsoft Windows XP.

Comunicaciones: Red de área local del tipo Ethernet de 100 Mbps.

Centro de Cómputos: Disponer de un lugar en un rack con energía, conexión de red y conexión a la consola de monitor y teclado del operador.

- Herramientas de construcción, generadores de código, compiladores:

  Entorno de desarrollo KAPPA-PC.

- Restricciones técnicas del entorno:

  Se utilizará el entorno de desarrollo de la empresa. No se tendrá acceso, interferencia y/o intercambio de datos y/o información con el entorno de producción.

- Requisitos de operación y seguridad del entorno de construcción:

  Como se trabajará con el entorno de desarrollo, se tendrá acceso completo a la PC de trabajo. No se tendrá acceso a recursos de producción.

  Como es norma de la empresa, la PC estará en el centro de cómputos y solo personal del mismo tiene acceso físico a la misma. En caso de necesitar acceder físicamente a la PC, habrá que interactuar con el/los operadores de turno.

Descripción de Subsistemas de Construcción

La asignación de subsistemas de construcción a nodos se muestra en la figura 4-62.

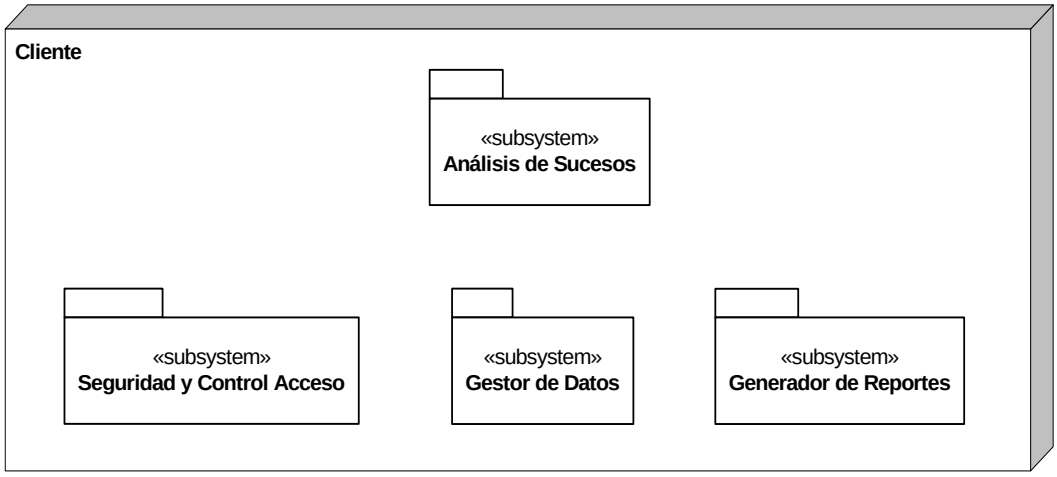


Figura 4-62. Asignación de subsistemas de construcción a nodos.

Se define que, para cada clase del diseño, le corresponde un componente de construcción. La definición de los componentes de construcción se muestra en la figura 4-63.

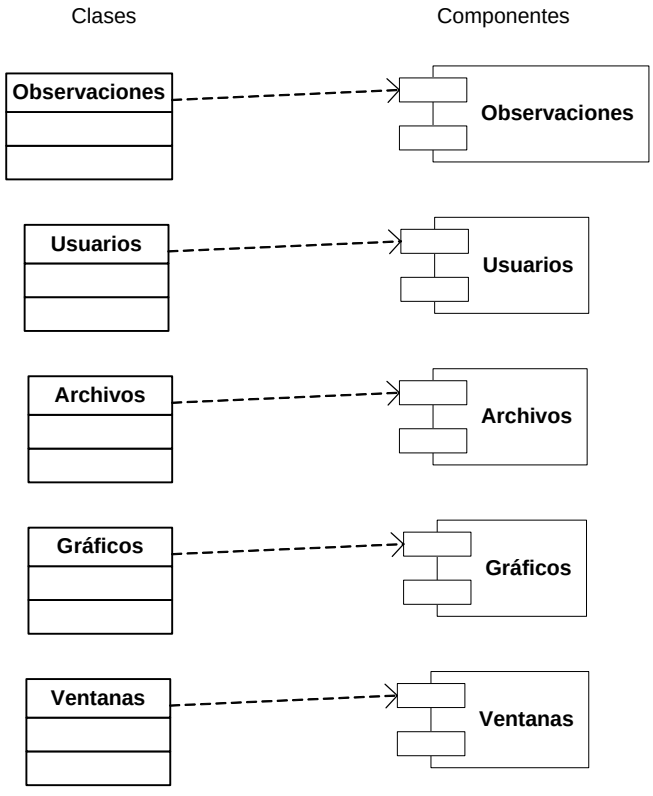


Figura 4-63. Representación de los componentes de construcción.

La agrupación de componentes en los subsistemas de construcción se muestra en las figuras 4-64 a 4-67.

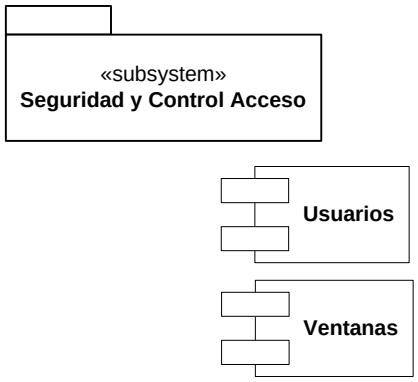


Figura 4-64. Componentes del subsistema de construcción Seguridad y Control de Acceso.

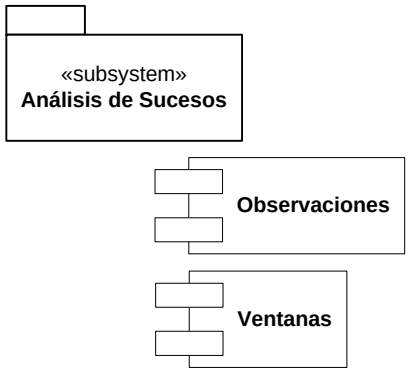


Figura 4-65. Componentes del subsistema de construcción Análisis de Sucesos.

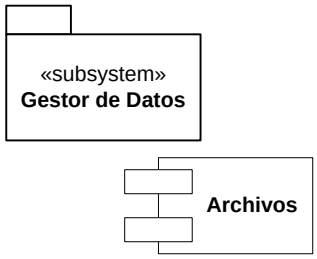


Figura 4-66. Componentes del subsistema de construcción Gestor de Datos.

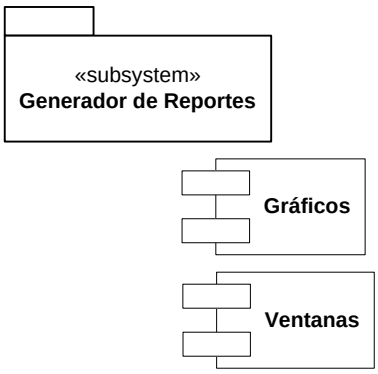


Figura 4-67. Componentes del subsistema de construcción Generador de Reportes.

Especificación de la Estructura Física de Datos.

Archivos de Salida.

Será necesario crear tres archivos de texto para utilizar como salida de la aplicación. Cada uno de ellos se corresponderá con un tipo de evento. El nombre no podrá ser mayor a 8 caracteres, no se deberán incluir caracteres especiales y la extensión debe ser *txt.* La estructura interna de ellos es la definida en la etapa de diseño.

Los nombres a definir son: *OBSVerde.txt, OBSAmari.txt, OBSRojo.txt*.

Archivo Histórico

Será necesario crear un archivo de texto para almacenar de los datos históricos de la aplicación. El nombre no podrá ser mayor a 8 caracteres, no se deberán incluir caracteres especiales y la extensión debe ser *txt.* La estructura interna del mismo es la definida la tarea previa.

El nombre a definir es: *Historic.txt*.

Plan de Pruebas

Especificación Técnica de Niveles de Prueba

Las pruebas que se llevarán a cabo son las siguientes y se detallan en las tablas 4-43 a 4-50.

Número Prueba	*PU01*
Objetivo	*Validar el módulo de acceso*
Requisitos	*Ejecutar la aplicación*
Caso de Prueba (pasos)	*- Ejecutar la aplicación* *- Ingresar usuario y clave válidos*
Resultado Esperado	*Ingresar al sistema*
Fecha Ejecución	
Resultado	
Notas	

Tabla 4-43. Diseño Caso 1 de Prueba Unitaria.

Número Prueba	*PU02*
Objetivo	*Validar el módulo de acceso y escritura de archivos*
Requisitos	*Ejecutar la aplicación*
Caso de Prueba (pasos)	*- Ejecutar la aplicación* *- Ingresar usuario y clave válidos* *- Realizar una lectura de datos y Verificar la escritura de la información.*
Resultado Esperado	*Lectura sin errores de datos y escritura sin errores de información*
Fecha Ejecución	
Resultado	
Notas	

Tabla 4-44. Diseño Caso 2 de Prueba Unitaria.

Número Prueba	*PU03*
Objetivo	*Validar el módulo de análisis*
Requisitos	*Ejecutar la aplicación*
Caso de Prueba (pasos)	*- Ejecutar la aplicación* *- Ingresar usuario y clave válidos* *- Realizar la lectura de datos y análisis de los mismos.* *- Verificar que las estadísticas y reportes generados son correctos.*
Resultado Esperado	*Estadísticas y reportes generados correctamente.*
Fecha Ejecución	
Resultado	
Notas	

Tabla 4-45. Diseño Caso 3 de Prueba Unitaria.

Número Prueba	*PI01*
Objetivo	*Validar correspondencia de controles de selección de usuarios con las ventanas mostradas en pantalla.*
Requisitos	*Ejecutar la aplicación*
Caso de Prueba (pasos)	*- Ejecutar en la aplicación el módulo de controles de selección de estadísticas de usuario.*
Resultado Esperado	*El sistema debe mostrar solo las ventanas que muestran la información seleccionada por el usuario*

Fecha Ejecución	
Resultado	
Notas	

Tabla 4-46. Diseño Caso 1 de Prueba de Integración.

Número Prueba	*PI02*
Objetivo	*Validar correspondencia de controles de selección de usuarios con los reportes generados.*
Requisitos	*Ejecutar la aplicación*
Caso de Prueba (pasos)	*- Ejecutar en la aplicación el módulo de controles de selección de reportes de usuario.*
Resultado Esperado	*El sistema debe mostrar solo los reportes que seleccionó el usuario.*
Fecha Ejecución	
Resultado	
Notas	

Tabla 4-47. Diseño Caso 2 de Prueba de Integración.

Número Prueba	*PS01*
Objetivo	*Validar la integración del sistema en su totalidad*
Requisitos	*Ejecutar la aplicación*
Caso de Prueba (pasos)	*- Ejecutar la aplicación* *- Ingresar usuario y clave válidos* *- El usuario debe seleccionar las estadísticas y reportes deseados.* *- Realizar la lectura de datos y análisis de los mismos.* *- Verificar que las estadísticas y reportes generados son correctos.*
Resultado Esperado	*El sistema debe mostrar las estadísticas y reportes que seleccionó el usuario.* *Las Estadísticas y Reportes deben ser generados correctamente.*
Fecha Ejecución	
Resultado	
Notas	

Tabla 4-48. Diseño Caso 1 de Prueba de Sistema.

Número Prueba	*PIm01*
Objetivo	*Comprobar el funcionamiento del sistema*
Requisitos	*Ejecutar la aplicación*
Caso de Prueba (pasos)	*- Ejecutar la aplicación* *- Ingresar usuario y clave válidos* *- El usuario debe seleccionar las estadísticas y reportes deseados.* *- Realizar la lectura de datos y análisis de los mismos.* *- Verificar que las estadísticas y reportes generados son correctos.*
Resultado Esperado	*El sistema debe funcionar correctamente.*
Fecha Ejecución	
Resultado	
Notas	

Tabla 4-49. Diseño Caso 1 de Prueba de Implantación.

Número Prueba	*PA01*
Objetivo	*Validar la respuesta del sistema a los requisitos especificados por el usuario*
Requisitos	*Ejecutar la aplicación*
Caso de Prueba (pasos)	*- Ejecutar la aplicación* *- Ingresar usuario y clave válidos* *- El usuario debe seleccionar las estadísticas y reportes deseados.* *- Realizar la lectura de datos y análisis de los mismos.* *- Verificar que las estadísticas y reportes generados son correctos.*
Resultado Esperado	*El sistema debe satisfacer la respuesta esperada por el usuario en un tiempo menor a 5 minutos y con un error menor a 30 %*
Fecha Ejecución	
Resultado	
Notas	

Tabla 4-50. Diseño Caso 1 de Prueba de Aceptación.

Planificación de las Pruebas

Las pruebas serán realizadas y coordinadas por el Analista / Desarrollador. El perfil usuario será ejecutado por el Líder de Seguridad y Control.

Se dispondrá de 5 días hábiles para realizar y documentar las pruebas.

Requisitos de documentación de Usuario

- Generar un documento de guía de uso para el Usuario Final.

  Consistirá de un documento con las ventanas de la aplicación y las funciones que el usuario debe realizar en cada una de ellas.

  Se entregará en forma electrónica en el mismo CD de instalación del producto final.

Aprobación del Diseño del Sistema de Información

En reunión de seguimiento, control y aprobación entre las partes, Tesista y Directora del proyecto, se dio por aprobada esta fase.

El jefe del proyecto comunica formalmente a los participantes, afectados y usuarios los resultados de la fase. Se utiliza el siguiente anuncio.

Estimados Colaboradores, Cumplo en informarles que la fase del Diseño del Sistema del proyecto "Análisis de Eventos de Seguridad en Servidores" ha sido aprobada satisfactoriamente. Desde ya muchas gracias por su participación y compromiso.

4.2.2.3.2 Control de Actividades

Actividades / Tareas	Desarrollo	Justificación
ACTIVIDAD DSI 1: DEFINICIÓN DE LA ARQUITECTURA DEL SISTEMA		
Tarea DSI 1.1: Definición de Niveles de Arquitectura	SI	Se dispone de la información necesaria.
Tarea DSI 1.2: Identificación de Requisitos de Diseño y Construcción	SI	Se dispone de la información necesaria.
Tarea DSI 1.3: Especificación de Excepciones	SI	Se dispone de la información necesaria.
Tarea DSI 1.4: Especificación de Estándares y Normas de Diseño y Construcción	SI	Se dispone de la información necesaria.
Tarea DSI 1.5: Identificación de Subsistemas de Diseño	SI	Se dispone de la información necesaria.
Tarea DSI 1.6: Especificación del Entorno Tecnológico	SI	Se dispone de la información necesaria.
Tarea DSI 1.7: Especificación de Requisitos de Operación y Seguridad	SI	Se dispone de la información necesaria.
ACTIVIDAD DSI 2: DISEÑO DE LA ARQUITECTURA DE SOPORTE		
Tarea DSI 2.1: Diseño de Subsistemas de Soporte	NO	No se considera necesario el desarrollo.
Tarea DSI 2.2: Identificación de Mecanismos Genéricos de Diseño	NO	No se considera necesario el desarrollo.
ACTIVIDAD DSI 3: DISEÑO DE CASOS DE USO REALES		
Tarea DSI 3.1: Identificación de Clases Asociadas a un Caso de Uso	SI	Se dispone de la información necesaria.
Tarea DSI 3.2: Diseño de la Realización de los Casos de Uso	SI	Se dispone de la información necesaria.
Tarea DSI 3.3: Revisión de la Interfaz de Usuario	SI	Se dispone de la información necesaria.
Tarea DSI 3.4: Revisión de Subsistemas de Diseño e Interfaces	SI	Se dispone de la información necesaria.
ACTIVIDAD DSI 4: DISEÑO DE CLASES		
Tarea DSI 4.1: Identificación de Clases Adicionales	SI	Se dispone de la información necesaria.
Tarea DSI 4.2: Diseño de Asociaciones y Agregaciones	NO	No es necesario el desarrollo.
Tarea DSI 4.3: Identificación de Atributos de las Clases	SI	Se dispone de la información necesaria.
Tarea DSI 4.4: Identificación de Operaciones de las Clases	SI	Se dispone de la información necesaria.
Tarea DSI 4.5: Diseño de la Jerarquía	NO	No es necesario el desarrollo.
Tarea DSI 4.6: Descripción de Métodos de las Operaciones	SI	Se dispone de la información necesaria.

Actividades / Tareas	Desarrollo	Justificación
Tarea DSI 4.7: Especificación de Necesidades de Migración y Carga Inicial de Datos	NO	No es necesario el desarrollo.
ACTIVIDAD DSI 5: DISEÑO DE LA ARQUITECTURA DE MÓDULOS DEL SISTEMA		
Tarea DSI 5.1: Diseño de Módulos del Sistema	SI	Se dispone de la información necesaria.
Tarea DSI 5.2: Diseño de Comunicaciones entre Módulos	SI	Se dispone de la información necesaria.
Tarea DSI 5.3: Revisión de la Interfaz de Usuario	NO	No es necesario el desarrollo.
ACTIVIDAD DSI 6: DISEÑO FÍSICO DE DATOS		
Tarea DSI 6.1: Diseño del Modelo Físico de Datos	SI	Se dispone de la información necesaria.
Tarea DSI 6.2: Especificación de los Caminos de Acceso a los Datos	SI	Se dispone de la información necesaria.
Tarea DSI 6.3: Optimización del Modelo Físico de Datos	NO	El sistema operativo satisface las necesidades establecidas en cuanto a que se ajusta a los requisitos de rendimiento exigidos.
Tarea DSI 6.4: Especificación de la Distribución de Datos	SI	Se dispone de la información necesaria.
ACTIVIDAD DSI 7: VERIFICACIÓN Y ACEPTACIÓN DE LA ARQUITECTURA DEL SISTEMA		
Tarea DSI 7.1: Verificación de las Especificaciones de Diseño	SI	Se dispone de la información necesaria.
Tarea DSI 7.2: Análisis de Consistencia de las Especificaciones de Diseño	SI	Se dispone de la información necesaria.
Tarea DSI 7.3: Aceptación de la Arquitectura del Sistema	SI	Se dispone de la información necesaria.
ACTIVIDAD DSI 8: GENERACIÓN DE ESPECIFICACIONES DE CONSTRUCCIÓN		
Tarea DSI 8.1: Especificación del Entorno de Construcción	SI	Se dispone de la información necesaria.
Tarea DSI 8.2: Definición de Componentes y Subsistemas de Construcción	SI	Se dispone de la información necesaria.
Tarea DSI 8.3: Elaboración de Especificaciones de Construcción	NO	No es necesario el desarrollo.
Tarea DSI 8.4: Elaboración de Especificaciones del Modelo Físico de Datos	NO	No es necesario el desarrollo.
ACTIVIDAD DSI 9: DISEÑO DE LA MIGRACIÓN Y CARGA INICIAL DE DATOS		
Tarea DSI 9.1: Especificación del Entorno de Migración	NO	No es necesaria una carga inicial de información, o una migración de datos de otros sistemas.
Tarea DSI 9.2: Diseño de Procedimientos de Migración y Carga Inicial	NO	No es necesaria una carga inicial de información, o una migración de datos de otros sistemas.
Tarea DSI 9.3: Diseño Detallado de	NO	No es necesaria una carga inicial

Actividades / Tareas	Desarrollo	Justificación
Componentes de Migración y Carga Inicial		de información, o una migración de datos de otros sistemas.
Tarea DSI 9.4: Revisión de la Planificación de la Migración	NO	No es necesaria una carga inicial de información, o una migración de datos de otros sistemas.
ACTIVIDAD DSI 10: ESPECIFICACIÓN TÉCNICA DEL PLAN DE PRUEBAS		
Tarea DSI 10.1: Especificación del Entorno de Pruebas	NO	No es necesario el desarrollo.
Tarea DSI 10.2: Especificación Técnica de Niveles de Prueba	SI	Se dispone de la información necesaria.
Tarea DSI 10.3: Revisión de la Planificación de Pruebas	SI	Se dispone de la información necesaria.
ACTIVIDAD DSI 11: ESTABLECIMIENTO DE REQUISITOS DE IMPLANTACIÓN		
Tarea DSI 11.1: Especificación de Requisitos de Documentación de Usuario	SI	Se dispone de la información necesaria.
Tarea DSI 11.2: Especificación de Requisitos de Implantación	NO	No es necesario el desarrollo, la información fue descripta en tareas anteriores.
ACTIVIDAD DSI 12: APROBACIÓN DEL DISEÑO DEL SISTEMA DE INFORMACIÓN		
Tarea DSI 12.1: Presentación y Aprobación del Diseño del Sistema de Información	SI	Se dispone de la información necesaria.

Tabla 4-51. Control de Actividades DSI.

4.2.2.4 Construcción del Sistema de Información (CSI)

4.2.2.4.1 Documento Entregable

DOCUMENTO DE CONSTRUCCIÓN DEL SISTEMA DE INFORMACIÓN

Entorno de Construcción

Se configurará la partición donde se colocarán los archivos de datos e información con un arreglo tipo RAID1.

Se asignarán los permisos NTFS a los usuarios de los departamentos de Auditoria y Seguridad y Control.

Se instalará el producto de desarrollo KAPPA-PC, en el equipo a utilizar.

Entorno de las Pruebas Unitarias

Las pruebas unitarias se realizarán directamente en el equipo donde se ejecutará la aplicación. Las pruebas serán realizadas y coordinadas por el Analista / Desarrollador. El perfil usuario será ejecutado por el Líder de Seguridad y Control. Se dispondrá de 1 día hábil para realizar y documentar las pruebas unitarias.

Resultados y Evaluación de las Pruebas Unitarias

Las pruebas Unitarias que se llevaron a cabo son las siguientes, tablas 4-52 a 4-54.

Número Prueba	*PU01*
Objetivo	*Validar el módulo de acceso*
Requisitos	*Ejecutar la aplicación*
Caso de Prueba (pasos)	*- Ejecutar la aplicación* *- Ingresar usuario y clave válidos* *- Ingresar usuario y clave No válidos*
Resultado Esperado	*Ingresar al sistema cuando se ingresan usuario y clave válidos.* *No Ingresar al sistema cuando se ingresan usuario y/o clave No válidos.*
Fecha Ejecución 1	*26/01/2008*
Resultado	*Se ingresó al Sistema sin problemas*
Notas	*Se ingresó una credencial de usuario y clave correctas*
Fecha Ejecución 2	*26/01/2008*
Resultado	*No se pudo ingresar al sistema. Se recibe el mensaje "El usuario o la clave es incorrecta".*

Notas	*Se ingresó una credencial de usuario incorrecta*
Fecha Ejecución 3	*26/01/2008*
Resultado	*No se pudo ingresar al sistema. Se recibe el mensaje "El usuario o la clave es incorrecta".*
Notas	*Se ingresó una clave de usuario incorrecta*
Fecha Ejecución 4	*26/01/2008*
Resultado	*No se pudo ingresar al sistema. Se recibe el mensaje "Ingrese un usuario y clave".*
Notas	*No se ingresó la credencial del usuario.*
Fecha Ejecución 5	*26/01/2008*
Resultado	*No se pudo ingresar al sistema. Se recibe el mensaje "Ingrese un usuario y clave".*
Notas	*No se ingresó la clave del usuario.*

Tabla 4-52. Ejecución Caso 1 de Prueba Unitaria.

Número Prueba	*PU02*
Objetivo	*Validar la existencia, lectura y escritura de archivos.*
Requisitos	*Ejecutar la aplicación.*
Caso de Prueba (pasos)	*- Ejecutar la aplicación* *- Ingresar usuario y clave válidos* *- Ingresar la ruta y nombre de los archivos de entrada y salida.* *- Realizar una lectura de datos y Verificar la escritura de la información.*
Resultado Esperado	*Lectura sin errores de datos y escritura sin errores de información.*
Fecha Ejecución	*26/01/2008*
Resultado	*Lectura de datos Satisfactoria*
Notas	*Se ingresó una ruta y nombre de archivo de entrada Válidos*
Fecha Ejecución	*26/01/2008*
Resultado	*Lectura de datos No Satisfactoria. Se recibe el mensaje "El Archivo de entrada no Existe".*
Notas	*Se ingresó una ruta de archivo de entrada incorrecta.*
Fecha Ejecución	*26/01/2008*
Resultado	*Lectura de datos No Satisfactoria. Se recibe el mensaje "El Archivo de entrada no Existe".*
Notas	*Se ingresó un nombre de archivo de entrada incorrecto.*
Fecha Ejecución	*26/01/2008*
Resultado	*Escritura de Información Satisfactoria*
Notas	*Se ingresó una ruta y nombre de archivos de salidas Válidos.*
Fecha Ejecución	*26/01/2008*
Resultado	*Escritura de Información No Satisfactoria. Se recibe el mensaje "El Archivo de salida no Existe".*

Notas	*Se ingresaron rutas de archivos de salidas incorrectas.*
Fecha Ejecución	*26/01/2008*
Resultado	*Escritura de Información No Satisfactoria. Se recibe el mensaje "El Archivo de salida no Existe".*
Notas	*Se ingresaron nombres de archivos de salidas incorrectos.*

Tabla 4-53. Ejecución Caso 2 de Prueba Unitaria.

Número Prueba	*PU03*
Objetivo	*Validar el módulo de análisis*
Requisitos	*Ejecutar la aplicación*
Caso de Prueba (pasos)	*- Ejecutar la aplicación* *- Ingresar usuario y clave válidos* *- Realizar la lectura de datos y análisis de los mismos.* *- Verificar que las estadísticas y reportes generados son correctos.*
Resultado Esperado	*Estadísticas y reportes generados correctamente.*
Fecha Ejecución	*26/01/2008*
Resultado	*Estadísticas y reportes generados correctamente.*
Notas	---

Tabla 4-54. Ejecución Caso 3 de Prueba Unitaria.

Los resultados de las pruebas se listan en la tabla 4-55.

Prueba	Evaluación Resultado	Comparación Resultados Obtenidos y Esperados	Necesidad Nueva Ejecución
PU01	Satisfactoria	Los resultados Obtenidos son conformes a los Esperados	No es necesaria
PU02	Satisfactoria	Los resultados Obtenidos son conformes a los Esperados	No es necesaria
PU03	Satisfactoria	Los resultados Obtenidos son conformes a los Esperados	No es necesaria

Tabla 4-55. Resultados de Ejecución de Pruebas Unitarias.

Entorno de Pruebas de Integración

Las pruebas de Integración se realizarán directamente en el equipo donde se ejecutará la aplicación. Las pruebas serán realizadas y coordinadas por el Analista / Desarrollador. El perfil usuario será ejecutado por el Líder de Seguridad y Control. Se dispondrá de 1 día hábil para realizar y documentar las pruebas de Integración.

Resultado de las Pruebas de Integración

Los resultados de las pruebas de integración se muestran en las tablas 4-56 a 4-58.

Número Prueba	*PI01*
Objetivo	*Validar correspondencia de controles de selección realizada por los usuarios con las ventanas mostradas en pantalla.*
Requisitos	*Ejecutar la aplicación*
Caso de Prueba (pasos)	*- Ejecutar en la aplicación el módulo de controles de selección de estadísticas de usuario y seleccionar estadísticas.*
Resultado Esperado	*El sistema debe mostrar solo las ventanas que muestran la información seleccionada por el usuario.*
Fecha Ejecución	*27/01/2008*
Resultado	*El sistema muestra solo las ventanas seleccionadas por el usuario.*
Notas	*Se seleccionan solo reportes de salida.*

Tabla 4-56. Ejecución Caso 1 de Prueba de Integración.

Número Prueba	*PI01b*
Objetivo	*Validar correspondencia de controles de selección realizada por los usuarios con las ventanas mostradas en pantalla.*
Requisitos	*Ejecutar la aplicación*
Caso de Prueba (pasos)	*- Ejecutar en la aplicación el módulo de controles de selección de estadísticas de usuario y no seleccionar estadísticas.*
Resultado Esperado	*El sistema no debe mostrar ventanas que muestran estadísticas.*
Fecha Ejecución	*27/01/2008*
Resultado	*El sistema no muestra ventanas de estadísticas.*
Notas	*---*

Tabla 4-57. Ejecución Caso 2 de Prueba de Integración.

Número Prueba	*PI02*
Objetivo	*Validar correspondencia de controles de selección realizada por los usuarios con los reportes generados.*
Requisitos	*Ejecutar la aplicación*
Caso de Prueba (pasos)	*- Ejecutar en la aplicación el módulo de controles de selección de reportes de usuario.*
Resultado Esperado	*El sistema debe mostrar solo los reportes que seleccionó el usuario.*
Fecha Ejecución	*27/01/2008*
Resultado	*El sistema muestra solo los reportes seleccionados por el usuario.*
Notas	*Se seleccionan solo reportes de salida.*

Tabla 4-58. Ejecución Caso 2 de Prueba de Integración.

Evaluación del Resultado de las Pruebas de Integración

Los resultados de las pruebas se listan en la tabla 4-59.

Prueba	Evaluación Resultado	Comparación Resultados Obtenidos y Esperados	Necesidad Nueva Ejecución
PI01	Satisfactoria	Los resultados Obtenidos son conformes a los Esperados	No es necesaria
PI01b	Satisfactoria	Los resultados Obtenidos son conformes a los Esperados. Esta prueba fue agregada en la fase de construcción.	No es necesaria
PI02	Satisfactoria	Los resultados Obtenidos son conformes a los Esperados	No es necesaria

Tabla 4-59. Resultados de Ejecución de Pruebas de Integración.

Entorno de Pruebas del Sistema

Las pruebas del Sistema se realizarán directamente en el equipo donde se ejecutará la aplicación. Las pruebas serán realizadas y coordinadas por el Analista / Desarrollador. El perfil usuario será ejecutado por el Líder de Seguridad y Control. Se dispondrá de 1 día hábil para realizar y documentar las pruebas del sistema.

Resultado de las Pruebas del Sistema

Los resultados de las pruebas del sistema se muestran en la tabla 4-60.

Número Prueba	*PS01*
Objetivo	*Validar la integración del sistema en su totalidad*
Requisitos	*Ejecutar la aplicación*
Caso de Prueba (pasos)	*- Ejecutar la aplicación* *- Ingresar usuario y clave válidos* *- El usuario debe seleccionar las estadísticas y reportes deseados.* *- Realizar la lectura de datos y análisis de los mismos.* *- Verificar que las estadísticas y reportes generados son correctos.*
Resultado Esperado	*El sistema debe permitir el ingreso si las credenciales son válidas.* *El sistema debe leer los datos de entrada desde el archivo correspondiente y escribir la información en los archivos de salidas si las rutas y los nombres de los mismos son válidos.* *El sistema debe mostrar las estadísticas y reportes que seleccionó el usuario.* *Las Estadísticas y Reportes deben ser generados correctamente.*

Fecha Ejecución	*28/01/2008*
Resultado	*Se ingresó al sistema.* *Se leyeron y procesaron los datos de entrada.* *Se generaron los archivos de salidas.* *Se visualizaron las estadísticas y reportes seleccionados.*
Notas	---

Tabla 4-60. Ejecución Caso 1 de Prueba de Sistema.

Evaluación del Resultado de las Pruebas del Sistema

Los resultados de las pruebas se listan en la tabla 4-61.

Prueba	Evaluación Resultado	Comparación Resultados Obtenidos y Esperados	Necesidad Nueva Ejecución
PS01	Satisfactoria	Los resultados Obtenidos son conformes a los Esperados	No es necesaria

Tabla 4-61. Resultados de Ejecución de Pruebas de Sistema.

Manual de Usuario

A continuación se incluye el Manual de uso del sistema para el Usuario Final.

Manual de Usuario Final

1. Ingreso al Sistema

Iniciar el sistema desde *Inicio, Archivo de Programas, Análisis y Control de Eventos*.

En la ventana *Ingreso al Sistema,* seleccionar el botón *Continuar*.

Aparecerá la ventana de fondo de escritorio *Análisis de Eventos de Seguridad*. En la ventana *Ingreso al Sistema,* ingresar el usuario y clave de acceso (tener en cuenta que ambos son sensibles a mayúsculas y minúsculas), seleccionar el botón *Ingresar.*

2. Análisis de Eventos

En la ventana *Módulo de Inicio,* seleccionar el botón *Módulo de Análisis*.

En la ventana *Configuración Vistas y Reportes,* seleccionar las opciones que se desean visualizar, seleccionar el botón *Continuar*.

En la ventana *Módulo de Análisis de Eventos,* ingresar el archivo de entrada, el archivo de salida de los eventos verdes, el archivo de salida de los eventos

amarillos y el archivo de salida de los eventos rojos, seleccionar el botón *Comenzar el Proceso de Análisis de Eventos…*

En la ventana *Atención,* seleccionar *OK*.

En caso que aparezca la ventana *Evento en Análisis*, seleccionar el botón *Continuar*, o *Cancelar* para volver a la ventana *Módulo de Inicio.*

En caso que aparezca la ventana *Módulo de Estadísticas*, seleccionar el botón *Continuar*, o *Cancelar* para volver a la ventana *Módulo de Inicio*.

En caso que aparezca la ventana *Gráfico de Secciones,* seleccionar el botón *Ver Gráfico*, luego seleccionar el botón *Continuar*, o *Cancelar* para volver a la ventana *Módulo de Inicio*.

En caso que aparezca la ventana *Información de Reglas,* seleccionar una regla desde el listado y presionar el botón *Ver Información de Regla*, luego seleccionar el botón *Continuar*, o *Cancelar* para volver a la ventana *Módulo de Inicio*.

En caso que aparezca la ventana *Información de Usuarios,* seleccionar el botón *Continuar*, o *Cancelar* para volver a la ventana *Módulo de Inicio*.

En caso que aparezca la ventana *Archivo de Salida,* seleccionar las opciones *Verdes*, *Amarillas* o *Rojas* para observar un determinado informe, luego seleccionar el botón *Finalizar* para volver a la ventana *Módulo de inicio.*

3. Consulta de Reportes

En la ventana *Módulo de Inicio,* seleccionar el botón *Módulo de Consulta de Reportes.*

En la ventana *Archivo de Salida,* seleccionar las opciones *Verdes*, *Amarillas* o *Rojas* para observar un determinado informe, luego seleccionar el botón *Finalizar* para volver a la ventana *Módulo de inicio.*

4. Consulta de Estadísticas Históricas

En la ventana *Módulo de Inicio,* seleccionar el botón *Módulo de Consulta de Estadísticas Históricas.*

En la ventana *Módulo de Estadísticas Históricas,* seleccionar las opciones *Total de Eventos* o *Tipo de Eventos* para observar un determinado informe, luego seleccionar el botón *Finalizar* para volver a la ventana *Módulo de inicio.*

5. Creación de Usuarios

En la ventana *Módulo de Inicio,* seleccionar el botón *Módulo de Seguridad.*

En la ventana *Módulo de Seguridad,* en el campo *ID Usuario*, ingresar la credencial de inicio del usuario. En el campo *Clave*, ingresar la clave del usuario. En el campo *Confirmar Clave*, ingresar nuevamente la clave para validar que sean iguales. Seleccionar las opciones de los módulos donde el usuario tendrá derechos. Seleccionar el botón *Crear Usuario*.

Seleccionar el botón *Finalizar* para volver a la ventana *Módulo de inicio.*

6. Cambio de Clave de Usuarios

En la ventana *Módulo de Inicio,* seleccionar el botón *Módulo de Seguridad.*

En la ventana *Módulo de Seguridad,* en el campo *ID Usuario*, ingresar la credencial de inicio del usuario. En el campo *Clave*, ingresar la nueva clave del usuario. En el campo *Confirmar Clave*, ingresar nuevamente la nueva clave para validar que sean iguales. Seleccionar el botón *Cambiar Clave*.

Seleccionar el botón *Finalizar* para volver a la ventana *Módulo de inicio.*

Especificación de la Formación a Usuarios Finales:

Esquema de Formación

Se coordinará un curso de capacitación para todos los usuarios finales.

Por el lapso de un mes se mantendrá una vía de comunicación fluida para evacuar cualquier duda. Los usuarios podrán canalizarlas a través de un correo electrónico a una dirección que se proveerá al finalizar el curso.

Materiales y Entornos de Formación

Se utilizará como guía el Manual de Usuario Final y se realizarán directamente en el equipo donde se ejecutará la aplicación. La capacitación será realizada y coordinada por el Analista / Desarrollador.

Aprobación del Sistema de Información

En reunión de seguimiento, control y aprobación entre las partes, Tesista y Directora del proyecto, se dio por aprobada esta fase.

El jefe del proyecto comunica formalmente a los participantes, afectados y usuarios los resultados de la fase. Se utiliza el siguiente anuncio.

Estimados Colaboradores,

Cumplo en informarles que la fase de Construcción del Sistema del proyecto "Análisis de Eventos de Seguridad en Servidores" ha sido aprobada satisfactoriamente.

Desde ya muchas gracias por su participación y compromiso.

4.2.2.4.2 Control de Actividades

Actividades / Tareas	Desarrollo	Justificación
ACTIVIDAD CSI 1: PREPARACIÓN DEL ENTORNO DE GENERACIÓN Y CONSTRUCCIÓN		
Tarea CSI 1.1: Implantación de la Base de Datos Física o Ficheros	NO	No es necesario el desarrollo.
Tarea CSI 1.2: Preparación del Entorno de Construcción	SI	Se dispone de la información necesaria.
ACTIVIDAD CSI 2: GENERACIÓN DEL CÓDIGO DE LOS COMPONENTES Y PROCEDIMIENTOS		
Tarea CSI 2.1: Generación del Código de Componentes	NO	Se realiza el desarrollo del software con KAPPA-PC.
Tarea CSI 2.2: Generación del Código de los Procedimientos de Operación y Seguridad	NO	Se realiza el desarrollo del software con KAPPA-PC.
ACTIVIDAD CSI 3: EJECUCIÓN DE LAS PRUEBAS UNITARIAS		
Tarea CSI 3.1: Preparación del Entorno de las Pruebas Unitarias	SI	Se dispone de la información necesaria.
Tarea CSI 3.2: Realización y Evaluación de las Pruebas Unitarias	SI	Se dispone de la información necesaria.
ACTIVIDAD CSI 4: EJECUCIÓN DE LAS PRUEBAS DE INTEGRACIÓN		
Tarea CSI 4.1: Preparación del Entorno de las Pruebas de Integración	SI	Se dispone de la información necesaria.
Tarea CSI 4.2: Realización de las Pruebas de Integración	SI	Se dispone de la información necesaria.
Tarea CSI 4.3: Evaluación del Resultado de las Pruebas de Integración	SI	Se dispone de la información necesaria.
ACTIVIDAD CSI 5: EJECUCIÓN DE LAS PRUEBAS DEL SISTEMA		
Tarea CSI 5.1: Preparación del Entorno de las Pruebas del Sistema	SI	Se dispone de la información necesaria.
Tarea CSI 5.2: Realización de las Pruebas del Sistema	SI	Se dispone de la información necesaria.
Tarea CSI 5.3: Evaluación del Resultado de las Pruebas del Sistema	SI	Se dispone de la información necesaria.
ACTIVIDAD CSI 6: ELABORACIÓN DE LOS MANUALES DE USUARIO		
Tarea CSI 6.1: Elaboración de los Manuales de Usuario	SI	Se dispone de la información necesaria.
ACTIVIDAD CSI 7: DEFINICIÓN DE LA FORMACIÓN DE USUARIOS FINALES		
Tarea CSI 7.1: Definición del Esquema de Formación	SI	Se dispone de la información necesaria.
Tarea CSI 7.2: Especificación de los Recursos y Entornos de Formación	SI	Se dispone de la información necesaria.
ACTIVIDAD CSI 8: CONSTRUCCIÓN DE LOS COMPONENTES Y PROCEDIMIENTOS DE MIGRACIÓN Y CARGA INICIAL DE DATOS		
Tarea CSI 8.1: Preparación del Entorno de	NO	No es necesaria una carga

Actividades / Tareas	Desarrollo	Justificación
Migración y Carga Inicial de Datos		inicial de información, o una migración de datos de otros sistemas.
Tarea CSI 8.2: Generación del Código de los Componentes y Procedimientos de Migración y Carga Inicial de Datos	NO	No es necesaria una carga inicial de información, o una migración de datos de otros sistemas.
Tarea CSI 8.3: Realización y Evaluación de las Pruebas de Migración y Carga Inicial de Datos	NO	No es necesaria una carga inicial de información, o una migración de datos de otros sistemas.
ACTIVIDAD CSI 9: APROBACIÓN DEL SISTEMA DE INFORMACIÓN		
Tarea CSI 9.1: Presentación y Aprobación del Sistema de Información	SI	Se dispone de la información necesaria.

Tabla 4-62. Control de Actividades CSI.

4.2.2.5 Implantación y Aceptación del Sistema (IAS)

4.2.2.5.1 Documento Entregable

DOCUMENTO DE IMPLANTACIÓN Y ACEPTACIÓN DEL SISTEMA

Plan de Implantación

El plan contempla las siguientes tareas:

- Formación necesaria para la implantación, tanto a usuarios finales como al equipo que se encarga de realizar las pruebas de implantación y aceptación del sistema:

  Antes de comenzar con la implantación el analista / programador realizará una reunión con el personal implicado en la misma para repasar y revisar que se satisfagan los requisitos necesarios, definidos en etapas previas.

- La preparación de la infraestructura necesaria para la incorporación del sistema al entorno de operación:

  El analista / programador junto con el coordinador y responsable del Centro de Cómputos deberán revisar que la infraestructura del centro de cómputos esté en condiciones y adecuada para el equipo que ejecutará la aplicación.

- La instalación de todos los componentes y procedimientos manuales y automáticos asociados a cada sistema de información implicado en la implantación:

  El analista / programador junto con el coordinador y responsable del Centro de Cómputos deberán revisar que los procedimientos utilizados en el Centro de Cómputos hayan sido actualizados con la información necesario para operar el nuevo equipo.

- La realización de las pruebas de implantación y aceptación del sistema defina en la fase de diseño que se muestran en las tablas 4-63 a 4-64.

Número Prueba	*PI01*
Objetivo	*Comprobar el funcionamiento del sistema*
Requisitos	*Ejecutar la aplicación*
Caso de Prueba (pasos)	*- Ejecutar la aplicación* *- Ingresar usuario y clave válidos* *- El usuario debe seleccionar las estadísticas y reportes*

	deseados. *- Realizar la lectura de datos y análisis de los mismos.* *- Verificar que las estadísticas y reportes generados son correctos.*
Resultado Esperado	*El sistema debe funcionar correctamente.*

Tabla 4-63. Caso 1 de Prueba de Aceptación

Número Prueba	*PA01*
Objetivo	*Validar la respuesta del sistema a los requisitos especificados por el usuario*
Requisitos	*Ejecutar la aplicación*
Caso de Prueba (pasos)	*- Ejecutar la aplicación* *- Ingresar usuario y clave válidos* *- El usuario debe seleccionar las estadísticas y reportes deseados.* *- Realizar la lectura de datos y análisis de los mismos.* *- Verificar que las estadísticas y reportes generados son correctos.*
Resultado Esperado	*El sistema debe satisfacer la respuesta esperada por el usuario en un tiempo menor a 5 minutos y con un error menor a 30%*

Tabla 4-64. Caso 1 de Prueba de Aceptación

Equipo de Implantación

El equipo de Implantación está formado por:

- El analista / Programador.

  Dedicación tiempo completo

  Responsabilidad: coordinar y verificar que la implantación se realice como se definió en el plan.

- El Líder de Seguridad y Control.

  Dedicación tiempo completo

  Responsabilidad: verificar que la implantación se realice como se definió en el plan desde el punto de vista del usuario final.

- El coordinador y responsable del Centro de Cómputos.

  Dedicación tiempo completo

Responsabilidad: coordinar y proveer del entorno físico necesario y verificar el correcto funcionamiento del mismo.

Plan de Formación a Usuarios Finales

Al plan definido en la etapa anterior, se complementa y define que los usuarios que deben tomar el curso de formación son:

- Personal del área de Seguridad y Control.
- Personal del área de Auditoria

Preparación de Instalación

Se realiza la instalación del Sistema Operativo Microsoft Windows XP, en el equipo. No se registran incidencias.

Producto Software.

Se realiza la instalación del nuevo sistema. Se realizan los procedimientos de resguardos de información. Se realizan los procedimientos de recuperación de información en una carpeta temporal. Se asignan los permisos necesarios en el sistema de archivos del sistema. No se registran incidencias.

Plan de pruebas

No es necesaria la producción de un plan de pruebas, el mismo ya fue definido en la fase de Diseño.

Resultado de las pruebas de Implantación

Los resultados de las pruebas de Implantación se muestran en la tabla 4-65.

Número Prueba	*PI01*
Objetivo	*Comprobar el funcionamiento del sistema*
Requisitos	*Ejecutar la aplicación*
Caso de Prueba (pasos)	*- Ejecutar la aplicación* *- Ingresar usuario y clave válidos* *- El usuario debe seleccionar las estadísticas y reportes deseados.* *- Realizar la lectura de datos y análisis de los mismos.* *- Verificar que las estadísticas y reportes generados son correctos.*
Resultado Esperado	*El sistema debe funcionar correctamente.*
Fecha Ejecución	*30/01/2008*
Resultado	*El sistema funciona correctamente.*

Notas	*Se realiza la ejecución y análisis de distintos archivos de entrada.*

Tabla 4-65. Ejecución Caso 1 de Prueba de Aceptación

Evaluación del resultado de las pruebas de implantación

La evaluación del resultado de las pruebas se muestra en la tabla 4-66.

Prueba	Evaluación Resultado	Comparación Resultados Obtenidos y Esperados	Necesidad Nueva Ejecución
PIm01	Satisfactoria	Los resultados Obtenidos son conformes a los Esperados	No es necesaria

Tabla 4-66. Resultados de Ejecución de Pruebas.

Plan de pruebas

No es necesaria la producción de un plan de pruebas, el mismo ya fue definido en la fase de Diseño.

Resultado de las Pruebas de Aceptación

Los resultados de las pruebas de Aceptación se muestran en la tabla 4-67.

Número Prueba	*PA01*
Objetivo	*Validar la respuesta del sistema a los requisitos especificados por el usuario*
Requisitos	*Ejecutar la aplicación*
Caso de Prueba (pasos)	*- Ejecutar la aplicación* *- Ingresar usuario y clave válidos* *- El usuario debe seleccionar las estadísticas y reportes deseados.* *- Realizar la lectura de datos y análisis de los mismos.* *- Verificar que las estadísticas y reportes generados son correctos.*
Resultado Esperado	*El sistema debe satisfacer la respuesta esperada por el usuario en un tiempo menor a 5 minutos y con un error menor a 30%*
Fecha Ejecución	*30/01/2008*
Resultado	*El sistema funciona correctamente y se obtienen las respuestas esperadas en los tiempos y formas planeadas.*
Notas	*Se realiza la ejecución y análisis de distintos archivos de entrada.*

Tabla 4-67. Ejecución Caso 1 de Prueba de Aceptación

Evaluación del Resultado de las Pruebas de Aceptación

La evaluación del resultado de las pruebas se muestra en la tabla 4-68.

Prueba	Evaluación Resultado	Comparación Resultados Obtenidos y Esperados	Necesidad Nueva Ejecución
PA01	Satisfactoria	Los resultados Obtenidos son conformes a los Esperados	No es necesaria

Tabla 4-68. Resultados de Ejecución de Pruebas.

Plan de Mantenimiento

El mantenimiento se llevará a cabo utilizando la misma infraestructura de Hardware y Software.

Las peticiones de mantenimiento deberán ser registradas y evaluadas. Los datos que se debe proporcionar son los siguientes: *Descripción de la Petición, Tipo Mantenimiento, Estado, Prioridad, Impacto, Responsable*.

En caso que se apruebe la misma, se deberá llevar un control de cambios.

Solo se realizará mantenimientos del tipo Evolutivo y Correctivo. Por el lapso de un mes luego de haber sido implantado el sistema, el mantenimiento será realizado por el mismo analista / programador.

Acuerdo de Nivel de Servicio

No será implementado en el entorno de producción por lo tanto no se compromete un Acuerdo de Nivel de Servicio.

Presentación del Sistema

Se recopila el presente estudio y se entrega a la Directora del proyecto.

Aprobación del sistema

En reunión de seguimiento, control y aprobación entre las partes, Tesista y Directora del proyecto, se dio por aprobada esta fase.

El jefe del proyecto comunica formalmente a los participantes, afectados y usuarios los resultados de la fase. Se utiliza el siguiente anuncio.

Estimados Colaboradores,

Cumplo en informarles que la fase de Implantación y Aceptación del Sistema del proyecto "Análisis de Eventos de Seguridad en Servidores" ha sido aprobada satisfactoriamente.

Desde ya muchas gracias por su participación y compromiso.

4.2.2.5.2 Control de Actividades

Actividades / Tareas	Desarrollo	Justificación
ACTIVIDAD IAS 1: ESTABLECIMIENTO DEL PLAN DE IMPLANTACIÓN		
Tarea IAS 1.1: Definición del Plan de Implantación	SI	Se dispone de la información necesaria.
Tarea IAS 1.2: Especificación del Equipo de Implantación	SI	Se dispone de la información necesaria.
ACTIVIDAD IAS 2: FORMACIÓN NECESARIA PARA LA IMPLANTACIÓN		
Tarea IAS 2.1: Preparación de la Formación del Equipo de Implantación	NO	No es necesario. El personal de Implantación tiene experiencia y el nuevo equipo se instala según el procedimiento estándar de la empresa.
Tarea IAS 2.2: Formación del Equipo de Implantación	NO	No es necesario. El personal de Implantación tiene experiencia y el nuevo equipo se instala según el procedimiento estándar de la empresa.
Tarea IAS 2.3: Preparación de la Formación a Usuarios finales	SI	Se dispone de la información necesaria.
Tarea IAS 2.4: Seguimiento de la Formación a Usuarios Finales	NO	Queda fuera del alcance del Analista/Programador.
ACTIVIDAD IAS 3: INCORPORACIÓN DEL SISTEMA AL ENTORNO DE OPERACIÓN		
Tarea IAS 3.1: Preparación de la Instalación	SI	Se dispone de la información necesaria.
Tarea IAS 3.2: Realización de la Instalación	SI	Se dispone de la información necesaria.
ACTIVIDAD IAS 4: CARGA DE DATOS AL ENTORNO DE OPERACIÓN		
Tarea IAS 4.1: Migración y Carga inicial de Datos	NO	No es necesaria una carga inicial de información, o una migración de datos de otros sistemas.
ACTIVIDAD IAS 5: PRUEBAS DE IMPLANTACIÓN DEL SISTEMA		
Tarea IAS 5.1: Preparación de las Pruebas de Implantación	SI	Se dispone de la información necesaria.
Tarea IAS 5.2: Realización de las Pruebas de implantación	SI	Se dispone de la información necesaria.
Tarea IAS 5.3: Evaluación del Resultado de las Pruebas de Implantación	SI	Se dispone de la información necesaria.
ACTIVIDAD IAS 6: PRUEBAS DE ACEPTACIÓN DEL SISTEMA		
Tarea IAS 6.1: Preparación de las Pruebas de Aceptación	SI	Se dispone de la información necesaria.
Tarea IAS 6.2: Realización de las Pruebas de Aceptación	SI	Se dispone de la información necesaria.

Actividades / Tareas	Desarrollo	Justificación
Tarea IAS 6.3: Evaluación del Resultado de las Pruebas de Aceptación	SI	Se dispone de la información necesaria.
ACTIVIDAD IAS 7: PREPARACIÓN DEL MANTENIMIENTO DEL SISTEMA		
Tarea IAS 7.1: Establecimiento de la Infraestructura para el Mantenimiento	SI	Se dispone de la información necesaria.
Tarea IAS 7.2: Formalización del Plan de Mantenimiento	SI	Se dispone de la información necesaria.
ACTIVIDAD IAS 8: ESTABLECIMIENTO DEL ACUERDO DE NIVEL DE SERVICIO		
Tarea IAS 8.1: Identificación de los Servicios	NO	Queda fuera del alcance del objetivo del presente estudio.
Tarea IAS 8.2: Descripción de las Propiedades de cada Servicio	NO	Queda fuera del alcance del objetivo del presente estudio.
Tarea IAS 8.3: Determinación del Acuerdo de Nivel de Servicio	SI	Se dispone de la información necesaria.
ACTIVIDAD IAS 9: PRESENTACIÓN Y APROBACIÓN DEL SISTEMA		
Tarea IAS 9.1: Convocatoria de la Presentación del Sistema	SI	Se dispone de la información necesaria.
Tarea IAS 9.2: Aprobación del Sistema	SI	Se dispone de la información necesaria.
ACTIVIDAD IAS 10: PASO A PRODUCCIÓN		
Tarea IAS 10.1: Preparación del Entorno de Producción	NO	En el presente estudio no se implementará el sistema en Producción.
Tarea IAS 10.2: Activación del Sistema en Producción	NO	En el presente estudio no se implementará el sistema en Producción.

Tabla 4-69. Control de Actividades IAS.

4.2.2.6 Mantenimiento de Sistema de Información (MSI)

4.2.2.6.1 Documento Entregable

DOCUMENTO DE

MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Catálogo de Peticiones, Aceptación/Rechazo, Asignación de Responsable

Petición 1- Envío automático de los reportes por correo electrónico al sector de Auditoria.

Mantenimiento Evolutivo

Estado: Rechazada

Prioridad: Baja

Impacto: Medio

Responsable: Lic. Javier Crosa

Petición 2- Compatibilidad con el sistema de backup para el resguardo de los reportes y salidas.

Mantenimiento Evolutivo.

Estado: Aceptada

Prioridad: Alta

Impacto: Alto

Responsable: Lic. Javier Crosa

Petición 3- Procesamiento de los eventos de seguridad de servidores de mensajería electrónica.

Mantenimiento Evolutivo

Estado: Rechazada

Prioridad: Baja

Impacto: Alto

Responsable: Lic. Javier Crosa

Petición 4- Procesamiento de los eventos de aplicaciones de servidores de aplicaciones varias.

Mantenimiento Evolutivo

Estado: Rechazada

Prioridad: Baja

Impacto: Alto

Responsable: Lic. Javier Crosa

Verificación de la Petición

Resultado del Estudio de la Petición

Petición 1- Envío automático de los reportes por correo electrónico al sector de Auditoria.

Para implementar esta petición es necesario utilizar un servicio SMTP. La empresa actualmente no cuenta con el mismo. La implementación requiere un detallado análisis de configuración y seguridad ya que si está mal configurado cualquier persona podría enviar mensajes.

Debido a esta falencia la petición es rechazada.

Petición 2- Compatibilidad con el sistema de backup para el resguardo de los reportes y salidas.

El producto software deberá situar los reportes y salidas generadas en una carpeta del Sistema Operativo. Luego el sistema de backup usado por la compañía podrá resguardar los mismos.

Esta petición fue aprobada.

Petición 3- Procesamiento de los eventos de seguridad de servidores de mensajería electrónica.

Esta funcionalidad podrá se implementada fácilmente, a través de un módulo adicional, cuando el sistema software esté estable y haya pasado las pruebas y aprobaciones. De todos modos esta función excede el propósito del presente trabajo. Por lo tanto la petición es rechazada.

Petición 4- Procesamiento de los eventos de aplicaciones de servidores de aplicaciones varias.

Idem a la petición anterior.

Propuesta de Solución

Petición 2, (Aceptada)- Compatibilidad con el sistema de backup para el resguardo de los reportes y salidas.

El aplicativo generará los archivos de salida correspondientes para que el sistema de backup pueda tomarlos y resguardarlo.

Catálogo de Peticiones:

Estudio del Impacto

El impacto de la modificación no es considerable. No se ven afectados otros sistemas de información.

Aceptación / Rechazo de la solución

La solución es aceptada. Se considera viable y coherente con las necesidades del negocio y la funcionalidad de sistema software.

Elementos Afectados

El proceso afectado al cambio es el que realiza la generación de los reportes de salida y las observaciones afectadas.

Afecta los archivos de salida de observaciones procesadas, archivos de salida de reportes, pantallas de selección de tipo de salidas, locación de los reportes en el File System.

No requiere cambios en el hardware.

Actividades y Tareas de los Procesos de Desarrollo y Modificación a Realizar

El costo asociado al cambio implica 16 horas del analista/programador y 3 horas del responsable de Seguridad y Control.

La fecha propuesta para el llevar a cabo el cambio es desde 19/02/2008 al 20/02/2008.

El cambio será llevado a cabo por el analista/programador.

Los puntos de control que permitan hacer un seguimiento del mismo son:

- Al finalizar la etapa de análisis.
- Al finalizar la etapa de codificación.
- Al finalizar la etapa de pruebas.

Plan de Pruebas de Regresión

Con el propósito de evitar que los cambios introducidos provoquen un comportamiento no deseado o errores adicionales, se realizaran las pertinentes pruebas de regresión. Ellas son:

- Selección de distintas carpetas en el File System
- Selección de distintos reportes y salidas

Evaluación del Cambio

El seguimiento del plan de acción da como resultado

- Las pruebas unitarias, de integración y del sistema se han realizado satisfactoriamente.
- Solo se han modificado los elementos y el proceso establecido.
- La funcionalidad introducida opera satisfactoriamente.

Resultado de las Pruebas de Regresión

- No se presentan comportamientos no deseados.
- No se detectan errores adicionales.

Evaluación del Resultado de las Pruebas de Regresión

El responsable de Seguridad y Control da por aprobadas las pruebas de Regresión.

Catálogo de Peticiones:

Nueva Versión y Aprobación

La petición 2 “Compatibilidad con el sistema de backup para el resguardo de los reportes y salidas” queda formalmente cerrada y aprobada.

En la tabla 4-70 se describe el registro estadístico de la petición.

Registro estadístico de la petición	
Tiempo empleado en el análisis	4 horas
Tiempo empleado en el estudio del impacto	2 horas
Tiempo empleado en la resolución del cambio	2 horas
Recursos empleados	19 horas 2 personas

Tabla 4-70. Registro estadístico de la petición.

4.2.2.6.2 Control de Actividades

Actividades / Tareas	Desarrollo	Justificación
ACTIVIDAD MSI 1: REGISTRO DE LA PETICIÓN		
Tarea MSI 1.1: Registro de la Petición	SI	Se dispone de la información necesaria.
Tarea MSI 1.2: Asignación de la Petición	SI	Se dispone de la información necesaria.
ACTIVIDAD MSI 2: ANÁLISIS DE LA PETICIÓN		
Tarea MSI 2.1: Verificación y Estudio de la Petición	SI	Se dispone de la información necesaria.
Tarea MSI 2.2: Estudio de la Propuesta de Solución	SI	Se dispone de la información necesaria.
ACTIVIDAD MSI 3: PREPARACIÓN DE LA IMPLEMENTACIÓN DE LA MODIFICACIÓN		
Tarea MSI 3.1: Identificación de Elementos Afectados	SI	Se dispone de la información necesaria.
Tarea MSI 3.2: Establecimiento del Plan de Acción	SI	Se dispone de la información necesaria.
Tarea MSI 3.3: Especificación del Plan de Pruebas de Regresión	SI	Se dispone de la información necesaria.
ACTIVIDAD MSI 4: SEGUIMIENTO Y EVALUACIÓN DE LOS CAMBIOS HASTA LA ACEPTACIÓN		
Tarea MSI 4.1: Seguimiento de los Cambios	SI	Se dispone de la información necesaria.
Tarea MSI 4.2: Realización de las Pruebas de Regresión	SI	Se dispone de la información necesaria.
Tarea MSI 4.3: Aprobación y Cierre de la Petición	SI	Se dispone de la información necesaria.

Tabla 4-71. Control de Actividades MSI.

4.2.3 Aseguramiento de la Calidad

4.2.3.1 Documento Entregable

DOCUMENTO DE ASEGURAMIENTO DE LA CALIDAD

Equipo de aseguramiento de calidad

El equipo de trabajo inicial necesario para determinar y valorar la conveniencia de establecer un plan de aseguramiento de calidad para las alternativas de solución propuestas estará formado por el tesista y el encargado del área usuaria o sea el Líder de Proyectos del sector de Seguridad y Control.

Sistemas de Información objeto de aseguramiento de calidad

El sistema de información que va a estar afectado por el plan de aseguramiento de calidad es "el sistema para Análisis de Eventos de Seguridad en Servidores, usando Técnicas de Minería de Datos".

Propiedades de calidad

Algunas de estas propiedades que permitirá evaluar la calidad en cuanto a las características de operación, facilidad de mantenimiento y adaptabilidad a nuevos entornos, pueden ser, por ejemplo, la facilidad de uso, eficiencia, seguridad, portabilidad, integridad y fiabilidad.

Plan de aseguramiento de calidad

El proyecto del sistema a desarrollar no será implementado directamente en una función productiva sino que será evaluado en un entorno de desarrollo o pruebas. Por lo tanto, durante este estudio, no será necesario someterlo a un minucioso y estricto plan de calidad.

De todos modos el equipo de aseguramiento de la calidad realiza la revisión de los siguientes tópicos y los resultados se muestran en las tablas 4-72 a 4-75.

- Análisis del Sistema

Tema	Resultado
Revisión de requisitos	Correcto
Revisión de consistencia	Correcto
Revisión del plan de pruebas	Correcto
Registro de la aprobación del Análisis del	Correcto

Tema	Resultado
Sistema de Información	

Tabla 4-72. Aseguramiento de Calidad. Análisis del Sistema.

- Diseño del Sistema

Tema	Resultado
Revisión de la arquitectura del sistema	Correcto
Registro de la aceptación de la arquitectura del sistema	Correcto
Revisión del diseño de las pruebas	Correcto
Revisión del plan de pruebas	Correcto
Revisión de los requisitos de implantación	Correcto
Registro de la aprobación del Diseño del sistema de Información	Correcto

Tabla 4-73. Aseguramiento de Calidad. Diseño del Sistema.

- Construcción del Sistema

Tema	Resultado
Revisión del código de componentes y procedimientos	Correcto
Revisión de la realización de las pruebas unitarias	Correcto
Revisión de la realización de las pruebas de integración	Correcto
Revisión de la realización de las pruebas del sistema	Correcto
Revisión de los manuales de usuario	Correcto
Revisión de la formación a usuarios finales	Correcto
Registro de la aprobación del sistema de información	Correcto

Tabla 4-74. Aseguramiento de Calidad. Construcción del Sistema.

- Implantación y Aceptación del Sistema

Tema	Resultado
Revisión del plan de implantación	Correcto
Revisión de las pruebas de implantación	Correcto
Registro de la aprobación de las pruebas de implantación por operación	Correcto

Tema	Resultado
Revisión de la realización de las pruebas de aceptación	Correcto
Registro de la aprobación de las pruebas de aceptación por el usuario	Correcto
Revisión del plan de mantenimiento	Correcto
Registro de la aprobación de la implantación del sistema	Correcto

Tabla 4-75. Aseguramiento de Calidad. Implantación del Sistema.

Informe de Revisión del Aseguramiento de Calidad

En reunión de seguimiento, control y aprobación entre las partes, Tesista y Directora del proyecto, se dio por aprobada esta fase.

4.2.3.2 Control de Actividades

Actividades / Tareas	Desarrollo	Justificación
ACTIVIDAD EVS-CAL 1: IDENTIFICACIÓN DE LAS PROPIEDADES DE CALIDAD PARA EL SISTEMA		
Tarea EVS-CAL 1.1: Constitución del Equipo de Aseguramiento de Calidad	SI	Se dispone de la información necesaria.
Tarea EVS-CAL 1.2: Determinación de los Sistemas de Información objeto de Aseguramiento de Calidad	SI	Se dispone de la información necesaria.
Tarea EVS-CAL 1.3: Identificación de las Propiedades de Calidad	SI	Se dispone de la información necesaria.
ACTIVIDAD EVS–CAL 2: ESTABLECIMIENTO DEL PLAN DE ASEGURAMIENTO DE CALIDAD		
Tarea EVS-CAL 2.1: Necesidad del Plan de Aseguramiento de Calidad para las Alternativas Propuestas	NO	La dimensión del Proyecto no justifica el desarrollo.
Tarea EVS-CAL 2.2: Alcance del Plan de Aseguramiento de Calidad	SI	Se dispone de la información necesaria.
Tarea EVS-CAL 2.3: Impacto en el Coste del Sistema	NO	La dimensión del Proyecto no justifica el desarrollo.
ACTIVIDAD EVS–CAL 3: ADECUACIÓN DEL PLAN DE ASEGURAMIENTO DE CALIDAD A LA SOLUCIÓN		
Tarea EVS-CAL 3.1: Ajuste del Plan de Aseguramiento de Calidad	NO	La dimensión del Proyecto no justifica el desarrollo.
Tarea EVS-CAL 3.2: Aprobación del Plan de Aseguramiento de Calidad	SI	Se dispone de la información necesaria.
ACTIVIDAD ASI-CAL 1: ESPECIFICACIÓN INICIAL DEL PLAN DE ASEGURAMIENTO DE CALIDAD		
Tarea ASI-CAL 1.1: Definición del Plan de Aseguramiento de Calidad para el Sistema de Información	SI	Se dispone de la información necesaria.
ACTIVIDAD ASI–CAL 2: ESPECIFICACIÓN DETALLADA DEL PLAN DE ASEGURAMIENTO DE CALIDAD		
Tarea ASI-CAL 2.1: Contenido del Plan de Aseguramiento de Calidad para el Sistema de Información	SI	Se dispone de la información necesaria.
ACTIVIDAD ASI-CAL 3: REVISIÓN DEL ANÁLISIS DE CONSISTENCIA		
Tarea ASI-CAL 3.1: Revisión del Catálogo de Requisitos	SI	Se dispone de la información necesaria.
Tarea ASI-CAL 3.2: Revisión de la Consistencia entre Productos	SI	Se dispone de la información necesaria.
ACTIVIDAD ASI-CAL 4: REVISIÓN DEL PLAN DE PRUEBAS		
Tarea ASI-CAL 4.1: Revisión del Plan de Pruebas	SI	Se dispone de la información necesaria.
ACTIVIDAD ASI-CAL 5: REGISTRO DE LA APROBACIÓN DEL ANÁLISIS DEL SISTEMA		
Tarea ASI-CAL 5.1: Registro de la	SI	Se dispone de la información

Actividades / Tareas	Desarrollo	Justificación
Aprobación del Análisis del Sistema de Información		necesaria.
ACTIVIDAD DSI–CAL 1: REVISIÓN DE LA VERIFICACIÓN DE LA ARQUITECTURA DEL SISTEMA		
Tarea DSI-CAL 1.1: Revisión de la Consistencia entre Productos del Diseño	SI	Se dispone de la información necesaria.
Tarea DSI-CAL 1.2: Registro de la Aceptación de la Arquitectura del Sistema	SI	Se dispone de la información necesaria.
ACTIVIDAD DSI–CAL 2: REVISIÓN DE LA ESPECIFICACIÓN TÉCNICA DEL PLAN DE PRUEBAS		
Tarea DSI-CAL 2.1: Revisión del Diseño de las Pruebas Unitarias, de Integración y de Sistema	SI	Se dispone de la información necesaria.
Tarea DSI-CAL 2.2: Revisión del Plan de Pruebas	SI	Se dispone de la información necesaria.
ACTIVIDAD DSI–CAL 3: REVISIÓN DE LOS REQUISITOS DE IMPLANTACIÓN		
Tarea DSI-CAL 3.1: Revisión de los Requisitos de Documentación de Usuario	SI	Se dispone de la información necesaria.
Tarea DSI-CAL 3.2: Revisión de los Requisitos de Implantación	SI	Se dispone de la información necesaria.
ACTIVIDAD DSI-CAL 4: REGISTRO DE LA APROBACIÓN DEL DISEÑO DEL SISTEMA DE INFORMACIÓN		
Tarea DSI-CAL 4.1: Registro de la Aprobación del Diseño del Sistema de Información	SI	Se dispone de la información necesaria.
ACTIVIDAD CSI–CAL 1: REVISIÓN DEL CÓDIGO DE COMPONENTES Y PROCEDIMIENTOS		
Tarea CSI-CAL 1.1: Revisión de Normas de Construcción	SI	Se dispone de la información necesaria.
ACTIVIDAD CSI–CAL 2: REVISIÓN DE LAS PRUEBAS UNITARIAS, DE INTEGRACIÓN Y DEL SISTEMA		
Tarea CSI-CAL 2.1: Revisión de la Realización de las Pruebas Unitarias	SI	Se dispone de la información necesaria.
Tarea CSI-CAL 2.2: Revisión de la Realización de las Pruebas de Integración	SI	Se dispone de la información necesaria.
Tarea CSI-CAL 2.3: Revisión de la Realización de las Pruebas del Sistema	SI	Se dispone de la información necesaria.
ACTIVIDAD CSI–CAL 3: REVISIÓN DE LOS MANUALES DE USUARIO		
Tarea CSI-CAL 3.1: Revisión de los Manuales de Usuario	SI	Se dispone de la información necesaria.
ACTIVIDAD CSI–CAL 4: REVISIÓN DE LA FORMACIÓN A USUARIOS FINALES		
Tarea CSI-CAL 4.1: Revisión de la Formación a Usuarios Finales	SI	Se dispone de la información necesaria.
ACTIVIDAD CSI-CAL 5: REGISTRO DE LA APROBACIÓN DEL SISTEMA DE INFORMACIÓN		
Tarea CSI-CAL 5.1: Registro de la	SI	Se dispone de la información

Actividades / Tareas	Desarrollo	Justificación
Aprobación del Sistema de Información		necesaria.
ACTIVIDAD IAS-CAL 1: REVISIÓN DEL PLAN DE IMPLANTACIÓN DEL SISTEMA		
Tarea IAS-CAL 1.1: Revisión del Plan de Implantación del Sistema	SI	Se dispone de la información necesaria.
ACTIVIDAD IAS–CAL 2: REVISIÓN DE LAS PRUEBAS DE IMPLANTACIÓN DEL SISTEMA		
Tarea IAS-CAL 2.1: Revisión de la Realización de las Pruebas de Implantación del Sistema	SI	Se dispone de la información necesaria.
Tarea DSI-CAL 2.2: Registro de la Aprobación de las Pruebas de Implantación del Sistema	SI	Se dispone de la información necesaria.
ACTIVIDAD IAS–CAL 3: REVISIÓN DE LAS PRUEBAS DE ACEPTACIÓN DEL SISTEMA		
Tarea IAS-CAL 3.1: Revisión de la Realización de las Pruebas de Aceptación de Sistema	SI	Se dispone de la información necesaria.
Tarea IAS-CAL 3.2: Registro de la Aprobación de las Pruebas de Aceptación de Sistema	SI	Se dispone de la información necesaria.
ACTIVIDAD IAS–CAL 4: REVISIÓN DEL PLAN DE MANTENIMIENTO DEL SISTEMA		
Tarea IAS-CAL 4.1: Revisión del Plan de Mantenimiento del Sistema	SI	Se dispone de la información necesaria.
ACTIVIDAD IAS–CAL 5: REGISTRO DE LA APROBACIÓN DE LA IMPLANTACIÓN DEL SISTEMA		
Tarea IAS-CAL 5.1: Registro de la Aprobación de la Implantación del Sistema	SI	Se dispone de la información necesaria.
ACTIVIDAD MSI-CAL 1: REVISIÓN DEL MANTENIMIENTO DEL SISTEMA DE INFORMACIÓN		
Tarea MSI-CAL 1.1: Revisión del Mantenimiento	SI	Se dispone de la información necesaria.
ACTIVIDAD MSI–CAL 2: REVISIÓN DEL PLAN DE PRUEBAS DE REGRESIÓN		
Tarea MSI-CAL 2.1: Comprobación de la Existencia del Plan de Pruebas de Regresión	NO	La dimensión del Proyecto no justifica el desarrollo.
ACTIVIDAD MSI–CAL3: REVISIÓN DE LA REALIZACIÓN DE LAS PRUEBAS DE REGRESIÓN		
Tarea MSI-CAL 3.1: Revisión de la Realización de las Pruebas de Regresión	NO	La dimensión del Proyecto no justifica el desarrollo.

Tabla 4-76. Control de Actividades Aseguramiento de la Calidad.

4.2.4 Interfaz de Seguridad

4.2.4.1 Documento Entregable

DOCUMENTO DE

INTERFAZ DE SEGURIDAD

Debido a la dimensión del proyecto y el entorno donde se aplicará (entorno de laboratorio), se definen a continuación, los aspectos de seguridad para todas las fases del proyecto.

Seguridad requerida en el Proceso de Ejecución de Actividades

El Responsable del sector de Seguridad y Control determina que será necesario supervisar la seguridad (niveles de autenticación, confidencialidad, integridad y disponibilidad) de los productos generados en las actividades de las fases del proyecto.

A tal fin, se asigna a cada participante del proyecto una credencial y clave de acceso a los recursos específicos a utilizar durante la ejecución del proceso, como así también para el acceso al repositorio de almacenamiento de documentos.

Seguridad de la Arquitectura Tecnológica

Características detalladas de seguridad

Se toma la arquitectura tecnológica y se analiza el nivel de seguridad, las vulnerabilidades, los riesgos y la posible gestión de los mismos. Para ello, se realizaran los siguientes pasos:

- Determinación de los principales recursos:
  - Entorno de Laboratorio,
  - Red de Laboratorio,
  - Servidor de Laboratorio.
- Identificación de las amenazas relevantes para cada uno de los recursos anteriores.
  - Entorno de Laboratorio: Falla Energética
  - Red de Laboratorio: Virus
  - Servidor de Laboratorio: Falla por Denegación de Servicio introducida por código malicioso

- Determinación del riesgo.
    - Entorno de Laboratorio: Riego Bajo.
    - Red de Laboratorio: Riego Bajo.
    - Servidor de Laboratorio: Riego Bajo.
- Selección de los mecanismos de salvaguarda oportunos que minimicen los riesgos.
    - Entorno de Laboratorio: Uso de Suministradores Continuos de Energía (UPS).
    - Red de Laboratorio: Uso de productos Antivirus.
    - Servidor de Laboratorio: Actualización de Software automática y periódica.

Seguridad para el Plan de Acción

A continuación se detallan los recursos lógicos y físicos necesarios para la activación de los servicios y mecanismos de salvaguarda.

- Suministradores Continuos de Energía (UPS). El mecanismo entra en funcionamiento automáticamente.
- Productos Antivirus. El mecanismo funciona continuamente y cuenta en alertas que notifican la aparición de infecciones.
- Actualización de Software automática y periódica. El mecanismo es activado manualmente por los administradores del mismo. Ellos, son notificados cuando es necesaria la ejecución.

Catalogación de los Productos Generados en los Procesos del Sistema de Información

Todos los productos generados (documentos, manuales, instructivos, catálogos, planillas) durante el proyecto serán guardados en el repositorio de almacenamiento de documentos asignado al mismo. Para accederlo es necesario autenticarse con las credenciales personales asignadas oportunamente.

Elaboración de Recomendaciones de Seguridad

Las recomendaciones de seguridad para la elaboración del proyecto y para el sistema son las siguientes.

- Todos los productos generados en el proceso deben ser guardados en el repositorio de almacenamiento de documentos.
- Autenticarse con las credenciales personales al repositorio de documentos.
- Solo utilizar los recursos otorgados para el proyecto.
- No utilizar recursos del entorno de producción.
- Registrar los accesos al sistema.
- Registrar las acciones realizadas con el sistema.
- Implementar credenciales de autenticación para ingresar al sistema.
- Asignar permisos de acceso, a los usuarios del sistema, propios del Sistema de Archivos (File System), sobre las carpetas de la aplicación.
- Asignar permisos sobre el servidor donde se ejecuta la aplicación, a los miembros del Centro de Cómputos para que solo puedan realizar el encendido y apagado del equipo.

Criterios de Seguridad del Plan de Pruebas

Se validan durante las pruebas los aspectos de seguridad inherentes al control de acceso a la aplicación, el registro de los accesos y el registro de las acciones ejecutadas.

Dichos controles están incluidos en el plan de pruebas conformado.

Revisión de Medidas de Seguridad del Entorno de Operación

El equipo de Seguridad refuerza las acciones relativas a procedimientos de seguridad y control de accesos, verificando, basándose en las particularidades del sistema, que se cubren las medidas de seguridad necesarias que hacen referencia al entorno de operación sobre el que se implantará el sistema.

4.2.4.2 Control de Actividades

Fases / Actividades / Tareas	Desarrollo	Justificación
PLANIFICACIÓN DE SISTEMAS DE INFORMACIÓN		
ACTIVIDAD PSI-SEG 1: PLANIFICACIÓN DE LA SEGURIDAD REQUERIDA EN EL PROCESO PLANIFICACIÓN DE SISTEMAS DE INFORMACIÓN		
Tarea PSI-SEG 1.1: Estudio de la Seguridad Requerida en el Proceso Planificación de Sistemas de Información	SI	Por la dimensión del proyecto se realizó una descripción general para todas las fases.
Tarea PSI-SEG 1.2: Organización y Planificación	NO	La dimensión del proyecto y Recursos necesarios no justifica el desarrollo
ACTIVIDAD PSI-SEG 2: EVALUACIÓN DEL RIESGO PARA LA ARQUITECTURA TECNOLÓGICA		
Tarea PSI-SEG 2.1: Estudio y Evaluación del Riesgo de las Alternativas de Arquitectura Tecnológica	SI	Se realizó la descripción para la solución.
Tarea PSI-SEG 2.2: Revisión de la Evaluación del Riesgo de las Alternativas de Arquitectura Tecnológica	SI	Se realizó la descripción para la solución.
ACTIVIDAD PSI-SEG 3: DETERMINACIÓN DE LA SEGURIDAD EN EL PLAN DE ACCIÓN.		
Tarea PSI-SEG 3.1: Determinación de la Seguridad en el Plan de Acción	SI	Se dispone de la información necesaria.
ACTIVIDAD PSI-SEG 4: CATALOGACIÓN DE LOS PRODUCTOS GENERADOS DURANTE EL PROCESO DE PLANIFICACIÓN DE SISTEMAS DE INFORMACIÓN		
Tarea PSI-SEG 4.1: Clasificación y Catalogación de los Productos Generados durante el Proceso de Planificación de Sistemas de Información	SI	Por la dimensión del proyecto se realizó una descripción general para todas las fases.
ESTUDIO DE VIABILIDAD DEL SISTEMA		
ACTIVIDAD EVS-SEG 1: ESTUDIO DE LA SEGURIDAD REQUERIDA EN EL PROCESO ESTUDIO DE VIABILIDAD DEL SISTEMA		
Tarea EVS-SEG 1.1: Estudio de la Seguridad Requerida en el Proceso Estudio de Viabilidad del Sistema	SI	Por la dimensión del proyecto se realizó una descripción general para todas las fases.
ACTIVIDAD EVS-SEG 2: SELECCIÓN DEL EQUIPO DE SEGURIDAD		
Tarea EVS-SEG 2.1: Selección del Equipo de Seguridad	NO	La dimensión del proyecto y Recursos necesarios no justifica el desarrollo
ACTIVIDAD EVS-SEG 3: RECOMENDACIONES ADICIONALES DE SEGURIDAD PARA EL SISTEMA DE INFORMACIÓN		
Tarea EVS-SEG 3.1: Elaboración de Recomendaciones de Seguridad	SI	Se dispone de la información necesaria.
ACTIVIDAD EVS-SEG 4: EVALUACIÓN DE LA SEGURIDAD DE LAS ALTERNATIVAS DE SOLUCIÓN		

Fases / Actividades / Tareas	Desarrollo	Justificación
Tarea EVS-SEG 4.1: Valoración y Evaluación de la Seguridad de las Alternativas de Solución	NO	La naturaleza del proyecto no justifica el desarrollo.
ACTIVIDAD EVS-SEG 5: EVALUACIÓN DETALLADA DE LA SEGURIDAD DE LA SOLUCIÓN PROPUESTA		
Tarea EVS-SEG 5.1: Descripción Detallada de la Seguridad de la Solución Propuesta.	SI	Se dispone de la información necesaria.
ACTIVIDAD EVS-SEG 6: CATALOGACIÓN DE LOS PRODUCTOS GENERADOS DURANTE EL PROCESO DE ESTUDIO DE VIABILIDAD DEL SISTEMA		
Tarea EVS-SEG 6.1: Clasificación y Catalogación de los Productos Generados durante el Proceso de Estudio de Viabilidad del Sistema	SI	Por la dimensión del proyecto se realizó una descripción general para todas las fases.
ANÁLISIS DEL SISTEMA DE INFORMACIÓN		
ACTIVIDAD ASI-SEG 1: ESTUDIO DE LA SEGURIDAD REQUERIDA EN EL PROCESO DE ANÁLISIS DEL SISTEMA DE INFORMACIÓN		
Tarea ASI-SEG 1.1: Estudio de la Seguridad Requerida en el Proceso de Análisis del Sistema de Información	SI	Por la dimensión del proyecto se realizó una descripción general para todas las fases.
ACTIVIDAD ASI-SEG 2: DESCRIPCIÓN DE LAS FUNCIONES Y MECANISMOS DE SEGURIDAD		
Tarea ASI-SEG 2.1: Estudio de las Funciones y Mecanismos de Seguridad a Implantar	SI	Se dispone de la información necesaria.
ACTIVIDAD ASI-SEG 3: DEFINICIÓN DE LOS CRITERIOS DE ACEPTACIÓN DE LA SEGURIDAD		
Tarea ASI-SEG 3.1: Actualización del Plan de Pruebas	SI	Se dispone de la información necesaria.
ACTIVIDAD ASI-SEG 4: CATALOGACIÓN DE LOS PRODUCTOS GENERADOS DURANTE EL PROCESO DE ANÁLISIS DEL SISTEMA DE INFORMACIÓN		
Tarea ASI-SEG 4.1: Clasificación y Catalogación de los Productos Generados Durante el Proceso de Análisis del Sistema de Información	SI	Por la dimensión del proyecto se realizó una descripción general para todas las fases.
DISEÑO DEL SISTEMA DE INFORMACIÓN		
ACTIVIDAD DSI-SEG 1: ESTUDIO DE LA SEGURIDAD REQUERIDA EN EL PROCESO DE DISEÑO DEL SISTEMA DE INFORMACIÓN		
Tarea DSI-SEG 1.1: Estudio de la Seguridad Requerida en el Proceso de Diseño del Sistema de Información	SI	Por la dimensión del proyecto se realizó una descripción general para todas las fases.
ACTIVIDAD DSI-SEG 2: ESPECIFICACIÓN DE REQUISITOS DE SEGURIDAD DEL ENTORNO TECNOLÓGICO		
Tarea DSI-SEG 2.1: Análisis de los Riesgos del Entorno Tecnológico	SI	Se dispone de la información necesaria.
ACTIVIDAD DSI-SEG 3: REQUISITOS DE SEGURIDAD DEL ENTORNO DE CONSTRUCCIÓN		

Fases / Actividades / Tareas	Desarrollo	Justificación
Tarea DSI-SEG 3.1: Identificación de los Requisitos de Seguridad del Entorno de Construcción	SI	Por la dimensión del proyecto se realizó una descripción general para todas las fases.
ACTIVIDAD DSI-SEG 4: DISEÑO DE PRUEBAS DE SEGURIDAD		
Tarea DSI-SEG 4.1: Diseño de las Pruebas de Seguridad	SI	Se realizó en la etapa de Diseño.
ACTIVIDAD DSI-SEG 5: CATALOGACIÓN DE LOS PRODUCTOS GENERADOS DURANTE EL PROCESO DE DISEÑO DEL SISTEMA DE INFORMACIÓN		
Tarea DSI-SEG 5.1: Clasificación y Catalogación de los Productos Generados durante el Proceso de Diseño del Sistema de Información	SI	Por la dimensión del proyecto se realizó una descripción general para todas las fases.
CONSTRUCCIÓN DEL SISTEMA DE INFORMACIÓN		
ACTIVIDAD CSI-SEG 1: ESTUDIO DE LA SEGURIDAD REQUERIDA EN EL PROCESO DE CONSTRUCCIÓN DEL SISTEMA DE INFORMACIÓN		
Tarea CSI-SEG 1.1: Estudio de la Seguridad Requerida en el Proceso de Construcción del Sistema de Información	SI	Por la dimensión del proyecto se realizó una descripción general para todas las fases.
ACTIVIDAD CSI-SEG 2: EVALUACIÓN DE LOS RESULTADOS DE PRUEBAS DE SEGURIDAD		
Tarea CSI-SEG 2.1: Estudio de los Resultados de Pruebas de Seguridad	SI	Se realizó en la etapa de Construcción.
ACTIVIDAD CSI-SEG 3: ELABORACIÓN DEL PLAN DE FORMACIÓN DE SEGURIDAD		
Tarea CSI-SEG 3.1: Elaboración del Plan de Formación de Seguridad	NO	La dimensión del proyecto y Recursos necesarios no justifica el desarrollo
ACTIVIDAD CSI-SEG 4: CATALOGACIÓN DE LOS PRODUCTOS GENERADOS DURANTE		
EL PROCESO DE CONSTRUCCIÓN DEL SISTEMA DE INFORMACIÓN		
Tarea CSI-SEG 4.1: Clasificación y Catalogación de los Productos Generados durante el Proceso de Construcción del Sistema de Información	SI	Por la dimensión del proyecto se realizó una descripción general para todas las fases.
IMPLANTACIÓN Y ACEPTACIÓN DEL SISTEMA.		
ACTIVIDAD IAS-SEG 1: ESTUDIO DE LA SEGURIDAD REQUERIDA EN EL PROCESO DE IMPLANTACIÓN Y ACEPTACIÓN DEL SISTEMA		
Tarea IAS-SEG 1.1: Estudio de la Seguridad Requerida en el Proceso de Implantación y Aceptación del Sistema	SI	Por la dimensión del proyecto se realizó una descripción general para todas las fases.
ACTIVIDAD IAS-SEG 2: REVISIÓN DE MEDIDAS DE SEGURIDAD DEL ENTORNO DE OPERACIÓN		
Tarea IAS-SEG 2.1: Revisión de Medidas de Seguridad del Entorno de Operación	SI	Se dispone de la información necesaria.
ACTIVIDAD IAS-SEG 3: EVALUACIÓN DE RESULTADOS DE PRUEBAS DE SEGURIDAD		

Fases / Actividades / Tareas	Desarrollo	Justificación
DE IMPLANTACIÓN DEL SISTEMA		
Tarea IAS-SEG 3.1: Estudio de los Resultados de Pruebas de Seguridad de Implantación del Sistema	SI	Se realizó en la etapa de Implantación.
ACTIVIDAD IAS-SEG 4: CATALOGACIÓN DE LOS PRODUCTOS GENERADOS DURANTE EL PROCESO DE IMPLANTACIÓN Y ACEPTACIÓN DEL SISTEMA		
Tarea IAS-SEG 4.1: Clasificación y Catalogación de los Productos Generados durante el Proceso Implantación y Aceptación del Sistema	SI	Por la dimensión del proyecto se realizó una descripción general para todas las fases.
ACTIVIDAD IAS-SEG 5: REVISIÓN DE MEDIDAS DE SEGURIDAD EN EL ENTORNO DE PRODUCCIÓN		
Tarea IAS-SEG 5.1: Revisión de Medidas de Seguridad en el Entorno de Producción	NO	El entorno donde se implantará el sistema no justifica el desarrollo
MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN		
ACTIVIDAD MSI-SEG 1: ESTUDIO DE LA SEGURIDAD REQUERIDA EN EL PROCESO MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN		
Tarea MSI-SEG 1.1: Estudio de la Seguridad Requerida en el Proceso Mantenimiento de Sistemas de Información	SI	Por la dimensión del proyecto se realizó una descripción general para todas las fases.
ACTIVIDAD MSI-SEG 2: ESPECIFICACIÓN E IDENTIFICACIÓN DE LAS FUNCIONES Y MECANISMOS DE SEGURIDAD		
Tarea MSI-SEG 2.1: Estudio de la Petición	NO	El entorno donde se implantará el sistema no justifica el desarrollo
Tarea MSI-SEG 2.2: Análisis de las Funciones y Mecanismos de Seguridad Afectados o Nuevos	NO	El entorno donde se implantará el sistema no justifica el desarrollo
ACTIVIDAD MSI-SEG 3: CATALOGACIÓN DE LOS PRODUCTOS GENERADOS DURANTE		
EL PROCESO DE MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN		
Tarea MSI-SEG 3.1: Clasificación y Catalogación de los Productos Generados durante el Proceso de Mantenimiento de Sistemas de Información	SI	Por la dimensión del proyecto se realizó una descripción general para todas las fases.

Tabla 4-77. Interfaz de Seguridad.

4.2.5 Gestión del Proyecto

4.2.5.1 Documento Entregable

DOCUMENTO DE GESTIÓN DEL PROYECTO

Definición General del Proyecto

Las características de los elementos a desarrollar se listan en el siguiente catálogo de clases.

Catálogo de clases

El catálogo de clases se describe en la tabla 4-78.

Nombre Clase	Métodos / Visibilidad	Parámetros
OBSERVACIONES	LEER() Visibilidad: Pública	DIA EVENTO HORA USUARIO
	APLICAR_REGLAS() Visibilidad: Pública	ID DIA EVENTO HORA USUARIO REGLA
	ESCRIBIR() Visibilidad: Pública	ID DIA EVENTO HORA USUARIO CLASIFICACION REGLA HORA_EJECUCION
USUARIO	CREAR() Visibilidad: Pública	ID CLAVE NOMBRE PERMISOS
	CAMBIAR_CLAVE() Visibilidad: Pública	ID CLAVE
	VALIDAR() Visibilidad: Pública	ID CLAVE PERMISOS
GRAFICOS	MOSTRAR() Visibilidad: Pública	EJE_X EJE_Y NOMBRE_EJE_X NOMBRE_EJE_Y ESCALA_EJE_X ESCALA_EJE_Y
	DIBUJAR() Visibilidad: Protegida	EJE_X EJE_Y ESCALA_EJE_X ESCALA_EJE_Y FUNCION

Nombre Clase	Métodos / Visibilidad	Parámetros
	OCULTAR() Visibilidad: Pública	No Requiere
ARCHIVOS	ABRIR() Visibilidad: Pública	NOMBRE RUTA PERMISOS BLOQUEO
	ESCRIBIR() Visibilidad: Pública	NOMBRE RUTA PERMISOS
	CERRAR() Visibilidad: Pública	NOMBRE RUTA
VENTANAS	MOSTRAR() Visibilidad: Pública	NOMBRE POSICIÓN_X POSICIÓN_Y ALTURA ANCHURA COLOR_FONDO
	MOVER() Visibilidad: Pública	NOMBRE MUEVE
	MINIMIZAR() Visibilidad: Pública	NOMBRE MINIMIZA
	MAXIMIZAR() Visibilidad: Pública	NOMBRE MAXIMIZA
	CERRAR() Visibilidad: Pública	NOMBRE CIERRA

Tabla 4-78. Gestión de Proyectos. Catalogo de Clases.

Esfuerzo estimado

El esfuerzo necesario para el desarrollo de los elementos listados anteriormente se lista a continuación. También se tienen en cuenta tareas no están encaminadas directamente al desarrollo de elementos del proyecto, pero que van a influir en el esfuerzo necesario para su realización. Se obtiene el esfuerzo estimado en horas distribuidas por procesos, en la tabla 4-79.

Actividad	Horas
Planificación del Sistema de Información	20
Estudio de Viabilidad del Sistema	20
Análisis del Sistema	50
Diseño del Sistema	50

Actividad	Horas
Construcción del Sistema	50
Implantación y Aceptación del Sistema	20
Mantenimiento del Sistema	20
Gestión del Proyecto	50
Seguridad	20
Gestión de la Configuración	20
Aseguramiento de la Calidad	20
Total	340

Tabla 4-79. Gestión de Proyectos. Estimación de Esfuerzo.

Planificación General del Proyecto

Estrategia de desarrollo

Se considera que la estrategia de desarrollo más adecuada a utilizar es Por Prototipos o Construcción Evolutiva, donde se genera un prototipo funcional en los primeros procesos del proyecto y el prototipo se va completando en sucesivas evaluaciones y revisiones, añadiendo nuevas funcionalidades y mejoras, hasta cubrir los requisitos completamente.

Estructura de actividades

La estructura del proyecto y los procesos principales e interfaces del desarrollo que se llevarán a cabo son los siguientes.

Estructura Principal

- Planificación de Sistemas de Información (PSI)
- Desarrollo de Sistemas de Información
    - Estudio de Viabilidad del Sistema (EVS)
    - Análisis del Sistema de Información (ASI)
    - Diseño del Sistema de Información (DSI)
    - Construcción del Sistema de Información (CSI)

- Implantación y Aceptación del Sistema (IAS)
- Mantenimiento de Sistema de Información (MSI)

Interfases

- Aseguramiento de la Calidad
- Gestión del Proyecto
- Gestión de la Configuración
- Seguridad

Catálogo de productos a generar

Los productos a generar, en función de las características concretas del proyecto se listan a continuación.

- Documento entregable de Gestión del Proyecto
- Documento entregable de Planificación de Sistemas de Información (PSI)
- Documento entregable de Estudio de Viabilidad del Sistema (EVS)
- Documento entregable de Análisis del Sistema de Información (ASI)
- Documento entregable de Diseño del Sistema de Información (DSI)
- Documento entregable de Construcción del Sistema de Información (CSI)
- Documento entregable de Implantación y Aceptación del Sistema (IAS)
- Documento entregable de Mantenimiento de Sistema de Información (MSI)
- Documento entregable de Aseguramiento de la Calidad
- Documento entregable de Seguridad
- Documento entregable de Gestión de la Configuración

- Aplicación (Sistema de Información)

Hitos del proyecto

A continuación en la tabla 4-80, se detallan las fechas de entrega de cada uno de los productos a desarrollar.

Producto	Fecha Estimada
Documento entregable de Gestión del Proyecto	01/10/2007
Documento entregable de Planificación de Sistemas de Información (PSI)	31/10/2007
Documento entregable de Estudio de Viabilidad del Sistema (EVS)	15/11/2007
Documento entregable de Análisis del Sistema de Información (ASI)	15/12/2007
Documento entregable de Diseño del Sistema de Información (DSI)	10/01/2008
Documento entregable de Construcción del Sistema de Información (CSI)	15/02/2008
Documento entregable de Implantación y Aceptación del Sistema (IAS)	01/03/2008
Documento entregable de Mantenimiento de Sistema de Información (MSI)	20/03/2008
Documento entregable de Aseguramiento de la Calidad	10/04/2008
Documento entregable de Seguridad	10/04/2008
Documento entregable de Gestión de la Configuración	10/04/2008
Aplicación (Sistema de Información)	02/05/2008

Tabla 4-80. Gestión del Proyecto. Hitos

Organización de los recursos

El tesista será el Tecnólogo, Analista y Programador.

Aceptación de la Planificación General del Proyecto

En reunión de seguimiento, control y aprobación entre las partes, Tesista y Directora del proyecto, se dio por aprobada esta fase.

Ficha de asignación de tarea

El tesista será el Tecnólogo, Analista y Programador. El seguimiento y control del proyecto lo hará Él mismo en conjunto con el encargado del área usuaria o sea el Líder de Proyectos del sector de Seguridad y Control.

Fichas de seguimiento de tareas

El seguimiento de las tareas se llevará a cabo revisando el estado de cada tarea entre el Tesista y el Líder de Proyectos del sector de Seguridad y Control, verificando su estado.

Para cada tarea se deberá informar:

- La fecha real de comienzo.
- El tiempo empleado hasta el momento en su realización.
- Apreciación del tiempo que queda para terminarla.
- El tanto por ciento de avance sobre el total.
- Los problemas o incidencias encontradas.

Ficha de Incidencia

Persigue conocer el impacto producido por una incidencia en cuanto a:

- Tareas afectadas por la incidencia.
- Horas de trabajo perdidas.
- Retrasos ocasionados.

Para ello será necesario completar la siguiente ficha de incidencias que se muestra en la tabla 4-81.

Impacto	Descripción
Sobre tareas	
En horas	
En fechas	
Solución propuesta	

Tabla 4-81. Gestión del Proyecto. Impacto sobre incidencias.

Informe de Seguimiento en el período

El informe debe recoger los objetivos alcanzados durante el período, incidencias y desviaciones detectadas junto con las acciones encaminadas a corregirlas, objetivos que se prevén para el siguiente período y las variaciones en los recursos materiales asignados para su realización.

Asunto	Descripción
Objetivos alcanzados durante el período	
Incidencias habidas durante el período	
Análisis de las desviaciones	
Previsión actual	
Acciones correctoras	
Objetivos previstos para el siguiente período	
Movimiento de recursos: humanos y materiales	

Tabla 4-82. Gestión del Proyecto. Informe de Seguimiento.

Esfuerzo Realmente Insumido en el Proyecto

El esfuerzo real que demandó el desarrollo del presente estudio se muestra en la tabla 4-83.

Actividad	Horas
Planificación del Sistema de Información	25
Estudio de Viabilidad del Sistema	24
Análisis del Sistema	70
Diseño del Sistema	74
Construcción del Sistema	64
Implantación y Aceptación del Sistema	28
Mantenimiento del Sistema	26
Gestión del Proyecto	24
Seguridad	14
Gestión de la Configuración	20
Aseguramiento de la Calidad	14
Total	383

Tabla 4-83. Gestión de Proyectos. Esfuerzo Real Insumido.

4.2.5.2 Control de Actividades

Actividades / Tareas	Desarrollo	Justificación
ACTIVIDADES DE INICIO DEL PROYECTO		
ACTIVIDAD GPI 1: ESTIMACIÓN DE ESFUERZO		
Tarea GPI 1.1: Identificación de Elementos a Desarrollar	SI	Se dispone de la información necesaria.
Tarea GPI 1.2: Cálculo del Esfuerzo	SI	Se dispone de la información necesaria.
ACTIVIDAD GPI 2: PLANIFICACIÓN		
Tarea GPI 2.1: Selección de la Estrategia de Desarrollo	SI	Se dispone de la información necesaria.
Tarea GPI 2.2: Selección de la Estructura de Actividades, Tareas y Productos	SI	Se dispone de la información necesaria.
Tarea GPI 2.3: Establecimiento del Calendario de Hitos y Entregas	SI	Se dispone de la información necesaria.
Tarea GPI 2.4: Planificación Detallada de Actividades y Recursos Necesarios	NO	La dimensión del proyecto y Recursos necesarios no justifica el desarrollo
Tarea GPI 2.5: Presentación y Aceptación de la Planificación General del Proyecto	SI	Se dispone de la información necesaria.
ACTIVIDADES DE SEGUIMIENTO Y CONTROL		
ACTIVIDAD GPS 1: ASIGNACIÓN DETALLADA DE TAREAS		
Tarea GPS 1.1: Asignación de Tarea	SI	Se dispone de la información necesaria.
ACTIVIDAD GPS 2: COMUNICACIÓN AL EQUIPO DEL PROYECTO		
Tarea GPS 2.1: Informar al Equipo del Proyecto	NO	La dimensión del proyecto y Recursos necesarios no justifica el desarrollo
ACTIVIDAD GPS 3: SEGUIMIENTO DE TAREAS		
Tarea GPS 3.1: Seguimiento de Tareas	SI	Se dispone de la información necesaria.
GESTIÓN DE INCIDENCIAS		
ACTIVIDAD GPS 4: ANÁLISIS Y REGISTRO DE LA INCIDENCIA		
Tarea GPS 4.1: Analizar Impacto	SI	Se dispone de la información necesaria.
Tarea GPS 4.2: Propuesta de Solución de la Incidencia	SI	Se dispone de la información necesaria.
Tarea GPS 4.3: Registrar la Incidencia	SI	Se dispone de la información necesaria.
GESTIÓN DE CAMBIOS EN LOS REQUISITOS		
ACTIVIDAD GPS 5: PETICIÓN DE CAMBIO DE REQUISITOS		
Tarea GPS 5.1: Registro de la Petición de	NO	La dimensión y objetivos del

Actividades / Tareas	Desarrollo	Justificación
Cambio de Requisitos		proyecto no justifica el desarrollo
ACTIVIDAD GPS 6: ANÁLISIS DE LA PETICIÓN DE CAMBIO DE REQUISITOS		
Tarea GPS 6.1: Estudio de la Petición de Cambio de Requisitos	NO	La dimensión y objetivos del proyecto no justifica el desarrollo
Tarea GPS 6.2 Impacto de la Petición de Cambio de Requisitos	NO	La dimensión y objetivos del proyecto no justifica el desarrollo
Tarea GPS 6.3 Estudio de Alternativas y Propuesta de Solución	NO	La dimensión y objetivos del proyecto no justifica el desarrollo
ACTIVIDAD GPS 7: APROBACIÓN DE LA SOLUCIÓN		
Tarea GPS 7.1: Aprobación de la Solución	NO	La dimensión y objetivos del proyecto no justifica el desarrollo
ACTIVIDAD GPS 8: ESTIMACIÓN DEL ESFUERZO Y PLANIFICACIÓN DE LA SOLUCIÓN		
Tarea GPS 8.1: Estimación de Esfuerzo para el Cambio	NO	La dimensión y objetivos del proyecto no justifica el desarrollo
Tarea GPS 8.2: Planificación de los Cambios	NO	La dimensión y objetivos del proyecto no justifica el desarrollo
ACTIVIDAD GPS 9: REGISTRO DEL CAMBIO DE REQUISITOS		
Tarea GPS 9.1: Registro del Cambio de Requisitos	NO	La dimensión y objetivos del proyecto no justifica el desarrollo
ACTIVIDAD GPS 10: FINALIZACIÓN DE LA TAREA		
Tarea GPS 10.1: Comprobación de la Tarea	SI	Se dispone de la información necesaria.
ACTIVIDAD GPS 11: ACTUALIZACIÓN DE LA PLANIFICACIÓN		
Tarea GPS 11.1: Actualización de Tareas	NO	La dimensión y objetivos del proyecto no justifica el desarrollo
Tarea GPS 11.2: Obtención de la Extrapolación	NO	La dimensión y objetivos del proyecto no justifica el desarrollo
Tarea GPS 11.3: Elaboración del Informe de Seguimiento	NO	La dimensión y objetivos del proyecto no justifica el desarrollo
ACTIVIDAD GPS 12: REUNIONES DE SEGUIMIENTO		
Tarea GPS 12.1: Reunión Interna de Seguimiento	SI	Se dispone de la información necesaria.
ACTIVIDAD GPS 13: ACEPTACIÓN		
Tarea GPS 13.1: Verificación de Aceptación Interna	SI	Se dispone de la información necesaria.

Actividades / Tareas	Desarrollo	Justificación
ACTIVIDADES DE FINALIZACIÓN		
ACTIVIDAD GPF 1: CIERRE DEL PROYECTO		
Tarea GPF 1.1: Inclusión en Histórico de Proyectos	SI	Se dispone de la información necesaria.
Tarea GPF 1.2: Archivo de la Documentación de Gestión del Proyecto	SI	Se dispone de la información necesaria.

Tabla 4-84. Control de Actividades Gestión del Proyecto.

4.2.6 Gestión de la Configuración

4.2.6.1 Documento Entregable

DOCUMENTO DE GESTIÓN DE LA CONFIGURACIÓN

Requisitos de Gestión de la Configuración

Se define una versión a cada instancia distinta de un elemento de configuración, que es almacenada en un repositorio, y que puede ser recuperada en cualquier momento para su uso o modificación.

A las distintas versiones que aparecen en el tiempo, según se va avanzando en el desarrollo de un elemento, se les llama revisiones y se identifican de manera única, utilizando un esquema numérico, donde cada nueva versión recibe un número sucesivo.

Se guardan versiones anteriores como punto de seguridad, al cual poder volver en caso de que un cambio efectuado no nos lleve al resultado deseado.

También se guardan versiones antiguas para poder reutilizar elementos que aparecían en ellas pero que fueron desechados en un momento dado.

La versión de cada documento consiste en la indicación al final del campo código de la combinación de dos dígitos separados por un punto. El primer dígito parte del valor uno, el segundo de cero.

Para la codificación de los mismos se usa un único código de identificación del tipo de sistemas de codificación "significativo".

El código se formará de la siguiente manera [***_#.#], donde

- [***], tres letras que hacen referencia al nombre del elemento.
- [_], un guión bajo.
- [#], corresponde a la versión.
- [.], un punto.
- [#], corresponde a la revisión.

Se definen las siguientes líneas base:

- Línea Base Funcional, que se establece al finalizar la fase de análisis y especificación de los requisitos del sistema.

- Línea Base de Diseño, que se establece al finalizar la fase de diseño. Comprende todos aquellos documentos en los que se define la arquitectura del producto software, así como el Plan de Pruebas.

- Línea Base de Producto, que se establece al finalizar la fase de pruebas. Comprende los programas creados y todos aquellos documentos que contienen la información relativa a las pruebas realizadas.

- Línea Base de Operación, que se establece al finalizar la fase de implantación. Comprende los manuales de usuario, guías de operación y mantenimiento, manuales de formación.

Plan de Gestión de la Configuración.

Se consideran como Elementos de Configuración del Software los siguientes componentes, listados en la tabla 4-85.

Producto	Tipo	Codificación
Planificación de Sistemas de Información	Documento	PSI_#.#
Presentación formal del Plan de Sistemas de Información	Documento	PFP_#.#
Estudio de Viabilidad del Sistema	Documento	EVS_#.#
Análisis del Sistema de Información	Documento	ASI_#.#
Diseño del Sistema de Información	Documento	DSI_#.#
Procedimiento de operación.	Documento	MOP_#.#
Plan de pruebas.	Documento	PRU_#.#
Construcción del Sistema de Información	Documento	CSI_#.#
Casos de prueba ejecutados y los resultados registrados.	Documento	PRR_#.#
Manual de usuario.	Documento	MUS_#.#
Implantación y Aceptación del Sistema	Documento	IAS_#.#
Mantenimiento de Sistema de Información	Documento	MSI_#.#
Peticiones de mantenimiento.	Documento	PMA_#.#
Aseguramiento de la Calidad	Documento	CAL_#.#
Interfaz de Seguridad	Documento	SEG_#.#
Gestión del Proyecto	Documento	GPR_#.#
Gestión de la Configuración	Documento	GCO_#.#
Código Fuente	Programa	CFT_#.#

Tabla 4-85. Elementos de Configuración.

Se establecen los siguientes tipos de bibliotecas de software:

- Biblioteca de trabajo: comprende el área de trabajo donde el analista/diseñador elabora los documentos del proyecto y donde el programador desarrollan el software, es decir, donde se realiza la codificación y pruebas unitarias. En esta biblioteca el control de cambios es informal.

- Biblioteca maestra: Se usa para almacenar Elementos de Configuración de Software liberados para la entrega al cliente. Los elementos en la biblioteca maestra se encuentran sujetos a un control de cambios formal y estricto. Esta biblioteca tiene fuertes restricciones de acceso para escritura.

- Biblioteca de Backup: se utiliza para resguardo de los elementos generados durante el proyecto.

Control de Cambios en la Configuración

Se consideran dos tipos de cambios:

- Corrección de un defecto

- Mejora del sistema

Se establecen los siguientes niveles de controles de cambios:

- Control de cambios informal: Antes de que el Elemento de Configuración del Software pase a formar parte de una línea base, el analista podrá realizar cualquier cambio justificado sobre él.

- Control de cambios formal: Se adopta cuando se entrega el producto al cliente y se transfieren los Elementos de Configuración de Software a la Biblioteca Maestra. Todo cambio deberá ser aprobado por el Coordinador de Seguridad y Control.

A continuación se definen las etapas del proceso formal, es decir, el proceso que hay que seguir para hacer un cambio sobre una línea base:

1. Iniciación del Cambio: se presenta una solicitud de cambio, que puede venir provocada por un problema que se ha detectado o por un cambio en los requisitos. La solicitud de cambio se creo con un aplicativo que la empresa posee.

2. Clasificación y registro de la solicitud de cambio.

3. Aprobación o rechazo inicial de la solicitud de cambio. El responsable es el Comité de Control de Cambios.

4. Evaluación de la solicitud de cambio, si ha sido aprobada, para calcular el esfuerzo técnico, los posibles efectos secundarios, el impacto global sobre otras funciones del sistema y el costo estimado del cambio. Como resultado se obtiene un Informe de Cambio.

5. Se presenta el Informe de Cambio al Comité de Control de Cambios. Si se considera que el cambio es beneficioso se genera una Orden de Cambio, que describe el cambio a realizar, las restricciones que se deben respetar y los criterios de revisión y de auditoría. La orden de cambio se creo con un aplicativo que la empresa posee.

6. Se realiza el cambio, entrando en un proceso de seguimiento y control.

7. Una vez finalizado el cambio, se certifica, mediante una revisión, que se ha efectuado correctamente el cambio y con ello se ha corregido el problema detectado o bien se han satisfecho los requisitos modificados.

8. Se notifica el resultado al originador del cambio.

Los estados para cada tipo de producto son los siguientes:

- En proceso de desarrollo: indica que el elemento está en construcción.
- Revisado: indica que el elemento fue revisado por el tutor de tesis y pasa nuevamente al estado de Desarrollo para aplicar correcciones.
- Cerrado: indica que el elemento está correcto, aprobado y resguardado.

Entorno Tecnológico

El entorno tecnológico que soporta la Gestión de Configuración de este proyecto es el siguiente:

- Aplicativo comercial, que utiliza la empresa, para generar las peticiones de cambios y las órdenes de cambios.
- Aplicativo comercial, que utiliza la empresa, para realizar resguardo de los elementos de configuración.
- El mismo equipo servidor, utilizado para desarrollar este estudio, para generar los distintos elementos de configuración.

Identificación y Registro de Cambios de Productos.

En la tabla 4-86 se registran los Elementos de configuración de software, las distintas versiones producidas, el estado y la fecha de las mismas.

Nombre	Versión	Estado	Fecha
Gestión del Proyecto	GPR_1.0	Revisado	13/08/2007
Gestión del Proyecto	**GPR_1.1**	**Cerrado**	**25/08/2007**
Planificación de Sistemas de Información	PSI_1.0	Revisado	12/09/2007
Planificación de Sistemas de Información	**PSI_2.0**	**Cerrado**	**20/09/2007**
Presentación formal del Plan de Sistemas de Información	**PFP_1.0**	**Cerrado**	**20/09/2007**
Estudio de Viabilidad del Sistema	EVS_1.0	Revisado	06/10/2007
Estudio de Viabilidad del Sistema	**EVS_2.0**	**Cerrado**	**15/10/2007**
Análisis del Sistema de Información	ASI_1.0	Revisado	05/11/2007
Análisis del Sistema de Información	ASI_2.0	Revisado	10/11/2007
Análisis del Sistema de Información	**ASI_2.1**	**Cerrado**	**21/11/2007**
Diseño del Sistema de Información	DSI_1.0	Revisado	10/12/2007
Diseño del Sistema de Información	DSI_2.0	Revisado	21/12/2007
Diseño del Sistema de Información	DSI_3.0	Revisado	27/12/2007
Diseño del Sistema de Información	**DSI_3.1**	**Cerrado**	**29/12/2007**
Procedimiento de operación.	**MOP_1.0**	**Cerrado**	**29/12/2007**
Plan de pruebas.	**PRU_1.0**	**Cerrado**	**29/12/2007**
Construcción del Sistema de Información	CSI_1.0	Revisado	11/01/2008
Construcción del Sistema de Información	CSI_2.0	Revisado	25/01/2008
Construcción del Sistema de Información	**CSI_3.0**	**Cerrado**	**31/01/2008**
Casos de prueba ejecutados y los resultados registrados.	**PRR_1.0**	**Cerrado**	**31/01/2008**
Manual de usuario.	**MUS_1.0**	**Cerrado**	**31/01/2008**
Implantación y Aceptación del Sistema	IAS_1.0	Revisado	10/02/2008
Implantación y Aceptación del Sistema	IAS_2.0	Revisado	13/02/2008
Implantación y Aceptación del Sistema	**IAS_2.1**	**Cerrado**	**15/02/2008**
Mantenimiento de Sistema de Información	MSI_1.0	Revisado	19/02/2008
Mantenimiento de Sistema de Información	**MSI_2.0**	**Cerrado**	**29/02/2008**
Peticiones de mantenimiento.	PMA_1.0	Revisado	05/03/2008
Peticiones de mantenimiento.	**PMA_1.1**	**Cerrado**	**15/03/2008**
Aseguramiento de la Calidad	CAL_1.0	Revisado	05/03/2008
Aseguramiento de la Calidad	**CAL_1.1**	**Cerrado**	**15/03/2008**
Interfaz de Seguridad	SEG_1.0	Revisado	05/03/2008
Interfaz de Seguridad	**SEG_2.0**	**Cerrado**	**15/03/2008**
Gestión de la Configuración	GCO_1.0	Revisado	15/07/2008
Gestión de la Configuración	**GCO_1.1**	**Cerrado**	**31/07/2008**
Código Fuente	CFT_1.0	Revisado	31/07/2007

Nombre	Versión	Estado	Fecha
Código Fuente	CFT_2.0	Revisado	25/09/2007
Código Fuente	CFT_3.0	Revisado	25/01/2008
Código Fuente	CFT_4.0	Revisado	21/02/2008
Código Fuente	CFT_4.1	Revisado	31/03/2008
Código Fuente	**CFT_5.0**	**Cerrado**	**31/07/2008**

Tabla 4-86. Identificación y Registro de Cambios de Productos.

4.2.6.2 Control de Actividades

Actividades / Tareas	Desarrollo	Justificación
ESTUDIO DE VIABILIDAD DEL SISTEMA		
ACTIVIDAD EVS-GC 1: DEFINICIÓN DE LOS REQUISITOS DE GESTIÓN DE CONFIGURACIÓN		
Tarea EVS-GC 1.1: Definición de los Requisitos de Gestión de Configuración	SI	Se dispone de la información necesaria.
ACTIVIDAD EVS-GC 2: ESTABLECIMIENTO DEL PLAN DE GESTIÓN DE LA CONFIGURACIÓN		
Tarea EVS-GC 2.1: Definición del Plan de Gestión de la Configuración	SI	Se dispone de la información necesaria.
Tarea EVS-GC 2.2: Especificación del Entorno Tecnológico para la Gestión de Configuración	SI	Se dispone de la información necesaria.
ANÁLISIS, DISEÑO, CONSTRUCCIÓN E IMPLANTACION Y ACEPTACIÓN DEL SISTEMA DE INFORMACIÓN		
ACTIVIDAD GC 1: IDENTIFICACIÓN Y REGISTRO DE PRODUCTOS		
Tarea GC 1.1: Identificación y Registro de los Productos de los Procesos en el Sistema de Gestión de la Configuración	SI	Se dispone de la información necesaria.
ACTIVIDAD GC 2: IDENTIFICACIÓN Y REGISTRO DEL PRODUCTO GLOBAL		
Tarea GC 2.1: Registro en el Sistema de Gestión de la Configuración del Producto Global de Proceso	SI	Se dispone de la información necesaria.
MANTENIMIENTO DEL SISTEMA DE INFORMACIÓN		
ACTIVIDAD MSI-GC 1 – REGISTRO DEL CAMBIO EN EL SISTEMA DE GESTIÓN DE LA CONFIGURACIÓN		
Tarea MSI-GC 1.1: Registro del Cambio en el Sistema de Gestión de la Configuración	SI	Se dispone de la información necesaria.
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	SI	Se dispone de la información necesaria.
Tarea MSI-GC 1.3: Registro de la Nueva Versión de los Sistemas de Información en el Sistema de Gestión de la Configuración	SI	Se dispone de la información necesaria.

Tabla 4-87. Control de Actividades Gestión de la Configuración.

5 ESTUDIO DE CASOS

Esta sección esta orientada a mostrar la utilidad de la aplicación en un dominio, es decir, como es ventajoso, al negocio, el desarrollo del presente trabajo. Es un análisis de nivel superior, a nivel de negocio. Describir las ventajas y los beneficios que se obtuvieron o los que se esperan obtener.

La experiencia gravitará en la producción de las Reglas de Decisión y cuatro Casos de Estudio.

Finalmente se presentarán las conclusiones.

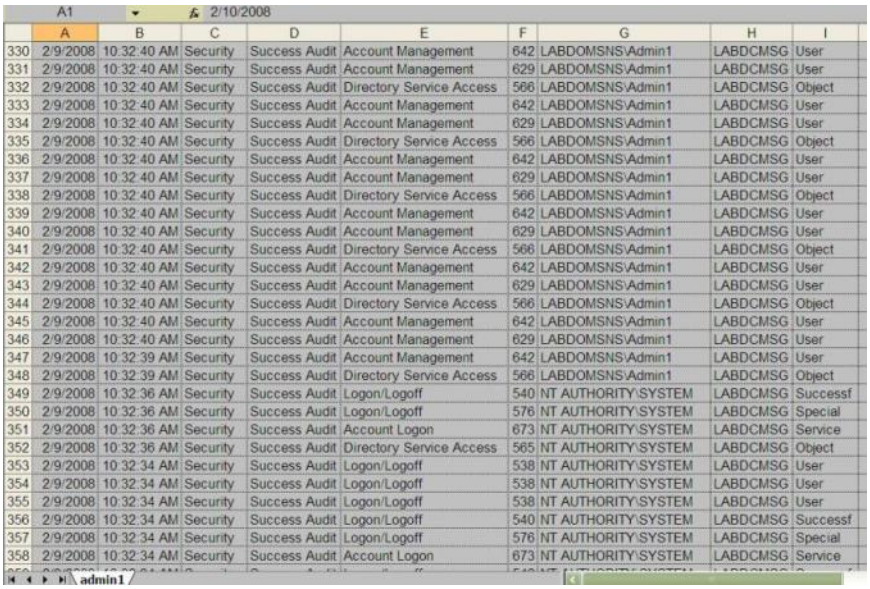
5.1 Producción de las Reglas de Decisión

Secuencia de pasos necesaria para producir las reglas de decisión.

1. Descargar los eventos de seguridad del servidor controlador de dominio.
2. Filtrar y guardar los registros que pertenecen a acciones realizadas por administradores de redes.
3. Normalizar los datos en base a la lógica, definida en el apartado 4.1.3.3 Construcción de Datos
4. Procesar los registros con la red neuronal SOM. Se utiliza la configuración especificada en el apartado 4.1.4.3 Construir el Modelo.
5. Clasificar los Clusters generados por SOM según el apartado 4.1.3.3 Construcción de Datos
6. Clasificar los registros según el apartado 4.1.3.3 Construcción de Datos
7. Procesar la salida de la red SOM con el árbol de decisión para obtener las reglas finales que se usarán para clasificar los eventos de seguridad. Se utiliza la configuración especificada en el apartado 4.1.4.3 Construir el Modelo.
8. Configurar las reglas de decisión en el sistema desarrollado.

Desarrollo de la Secuencia de pasos necesaria para producir las reglas de decisión.

1. Exportar el archivo del Visor de Eventos de Seguridad a un archivo del tipo CSV. El archivo que se obtiene se muestra en la figura 5-1.



	A	B	C	D	E	F	G	H	I
330	2/9/2008	10:32:40 AM	Security	Success Audit	Account Management	642	LABDOMSNS\Admin1	LABDCMSG	User
331	2/9/2008	10:32:40 AM	Security	Success Audit	Account Management	629	LABDOMSNS\Admin1	LABDCMSG	User
332	2/9/2008	10:32:40 AM	Security	Success Audit	Directory Service Access	566	LABDOMSNS\Admin1	LABDCMSG	Object
333	2/9/2008	10:32:40 AM	Security	Success Audit	Account Management	642	LABDOMSNS\Admin1	LABDCMSG	User
334	2/9/2008	10:32:40 AM	Security	Success Audit	Account Management	629	LABDOMSNS\Admin1	LABDCMSG	User
335	2/9/2008	10:32:40 AM	Security	Success Audit	Directory Service Access	566	LABDOMSNS\Admin1	LABDCMSG	Object
336	2/9/2008	10:32:40 AM	Security	Success Audit	Account Management	642	LABDOMSNS\Admin1	LABDCMSG	User
337	2/9/2008	10:32:40 AM	Security	Success Audit	Account Management	629	LABDOMSNS\Admin1	LABDCMSG	User
338	2/9/2008	10:32:40 AM	Security	Success Audit	Directory Service Access	566	LABDOMSNS\Admin1	LABDCMSG	Object
339	2/9/2008	10:32:40 AM	Security	Success Audit	Account Management	642	LABDOMSNS\Admin1	LABDCMSG	User
340	2/9/2008	10:32:40 AM	Security	Success Audit	Account Management	629	LABDOMSNS\Admin1	LABDCMSG	User
341	2/9/2008	10:32:40 AM	Security	Success Audit	Directory Service Access	566	LABDOMSNS\Admin1	LABDCMSG	Object
342	2/9/2008	10:32:40 AM	Security	Success Audit	Account Management	642	LABDOMSNS\Admin1	LABDCMSG	User
343	2/9/2008	10:32:40 AM	Security	Success Audit	Account Management	629	LABDOMSNS\Admin1	LABDCMSG	User
344	2/9/2008	10:32:40 AM	Security	Success Audit	Directory Service Access	566	LABDOMSNS\Admin1	LABDCMSG	Object
345	2/9/2008	10:32:40 AM	Security	Success Audit	Account Management	642	LABDOMSNS\Admin1	LABDCMSG	User
346	2/9/2008	10:32:40 AM	Security	Success Audit	Account Management	629	LABDOMSNS\Admin1	LABDCMSG	User
347	2/9/2008	10:32:39 AM	Security	Success Audit	Account Management	642	LABDOMSNS\Admin1	LABDCMSG	User
348	2/9/2008	10:32:39 AM	Security	Success Audit	Directory Service Access	566	LABDOMSNS\Admin1	LABDCMSG	Object
349	2/9/2008	10:32:36 AM	Security	Success Audit	Logon/Logoff	540	NT AUTHORITY\SYSTEM	LABDCMSG	Successf
350	2/9/2008	10:32:36 AM	Security	Success Audit	Logon/Logoff	576	NT AUTHORITY\SYSTEM	LABDCMSG	Special
351	2/9/2008	10:32:36 AM	Security	Success Audit	Account Logon	673	NT AUTHORITY\SYSTEM	LABDCMSG	Service
352	2/9/2008	10:32:36 AM	Security	Success Audit	Directory Service Access	565	NT AUTHORITY\SYSTEM	LABDCMSG	Object
353	2/9/2008	10:32:34 AM	Security	Success Audit	Logon/Logoff	538	NT AUTHORITY\SYSTEM	LABDCMSG	User
354	2/9/2008	10:32:34 AM	Security	Success Audit	Logon/Logoff	538	NT AUTHORITY\SYSTEM	LABDCMSG	User
355	2/9/2008	10:32:34 AM	Security	Success Audit	Logon/Logoff	538	NT AUTHORITY\SYSTEM	LABDCMSG	User
356	2/9/2008	10:32:34 AM	Security	Success Audit	Logon/Logoff	540	NT AUTHORITY\SYSTEM	LABDCMSG	Successf
357	2/9/2008	10:32:34 AM	Security	Success Audit	Logon/Logoff	576	NT AUTHORITY\SYSTEM	LABDCMSG	Special
358	2/9/2008	10:32:34 AM	Security	Success Audit	Account Logon	673	NT AUTHORITY\SYSTEM	LABDCMSG	Service

Figura 5-1. Archivo exportado del Visor de Eventos de Seguridad.

2. Del archivo anterior se eliminan los registros que no pertenecen a los administradores de redes. Adicionalmente se eliminan los atributos redundantes e irrelevantes. Según se muestra en las figuras 5-2 y 5-3.

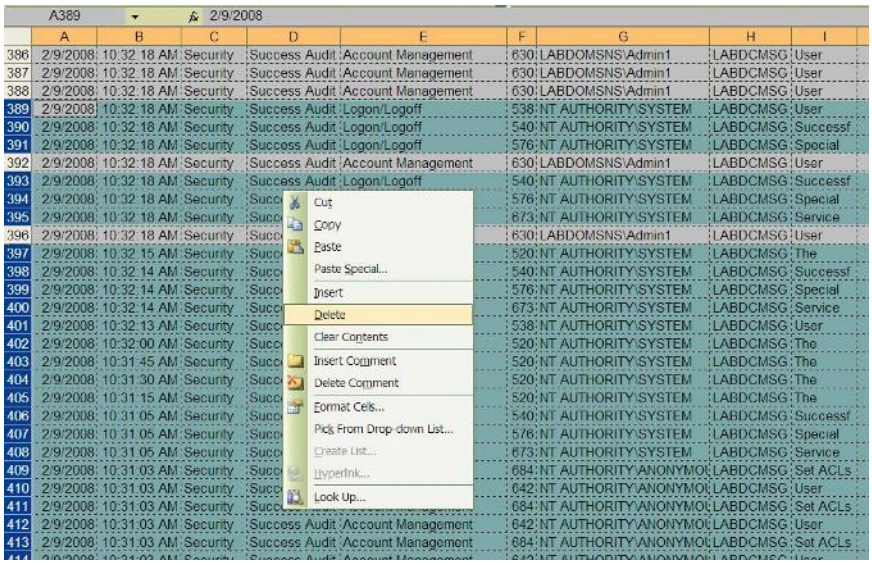


Figura 5-2. Eliminación de registros irrelevantes.

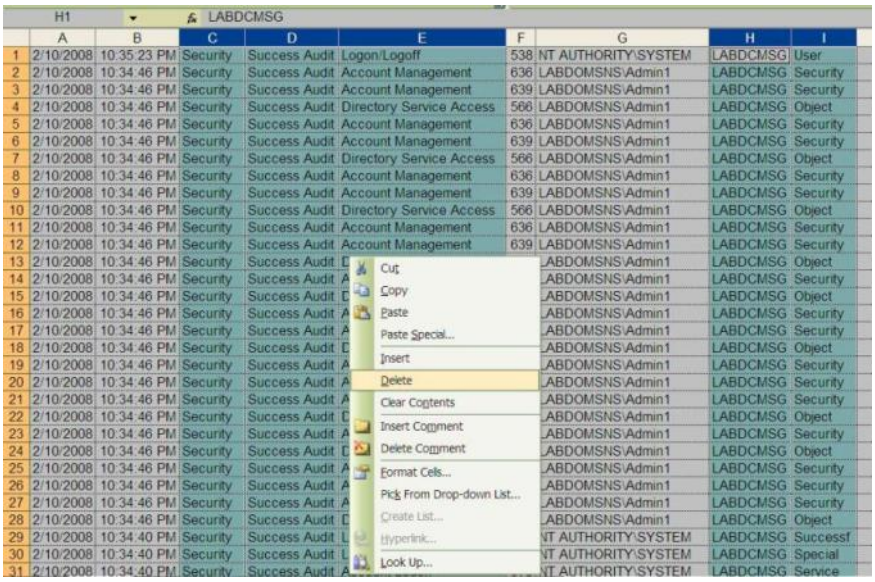


Figura 5-3. Eliminación de atributos irrelevantes.

3. Normalización de los eventos para que la red neuronal pueda procesarlos. Al finalizar el proceso queda el archivo de entrada para la red neuronal SOM. Según se muestra en las tablas 5-1 a 5-4.

Evento	Codificación en SOM	Descripción
566	1	Object Operation
624	2	User Account Created
626	3	User Account Enabled
628	4	User Account password set
629	5	User Account Disabled
630	6	User Account Deleted
636	7	Local Group Member Added
639	8	Local Group Changed
642	9	User Account Changed

Tabla 5-1. Codificación de eventos.

Usuario	Codificación en SOM
Admin1	1
Admin2	2
Admin3	3
Admin4	4
Admin5	5

Usuario	Codificación en SOM
Admin6	6

Tabla 5-2. Codificación de Usuarios.

Día / Horario	Codificación en SOM
Lunes a Viernes	1
Sábados y Domingos	2
09:00 a 18:00 horas	1
18:01 a 08:59 horas	2

Tabla 5-3. Codificación de Días y Horarios.

	A	B	C	D
1	día	hora	evento	user
2	1	2	1	1
3	1	2	1	1
4	1	2	1	1
5	1	2	1	1
6	1	1	2	1
7	1	1	2	2
8	2	2	2	2
9	2	2	2	3
10	1	1	2	4
11	1	1	2	5
12	1	1	2	6
13	2	2	2	3
14	2	2	2	4

Figura 5-4. Extracto del Archivo de entrada de la red neuronal con los Eventos Normalizados.

4. Procesar los registros con la red neuronal SOM. Consiste en configurar los parámetros, cargar los eventos a procesar y ejecutarla un número de veces hasta que se considera está entrenada. Luego se clasifican los grupos o clusters obtenidos, en base al número de observaciones de cada uno de ellos.

   La configuración utilizada es la siguiente: Cantidad de Observaciones= 16807; Número de variables = 4; Dimensiones del mapa = 4; Número de ciclos de entrenamiento de la red: 10; Parámetros de aprendizaje= 0.9, 0.1 y Exponential; Valor de Sigma para la vecindad Gaussiana = 50%, 1% y Exponential.

   Se necesitaron 9 ejecuciones de la red neuronal para que la misma alcance su mejor estado de entrenamiento y se estabilice. Al finalizar el

proceso de entrenamiento se obtienen los siguientes grupos. Según se muestra en la tabla 5-4.

Cluster	Observaciones
1	68
2	69
3	1855
4	7563
5	23
6	82
7	49
8	3076
9	199
10	57
11	230
12	320
13	255
14	2663
15	298

Tabla 5-4. Distribución de las observaciones en los clusters.

5. Clasificar los Grupos. Se realiza la clasificación de los clusters fundados en la siguiente lógica:

   - Si la cantidad de observaciones del grupo es menor al 1% del total de observaciones procesadas por SOM se considera que el cluster tiene observaciones fraudulentas.

   - Si la cantidad de observaciones del grupo varía entre 1% y 10% del total de observaciones procesadas por SOM se considera que el cluster tiene observaciones dudosas.

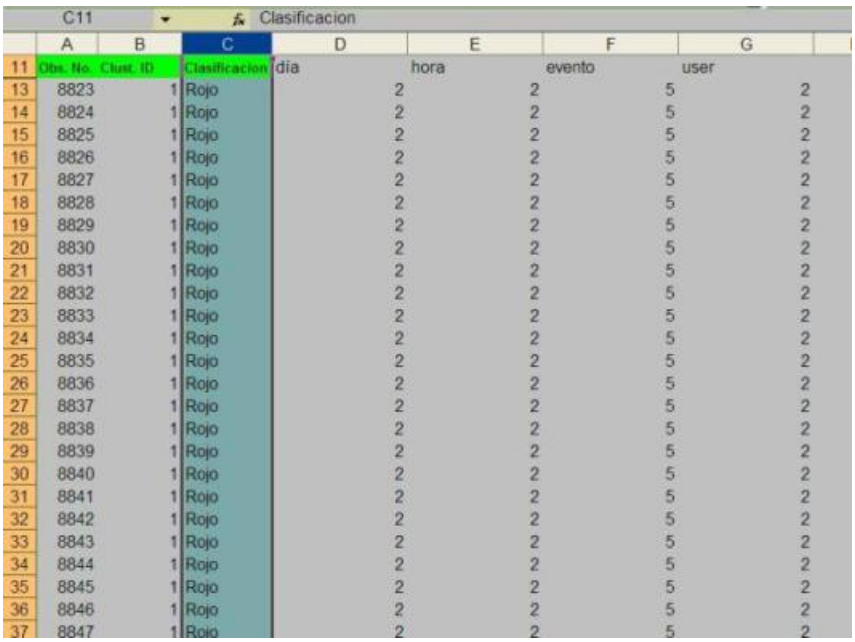
   - Si la cantidad de observaciones del grupo es mayor a 10% del total de observaciones procesadas por SOM se considera que el cluster tiene observaciones normales. Según se muestra en la tabla 5-5.

Grupo	Clasificación
1	Rojo
2	Rojo

Grupo	Clasificación
3	Verde
4	Verde
5	Rojo
6	Rojo
7	Rojo
8	Verde
9	Amarillo
10	Rojo
11	Amarillo
12	Amarillo
13	Amarillo
14	Verde
15	Amarillo

Tabla 5-5. Clasificación de los Cluster generados por SOM.

6. En el archivo de salida de SOM, en la solapa Data, se encuentran listadas todas la observaciones procesadas junto con un ID y el cluster al cual pertenecen. Se agrega una columna adicional con la clasificación de cada una de ellas (asignada en el paso anterior en base al grupo que pertenece). Según se muestra en la figura 5-5.



	A	B	C	D	E	F	G
11	Obs. No.	Clust. ID	Clasificacion	dia	hora	evento	user
13	8823	1	Rojo	2	2	5	2
14	8824	1	Rojo	2	2	5	2
15	8825	1	Rojo	2	2	5	2
16	8826	1	Rojo	2	2	5	2
17	8827	1	Rojo	2	2	5	2
18	8828	1	Rojo	2	2	5	2
19	8829	1	Rojo	2	2	5	2
20	8830	1	Rojo	2	2	5	2
21	8831	1	Rojo	2	2	5	2
22	8832	1	Rojo	2	2	5	2
23	8833	1	Rojo	2	2	5	2
24	8834	1	Rojo	2	2	5	2
25	8835	1	Rojo	2	2	5	2
26	8836	1	Rojo	2	2	5	2
27	8837	1	Rojo	2	2	5	2
28	8838	1	Rojo	2	2	5	2
29	8839	1	Rojo	2	2	5	2
30	8840	1	Rojo	2	2	5	2
31	8841	1	Rojo	2	2	5	2
32	8842	1	Rojo	2	2	5	2
33	8843	1	Rojo	2	2	5	2
34	8844	1	Rojo	2	2	5	2
35	8845	1	Rojo	2	2	5	2
36	8846	1	Rojo	2	2	5	2
37	8847	1	Rojo	2	2	5	2

Figura 5-5. Clasificación de cada Observación.

7. Procesar la salida de la red SOM con el árbol de decisión para obtener las reglas finales que se usarán para clasificar los eventos de seguridad. Las reglas de decisión se listan a continuación en la tabla 5-6.

Regla	Condición
Rule1	IF hora = 1 THEN Clasificacion = verde
Rule2	IF { evento = 1 OR evento = 7 } AND hora = 2 THEN Clasificacion = amarillo
Rule3	IF evento = 2 AND hora = 2 THEN Clasificacion = amarillo
Rule4	IF evento = 3 AND hora = 2 AND user = 1 THEN Clasificacion = amarillo
Rule5	IF evento = 3 AND hora = 2 AND user = 2 THEN Clasificacion = amarillo
Rule6	IF día = 1 AND evento = 4 AND hora = 2 THEN Clasificacion = rojo
Rule7	IF día = 2 AND hora = 2 THEN Clasificacion = amarillo
Rule8	IF evento = 6 AND hora = 2 THEN Clasificacion = amarillo
Rule9	IF evento = 6 AND hora = 2 AND user = 2 THEN Clasificacion = amarillo
Rule10	IF día = 1 AND evento = 8 AND hora = 2 THEN Clasificacion = rojo
Rule11	IF evento = 9 AND hora = 2 AND user = 2 THEN Clasificacion = amarillo
Rule12	IF hora = 2 AND user = 5 THEN Clasificacion = rojo
Rule13	IF día = 1 AND { evento = 2 OR evento = 3 } AND hora = 2 AND user = 6 THEN Clasificacion = rojo
Rule14	IF día = 2 AND { evento = 2 OR evento = 3 }

Regla	Condición
	AND hora = 2 AND user = 6 THEN Clasificacion = amarillo
Rule15	IF evento = 5 AND hora = 2 AND user = 1 THEN Clasificacion = rojo
Rule16	IF día = 1 AND evento = 5 AND hora = 2 AND user = 2 THEN Clasificacion = amarillo
Rule17	IF día = 2 AND evento = 5 AND hora = 2 AND user = 1 THEN Clasificacion = amarillo
Rule18	IF día = 2 AND evento = 5 AND hora = 2 AND user = 2 THEN Clasificacion = rojo
Rule19	IF día = 2 AND evento = 6 AND hora = 2 AND user = 6 THEN Clasificacion = amarillo
Rule20	IF día = 1 AND evento = 9 AND hora = 2 AND {user = 1 OR user = 6} THEN Clasificacion = rojo
Rule21	IF día = 2 AND evento = 9 AND hora = 2 THEN Clasificacion = amarillo

Tabla 5-6. Reglas de Decisión.

8. Configurar las reglas de decisión en el sistema desarrollado. Utilizando la interfaz de KAPPA-PC, en el módulo de configuración del motor de reglas, se cargan las reglas obtenidas.

   Para lograr una clasificación óptima de registros es necesario asignar una prioridad a las reglas. En Kappa-PC las reglas con el atributo *Prioridad* más alto se aplican primero, por lo tanto las reglas más generales, con menor número de condiciones, se le asignan la prioridad más pequeña.

   En la figura 5-6 se puede apreciar la ventana de configuración de las reglas de decisión en Kappa-PC.

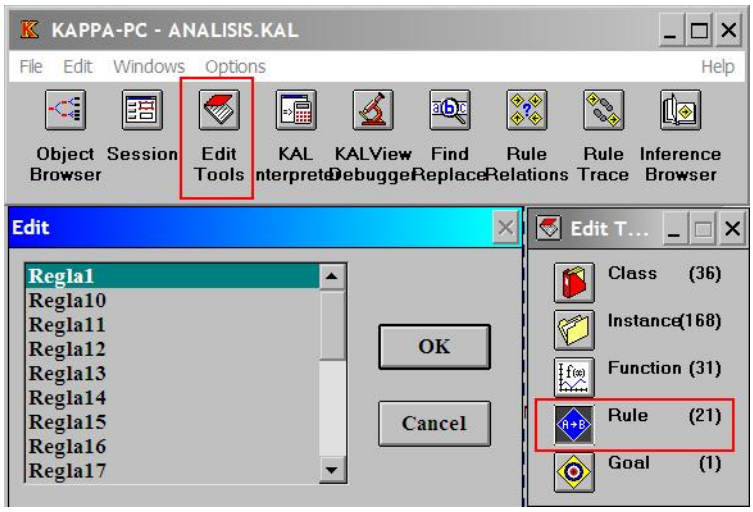


Figura 5-6. Configuración de las reglas de decisión en Kappa-PC.

5.2 Caso 1

Se analizarán los eventos clasificados como Rojos de una muestra que mezcle horario laboral y no laboral.

La secuencia de pasos necesaria para llegar a cabo el caso es la siguiente.

1. Descargar los eventos de seguridad del servidor controlador de dominio.
2. Filtrar y guardar los registros que pertenecen a acciones realizadas por administradores de redes.
3. Normalizar los datos en base a la lógica, definida en el apartado 4.1.3.3 Construcción de Datos.
4. Preparar el archivo de entrada con los datos a procesar (figura 5-7).

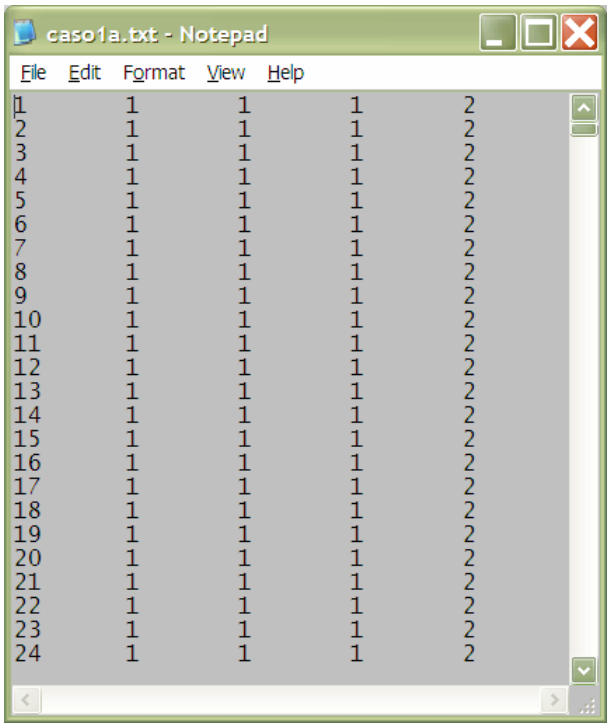


Figura 5-7. Caso de Estudio 1: Archivo de entrada con los datos a procesar.

5. En las figuras 5-8 a 5-12 se muestran las ventanas de la aplicación cuando se ejecuta el análisis de los datos.

Figura 5-8. Caso de Estudio 1: Selección del Archivo de entrada.

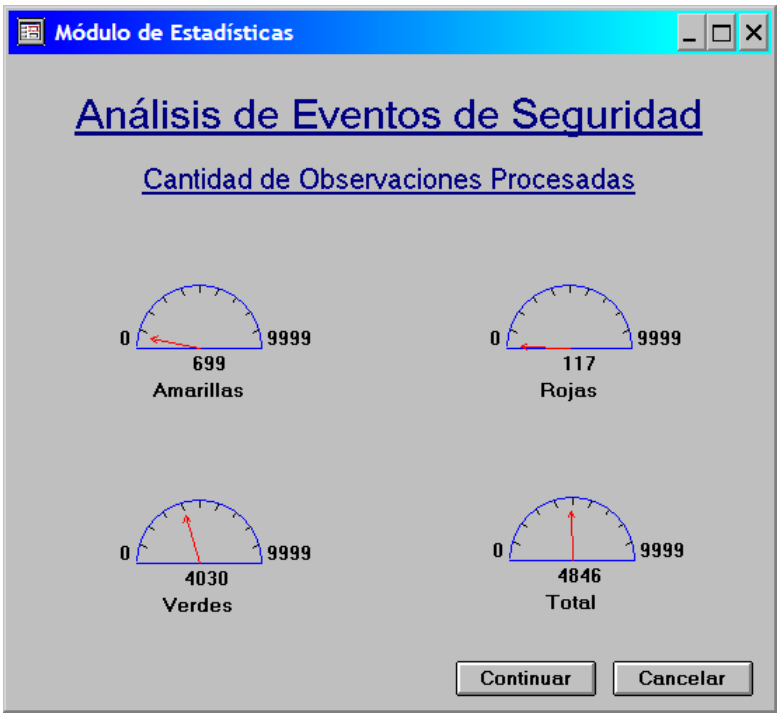


Figura 5-9. Caso de Estudio 1: Cantidad de Observaciones Analizadas por tipo.

Figura 5-10. Caso de Estudio 1: Gráfico de Secciones.

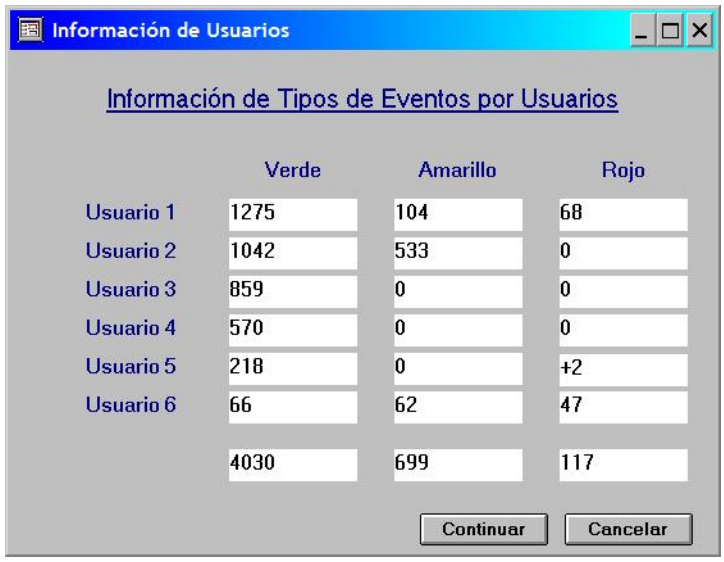


Figura 5-11. Caso de Estudio 1: Información de Observaciones Analizadas por Usuario y Tipo.

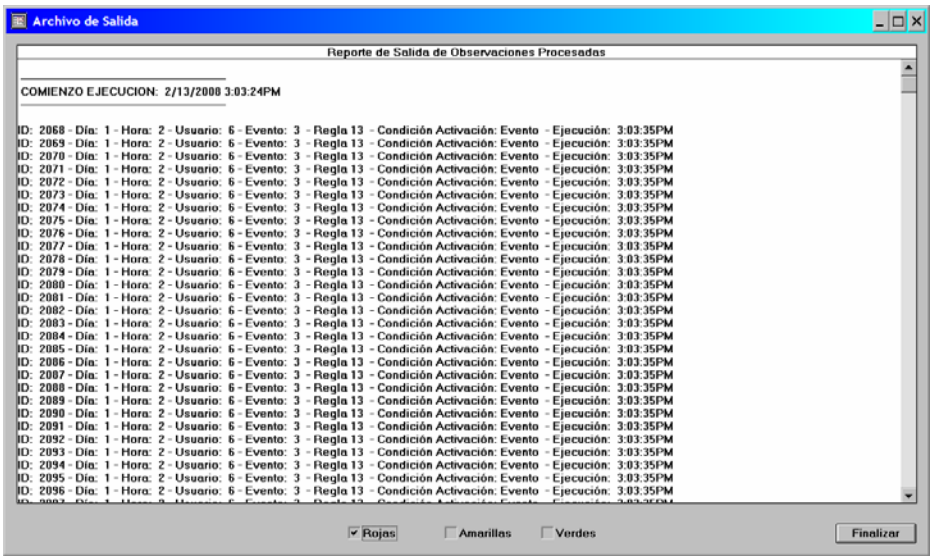


Figura 5-12. Caso de Estudio 1: Archivo de Salida de Observaciones Analizadas.

6. Analizar las estadísticas y reportes de salida.

   Se procesaron 4846 observaciones. Tiempo insumido 30 segundos.

   Cantidad de Observaciones Verdes: 4030 (83.2%)

   Cantidad de Observaciones Amarillas: 699 (14.4%)

   Cantidad de Observaciones Rojas: 117 (2.4%)

   Análisis de las Observaciones Rojas:

Se toma como referencia las siguientes tablas y figuras donde se muestran la información y los datos necesarios.

- Las operaciones que pueden realizar los administradores de redes. Tabla 5-7. (aquellas que están habilitados a realizar como tarea habitual).

- La codificación de los eventos. Apartado 8.1 Producción de las Reglas de Decisión. Tabla 5-1. Codificación de eventos.

- La codificación de los días y horarios. Apartado 8.1 Producción de las Reglas de Decisión. Tabla 5-3. Codificación de Días y Horarios.

- La codificación de los usuarios administradores. Apartado 8.1 Producción de las Reglas de Decisión. Tabla 5-2. Codificación de usuarios.

- El extracto del archivo de salida de las observaciones rojas. Figura 5-13.

HABILITACION OFICIAL DE TAREAS				
ALTAS				
	HORARIO NORMAL	DIA NO LABORAL	HORARIO NO LABORAL	DIA Y HORARIO NO LABORAL
ADMIN1	SI	SI	SI	SI
ADMIN2	SI	SI	SI	NO
ADMIN3	SI	NO	NO	NO
ADMIN4	SI	NO	NO	NO
ADMIN5	SI	NO	NO	NO
ADMIN6	NO	SI	SI	SI
BAJAS				
ADMIN1	SI	SI	SI	SI
ADMIN2	SI	SI	SI	SI
ADMIN3	SI	NO	NO	NO
ADMIN4	NO	NO	NO	NO
ADMIN5	NO	NO	NO	NO
ADMIN6	SI	SI	SI	SI

HABILITACION OFICIAL DE TAREAS				
MODIFICACIONES				
ADMIN1	SI	SI	SI	SI
ADMIN2	SI	SI	SI	SI
ADMIN3	SI	NO	NO	NO
ADMIN4	SI	NO	NO	NO
ADMIN5	SI	NO	NO	NO
ADMIN6	SI	SI	SI	SI

Tabla 5-7. Caso de Estudio 1: Operaciones que pueden realizar los administradores de redes.

```
 ------------------------------------------------
 COMIENZO EJECUCION:  2/14/2008 10:23:39AM
 ------------------------------------------------

ID:  2068 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2069 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2070 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2071 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2072 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2073 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2074 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2075 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2076 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2077 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2078 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2079 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2080 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2081 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2082 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2083 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2084 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2085 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2086 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2087 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2088 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2089 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2090 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2091 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2092 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2093 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2094 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2095 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2096 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2097 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2098 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2099 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2100 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2101 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2102 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2103 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2104 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2105 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2106 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2107 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2108 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2109 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2110 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2111 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2112 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2113 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2114 - Día:  1 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 13  - …
ID:  2141 - Día:  2 - Hora:  2 - Usuario:  5 - Evento:  3  - Regla 12  - …
ID:  2224 - Día:  2 - Hora:  2 - Usuario:  5 - Evento:  5  - Regla 12  - …
ID:  2483 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  8  - Regla 10  - …
ID:  2484 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  8  - Regla 10  - …
ID:  2485 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  8  - Regla 10  - …
ID:  2486 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  8  - Regla 10  - …
ID:  2487 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  8  - Regla 10  - …
ID:  2488 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  8  - Regla 10  - …
ID:  2489 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  8  - Regla 10  - …
```

```
ID:  2490 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  8  - Regla 10  - …
ID:  2491 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  8  - Regla 10  - …
ID:  2492 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  8  - Regla 10  - …
ID:  2493 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  8  - Regla 10  - …
ID:  2495 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  8  - Regla 10  - …
ID:  2496 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  8  - Regla 10  - …
ID:  2497 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  8  - Regla 10  - …
ID:  2498 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  8  - Regla 10  - …
ID:  2499 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  8  - Regla 10  - …
ID:  2500 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  8  - Regla 10  - …
ID:  2501 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  8  - Regla 10  - …
ID:  2502 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  8  - Regla 10  - …
ID:  2503 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  8  - Regla 10  - …
ID:  2504 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  8  - Regla 10  - …
ID:  2505 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  8  - Regla 10  - …
ID:  3293 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3294 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3295 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3296 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3297 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3298 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3299 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3300 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3301 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3302 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3303 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3304 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3305 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3306 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3307 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3308 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3309 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3310 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3311 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3312 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3313 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3314 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3315 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3316 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3317 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3318 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3319 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3320 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3321 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3322 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3323 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3324 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3325 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3326 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3327 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3328 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3329 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3330 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3331 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3332 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3333 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3334 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3335 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3336 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3337 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …
ID:  3338 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  9  - Regla 20  - …

 ------------------------------------------------
 FIN EJECUCION:  2/14/2008 10:24:05AM
 ------------------------------------------------
```

Figura 5-13. Caso de Estudio 1: Extracto del archivo de Salida de Observaciones Rojas.

Las observaciones con *ID 2068 a 2114* corresponden al administrador de red *Admin6*, la tarea realizada generó el *evento 3* "*User Account Enabled*" y los hizo un *Día Normal* (Lunes a Viernes) pero en *Horario No Laboral*. Si consultamos la tabla "Habilitación Oficial de Tareas", este usuario puede realizar Altas y Modificaciones en *Horario No Laboral* por lo tanto estos registros se pueden ignorar. De todos modos el sector de Seguridad y Control deberá pedir la justificación de las tareas ya que no son habituales.

Las observaciones con *ID 2141 y 2224* corresponden al administrador de red *Admin5*, las tareas realizadas generaron los *eventos 3* "*User Account Enabled*" y *5* "*User Account Disabled*" y los hizo en *Día y Horario No Laborales*. Si consultamos la tabla "Habilitación Oficial de Tareas", este usuario NO puede realizar ninguna tarea en *Días y Horarios No Laborales* por lo tanto estos registros motivan activar una alarma. El sector de Seguridad y Control deberá convocar al administrador de red que utiliza la cuenta *Admin5* para que dé las explicaciones que correspondan y actuará en consecuencia.

Las observaciones con *ID 2483 a 2505* corresponden al administrador de red *Admin1*, la tarea realizada generó el *evento 8* "*Local Group Changed*" y los hizo un *Día Normal* (Lunes a Viernes) pero en *Horario No Laboral*. Si consultamos la tabla "Habilitación Oficial de Tareas", este usuario puede realizar Modificaciones en *Horario No Laboral* por lo tanto estos registros se pueden ignorar. De todos modos el sector de Seguridad y Control deberá pedir la justificación de las tareas ya que no son habituales.

Las observaciones con *ID 3293 a 3338* corresponden al administrador de red *Admin1*, la tarea realizada generó el *evento 9* "*User Account Changed*" y los hizo un *Día Normal* (Lunes a Viernes) pero en *Horario No Laboral*. Si consultamos la tabla "Habilitación Oficial de Tareas", este usuario puede realizar Modificaciones en *Horario No Laboral* por lo tanto estos registros se pueden ignorar. De todos modos el sector de Seguridad y Control deberá pedir la justificación de las tareas ya que no son habituales.

5.3 Caso 2

Se analizarán todos los eventos de una muestra que mezcle horario laboral y no laboral pero se ensaya una experiencia particular que consiste en generar la mayoría de los eventos que no están autorizados de manera de poder calcular el porcentual de error de la aplicación.

La secuencia de pasos necesaria para llegar a cabo el Caso de Estudio es la siguiente.

1. Descargar los eventos de seguridad del servidor controlador de dominio.

2. Filtrar y guardar los registros que pertenecen a acciones realizadas por administradores de redes.

3. Normalizar los datos en base a la lógica, definida en el apartado 4.1.3.3 Construcción de Datos.

4. Preparar el archivo de entrada con los datos a procesar (figura 5-14).

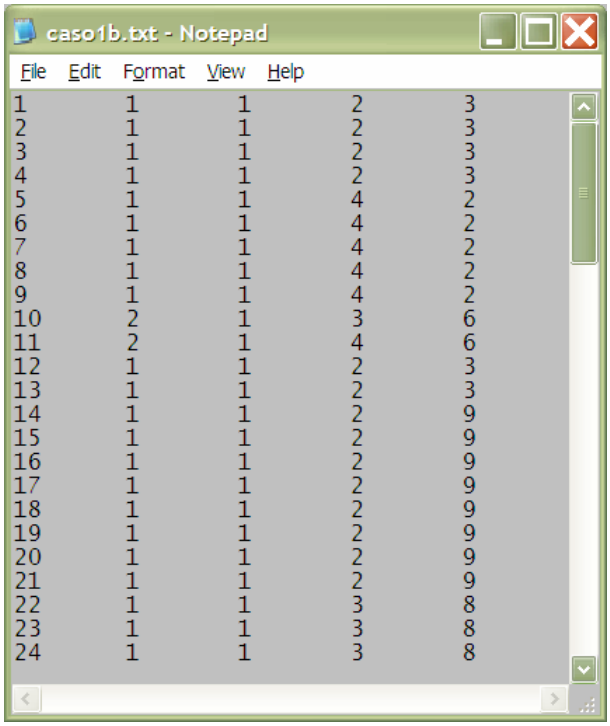


Figura 5-14. Caso de Estudio 2: Archivo de entrada con los datos a procesar.

5. En las figuras 5-15 a 5-19 se muestran las ventanas de la aplicación cuando se ejecuta el análisis de los datos.

Figura 5-15. Caso de Estudio 2: Selección del Archivo de entrada.

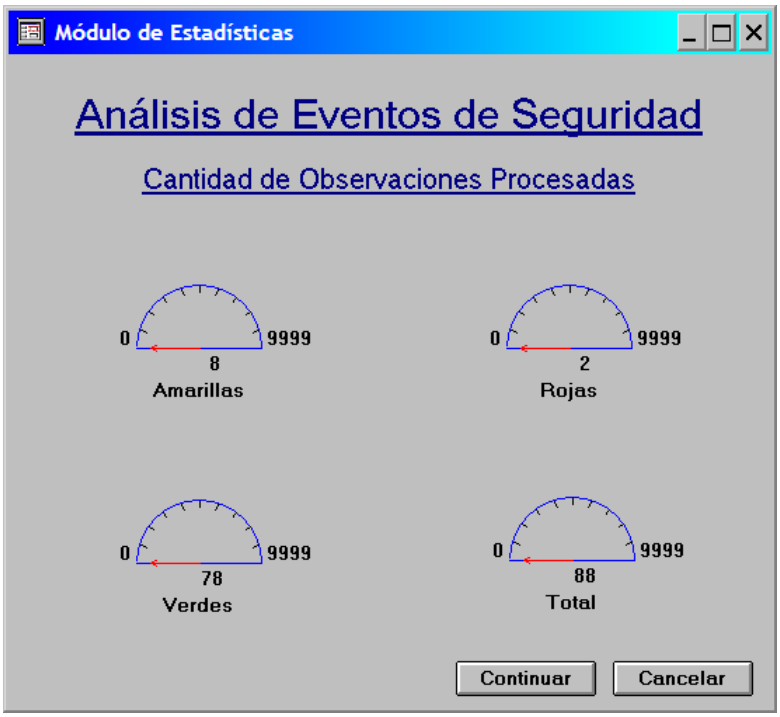


Figura 5-16. Caso de Estudio 2: Cantidad de Observaciones Analizadas por tipo.

Figura 5-17. Caso de Estudio 2: Gráfico de Secciones.

Figura 5-18. Caso de Estudio 2: Información de Observaciones Analizadas por Usuario y Tipo.

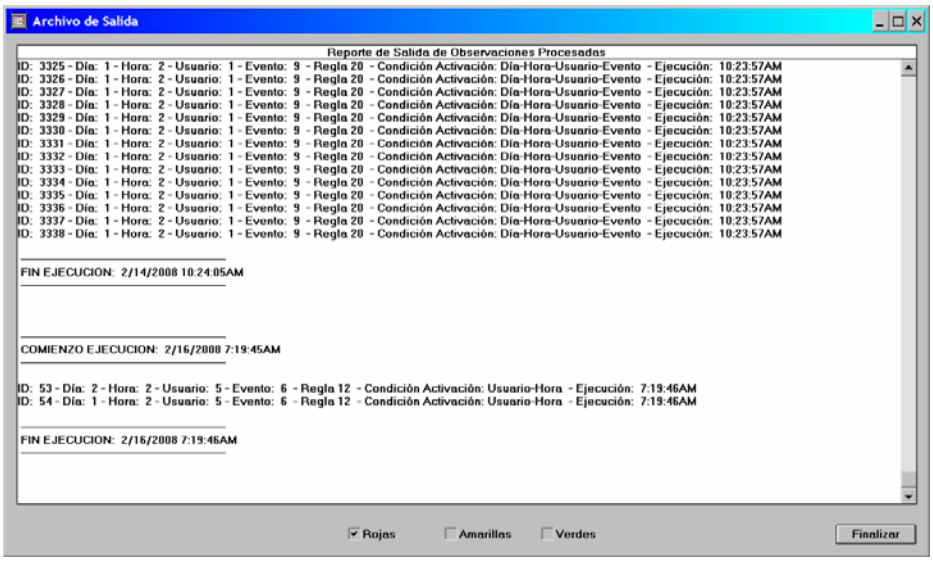


Figura 5-19. Caso de Estudio 2: Archivo de Salida de Observaciones Analizadas.

6. Analizar las estadísticas y reportes de salida.

   Se procesaron 88 observaciones. Tiempo insumido 2 segundos.

   Cantidad de Observaciones Verdes: 78 (88.6%)

   Cantidad de Observaciones Amarillas: 8 (9.1%)

   Cantidad de Observaciones Rojas: 2 (2.3%)

   Análisis de las Observaciones:

Se toma como referencia las siguientes tablas y figuras donde se muestran la información y los datos necesarios.

- Las operaciones que pueden realizar los administradores de redes. Caso 1. Tabla 5-7. (aquellas que están habilitados a realizar como tarea habitual).

- La codificación de los eventos. Apartado 8.1 Producción de las Reglas de Decisión. Tabla 5-1. Codificación de eventos.

- La codificación de los días y horarios. Apartado 8.1 Producción de las Reglas de Decisión. Tabla 5-3. Codificación de Días y Horarios.

- La codificación de los usuarios administradores. Apartado 8.1 Producción de las Reglas de Decisión. Tabla 5-2. Codificación de usuarios.

- El extracto del archivo de salida de las observaciones Rojas, Amarillas y Verdes. Figura 5-20 a 8-22.

Observaciones Rojas:

```
 ------------------------------------------------
 COMIENZO EJECUCION:  2/16/2008 7:19:45AM
 ------------------------------------------------

ID:  53 - Día:  2 - Hora:  2 - Usuario:  5 - Evento:  6  - Regla 12  - …
ID:  54 - Día:  1 - Hora:  2 - Usuario:  5 - Evento:  6  - Regla 12  - …

 ------------------------------------------------
 FIN EJECUCION:  2/16/2008 7:19:46AM
 ------------------------------------------------
```

Figura 5-20. Caso de Estudio 2: Extracto del archivo de Salida de Observaciones Rojas.

Las observaciones con *ID 53 y 54* corresponden al administrador de red *Admin5*, las tareas realizadas generaron el *evento 6* "*User Account Deleted*" y los hizo en *Día no Laboral* al primero, *Día Laboral* al segundo *y Horario No Laborales*. Si consultamos la tabla "Habilitación Oficial de Tareas", este usuario NO puede realizar la tarea mencionada en ningún caso por lo tanto estos registros motivan activar una alarma. El sector de Seguridad y Control deberá convocar al administrador de red que utiliza la cuenta *Admin5* para que dé las explicaciones que correspondan y actuará en consecuencia.

Observaciones Amarillas:

```
 ------------------------------------------------
 COMIENZO EJECUCION:  2/16/2008 7:19:45AM
 ------------------------------------------------

ID:  43 - Día:  1 - Hora:  2 - Usuario:  3 - Evento:  6  - Regla 8  - …
```

```
ID:  44 - Día:  1 - Hora:  2 - Usuario:  4 - Evento:  6  - Regla 8  - …
ID:  61 - Día:  2 - Hora:  2 - Usuario:  6 - Evento:  7  - Regla 2  - …
ID:  62 - Día:  2 - Hora:  2 - Usuario:  6 - Evento:  7  - Regla 2  - …
ID:  63 - Día:  2 - Hora:  2 - Usuario:  6 - Evento:  7  - Regla 2  - …
ID:  73 - Día:  1 - Hora:  2 - Usuario:  1 - Evento:  6  - Regla 8  - …
ID:  74 - Día:  2 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 14  - …
ID:  75 - Día:  2 - Hora:  2 - Usuario:  6 - Evento:  3  - Regla 14  - …

 ------------------------------------------------
 FIN EJECUCION:  2/16/2008 7:19:46AM
 ------------------------------------------------
```

Figura 5-21. Caso de Estudio 2: Extracto del archivo de Salida de Observaciones Amarillas.

La observación con *ID 43* corresponde al administrador de red *Admin3*, la tarea realizada generó el *evento 6* "*User Account Deleted*" y la hizo un *Día Normal* (Lunes a Viernes) en *Horario No Laboral*. Si consultamos la tabla "Habilitación Oficial de Tareas", este usuario NO puede realizar esta tarea en *Horarios No Laborales* por lo tanto este registro debe activar una alarma y notificar al sector de Seguridad y Control. Cabe aclarar que este evento tendría que haber sido clasificado como Rojo.

Para la observación con *ID 44* vale el mismo razonamiento y aclaración de la observación con *ID 43*.

Las observaciones con *ID 61 a 63* corresponden al administrador de red *Admin6*, la tarea realizada generó el *evento 6* "*Local Group Member Added*" y los hizo en *Día y Horario No Laboral*. Si consultamos la tabla "Habilitación Oficial de Tareas", este usuario puede realizar Modificaciones en *Horarios No Laborales* por lo tanto estos registros se pueden ignorar. De todos modos el sector de Seguridad y Control deberá pedir la justificación de las tareas ya que no son habituales. Es correcto que aparezcan como Amarillas.

Para la observación con *ID 73* vale el mismo razonamiento de las observaciones con *ID 61 a 63*.

Para las observaciones con *ID 74* y *75* vale el mismo razonamiento de las observaciones con *ID 61 a 63*.

Observaciones Verdes:

```
 ------------------------------------------------
 COMIENZO EJECUCION:  2/16/2008 7:19:45AM
 ------------------------------------------------

ID:  1 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  3  - Regla 1  - …
ID:  2 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  3  - Regla 1  - …
ID:  3 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  3  - Regla 1  - …
ID:  4 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  3  - Regla 1  - …
ID:  5 - Día:  1 - Hora:  1 - Usuario:  4 - Evento:  2  - Regla 1  - …
ID:  6 - Día:  1 - Hora:  1 - Usuario:  4 - Evento:  2  - Regla 1  - …
ID:  7 - Día:  1 - Hora:  1 - Usuario:  4 - Evento:  2  - Regla 1  - …
ID:  8 - Día:  1 - Hora:  1 - Usuario:  4 - Evento:  2  - Regla 1  - …
ID:  9 - Día:  1 - Hora:  1 - Usuario:  4 - Evento:  2  - Regla 1  - …
ID:  10 - Día:  2 - Hora:  1 - Usuario:  3 - Evento:  6  - Regla 1  - …
ID:  11 - Día:  2 - Hora:  1 - Usuario:  4 - Evento:  6  - Regla 1  - …
```

```
ID:  12 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  3  - Regla 1  - …
ID:  13 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  3  - Regla 1  - …
ID:  14 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  9  - Regla 1  - …
ID:  15 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  9  - Regla 1  - …
ID:  16 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  9  - Regla 1  - …
ID:  17 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  9  - Regla 1  - …
ID:  18 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  9  - Regla 1  - …
ID:  19 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  9  - Regla 1  - …
ID:  20 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  9  - Regla 1  - …
ID:  21 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  9  - Regla 1  - …
ID:  22 - Día:  1 - Hora:  1 - Usuario:  3 - Evento:  8  - Regla 1  - …
ID:  23 - Día:  1 - Hora:  1 - Usuario:  3 - Evento:  8  - Regla 1  - …
ID:  24 - Día:  1 - Hora:  1 - Usuario:  3 - Evento:  8  - Regla 1  - …
ID:  25 - Día:  1 - Hora:  1 - Usuario:  3 - Evento:  8  - Regla 1  - …
ID:  26 - Día:  1 - Hora:  1 - Usuario:  3 - Evento:  8  - Regla 1  - …
ID:  27 - Día:  1 - Hora:  1 - Usuario:  3 - Evento:  8  - Regla 1  - …
ID:  28 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  9  - Regla 1  - …
ID:  29 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  9  - Regla 1  - …
ID:  30 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  9  - Regla 1  - …
ID:  31 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  9  - Regla 1  - …
ID:  32 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  9  - Regla 1  - …
ID:  33 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  9  - Regla 1  - …
ID:  34 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  9  - Regla 1  - …
ID:  35 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  9  - Regla 1  - …
ID:  36 - Día:  1 - Hora:  1 - Usuario:  6 - Evento:  9  - Regla 1  - …
ID:  37 - Día:  1 - Hora:  1 - Usuario:  6 - Evento:  9  - Regla 1  - …
ID:  38 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  3  - Regla 1  - …
ID:  39 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  3  - Regla 1  - …
ID:  40 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  3  - Regla 1  - …
ID:  41 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  3  - Regla 1  - …
ID:  42 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  3  - Regla 1  - …
ID:  45 - Día:  1 - Hora:  1 - Usuario:  3 - Evento:  3  - Regla 1  - …
ID:  46 - Día:  1 - Hora:  1 - Usuario:  3 - Evento:  3  - Regla 1  - …
ID:  47 - Día:  1 - Hora:  1 - Usuario:  3 - Evento:  3  - Regla 1  - …
ID:  48 - Día:  1 - Hora:  1 - Usuario:  6 - Evento:  1  - Regla 1  - …
ID:  49 - Día:  1 - Hora:  1 - Usuario:  5 - Evento:  6  - Regla 1  - …
ID:  50 - Día:  1 - Hora:  1 - Usuario:  3 - Evento:  3  - Regla 1  - …
ID:  51 - Día:  1 - Hora:  1 - Usuario:  3 - Evento:  3  - Regla 1  - …
ID:  52 - Día:  1 - Hora:  1 - Usuario:  3 - Evento:  3  - Regla 1  - …
ID:  55 - Día:  2 - Hora:  1 - Usuario:  5 - Evento:  6  - Regla 1  - …
ID:  56 - Día:  1 - Hora:  1 - Usuario:  4 - Evento:  8  - Regla 1  - …
ID:  57 - Día:  1 - Hora:  1 - Usuario:  4 - Evento:  8  - Regla 1  - …
ID:  58 - Día:  1 - Hora:  1 - Usuario:  4 - Evento:  8  - Regla 1  - …
ID:  59 - Día:  2 - Hora:  1 - Usuario:  1 - Evento:  6  - Regla 1  - …
ID:  60 - Día:  2 - Hora:  1 - Usuario:  1 - Evento:  6  - Regla 1  - …
ID:  64 - Día:  1 - Hora:  1 - Usuario:  1 - Evento:  2  - Regla 1  - …
ID:  65 - Día:  1 - Hora:  1 - Usuario:  1 - Evento:  2  - Regla 1  - …
ID:  66 - Día:  1 - Hora:  1 - Usuario:  1 - Evento:  2  - Regla 1  - …
ID:  67 - Día:  1 - Hora:  1 - Usuario:  1 - Evento:  2  - Regla 1  - …
ID:  68 - Día:  1 - Hora:  1 - Usuario:  1 - Evento:  2  - Regla 1  - …
ID:  69 - Día:  2 - Hora:  1 - Usuario:  1 - Evento:  9  - Regla 1  - …
ID:  70 - Día:  2 - Hora:  1 - Usuario:  1 - Evento:  9  - Regla 1  - …
ID:  71 - Día:  2 - Hora:  1 - Usuario:  1 - Evento:  9  - Regla 1  - …
ID:  72 - Día:  2 - Hora:  1 - Usuario:  1 - Evento:  6  - Regla 1  - …
ID:  76 - Día:  2 - Hora:  1 - Usuario:  6 - Evento:  3  - Regla 1  - …
ID:  77 - Día:  2 - Hora:  1 - Usuario:  6 - Evento:  3  - Regla 1  - …
ID:  78 - Día:  2 - Hora:  1 - Usuario:  2 - Evento:  8  - Regla 1  - …
ID:  79 - Día:  2 - Hora:  1 - Usuario:  2 - Evento:  8  - Regla 1  - …
ID:  80 - Día:  2 - Hora:  1 - Usuario:  2 - Evento:  8  - Regla 1  - …
ID:  81 - Día:  2 - Hora:  1 - Usuario:  2 - Evento:  8  - Regla 1  - …
ID:  82 - Día:  2 - Hora:  1 - Usuario:  2 - Evento:  8  - Regla 1  - …
ID:  83 - Día:  1 - Hora:  1 - Usuario:  3 - Evento:  3  - Regla 1  - …
ID:  84 - Día:  1 - Hora:  1 - Usuario:  3 - Evento:  3  - Regla 1  - …
ID:  85 - Día:  1 - Hora:  1 - Usuario:  3 - Evento:  3  - Regla 1  - …
ID:  86 - Día:  1 - Hora:  1 - Usuario:  3 - Evento:  3  - Regla 1  - …
ID:  87 - Día:  1 - Hora:  1 - Usuario:  3 - Evento:  3  - Regla 1  - …
ID:  88 - Día:  1 - Hora:  1 - Usuario:  3 - Evento:  3  - Regla 1  - …

 ---------------------------------------------------
 FIN EJECUCION:  2/16/2008 7:19:46AM
 ---------------------------------------------------
```

Figura 5-22. Caso de Estudio 2: Extracto del archivo de Salida de Observaciones Verdes.

Al observar cada registro, se puede concluir a simple vista que todas las observaciones con *Hora = 1* (Normal) fueron clasificadas como verdes, sin importar el resto de los atributos. Este es un error de la aplicación que generaliza los eventos.

5.4 Caso 3

Se analizarán eventos de una muestra que contenga registros de un administrador de sistemas que no fue considerado durante el entrenamiento de la red neuronal. El usuario en cuestión aparece con la codificación número 7.

La secuencia de pasos necesaria para llegar a cabo el Caso de Estudio es la siguiente.

1. Descargar los eventos de seguridad del servidor controlador de dominio.

2. Filtrar y guardar los registros que pertenecen a acciones realizadas por administradores de redes.

3. Normalizar los datos en base a la lógica, definida en el apartado 4.1.3.3 Construcción de Datos.

4. Preparar el archivo de entrada con los datos a procesar (Figura 5-23).

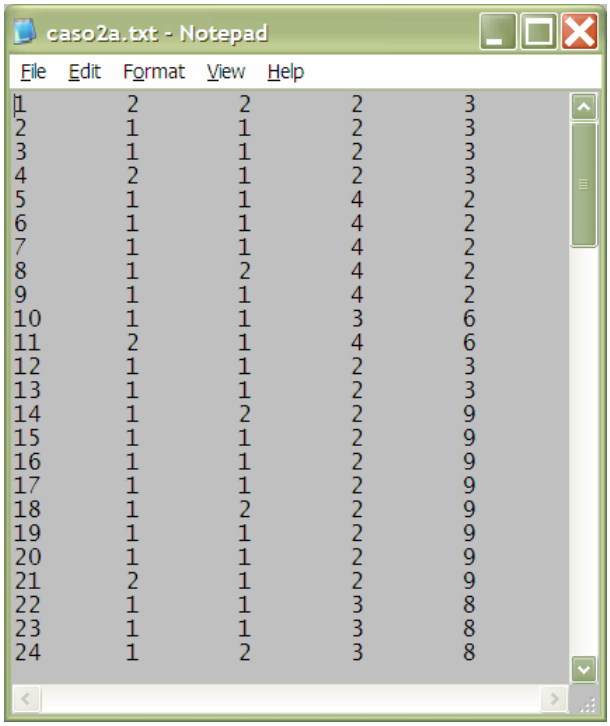


Figura 5-23. Caso de Estudio 3: Archivo de entrada con los datos a procesar.

5. En las figuras 5-24 a 5-26 se muestran las ventanas de la aplicación cuando se ejecuta el análisis de los datos.

Figura 5-24. Caso de Estudio 3: Selección del Archivo de entrada.

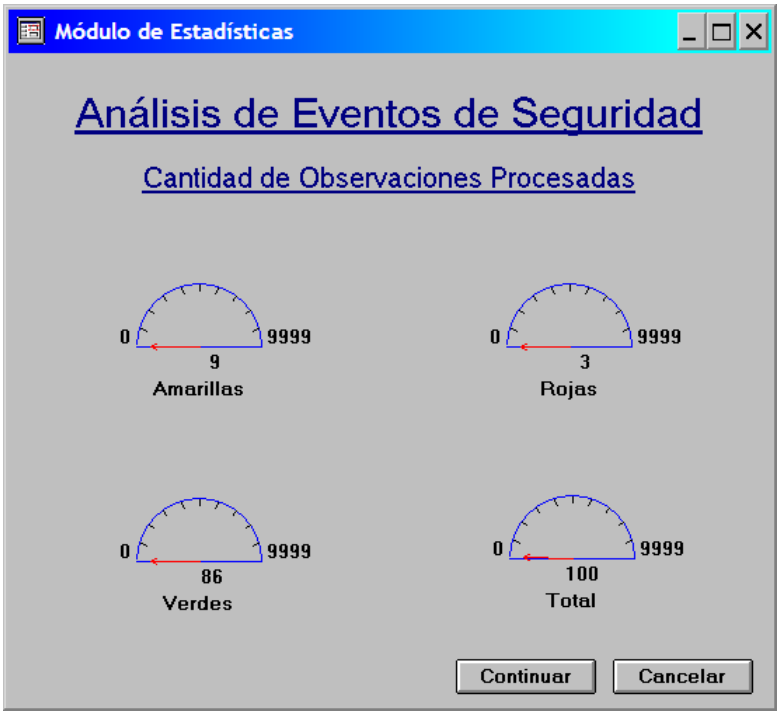


Figura 5-25. Caso de Estudio 3: Cantidad de Observaciones Analizadas por tipo.

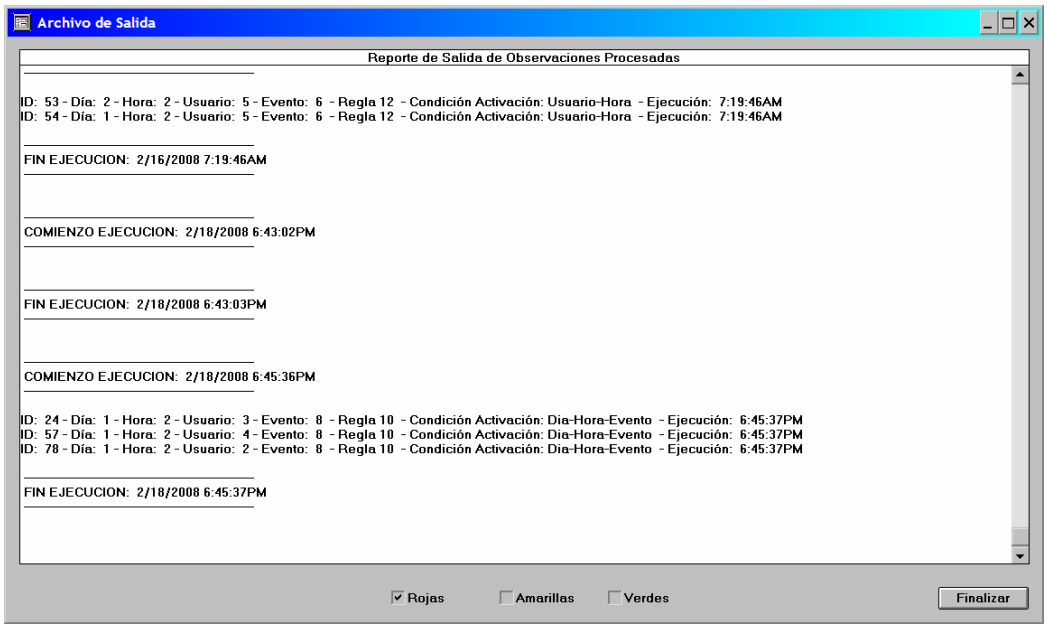


Figura 5-26. Caso de Estudio 3: Archivo de Salida de Observaciones Analizadas.

6. Analizar las estadísticas y reportes de salida.

   Se procesaron 100 observaciones. Tiempo insumido 2 segundos.

   Cantidad de Observaciones Verdes: 86 (86%)

   Cantidad de Observaciones Amarillas: 9 (9%)

   Cantidad de Observaciones Rojas: 3 (3%)

   Cantidad de Observaciones Sin Procesar: 2 (2%)

   Análisis de las Observaciones:

   Se toma como referencia las siguientes tablas y figuras donde se muestran la información y los datos necesarios.

   - Las operaciones que pueden realizar los administradores de redes. Caso 1. Tabla 5-7. (aquellas que están habilitados a realizar como tarea habitual).

   - La codificación de los eventos. Apartado 8.1 Producción de las Reglas de Decisión. Tabla 5-1. Codificación de eventos.

   - La codificación de los días y horarios. Apartado 8.1 Producción de las Reglas de Decisión. Tabla 5-3. Codificación de Días y Horarios.

- La codificación de los usuarios administradores. Apartado 8.1 Producción de las Reglas de Decisión. Tabla 5-2. Codificación de usuarios.

- El extracto del archivo de salida de las observaciones Rojas, Amarillas y Verdes. Figura 5-27 a 8-29.

Observaciones Rojas:

```
 ------------------------------------------------
 COMIENZO EJECUCION:  2/18/2008 6:45:36PM
 ------------------------------------------------

ID:  24 - Día:  1 - Hora:  2 - Usuario:  3 - Evento:  8  - Regla 10  …
ID:  57 - Día:  1 - Hora:  2 - Usuario:  4 - Evento:  8  - Regla 10  …
ID:  78 - Día:  1 - Hora:  2 - Usuario:  2 - Evento:  8  - Regla 10  …
 ------------------------------------------------
 FIN EJECUCION:  2/18/2008 6:45:37PM
 ------------------------------------------------
```

Figura 5-27. Caso de Estudio 3: Extracto del archivo de Salida de Observaciones Rojas.

Las observaciones con *ID 24 y 57* fueron bien clasificadas.

La observación con *ID 78* no fue correctamente clasificada, corresponde a Verdes, el sector de Seguridad y Control deberá ignorarla.

No aparecen registros del Usuario con *ID 7*.

Observaciones Amarillas:

```
 ------------------------------------------------
 COMIENZO EJECUCION:  2/18/2008 6:45:36PM
 ------------------------------------------------

ID:  1 - Día:  2 - Hora:  2 - Usuario:  2 - Evento:  3  - Regla 5  …
ID:  8 - Día:  1 - Hora:  2 - Usuario:  4 - Evento:  2  - Regla 3  …
ID:  14 - Día:  1 - Hora:  2 - Usuario:  2 - Evento:  9  - Regla 11  …
ID:  18 - Día:  1 - Hora:  2 - Usuario:  2 - Evento:  9  - Regla 11  …
ID:  30 - Día:  1 - Hora:  2 - Usuario:  2 - Evento:  9  - Regla 11  …
ID:  62 - Día:  2 - Hora:  2 - Usuario:  6 - Evento:  7  - Regla 2  …
ID:  68 - Día:  2 - Hora:  2 - Usuario:  1 - Evento:  2  - Regla 3  …
ID:  97 - Día:  2 - Hora:  2 - Usuario:  7 - Evento:  9  - Regla 21 - Condición
Activación: Día-Hora-Evento …
ID:  100 - Día:  2 - Hora:  2 - Usuario:  7 - Evento:  3  - Regla 7 - Condición
Activación: Día-Hora …

 ------------------------------------------------
 FIN EJECUCION:  2/18/2008 6:45:37PM
 ------------------------------------------------
```

Figura 5-28. Caso de Estudio 3: Extracto del archivo de Salida de Observaciones Amarillas.

Las observaciones fueron bien clasificadas.

Aparecen registros del Usuario con *ID 7*, pero la condición de activación de la regla fueron otros atributos.

Observaciones Verdes:

```
------------------------------------------------
 COMIENZO EJECUCION:  2/18/2008 6:45:36PM
 ------------------------------------------------
```

```
ID:  2 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  3  - Regla 1  …
ID:  3 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  3  - Regla 1  …
ID:  4 - Día:  2 - Hora:  1 - Usuario:  2 - Evento:  3  - Regla 1  …
ID:  5 - Día:  1 - Hora:  1 - Usuario:  4 - Evento:  2  - Regla 1  …
ID:  6 - Día:  1 - Hora:  1 - Usuario:  4 - Evento:  2  - Regla 1  …
ID:  7 - Día:  1 - Hora:  1 - Usuario:  4 - Evento:  2  - Regla 1  …
ID:  9 - Día:  1 - Hora:  1 - Usuario:  4 - Evento:  2  - Regla 1  …
ID:  10 - Día:  1 - Hora:  1 - Usuario:  3 - Evento:  6  - Regla 1  …
ID:  11 - Día:  2 - Hora:  1 - Usuario:  4 - Evento:  6  - Regla 1  …
ID:  12 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  3  - Regla 1  …
ID:  13 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  3  - Regla 1  …
ID:  15 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  9  - Regla 1  …
ID:  16 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  9  - Regla 1  …
ID:  17 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  9  - Regla 1  …
ID:  19 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  9  - Regla 1  …
ID:  20 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  9  - Regla 1  …
ID:  21 - Día:  2 - Hora:  1 - Usuario:  2 - Evento:  9  - Regla 1  …
ID:  22 - Día:  1 - Hora:  1 - Usuario:  3 - Evento:  8  - Regla 1  …
ID:  23 - Día:  1 - Hora:  1 - Usuario:  3 - Evento:  8  - Regla 1  …
ID:  25 - Día:  1 - Hora:  1 - Usuario:  3 - Evento:  8  - Regla 1  …
ID:  26 - Día:  1 - Hora:  1 - Usuario:  3 - Evento:  8  - Regla 1  …
ID:  27 - Día:  2 - Hora:  1 - Usuario:  3 - Evento:  8  - Regla 1  …
ID:  28 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  9  - Regla 1  …
ID:  29 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  9  - Regla 1  …
ID:  31 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  9  - Regla 1  …
ID:  32 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  9  - Regla 1  …
ID:  33 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  9  - Regla 1  …
ID:  34 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  9  - Regla 1  …
ID:  35 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  9  - Regla 1  …
ID:  36 - Día:  1 - Hora:  1 - Usuario:  6 - Evento:  9  - Regla 1  …
ID:  37 - Día:  1 - Hora:  1 - Usuario:  6 - Evento:  9  - Regla 1  …
ID:  38 - Día:  2 - Hora:  1 - Usuario:  2 - Evento:  3  - Regla 1  …
ID:  39 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  3  - Regla 1  …
ID:  40 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  3  - Regla 1  …
ID:  41 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  3  - Regla 1  …
ID:  42 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  3  - Regla 1  …
ID:  43 - Día:  1 - Hora:  1 - Usuario:  3 - Evento:  6  - Regla 1  …
ID:  44 - Día:  1 - Hora:  1 - Usuario:  4 - Evento:  6  - Regla 1  …
ID:  46 - Día:  1 - Hora:  1 - Usuario:  3 - Evento:  3  - Regla 1  …
ID:  47 - Día:  1 - Hora:  1 - Usuario:  3 - Evento:  3  - Regla 1  …
ID:  48 - Día:  2 - Hora:  1 - Usuario:  6 - Evento:  1  - Regla 1  …
ID:  49 - Día:  1 - Hora:  1 - Usuario:  5 - Evento:  6  - Regla 1  …
ID:  50 - Día:  1 - Hora:  1 - Usuario:  3 - Evento:  3  - Regla 1  …
ID:  51 - Día:  1 - Hora:  1 - Usuario:  3 - Evento:  3  - Regla 1  …
ID:  52 - Día:  1 - Hora:  1 - Usuario:  3 - Evento:  3  - Regla 1  …
ID:  53 - Día:  1 - Hora:  1 - Usuario:  5 - Evento:  6  - Regla 1  …
ID:  54 - Día:  2 - Hora:  1 - Usuario:  5 - Evento:  6  - Regla 1  …
ID:  55 - Día:  1 - Hora:  1 - Usuario:  5 - Evento:  6  - Regla 1  …
ID:  56 - Día:  1 - Hora:  1 - Usuario:  4 - Evento:  8  - Regla 1  …
ID:  58 - Día:  1 - Hora:  1 - Usuario:  4 - Evento:  8  - Regla 1  …
ID:  59 - Día:  1 - Hora:  1 - Usuario:  1 - Evento:  6  - Regla 1  …
ID:  60 - Día:  1 - Hora:  1 - Usuario:  1 - Evento:  6  - Regla 1  …
ID:  61 - Día:  1 - Hora:  1 - Usuario:  6 - Evento:  7  - Regla 1  …
ID:  63 - Día:  1 - Hora:  1 - Usuario:  6 - Evento:  7  - Regla 1  …
ID:  64 - Día:  1 - Hora:  1 - Usuario:  1 - Evento:  2  - Regla 1  …
ID:  65 - Día:  1 - Hora:  1 - Usuario:  1 - Evento:  2  - Regla 1  …
ID:  66 - Día:  2 - Hora:  1 - Usuario:  1 - Evento:  2  - Regla 1  …
ID:  67 - Día:  1 - Hora:  1 - Usuario:  1 - Evento:  2  - Regla 1  …
ID:  69 - Día:  1 - Hora:  1 - Usuario:  1 - Evento:  9  - Regla 1  …
ID:  70 - Día:  1 - Hora:  1 - Usuario:  1 - Evento:  9  - Regla 1  …
ID:  71 - Día:  1 - Hora:  1 - Usuario:  1 - Evento:  9  - Regla 1  …
ID:  72 - Día:  1 - Hora:  1 - Usuario:  1 - Evento:  6  - Regla 1  …
ID:  73 - Día:  1 - Hora:  1 - Usuario:  1 - Evento:  6  - Regla 1  …
ID:  74 - Día:  2 - Hora:  1 - Usuario:  6 - Evento:  3  - Regla 1  …
ID:  75 - Día:  1 - Hora:  1 - Usuario:  6 - Evento:  3  - Regla 1  …
ID:  76 - Día:  1 - Hora:  1 - Usuario:  6 - Evento:  3  - Regla 1  …
ID:  77 - Día:  1 - Hora:  1 - Usuario:  6 - Evento:  3  - Regla 1  …
ID:  79 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  8  - Regla 1  …
ID:  80 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  8  - Regla 1  …
ID:  81 - Día:  2 - Hora:  1 - Usuario:  2 - Evento:  8  - Regla 1  …
ID:  82 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  8  - Regla 1  …
ID:  83 - Día:  1 - Hora:  1 - Usuario:  3 - Evento:  3  - Regla 1  …
ID:  84 - Día:  1 - Hora:  1 - Usuario:  3 - Evento:  3  - Regla 1  …
ID:  85 - Día:  1 - Hora:  1 - Usuario:  3 - Evento:  3  - Regla 1  …
ID:  86 - Día:  1 - Hora:  1 - Usuario:  3 - Evento:  3  - Regla 1  …
ID:  87 - Día:  2 - Hora:  1 - Usuario:  3 - Evento:  3  - Regla 1  …
ID:  89 - Día:  1 - Hora:  1 - Usuario:  7 - Evento:  1  - Regla 1  …
ID:  90 - Día:  1 - Hora:  1 - Usuario:  7 - Evento:  2  - Regla 1  …
ID:  91 - Día:  1 - Hora:  1 - Usuario:  7 - Evento:  3  - Regla 1  …
ID:  92 - Día:  1 - Hora:  1 - Usuario:  7 - Evento:  4  - Regla 1  …
ID:  93 - Día:  1 - Hora:  1 - Usuario:  7 - Evento:  5  - Regla 1  …
ID:  94 - Día:  1 - Hora:  1 - Usuario:  7 - Evento:  6  - Regla 1  …
ID:  95 - Día:  1 - Hora:  1 - Usuario:  7 - Evento:  7  - Regla 1  …
ID:  96 - Día:  1 - Hora:  1 - Usuario:  7 - Evento:  8  - Regla 1  - Condición
Activación: Hora  -…
ID:  98 - Día:  1 - Hora:  1 - Usuario:  7 - Evento:  1  - Regla 1  …
```

```
ID:  99 - Día:  1 - Hora:  1 - Usuario:  7 - Evento:  2  - Regla 1  - Condición
Activación: Hora  -…

 ------------------------------------------------
 FIN EJECUCION:  2/18/2008 6:45:37PM
 ------------------------------------------------
```

Figura 5-29. Caso de Estudio 3: Extracto del archivo de Salida de Observaciones Verdes.

Todas las observaciones con *Hora = 1* (Normal) fueron clasificadas como verdes, sin importar el resto de los atributos. Este es un error de la aplicación que generaliza los eventos.

Aparecen registros del Usuario con *ID 7*, pero la condición de activación de la regla fueron otros atributos.

5.5 Caso 4

Se analizarán eventos de una muestra que contenga registros de eventos que no fueron estimados durante el entrenamiento de la red neuronal. Los eventos en cuestión aparecen con la codificación número 10, 11 y 12.

La secuencia de pasos necesaria para llegar a cabo el Caso de Estudio es la siguiente.

1. Descargar los eventos de seguridad del servidor controlador de dominio.
2. Filtrar y guardar los registros que pertenecen a acciones realizadas por administradores de redes.
3. Normalizar los datos en base a la lógica, definida en el apartado 4.1.3.3 Construcción de Datos.
4. Preparar el archivo de entrada con los datos a procesar (Figura 5-30).

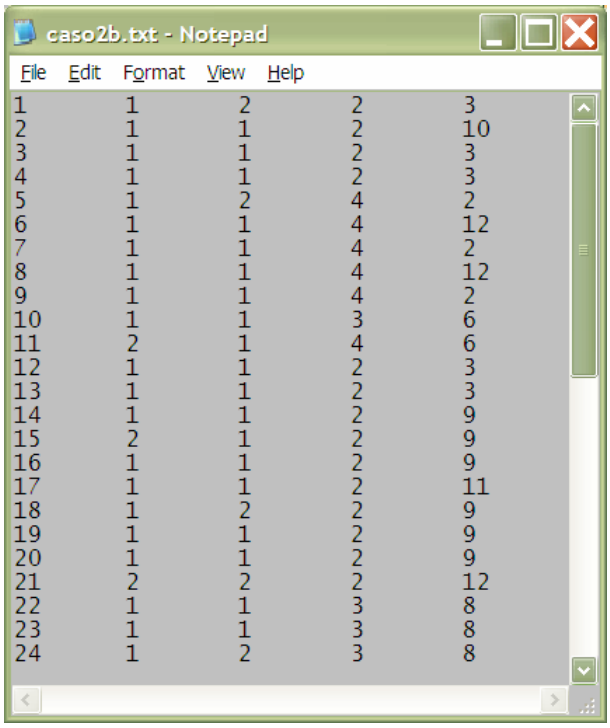


Figura 5-30. Caso de Estudio 4: Archivo de entrada con los datos a procesar.

5. En las figuras 5-31 a 5-34 se muestran las ventanas de la aplicación cuando se ejecuta el análisis de los datos.

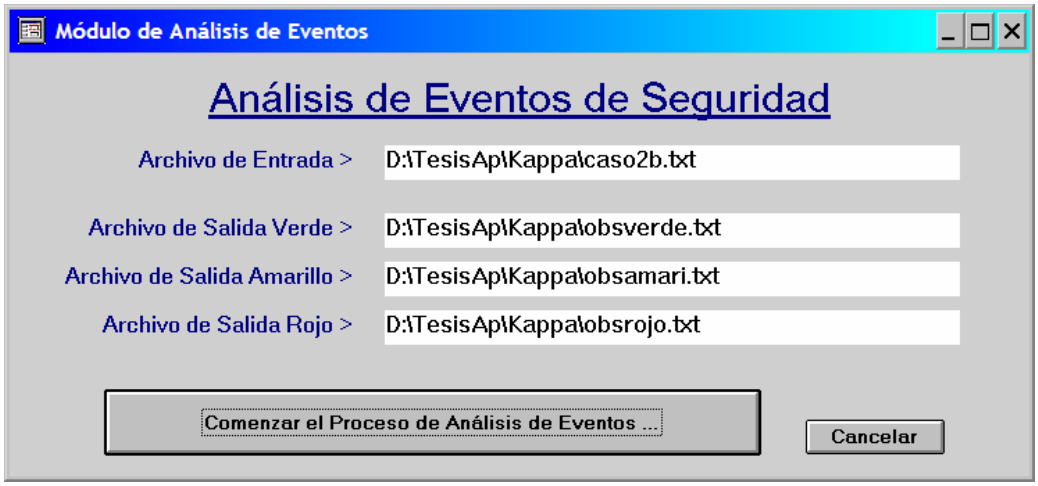


Figura 5-31. Caso de Estudio 4: Selección del Archivo de entrada.

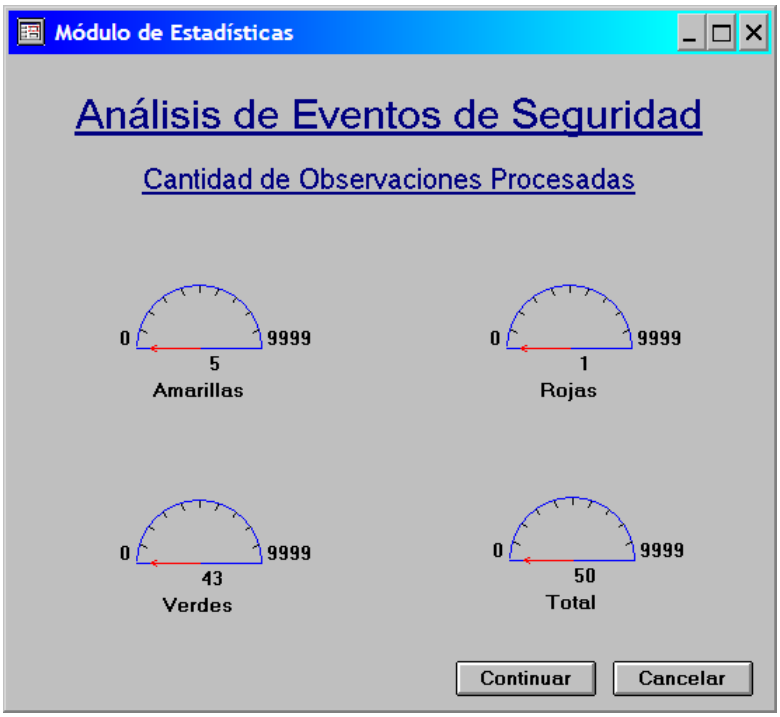


Figura 5-32. Caso de Estudio 4: Cantidad de Observaciones Analizadas por tipo.

Figura 5-33. Caso de Estudio 4: Gráfico de Secciones.

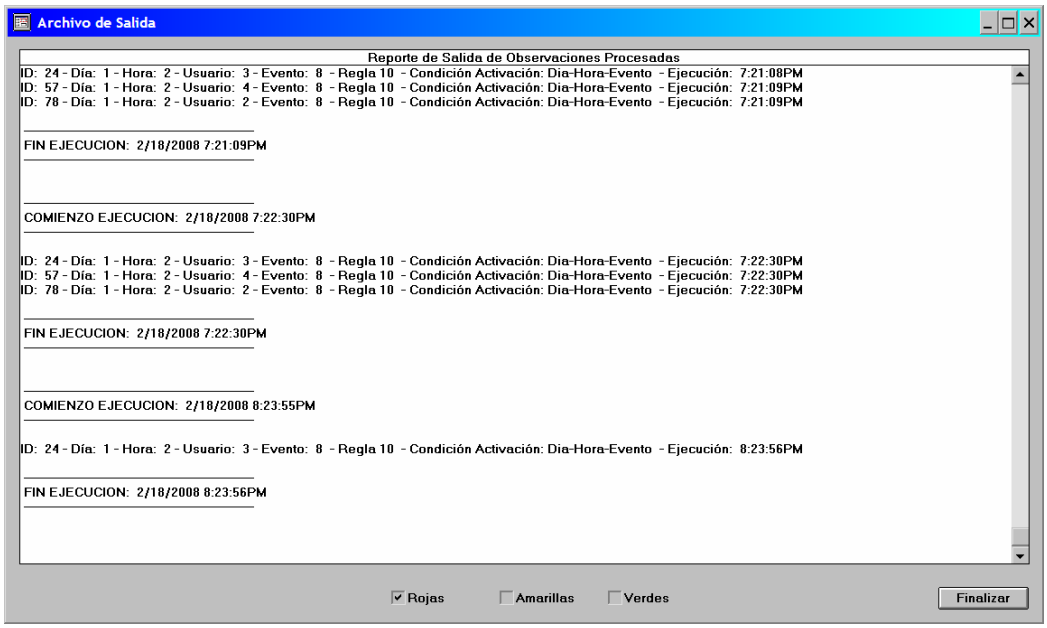


Figura 5-34. Caso de Estudio 4: Archivo de Salida de Observaciones Analizadas.

6. Analizar las estadísticas y reportes de salida.

   Se procesaron 50 observaciones. Tiempo insumido 1 segundos.

   Cantidad de Observaciones Verdes: 43 (86%)

   Cantidad de Observaciones Amarillas: 5 (10%)

   Cantidad de Observaciones Rojas: 1 (2%)

   Cantidad de Observaciones Perdidas: 1 (2%)

   Análisis de las Observaciones:

   Se toma como referencia las siguientes tablas y figuras donde se muestran la información y los datos necesarios.

   - Las operaciones que pueden realizar los administradores de redes. Caso 1. Tabla 5-7. (aquellas que están habilitados a realizar como tarea habitual).

   - La codificación de los eventos. Apartado 8.1 Producción de las Reglas de Decisión. Tabla 5-1. Codificación de eventos.

   - La codificación de los días y horarios. Apartado 8.1 Producción de las Reglas de Decisión. Tabla 5-3. Codificación de Días y Horarios.

- La codificación de los usuarios administradores. Apartado 8.1 Producción de las Reglas de Decisión. Tabla 5-2. Codificación de usuarios.

- El extracto del archivo de salida de las observaciones Rojas, Amarillas y Verdes. Figura 5-35 a 8-37.

Observaciones Rojas:

```
-------------------------------------------------
 COMIENZO EJECUCION:  2/18/2008 8:23:55PM
 -------------------------------------------------

ID:  24 - Día:  1 - Hora:  2 - Usuario:  3 - Evento:  8  - Regla 10  …

 -------------------------------------------------
 FIN EJECUCION:  2/18/2008 8:23:56PM
 -------------------------------------------------
```

Figura 5-35. Caso de Estudio 4: Extracto del archivo de Salida de Observaciones Rojas.

La observación con *ID 24* fue bien clasificada.

No aparecen registros de Eventos con *ID 10, 11 o 12*.

Observaciones Amarillas:

```
-------------------------------------------------
 COMIENZO EJECUCION:  2/18/2008 8:23:55PM
 -------------------------------------------------

ID:  1 - Día:  1 - Hora:  2 - Usuario:  2 - Evento:  3  - Regla 5  …
ID:  5 - Día:  1 - Hora:  2 - Usuario:  4 - Evento:  2  - Regla 3  …
ID:  18 - Día:  1 - Hora:  2 - Usuario:  2 - Evento:  9  - Regla 11  …
ID:  21 - Día:  2 - Hora:  2 - Usuario:  2 - Evento:  12  - Regla 7  - Condición
Activación: Día-Hora …
ID:  30 - Día:  1 - Hora:  2 - Usuario:  2 - Evento:  9  - Regla 11  …

 -------------------------------------------------
 FIN EJECUCION:  2/18/2008 8:23:56PM
 -------------------------------------------------
```

Figura 5-36. Caso de Estudio 4: Extracto del archivo de Salida de Observaciones Amarillas.

Las observaciones fueron bien clasificadas.

Aparecen un registro de un Evento con *ID 12*, pero la condición de activación de la regla fueron otros atributos.

Observaciones Verdes:

```
-------------------------------------------------
 COMIENZO EJECUCION:  2/18/2008 8:23:55PM
 -------------------------------------------------

ID:  2 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  10  - Regla 1  …
ID:  3 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  3  - Regla 1  …
ID:  4 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  3  - Regla 1  …
ID:  6 - Día:  1 - Hora:  1 - Usuario:  4 - Evento:  12  - Regla 1  …
ID:  7 - Día:  1 - Hora:  1 - Usuario:  4 - Evento:  2  - Regla 1  …
ID:  8 - Día:  1 - Hora:  1 - Usuario:  4 - Evento:  12  - Regla 1  …
ID:  9 - Día:  1 - Hora:  1 - Usuario:  4 - Evento:  2  - Regla 1  …
ID:  10 - Día:  1 - Hora:  1 - Usuario:  3 - Evento:  6  - Regla 1  …
ID:  11 - Día:  2 - Hora:  1 - Usuario:  4 - Evento:  6  - Regla 1  …
ID:  12 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  3  - Regla 1  …
ID:  13 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  3  - Regla 1  …
```

```
ID:  14 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  9  - Regla 1  …
ID:  15 - Día:  2 - Hora:  1 - Usuario:  2 - Evento:  9  - Regla 1  …
ID:  16 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  9  - Regla 1  …
ID:  17 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  11  - Regla 1  - Condición
Activación: Hora  -…
ID:  19 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  9  - Regla 1  …
ID:  20 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  9  - Regla 1  …
ID:  22 - Día:  1 - Hora:  1 - Usuario:  3 - Evento:  8  - Regla 1  …
ID:  23 - Día:  1 - Hora:  1 - Usuario:  3 - Evento:  8  - Regla 1  …
ID:  25 - Día:  1 - Hora:  1 - Usuario:  3 - Evento:  8  - Regla 1  …
ID:  26 - Día:  1 - Hora:  1 - Usuario:  3 - Evento:  8  - Regla 1  …
ID:  27 - Día:  2 - Hora:  1 - Usuario:  3 - Evento:  8  - Regla 1  …
ID:  28 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  9  - Regla 1  …
ID:  29 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  9  - Regla 1  …
ID:  31 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  9  - Regla 1  …
ID:  32 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  9  - Regla 1  …
ID:  33 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  10  - Regla 1  …
ID:  34 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  9  - Regla 1  …
ID:  35 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  9  - Regla 1  …
ID:  36 - Día:  1 - Hora:  1 - Usuario:  6 - Evento:  9  - Regla 1  …
ID:  37 - Día:  1 - Hora:  1 - Usuario:  6 - Evento:  9  - Regla 1  …
ID:  38 - Día:  2 - Hora:  1 - Usuario:  2 - Evento:  11  - Regla 1  …
ID:  39 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  3  - Regla 1  …
ID:  40 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  3  - Regla 1  …
ID:  41 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  3  - Regla 1  …
ID:  42 - Día:  1 - Hora:  1 - Usuario:  2 - Evento:  3  - Regla 1  …
ID:  43 - Día:  1 - Hora:  1 - Usuario:  3 - Evento:  6  - Regla 1  …
ID:  44 - Día:  1 - Hora:  1 - Usuario:  4 - Evento:  6  - Regla 1  …
ID:  46 - Día:  1 - Hora:  1 - Usuario:  3 - Evento:  3  - Regla 1  …
ID:  47 - Día:  1 - Hora:  1 - Usuario:  3 - Evento:  3  - Regla 1  …
ID:  48 - Día:  2 - Hora:  1 - Usuario:  6 - Evento:  11  - Regla 1  - Condición
Activación: Hora  -…
ID:  49 - Día:  1 - Hora:  1 - Usuario:  5 - Evento:  6  - Regla 1  …
ID:  50 - Día:  1 - Hora:  1 - Usuario:  3 - Evento:  12  - Regla 1  …

 ------------------------------------------------
 FIN EJECUCION:  2/18/2008 8:23:56PM
 ------------------------------------------------
```

Figura 5-37. Caso de Estudio 4: Extracto del archivo de Salida de Observaciones Verdes.

Aparecen registros de Eventos con *ID 10, 11 y 12*, pero la condición de activación de la regla fueron otros atributos.

5.6 Conclusiones del Estudio de Casos

La aplicación reduce el análisis en detalle al 2,3% (en promedio) del total de registros y a una revisión menos detallada al 11,75% (en promedio) del total.

Contrae el tiempo insumido en la tarea en un 75%. Sin este sistema 8 horas, utilizando el mismo, solo 2 horas.

Se logra una reducción de los costos y recursos necesarios para llevar a cabo el análisis. Lo cual, es un gran incentivo para que la gerencia promueva la auditoria de los eventos de seguridad y no los ignorare.

El hecho de detectar tareas administrativas no autorizadas y poder aplicar acciones correctivas veloz y ágilmente, incrementa la confianza y seguridad en los sistemas de información del negocio.

En el peor de los casos la aplicación arrojará error del 18.9% (menor al definido en la etapa de análisis, 30%).

Detalle de las conclusiones de cada Caso de Estudio:

Caso 1

Permitió detectar dos tareas administrativas no autorizadas de forma rápida y sencilla dentro de una muestra de 4846 registros.

Permitió detectar varias tareas que si bien están autorizadas fueron realizadas en horario no laboral y deben ser justificadas.

Caso 2

Permitió detectar cuatro tareas administrativas no autorizadas de forma rápida y sencilla dentro de una muestra de 88 registros. Dos fueron clasificadas con Rojas y las otras como Amarillas.

Permitió detectar varias tareas que si bien están autorizadas fueron realizadas en horario no laboral y deben ser justificadas.

Todas las observaciones con *Hora = 1* (Normal) fueron clasificadas como verdes, sin importar el resto de los atributos. Este es un error de la aplicación que generaliza los eventos. Observando la Tabla 5-7. (aquellas que están habilitados a realizar como tarea habitual), la aplicación clasificará incorrectamente las operaciones realizadas en *hora = 1 y día = 2* para el caso de los administradores con *ID 3, 4 y 5*.

Caso 3

La aplicación dejó sin procesar 2 observaciones. Se debe a registros generados por el administrador con ID 7. El comportamiento es esperado porque este tipo de acciones no fueron consideradas durante el entrenamiento de la red y producción de reglas de decisión. Otras observaciones, generadas por este mismo ID de usuario, fueron clasificadas pero la condición de activación de la regla fueron otros atributos distintos al ID de usuario. Para mitigar esta conducta, se instruye a los usuarios del sistema desarrollado en el presente trabajo de tesis que será mandatorio volver a entrenar la aplicación cuando cambian los administradores de red; cabe mencionar que éste es un hecho poco frecuente.

El sistema no genera el gráfico de secciones porque no coinciden los valores de las observaciones clasificadas con el total de las mismas.

Caso 4

La aplicación dejó sin procesar 1 observación. Tuvo el mismo comportamiento que en el Caso de Estudio anterior.

Para mitigar esta conducta, se determina que será mandatorio volver a entrenar la aplicación desarrollada en el presente trabajo de tesis cuando cambian las operaciones y tareas realizadas por los administradores de red. De todos modos este hecho es poco frecuente.

Análisis de Error

A continuación se realiza un análisis detallado de error de cada regla tomando como referencia la Tabla 5-7. (Operaciones que pueden realizar los administradores de redes).

Regla	Condición	Error
Rule1	IF hora = 1 THEN Clasificacion = verde	Error = 4.2% en el peor de los casos. (9 operaciones) / (6 usuarios x 4 horarios x 9 operaciones de ABM) * 100
Rule2	IF { evento = 1 OR evento = 7 } AND hora = 2 THEN Clasificacion = amarillo	Error = 1.4% en el peor de los casos. (3 operaciones) / (6 usuarios x 4 horarios x 9 operaciones de ABM) * 100
Rule3	IF evento = 2 AND hora = 2 THEN Clasificacion = amarillo	Error = 1.4% en el peor de los casos. (3 operaciones) / (6 usuarios x 4 horarios x 9 operaciones de ABM) * 100
Rule4	IF evento = 3 AND hora = 2 AND user = 1 THEN Clasificacion = amarillo	Error = 0%
Rule5	IF evento = 3 AND hora = 2 AND user = 2 THEN Clasificacion = amarillo	Error = 0%
Rule6	IF día = 1 AND evento = 4 AND hora = 2 THEN Clasificacion = rojo	Error = 1.4% en el peor de los casos. (3 operaciones) / (6 usuarios x 4 horarios x 9 operaciones de ABM) * 100
Rule7	IF día = 2 AND hora = 2 THEN Clasificacion = amarillo	Error = 3.2% en el peor de los casos. (7 operaciones) / (6 usuarios x 4 horarios x 9 operaciones de ABM) * 100
Rule8	IF evento = 6 AND hora = 2 THEN Clasificacion = amarillo	Error = 1.4% en el peor de los casos. (3 operaciones) / (6 usuarios x 4 horarios x 9 operaciones de ABM) * 100
Rule9	IF evento = 6 AND hora = 2 AND user = 2 THEN Clasificacion = amarillo	Error = 0%

Regla	Condición	Error
Rule10	IF día = 1 AND evento = 8 AND hora = 2 THEN Clasificacion = rojo	Error = 1.4% en el peor de los casos. (3 operaciones) / (6 usuarios x 4 horarios x 9 operaciones de ABM) * 100
Rule11	IF evento = 9 AND hora = 2 AND user = 2 THEN Clasificacion = amarillo	Error = 0%
Rule12	IF hora = 2 AND user = 5 THEN Clasificacion = rojo	Error = 0%
Rule13	IF día = 1 AND { evento = 2 OR evento = 3 } AND hora = 2 AND user = 6 THEN Clasificacion = rojo	Error = 0.9% en el peor de los casos. (2 operaciones) / (6 usuarios x 4 horarios x 9 operaciones de ABM) * 100
Rule14	IF día = 2 AND { evento = 2 OR evento = 3 } AND hora = 2 AND user = 6 THEN Clasificacion = amarillo	Error = 0%
Rule15	IF evento = 5 AND hora = 2 AND user = 1 THEN Clasificacion = rojo	Error = 0.9% en el peor de los casos. (2 operaciones) / (6 usuarios x 4 horarios x 9 operaciones de ABM) * 100
Rule16	IF día = 1 AND evento = 5 AND hora = 2 AND user = 2 THEN Clasificacion = amarillo	Error = 0%
Rule17	IF día = 2 AND evento = 5 AND hora = 2 AND user = 1 THEN Clasificacion = amarillo	Error = 0%
Rule18	IF día = 2 AND evento = 5 AND hora = 2 AND user = 2 THEN Clasificacion = rojo	Error = 0.9% en el peor de los casos. (2 operaciones) / (6 usuarios x 4 horarios x 9 operaciones de ABM) * 100
Rule19	IF día = 2 AND evento = 6 AND hora = 2 AND user = 6 THEN Clasificacion = amarillo	Error = 0%
Rule20	IF día = 1 AND evento = 9 AND hora = 2 AND {user = 1 OR user = 6} THEN Clasificacion = rojo	Error = 0.9% en el peor de los casos. (2 operaciones) / (6 usuarios x 4 horarios x 9 operaciones de ABM) * 100
Rule21	IF día = 2 AND evento = 9 AND hora = 2	Error = 0.9% en el peor de los casos. (2 operaciones) / (6 usuarios x 4 horarios x 9 operaciones de ABM) *

Regla	Condición	Error
	THEN Clasificacion = amarillo	100
	ERROR TOTAL	**18.9 %**

Tabla 5-8. Análisis de Error de las Reglas de Decisión.

6 CONCLUSIONES

6.1 Aportes

- La efectividad del sistema depende de la cantidad de clusters (el tamaño de la matriz) utilizados durante el entrenamiento de la red neuronal. Consecuentemente cuanto más grupos se empleen, más precisa será nuestra red.

  Las desventajas que emergen, cuando se manipulan matrices grandes, son el incremento del tiempo de entrenamiento de la red, el acrecentamiento de la cantidad de reglas de decisión, como así también el aumento del tiempo de clasificación de las observaciones.

  Durante el estudio de los casos se infiere que la cantidad de clusters utilizados en la red neuronal no fue suficiente para lograr agrupar conveniente los registros. Por ejemplo, la red no llegó a subdividir el grupo de los registros con *Hora Normal*, esto produjo que el Árbol de Decisión generalizara las entradas en una regla con un único atributo, es decir Si *Hora = 1* Entonces *Clase = Verde*. La situación puede detectarse fácilmente y ocurre cuando nos encontramos con reglas que tengan longitud = 1.

  Sin embargo, el error del sistema (18,9%) es menor al definido en la etapa de análisis (30%), por lo tanto no será necesario volver a entrenar la red neuronal con más grupos y producir nuevas reglas.

  Al momento de elegir el tamaño de la matriz para reducir el error esperado, hay que tener en presente la siguiente formula.

  ⇩ error ⇨ tiempo de procesamiento ⇧

- Cuando se utilice el algoritmo de *NNClust.xls* para entrenar la red neuronal SOM, se recomienda reducir la muestra de eventos repetidos, esta práctica ayuda a reducir drásticamente el tiempo insumido en el proceso.

- Cuando se analizan registros que contienen valores de atributos nuevos, es decir, que no fueron considerados durante las etapas de entrenamiento de la red neuronal y producción de reglas de decisión, será necesario entrenar la red nuevamente. Este es un comportamiento esperado porque se están analizando datos que la red no conoce.

- La aplicación reduce el análisis en detalle a menos del 5% del total de registros y a una revisión menos detallada menor al 15% del total, en todos los casos.

- Permitió detectar tareas administrativas no autorizadas de forma rápida y sencilla dentro de las muestras de registros.

- Permitió detectar tareas, que si bien están autorizadas, fueron realizadas en horario no laboral y deben ser justificadas.

- Permitió reducir el tiempo insumido en la tarea en un 75%. Sin utilizar este sistema insumía 8 horas, usando este sistema se invierten solo 2 horas.

6.2 Futuras líneas de investigación

- Con respecto a Minería de Datos (1)

  Una alternativa es utilizar una distribución de frecuencia acerca del comportamiento de cada administrador de red.

  El proceso consiste en obtener el patrón de comportamiento general de los administradores de red usando la red neuronal. Luego se presentan a la Red los nuevos eventos a evaluar, para obtener a que patrón pertenece ese evento. Una vez obtenida esta información, se adapta el perfil del usuario que generó el suceso para reflejar que la distribución de frecuencia, asociada a ese administrador, muestre una probabilidad mayor para realizar esta tarea. El proceso de actualización de la distribución de frecuencia se realiza por cada nuevo evento a evaluar.

  Finalmente para detectar si el administrador se desvía de su patrón habitual, se compara el perfil actual con el perfil histórico del usuario. Si la diferencia es mayor a un determinado valor entonces se considera que el gestor de la tarea ha cometido una infracción y se envía una alarma. Como los perfiles son distribuciones de frecuencia se utilizaría una distancia vectorial para compararlos.

- Con respecto a Minería de Datos (2)

  Analizar la viabilidad de utilizar la herramienta desarrollada en la Tesis de Magíster “Herramienta De Integración De Algoritmos De Inducción Y Mapas Auto-Organizados” durante las etapas de Entrenamiento de la Red y Producción de Reglas de Decisión.

- Con respecto a la aplicación del Sistema

  Implementar el sistema desarrollado en esta tesis para analizar los archivos de sucesos de servidores de aplicaciones, por ejemplo servidores de Correo Electrónico, servidores WEB, para predecir y/o alertar cuando existe un problema o un comportamiento no conocido de la aplicación siendo monitoreada.

- Con respecto al Sistema Desarrollado

  Desarrollar un módulo que analizar automáticamente los archivos de salida de las observaciones Rojas, Amarillas y Verdes. Con éste, no se requerirá que el trabajo sea realizado por una persona, entonces los tiempos de análisis se reducirán drásticamente. Deberá utilizarse una tabla que contemple las actividades que los administradores de redes pueden y no pueden realizar.

7 ANEXO

7.1 Las redes neuronales

Las redes neuronales son modelos que intentan reproducir el comportamiento del cerebro. Cualquier modelo de red neuronal consta de dispositivos elementales de proceso: las neuronas. A partir de ellas, se pueden generar representaciones específicas. La neurona artificial pretende mimetizar las características más importantes de las neuronas biológicas. Cada neurona i-ésima está caracterizada en cualquier instante por un valor numérico denominado *estado de activación*, una *función de activación* que transforma el estado actual de activación en una señal de salida y_i. Dicha señal de salida es enviada a través de canales de comunicación unidireccionales a otras unidades de la red; en estos canales, la señal se modifica de acuerdo con la sinapsis (el peso w_{ij}) asociada a cada uno de ellos según una determinada regla. Las señales moduladas que han llegado a la unidad j-ésima se combinan entre ellas, generando así la entrada total. (Figura 7-1)

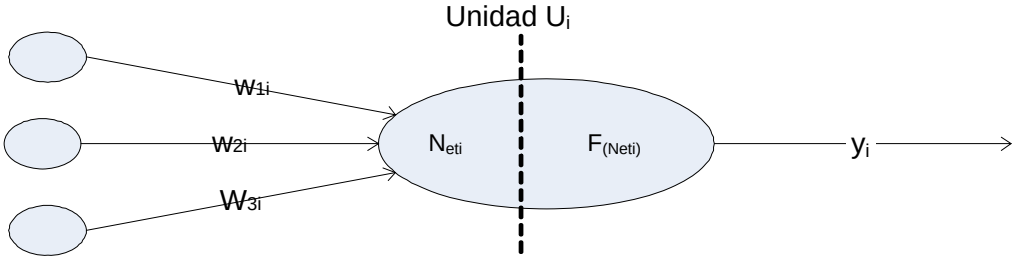


Figura 7-1. Esquema de una Red Neuronal.

$$\text{Ne } t_i = \sum_{i}^{j} y_i \, w_{ij}$$

El modelo de Red Neuronal a utilizar en el presente trabajo es el propuesto por Kohonen y se denomina Mapa Auto Organizado (Self Organizing Map - SOM).

El mapa auto organizado (SOM) tiene la propiedad de preservar la topología, la cual captura un importante aspecto del rasgo de mapas en la corteza cerebral de los animales más inteligentes. En una topología donde se conservan los mapas, los patrones de entrada cercanos, deberían activar unidades de salida cercanas en

el mapa. La arquitectura de la red consiste básicamente en un arreglo bidimensional de unidades, cada una conectada a todos los "n" nodos de entrada.

"wg" denota el vector n-dimensional asociado con la unidad ("i", "j") del arreglo. Cada neurona computa la distancia Euclidiana entre el vector de entrada "x" y el vector de pesos almacenado "wy". SOM es un tipo especial de red de aprendizaje competitiva que define un entorno espacial para cada unidad de salida. La forma del entorno local puede ser cuadrada, rectangular, o redonda. El tamaño inicial del entorno es a menudo definido en "1/2" a "2/3" del tamaño de la red y se reduce el tiempo según un horario programado (por ejemplo, una función decreciente exponencial). Durante el aprendizaje competitivo, todos los vectores de peso asociaron con el ganador y sus unidades vecinas son actualizadas. El modelo SOM de Kohonen puede usarse para la proyección de datos multivaluados, aproximación de densidad, y agrupamiento. Han sido aplicadas con éxito en las áreas de reconocimiento de voz, procesamiento de imágenes, robótica, y control de procesos. Los parámetros de configuración incluyen la dimensionalidad del arreglo de la neurona, el número de neuronas en cada dimensión, la forma de la vecindad, la reducción de la vecindad, y la tasa de aprendizaje. [Kohonen T., 1997].

7.2 Árboles de Decisión

La familia de los Top Down Induction Trees (TDIDT) pertenece a los métodos inductivos del Aprendizaje Automático que aprenden a partir de ejemplos preclasificados. En Minería de Datos, se utilizan para modelar las clasificaciones en los datos mediante árboles de decisión.

ID3 (Induction Decision Trees) es el sistema que más impacto ha tenido en la Minería de Datos. Es un sistema de aprendizaje supervisado que construye árboles de decisión a partir de un conjunto de ejemplos. Estos ejemplos son tuplas, donde el dominio de cada atributo de estas tuplas está limitado a un conjunto de valores. ID3 genera descripciones que clasifican cada uno de los ejemplos del conjunto de entrenamiento.

El nivel de precisión en la clasificación es alto. Sin embargo, los árboles son demasiado frondosos, lo cual conlleva a una difícil interpretación. En esos casos pueden ser transformados en reglas de decisión para hacerlos más comprensibles. [Ochoa M *et al*, 2005].

7.2.1 Transformación a Reglas de Decisión

Los árboles de decisión demasiado grandes son difíciles de entender porque cada nodo debe ser interpretado dentro del contexto fijado por las ramas anteriores.

Cada prueba tiene sentido, solamente, si se analiza junto con los resultados de las pruebas previas. Además, la estructura de árbol puede hacer que un concepto en particular quede fragmentado, lo cual hace que el árbol sea aún más difícil de entender. Una manera de solucionar este problema es cambiando el método de representación, por ejemplo, a reglas de decisión.

Si el camino recorrido desde la raíz a cada hoja, fuese transformado directamente en una regla de producción, dicha regla podría ser expresada como una conjunción de todas las condiciones que deben ser satisfechas para llegar a la hoja.

Al hablar de reglas de decisión o de producción nos referimos a una estructura de la forma:

Si atributo1=valorX y atributo2=valorY … y atributo#=valorZ
Entonces claseK

[Ochoa M *et al*, 2005].

7.3 Sistema de desarrollo Kappa-PC

El sistema de desarrollo de KAPPA-PC permite escribir aplicaciones en un ambiente gráfico de alto nivel y genera código estándar C y rutinas GUI. KAPPA-PC se usa para construir aplicaciones de misión críticas que forman el núcleo de las operaciones de negocio y ofrece una amplia gama de herramientas para construir y usar aplicaciones.

Para observar y controlar el funcionamiento de una aplicación, se pueden usar una variedad de imágenes gráficas en la interfaz de KAPPA-PC e indicadores para mostrar los valores de parámetros importantes y observar cómo cambian mientras sistema está en el funcionamiento.

KAPPA-PC proporciona un ambiente de desarrollo donde se puede escoger la manera de desarrollar una aplicación. Se puede usar programación orientada a objetos, razonamiento basado en reglas, programación tradicional o una combinación de algunos de estos métodos. [Kappa, 2007]

7.3.1 Razonamiento Basado en Reglas versus Programación Convencional

Una regla es similar a una declaración condicional en un programa convencional:

si esto, entonces eso.

Las reglas en KAPPA-PC vienen provistas con un motor de inferencia y un programa especial para el manejo de reglas de modo de aplicarlas apropiadamente. Por el contrario, en un programa convencional, hay que indicar explícitamente cuando deben aplicarse las declaraciones condicionales.

Adicionalmente, las reglas, con variables, pueden ser mucho más eficaces para codificar información. Una sola regla con una variable puede representar varios objetos; los programas convencionales, por otro lado, deben representar cada objeto como una entidad individual. [Kappa, 2007]

7.3.2 ¿Cuando deben Usarse las Reglas?

Si un proceso del razonamiento requiere sólo unas condiciones, pero en cambio requiere una serie predeterminada de pasos, las reglas son inapropiadas. Este es el caso para la mayoría los cálculos matemáticos.

Las reglas son útiles si las condiciones pueden subdividirse en pequeñas reglas, y si la estructura de control proporcionara por el motor de inferencia es apropiado.

El lenguaje de programación de KAPPA-PC, KAL, proporciona los medios para realizar una aplicación que siga un Razonamiento Basado en Reglas. [Kappa, 2007]

8 REFERENCIAS

- [Aránzazu C., 2005].

  Aránzazu C., Mantenimiento del Software. 41 páginas. Material del Magíster de Ingeniería de Software, ITBA.

- [Britos P, 2007].

  Britos P. Objetivos de Negocio y Procesos de Minería de Datos Basados en Sistemas Inteligentes. http://www.itba.edu.ar/capis/rtis/rtis-7-1/Objetivos-de-Negocio-y-Procesos-de-MD-basado-SI.pdf. Página vigente al 11/09/2007.

- [Chapman *et al*, 2000].

  Chapman, P., Clinton, J., Keber, R., Khabaza, T., Reinartz, T., Shearer, C., Wirth, R. 2000. CRISP-DM 1.0 - Step by step data mining guide. SPSS. http://www.crisp-dm.org/CRISPWP-0800.pdf. Página vigente al 05/09/2007.

- [COCOMO, 2007].

  El Modelo COCOMO. http://es.wikipedia.org/wiki/COCOMO. Página vigente al 07/09/2007.

- [CTree, 2007].

  Classification Tree in Excel. http://www.geocities.com/adotsaha/CTree/CtreeinExcel.html. Página vigente al 11/09/2007.

- [ELAP, 2007].

  Event Log Analyzer Pro. http://www.dv.co.yu/elap/index.htm. Página vigente al 17/03/2007.

- [Fernández E., 2006].

  Fernández E. 2006. Tesis de Magíster en Ingeniería de Software, Asistente para la Gestión de Documentos de Proyectos de Explotación de Datos. Universidad Politécnica de Madrid – Instituto Tecnológico de Buenos Aires.

- [GFI, 2007].

  Events Manager. http://www.gfihispana.com/es/eventsmanager. Página vigente al 16/03/2007.

- [Han & Lamber, 2000].

  Han & Lamber. Data Mining: Concepts and Techniques. 500 páginas. Morgan Kaufmann, 1st edition. 2000.

- [ISO 27000, 2007].

  El portal de ISO 27000 en Español. http://www.iso27000.es. Página vigente al 05/09/2007.

- [Jain *et al*, 1996].

  Jain *et al*. Artificial Neural Network: A Tutorial. http://www.cse.msu.edu/~cse802/notes/ArtificialNeuralNetworks.pdf. Página vigente al 28/08/2007.

- [Kappa, 2007].

  Kappa-PC 2.4 Online Help.

- [Kohonen T., 1997].

  Kohonen T. Self Organizing Maps. 426 páginas. Springer, 2nd edition. 1997.

- [MachineEngine, 2007].

  EventLog Analizer. http://manageengine.adventnet.com/products/eventlog /index.html. Página vigente al 16/03/2007.

- [Merlino H., 2005].

  Merlino H. 2005. Tesis de Magíster en Ingeniería de Software, Ambiente de Integración de Herramientas para Exploración de Datos Centrados en la Web. Instituto Tecnológico de Buenos Aires.

- [Métrica, 2008].

  Consejo Superior de Administración Electrónica. MÉTRICA VERSIÓN 3, Metodología de Planificación, Desarrollo y Mantenimiento de sistemas de información http://www.csi.map.es/csi/metrica3/. Página vigente al 30/01/2008.

- [NETIQ, 2007].

  Security Manager. http://www.netiq.com/products/sm/log.asp. Página vigente al 18/03/2007.

- [Northcutt *et al*, 2005].

  Northcutt *et al*. The log Management Industry – An Untapped Market. https://www.sans.org/webcasts/20050426_analyst_report.pdf. Página vigente al 15/03/2007.

- [OCDE, 2007].

  Organización para la Cooperación y el Desarrollo Económico. http://es.wikipedia.org/wiki/Organizaci%C3%B3n_para_la_Cooperaci%C3%B3n_y_el_Desarrollo_Econ%C3%B3mico. Página vigente al 15/04/2007.

- [Ochoa M *et al*, 2005].

  Ochoa M., Britos P. Herramienta de Agrupamiento con Redes Neuronales. 10 páginas. Material del Magíster de Ingeniería de Software, ITBA.

- [Ochoa M *et al*, 2005].

  Ochoa M., Britos P. Herramienta para la Utilización del Algoritmo de Inducción C4.5. 13 páginas. Material del Magíster de Ingeniería de Software, ITBA.

- [OMG, 2008].

  The Object Management Group (OMG). http://www.omg.org/. Página vigente al 07/02/2008.

- [PRISM, 2007].

  Event Tracker. http://www.eventlogmanager.com/. Página vigente al 17/03/2007.

- [RAE, 2007].

  Real Academia Española. http://www.rae.es. Página vigente al 29/10/2007.

- [Sal E., 2007].

  Sal E. 2007. Tesis de Magíster en Ingeniería de Software, Herramienta de Integración de Algoritmos de Inducción y Mapas Auto-Organizados. Instituto Tecnológico de Buenos Aires.

- [Schilliró, 2006].

  Fraudes corporativos, ¿cómo combatirlos desde la seguridad informática? http://www.materiabiz.com/mbz/ityoperaciones/nota.vsp?tok=1193373718872&nid=32134. Página vigente al 15/04/2007.

- [Seguridad, 2007].

  Seguridad de la Información. http://www.segu-info.com.ar. Página vigente al 29/10/2007.

- [SEI, 2008].

  Carnegie Mellon's Software Engineering Institute (SEI). http://www.sei.cmu.edu/. Página vigente al 08/02/2008.

- [SOM, 2007].

  Neural Network Based Clustering using Self Organizing Map (SOM) in Excel. http://www.geocities.com/adotsaha/NN/SOMinExcel.html. Página vigente al 11/09/2007.

- [SOX, 2002].

  One Hundred Seventh Congress of the United States of America, At the Second Session. http://fl1.findlaw.com/news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf. Página vigente al 15/03/2007.

- [Wikipedia, 2007].

  Enciclopedia de contenido libre. http://es.wikipedia.org/wiki/Portada. Página vigente al 30/10/2007.