Código: TI-PSI-09

Política de borrado seguro

Versión 1

Realizado por:

Marco Antonio Villan

Fecha:

10/08/2023

Índice

POLÍTICAS, ESTÁNDARES Y PROCEDIMIENTOS DE TI

Objetivo

El presente documento tiene como objetivo definir la política de borrado seguro y la utilización de herramientas y métodos de eliminación definitiva de datos en dispositivos móviles, laptops y pc's de escritorio cómo se especifican en las políticas **TI-PO-01 Telefonía Móvil Institucional, TI-ES-01 Equipo portátil de comunicaciones, ES-01 Equipamiento Puesto de Trabajo y TI-PO-03 Puesto de trabajo.**

Alcance

La siguiente política aplica a todo el proceso de borrado seguro de datos e información ya que la eliminación de archivos no implica que no puedan ser recuperados. A partir de la presente política se debe establecer un procedimiento técnico que asegure que los archivos, datos, datos sensibles e información eliminados no puedan ser recuperados de discos rígidos, dispositivos móviles y discos de estado sólido.

Políticas asociadas

- TI-PSI-01 - Política de Seguridad de la Información
- TI-PSI-04 - Política de Backups y Disaster Recovery Plan (DRP)
- TI-PSI-06 - Política de relación con proveedores
- TI-PSI-11 - Política de destrucción de papel y soporte informático.
- TI-PR-02 - Procedimiento de borrado seguro
- TI-PR-03 - Procedimiento de ABM de colaboradores, docentes y directivos
- TI-PO-01 - Telefonía Móvil Institucional
- TI-ES-01 - Equipo portátil de comunicaciones
- ES-01 - Equipamiento Puesto de Trabajo y TI-PO-03 Puesto de trabajo.

Responsabilidades

Es responsabilidad del departamento de Tecnología de la Información de implementar las medidas necesarias para la eliminación segura de datos en dispositivos móviles, laptops y pc´s de escritorio.

Es responsabilidad de Soporte de Campo seguir los lineamientos del procedimiento **TI-PR-02 - Procedimiento de borrado seguro**

Identificación de activos

Se tendrá un registro y control de los activos que posee el Instituto Tecnológico de Buenos Aires centralizado en una solución brindada por el Departamento de Tecnología de la Información. También, se deben identificar:

- Tipo de dispositivo
- Tipo de almacenamiento
- Custodio
- Responsable
- Estado

Gestión adecuada de soportes electrónicos

El personal responsable supervisará y documentará todas las operaciones como mantenimiento, reparación, sustitución y archivo de los dispositivos que almacenan datos e información de la Institución, esto incluye también aquellos que son utilizados para realizar copias de respaldo.

En relación al almacenamiento en la nube, el proveedor debe contar con las medidas técnicas para asegurar y garantizar que todos los datos e información que el Instituto Tecnológico de Buenos Aires decida eliminar en forma permanente no pueda ser recuperada por medio de ningún tipo de método o software. Este punto también debe ser identificado en la política **TI-PSI-06 - Política de relación con proveedores.**

A partir de la aprobación de la presente política se implementarán procedimientos de eliminación segura de datos para evitar que los datos puedan ser recuperados por terceros. Se debe implementar la sobre escritura de datos en iteraciones para que en el caso que se utilice software de recuperación los datos no puedan ser identificados.

Todo el proceso de eliminación de datos será documentado para dejar registro y contará con la aceptación por parte del solicitante ya que se informará que toda la información contenida no va a poder ser recuperada. Por otro lado, también se registrará cuando no fuese posible realizar la eliminación lógica, por lo que se implementará la política **TI-PSI-11 - Política de destrucción de papel y soporte informático**, para asegurar que la información almacenada no pueda ser recuperada en caso de desuso de los dispositivos.

Los procedimientos antes mencionados serán aplicables a los teléfonos celulares, laptops, servidores, pc´s de escritorio, servidores en la nube, almacenamiento externo, HD, HD SSD, memorias flash, cds, dvds, y todo tipo de hardware que permita almacenar datos del Instituto Tecnológico de Buenos Aires.

Gestión adecuada de soportes físicos

En el caso de disponer de documentación en soporte papel en almacenamiento físico, se aplicará la presente política. Se identificará la criticidad de los datos contenidos en los medios de soporte papel y su posterior eliminación de manera segura establecida en la política **TI-PSI-11 - Política de destrucción de papel y soporte informático.**

Se debe evitar la eliminación de la documentación de manera manual y se deben utilizar dispositivos técnicos que no permitan el trashing, que es un tipo de ataque donde un tercero puede obtener información confidencial a través de la documentación desechada. Se debe utilizar un proceso de triturado para destruir el papel mencionado en la política de destrucción de soporte papel e informático.

Supervisión y documentación

En todos los casos, los procesos de borrado seguro y eliminación de documentación en papel serán supervisados y documentados por el personal del Departamento de Tecnología de la Información.

Se documentará cada proceso de eliminación segura para dejar registro en caso de auditorías en Seguridad de la Información o en caso de que sea solicitado por las autoridades competentes.

Reutilización de soportes electrónicos

En el caso de reutilizar componentes para nuevos colaboradores o staff, previamente se deben implementar técnicas de borrado seguro para que la información no pueda ser recuperada, con las herramientas recomendadas en la presente política y siguiendo los lineamientos del procedimiento **TI-PR-02 - Política de borrado seguro**.

Herramientas recomendadas

El Departamento de Tecnología de la Información asignará las herramientas para realizar el borrado seguro de los dispositivos a nivel local en el caso que se requiera eliminar carpetas o documentación en forma segura para que no pueda ser recuperada. Se establecen las herramientas en el procedimiento **TI-PR-02 - Política de borrado seguro**.

Destrucción de soportes electrónicos

Los soportes electrónicos que no son utilizados por la institución deben cumplir con el procedimiento **TI-PR-02 - Política de borrado seguro**.

Borrado de cuentas de usuario

Las cuentas de usuario ITBA son creadas y asignadas a un usuario único. En el caso que se realice la baja del usuario en la institución, las cuentas no pueden ser eliminadas ni reutilizadas por un nuevo usuario.

Todos los procedimientos relacionados con Altas, bajas y modificaciones de usuario se encuentran en el documento **TI-PR-03 Procedimiento de ABM de colaboradores, docentes y directivos**.

Preguntas o Comentarios
Comunicarse por los canales habilitados a la Mesa de Ayuda de TI

Fecha de Aprobación:
04/09/2023

Fecha de Entrada en Vigencia:
04/09/2023

Historial de revisiones:

Versión	Fecha	Revisado por
1	10/08/2023	Martín Giller