Política de Borrado Seguro

Aprobación y Control de Cambios

Para garantizar el cumplimiento el documento debe ser aprobado por un miembro de la Alta Dirección.

Aprobación:

Código del Documento	Versión	Fecha	Creado por:	Aprobado por:	Nivel de Confidencialidad
CA-001	1.0	11/08/2022	Thomas Purcell	Thomas Purcell	Alto

En caso de ser necesario en el futuro se utilizará el siguiente control de cambios

Fecha	Versión	Fecha	Modificado por:	Aprobado por:	Descripción de la modificación

Objeto

Establecer, difundir y verificar el cumplimiento de buenas prácticas para la destrucción segura de material confidencial, y los métodos de borrado seguro que garantizan la adecuada gestión del ciclo de vida desde el punto de vista de la seguridad de la información.

Ámbito de Aplicación

Se aplica a todo el ámbito de actuación de Teloaudito y sus contenidos se alinean a las directrices de carácter más general definidas en la Política de Seguridad de la Información y en las Normas de Seguridad.

Es de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en Teloaudito, incluyendo el personal de proveedores externos, cuando sean usuarios de los Sistemas de Información de Teloaudito

En el ámbito de la presente normativa, se entiende por usuario cualquier empleado perteneciente o ajeno a Teloaudito, así como personal de organizaciones privadas externas, entidades

colaboradoras o cualquier otro con algún tipo de vinculación con Teloaudito y que utilice o posea acceso a los Sistemas de Información de Teloaudito.

Roles y Responsabilidades

CISO: Se encarga de promulgar la política de seguridad de la información. Un componente de esta política es la disposición de la información y la desinfección de los medios. El CISO, como custodio de la información, es responsable de asegurar que los requisitos de desinfección organizacional o local sigan las directrices de este documento.

Propietario del Sistema de Información: El propietario del sistema de información debe asegurarse de que los acuerdos contractuales o de mantenimiento estén en lugar y son suficientes para proteger la confidencialidad de los medios y la información del sistema acorde con el impacto de la divulgación de dicha información en la organización.

Propietario de la Información: El propietario de la información debe asegurarse de que la supervisión adecuada del mantenimiento de los medios in situ por proveedores de servicios, cuando sea necesario. El propietario de la información también es responsable de garantizar que entienden completamente la sensibilidad de la información bajo su control y que los usuarios del la información es consciente de su confidencialidad y los requisitos básicos para la desinfección de los medios.

Usuario: Los usuarios tienen la responsabilidad de conocer y comprender la confidencialidad de la información que están utilizando para realizar su trabajo asignado y garantizar el manejo adecuado de información

Borrado Seguro y Destrucción de la Información

Métodos que no destruyen la información de forma segura

Cuando se utilizan métodos de borrado dispuestos por el propio sistema operativo como con la opción «eliminar» o la tecla «Supr» o «Delete», se realiza el borrado exclusivamente en la «lista de archivos» sin que se elimine realmente el contenido del archivo, que permanece en la zona de almacenamiento hasta que se reutilice este espacio con un nuevo archivo. Por tanto, toda aquella acción que no conlleve la eliminación, tanto de la información de la «lista de archivos» como del contenido del mismo, no consigue destruir eficazmente dicha información. De forma específica, no son métodos de destrucción segura:

- Los comandos de borrado del sistema operativo acceden a la «lista de archivos» y marcan el archivo como suprimido, pero su contenido permanece intacto.
- Al formatear un dispositivo normalmente se sobre-escribe el área destinada a la «lista de archivos» sin que el área de datos donde se encuentra el contenido de los archivos haya sido alterada.

Métodos de destrucción de la información

Los medios eficaces que evitan completamente la recuperación de los datos contenidos en los dispositivos de almacenamiento son: la des magnetización, la destrucción, la sobre escritura en la totalidad del área de almacenamiento de la información, y el borrado con herramientas de borrado seguro.

Des magnetización

La des magnetización consiste en la exposición de los soportes de almacenamiento a un potente campo magnético, proceso que elimina los datos almacenados en el dispositivo. Este método es válido para la destrucción de datos de los dispositivos magnéticos, como por ejemplo, los discos duros, disquetes, cintas magnéticas de backup, etc. Cada dispositivo, según su tamaño, forma y el tipo de soporte magnético de que se trate, necesita de una potencia específica para asegurar la completa polarización de todas las partículas.

Destrucción física

El objetivo de la destrucción física es la inutilización del soporte que almacena la información en el dispositivo para evitar la recuperación posterior de los datos que almacena. Existen diferentes tipos de técnicas y procedimientos para la destrucción de medios de almacenamiento:

- Desintegración, pulverización, fusión e incineración: son métodos diseñados para destruir por completo los medios de almacenamiento. Estos métodos suelen llevarse a cabo en una destructora de metal o en una planta de incineración autorizada, con las capacidades específicas para realizar estas actividades de manera eficaz, segura y sin peligro.
- Trituración: las trituradoras de papel se pueden utilizar para destruir los medios de almacenamiento flexibles. El tamaño del fragmento de la basura debe ser lo suficientemente pequeño para que haya una seguridad razonable en proporción a la confidencialidad de los datos que no pueden ser reconstruidos. Los medios ópticos de almacenamiento (CD, DVD, magneto-ópticos) deben ser destruidos por pulverización, trituración de corte transversal o incineración. Cuando el material se desintegra o desmenuza, todos los residuos se reducen a cuadrados de cinco milímetros (5mm) de lado.

En el caso de los discos duros se deberá asegurar que los platos internos del disco han sido destruidos eficazmente, no sólo la cubierta externa.

Sobre-escritura

La sobre-escritura consiste en la escritura de un patrón de datos sobre los datos contenidos en los dispositivos de almacenamiento. Para asegurar la completa destrucción de los datos se debe escribir la totalidad de la superficie de almacenamiento. La sobre-escritura se realiza accediendo al contenido de los dispositivos y modificando los valores almacenados,

por lo que no se puede utilizar en aquellos que están dañados ni en los que no son regrabables, como los CD y DVD.

Tipo de destrucción más adecuado dependiendo el tipo de soporte

Soporte	Tipo	Destrucción Física	Des magnetización	Sobre Escritura
Discos Duros	Magnético	√	√	√
Discos Flexibles	Magnético	√	√	√
Cintas Backup	Magnético	√	√	√
CD	Óptico	√	X	X
DVD	Óptico	√	X	X
Blue-ray Disc	Óptico	√	X	X
Pen Drive	Electrónico	√	X	√
Discos Duros SSD	Electrónico	√	X	√

Lineamientos para Sanitización de Medios

La empresa adopta las mejores prácticas definidas en el National Institute of Standards and Technology (NIST), documento “Guidelines for Media Sanitization” Nist Special Publication

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

Excepciones

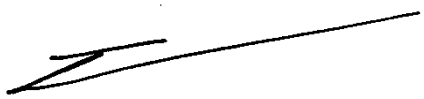
No se considera ninguna excepción a lo expuesto en la presente política, ni procedimiento para permitir su no aplicación.

En caso de existir alguna necesidad que requiera el no cumplimiento de parte o la totalidad de esta política, deberá existir autorización expresa de [Área/Gerencia Correspondiente].

Referencias

Instituto Nacional de Ciberseguridad (INCIBE). España. https://www.incibe.es/

National Institute of Standards and Technology (NIST). USA.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf



Thomas Purcell Goudie
Gerente General
Actividades de Asesoría Comercial Ltda