EthicsGlobal

POLÍTICA DE ELIMINACIÓN Y DESTRUCCIÓN

Código:	SGSI-PED-01
Versión:	2.0
Fecha de la versión:	17-ene-2022
Creado por:	Javier Flores
Aprobado por:	Dirección General
Nivel de confidencialidad:	Uso interno

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
26-sep-2018	1.0	Javier Flores	Primera versión.
06-ene-2021	1.5	Depto. Seguridad de la información	Complemento a la versión
07-sept-2021	2.0	Depto. Seguridad de la información	Revisión de versión y anexo de checklist de cumplimiento
17-ene-2022	2.0	Denice Arroyo	Revisión de versión

Tabla de contenido

1. Objetivo, alcance y usuarios

El objetivo del presente documento es garantizar que la información almacenada en equipos y soportes sea borrada o eliminada de forma segura.

Este documento se aplica a todo el alcance del Sistema de gestión de seguridad de la información (SGSI); es decir, a toda la tecnología de la información y de la comunicación, como también a la documentación dentro del alcance del SGSI.

Los usuarios de este documento son todos los empleados de EthicsGlobal.

2. Documentos de referencia

- Norma ISO/IEC 27001, puntos A.8.3.2, A.11.2.7
- Política de seguridad de la información
- [Política de Clasificación de la Información]
- [Inventario de activos]

3. Eliminación y destrucción de equipos y soportes

Todos los datos y software con licencia almacenado en soportes móviles (por ej., CD, DVD, unidades USB, tarjetas de memoria, etc., y también en papel) y en todos los equipos que tienen soportes de almacenaje (por ej., ordenadores, teléfonos móviles, etc.) deben ser borrados, o se debe destruir el soporte, antes de ser eliminados o reutilizados.

La persona responsable de borrar los datos o destruir el soporte debe informar al propietario del activo en cuestión acerca del borrado o eliminación de datos, y el propietario del activo debe actualizar el Inventario de activos.

3.1. Equipos

El personal de soporte TI responsable con autorización del CISO es el responsable de verificar y borrar datos de los equipos, salvo que la Política para manejo de información clasificada establezca otra cosa. Los datos deben ser borrados restaurando el equipo a la configuración de fábrica lo que puede incluir una completa reinstalación del Sistema Operativo del equipo, pero si, teniendo en cuenta la sensibilidad de los datos, si el proceso no es suficientemente seguro, entonces los soportes de almacenaje deben ser destruidos.

3.2. Soportes móviles de almacenaje

El personal de soporte IT responsable con autorización del CISO es el responsable de borrar datos de los soportes móviles de almacenaje, salvo que la Política para manejo de información clasificada establezca otra cosa. Los datos deben ser borrados realizando un formateo seguro del soporte, pero si, teniendo en cuenta la sensibilidad de los datos, si el proceso de borrado no es suficientemente seguro, entonces los soportes de almacenaje deben ser destruidos.

3.2.1. Reutilización de soportes móviles

Si queremos reutilizar un soporte que ya contiene datos, debemos utilizar la opción de sobreescritura para garantizar un borrado total de la información. La sobreescritura se puede utilizar en todos los dispositivos regrabables (discos duros, pendrives, UBS, etc.) siempre que el dispositivo no este dañado.

3.2.2. Antes de deshacernos de los soportes móviles

Cuando queremos desechar algún soporte de almacenamiento porque ya no funcione o porque se haya quedado obsoleto debemos utilizar los métodos de desmagnetización o destrucción física. Cualquiera de estos dos métodos imposibilita la reutilización del dispositivo.

3.3. Soportes en papel

Los empleados de la organización que manejan documentos individuales son responsables de destruir los soportes en papel, salvo que la Política de clasificación de la información clasificada establezca otra cosa. Los soportes en papel se destruyen en trituradoras de papel.

3.4. Borrado y destrucción de registros; comisión para la destrucción de información

Se deben llevar registros de todo el borrado o destrucción de datos clasificados como "Restringido" y "Confidencial". Los registros deben incluir la siguiente información: datos sobre los soportes, fecha de borrado o destrucción, método de borrado o destrucción, persona que realizó el proceso.

Toda la información clasificada como "Confidencial" debe ser borrada o destruida ante la presencia de una comisión integrada por personas autorizadas a acceder a dicha información.

3.5. Borrado y destrucción de datos en la nube

Se deben llevar registros de todo el borrado o destrucción de datos clasificados como "Restringido" y "Confidencial". El CISO es la única entidad que podrá eliminar, borrar, destruir cualquier tipo de información almacenada en la nube de Amazon dedicada a EthicsGlobal (base de datos y archivos estáticos). En todos los casos de destrucción electrónica se debe borrar la información original, todas sus copias y sus respectivos respaldos de seguridad.

Para la eliminación de datos en la nube se deberá seguir una o algunas de las siguientes metodologías:

- American DoD 5220-22M Standard Wipe
- Canadian RCMP TSSIT OPS-II Standard Wipe
- Pseudo random data
- North Atlantic Threaty Organization-NATO standard
- Método Gutmann

Toda la información clasificada como "Confidencial" debe ser borrada o destruida ante la presencia de una comisión integrada por personas autorizadas a acceder a dicha información.

4. Controles de revisión

A continuación, se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo a borrado seguro y gestión de soportes.

Los controles se clasificarán en dos niveles de complejidad:

- Basico (B): El esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes.
- Avanzado (A) El esfuerzo y los recursos necesarios para implantarlo son considerables. Se necesitan programas que requieren configuraciones complejas.

Los controles podrán tener el siguiente alcance:

- Procesos (PRO): Aplica a la dirección o al personal de gestión.
- Tecnología (TEC): Aplica al personal técnico especializado.
- Personas (PER): Aplica a todo el personal.

NIVEL	ALCANCE	CONTROL	
B	POR	**Inventario de activos** Realizas un seguimiento de los dispositivos que están en funcionamiento, las personas o departamentos responsables, la información contenida en ellos y su clasificación en función del grado de criticidad para el negocio.	
B	PRO/TEC	**Gestión de soportes** Supervisas los dispositivos que almacenan información corporativa, en particular aquellos que se utilizan para realizar copias de seguridad, documentando cualquier operación realizada sobre los mismos: mantenimiento, reparación, sustitución, etc.	
A	PRO/TEC	**Eliminación de la información en soportes no electrónicos** Utilizas el proceso de triturado para destruir la información de los soportes no electrónicos (papel y soportes magnéticos).	
A	PRO/TEC	**Eliminación de la información para la reutilización de soportes electrónicos** Optas por el proceso de sobrescritura cuando quieres	

		reutilizar un soporte todavía en buen estado.	
A	PRO/TEC	**Eliminación de la información antes de deshacernos de soportes electrónicos** Usas el proceso de desmagnetización o de destrucción física antes de desechar el soporte de almacenamiento.	
A	PRO/TEC	**Eliminación de la información almacenada en la nube** Para la eliminación de datos en la nube de AWS utilizas una o más de las siguientes metodologías: • American DoD 5220-22M Standard Wipe • Canadian RCMP TSSIT OPS-II Standard Wipe • Pseudo random data • North Atlantic Threaty Organization-NATO standard • Método Gutmann	

5. Gestión de registros guardados en base a este documento

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención
Borrado o destrucción de registros - en papel	Archivero de administración general	Gerente de administración.	El gabinete tiene cerradura, las llaves están en custodia del gerente de administración.	Los registros son almacenados por el plazo de 5 años.

6. Validez y gestión de documentos

Este documento es válido hasta el 09-may-2022.

El propietario de este documento es el CISO, que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de incidentes que surgen por no borrar o destruir información de la forma especificada en el presente documento.
- Cantidad de procesos de destrucción de información con altos niveles de confidencialidad para los cuales no se lleva un registro.