PR-SGI-008

Borrado seguro de Información

Responsables

Elaboró:	Soporte Técnico
Revisó:	Control de Documentos
Aprobó:	Gerente de Operaciones

Control de versiones

Versión	Fecha	Descripción del cambio
1	31/01/19	Emisión inicial
2	19/08/22	Actualización de formato y revisión general del documento

Clave del formato de procedimiento: F-SGI-002 v3
Comentarios o dudas: sgi@silent4business.com

Contenido

1. Objetivo del procedimiento

Definir los pasos para eliminar de forma segura la información de Silent4Business o de cualquier otro tercero bajo su responsabilidad que tenga carácter confidencial, garantizando los niveles de seguridad de esta y poder eliminar el riesgo de que a través de basura, dispositivos o software se pueda recuperar información confidencial que sobre estos medios se haya podido grabar.

2. Alcance

El presente documento es de aplicabilidad del Sistema de Gestión Integral (SGI), es de uso del área de seguridad de la información, aplica a toda la información digital del personal o terceros que Silent4business tenga en su poder, dando cumplimiento a las reglamentaciones a que hubiere lugar, buscando garantizar la seguridad y privacidad de los datos custodiados por la Organización, velando por que la información sea eliminada de forma segura y que no pueda ser recuperable posteriormente.

3. Definiciones

- **Activo de información:** Cualquier componente (humano, tecnológico, software,documental o de infraestructura) que soporta uno o más procesos de negocios de la Organización y, en consecuencia, debe ser protegido.

- **Confidencialidad:** es la garantía de que la información no está disponible o divulgada a personas, Organización es o procesos no autorizados.

- **Control:** es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye policías, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.

- **Custodio del activo de información:** es la unidad organizacional o proceso, de-signado por los propietarios, encargado de mantener las medidas de protecciónestablecidas sobre los activos de información confiados.

- **Disponibilidad:** es la garantía de que los usuarios autorizados tienen acceso a lainformación y a los activos asociados cuando lo requieren.

- **Integridad:** es la protección de la exactitud y estado completo de los activos.

- **Inventario de activos de información:** es una lista ordenada y documentada delos activos de información pertenecientes a la Organización.

- **Propietario de la información:** es la unidad organizacional o proceso donde secrean los activos de información.

- **Recursos tecnológicos:** son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de Silent4business.

- **Responsable por el activo de información:** es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.

- **SGI:** Sistema de Gestión Integral.

- **Sistema de información:** es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas.

4. Responsabilidades

Rol	Responsabilidades y/o funciones
Líder SGI	• Emitir y vigilar que se cumpla este procedimiento para conservar el nivel de confidencialidad de la información y actualizar este documento de acuerdo con las necesidades del negocio. • Debe verificar que el borrado seguro de la información se halla efectuado correcta-mente, en el medio respectivo.
Propietario de activos de Información	• Solicitar el borrado seguro de información.
Soporte Interno	• Ejecutar el borrado seguro sobre dispositivos.
Gerente de Operaciones	• Consolidar los resultados y reportárselos al Líder SGI.

5. Descripción de actividades

No.	Actividad	Responsable	Descripción de la actividad	Registro
Inicio del procedimiento				
1.	Solicitar el borrado seguro	Propietario de activos de Información	El responsable de la información o del activo de T.I que contenga la información a borrar debe solicitarlo a Soporte Interno mediante la herramienta que la organización designa Soporte interno efectúa el registro de la solicitud mediante la herramienta de gestión de T.I.	Registro en la herramienta
2.	Verificar el estadodel activo de T.I.	Soporte Técnico	Antes de comenzar a efectuar el borrado seguro es recomendable verificar el estado de los medios de almacenamiento activos, a través de herramientas tecno-lógicas establecidas para este fin. ¿Aplicar borrado seguro? Si: Ir al paso 3. No: Ir al paso 6.	No aplica.
3.	Ejecutar borrado seguro	Soporte Técnico	Efectúa el procedimiento del numeral N°5 de la presente guía según sea el caso	Emisión de certificado de borrado seguro de información
4.	Consolidar los resultados y reportárselos al Líder SGI.	Gerente de Operaciones	Consolidar los resultados y reportárselos al Líder SGI. Reúso: Efectuada la valoración técnica del activode T.I. se entrega a recursos físicos para la reubicación dentro de las áreas de la SILENT4BUSINESS o para ser donados a terceros. Baja: Efectuada la valoración técnica del activo de T.I. y se procederá con la destrucciónfísica de acuerdo con el numeral N° 5 dela presente guía según sea el caso. Se documenta la actividad mediante la base de conocimiento de la herramienta de Gestión anexándole la documentación pertinente a la solicitud respectiva.	No aplica.

5.	Verificar que el borrado seguro de la información.	Líder SGI	Verificar que el borrado seguro de la información se halla efectuado correctamente, en el medio respectivo. Fin del procedimiento.	No aplica
6.	No se realiza el borrado, se notifica alJefe inmediato y Líder SGI	Soporte Técnico	Verificar que el borrado seguro de la información se halla efectuado correctamente, en el medio respectivo. Fin del procedimiento.	No aplica
Fin del procedimiento.				

6. Documentos relacionados

- M-SGI-002 Manual de políticas del SGI

7. Anexos

Este Procedimiento se enfoca en toda la información que se encuentre en cualquiera de los siguientes medios de almacenamiento: Discos Duros internos y externos, Memorias USB, Documentación impresa o cualquier otro medio de almacenamiento.

- **Almacenamiento:** Los datos que se recopilan en los soportes de almacenamiento pueden constituir información muy delicada y su indebida divulgación no solo puede afectar a la propia Organización, ya que los funcionarios u otras Organización es también pueden verse perjudicados. Por ello, el primer paso en la gestión segura de la información es realizar una clasificación de los datos y un almacenamiento adecuados, en base a unas políticas establecidas y actualizadas.
- **Recuperación**: Las pérdidas de datos son acontecimientos comunes en las empresas, a veces por causas fortuitas y otras veces por fallos humanos o en los equipos. En este sentido, las técnicas de recuperación de la información son una herramienta imprescindible en las organizaciones, ya que permiten restaurar la actividad y asegurar su continuidad.
- **Borrado seguro**: Por último, cuando la información ha sido tratada en la Organización y llega al final de su vida útil, debe ser eliminada de forma segura, para evitar que pueda caer en manos de terceros y sea recuperada.

Este Procedimiento aplica para los medios que hayan sido alquilados, que se vayan a dar de baja de inventarios, incinerar, vender, entregarlos como parte de otras compras, que se va- yan a donar, o que sean reubicados dentro de las áreas de la SILENT4BUSINESS y en los que en algún momento se almacenó información confidencial se les debe aplicar de igual forma el proceso descrito en la presente guía.

Normas de cumplimiento obligatorio

El responsable de la información debe revisar que se hayan realizado las copias de seguridad, las pruebas y el borrado seguro de la información.
Cuando se haya dado la autorización por el responsable de la información, el área responsable debe dar un borrado a la información dependiendo del medio en que reposa; para cumplir con este requerimiento se pueden utilizar cualquiera de los siguientes métodos según sea conveniente.

•**Desmagnetización:** La desmagnetización 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.

- **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.
    - **Desintegración, pulverización, fusión e incineración**: son métodos diseña-dos 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 me-dios 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, magnetoópticos), de-ben ser destruidos por pulverización, trituración de corte transversal o incineración.
- **Sobreescritura:** La sobreescritura 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, para dispositivos electrónicos se debe utilizar un software que efectué borrado a bajo nivel, guardando los registros como evidencia de la destrucción de la información.