

|   |                |   |
|---|----------------|---|
| <br><b>Gobierno del Ecuador</b><br>GUILLERMO LASO<br>PRESIDENTE |                | <b>SEGURIDAD DE LA INFORMACIÓN</b><br><br><b>PROCEDIMIENTO DE RESGUARDO, CONSERVACIÓN Y ELIMINACIÓN/DESTRUCCIÓN DE INFORMACIÓN.</b> |
| <b>Fecha:</b>   | <b>Página:</b> |   |
| 28/03/2023  | 1 de 11        |   |
| <b>ÁREA REQUIRIENTE:</b>  |                | <b>GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN</b>  |

## PROCEDIMIENTO DE RESGUARDO, CONSERVACIÓN Y ELIMINACIÓN DE INFORMACIÓN.

**Elaborado Por:**

| Fecha      | Nombre        | Cargo   | Versión | Firma |
|------------|---------------|---|---------|-------|
| 28/03/2023 | Diego Moreira | Asistente de Tecnologías de la Información y Comunicación | 4.0     |       |

**Revisado Por:**

| Fecha      | Nombre        | Cargo  | Versión | Firma |
|------------|---------------|--|---------|-------|
| 28/03/2023 | Jose Alcarraz | Analista de Tecnologías de la Información y Comunicación | 4.0     |       |

**Aprobado Por:**

| Fecha      | Nombre           | Cargo                   | Versión | Firma |
|------------|------------------|-------------------------|---------|-------|
| 28/03/2023 | Ronald Sarmiento | Director Administrativo | 4.0     |       |

| Versión | Fecha      | Descripción cambios | Elaborado por: | Solicitado por:  |
|---------|------------|---------------------|----------------|------------------|
| 1.0     | 24/03/2023 |                     | Diego Moreira  | Ronald Sarmiento |
| 2.0     | 24/03/2023 |                     | Diego Moreira  | Ronald Sarmiento |
| 3.0     | 27/03/2023 |                     | Diego Moreira  | Ronald Sarmiento |
| 4.0     | 28/03/2023 |                     | Diego Moreira  | Ronald Sarmiento |

*Toda la información contenida en este documento es considerada privilegiada y confidencial, ya que este material incluye descripciones metodológicas de propiedad exclusiva de la Secretaría Técnica Ecuador Crece sin Desnutrición Infantil. Ninguna parte de este documento podrá ser reproducida por cualquier medio sin la previa Autorización escrita.*

## Contenido

|   |    |
|---|----|
| 1. Antecedentes.....  | 4  |
| 2. Objetivo .....   | 5  |
| 3. Medidas generales .....                                      | 5  |
| 4. Seguridad de la información (resguardo - conservación) ..... | 6  |
| 5. Protocolo para la destrucción de archivos .....              | 8  |
| 6. Glosario .....   | 10 |

|  |                |  |
|--|----------------|--|
|  <p><b>Gobierno del Ecuador</b><br/>GUILLERMO LASSO<br/>PRESIDENTE</p> |                | <p><b>SEGURIDAD DE LA INFORMACIÓN</b></p> <p><b>PROCEDIMIENTO DE RESGUARDO, CONSERVACIÓN Y ELIMINACIÓN/DESTRUCCIÓN DE INFORMACIÓN.</b></p> |
| <b>Fecha:</b>  | <b>Página:</b> |  |
| 28/03/2023   | 4 de 11        |  |
| <b>ÁREA REQUIRIENTE:</b>   |                | <b>GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN</b>   |

## 1. Antecedentes

Mediante acuerdo Ministerial Nro. 025-2019 del 20 de septiembre del 2019 se expide el Esquema Gubernamental de Seguridad de la Información – EGSi (versión 2.0) siendo el análisis técnico el siguiente: *“(…) Esta guía está diseñada para que las instituciones públicas de la APCID la usen como referencia a la hora de seleccionar controles dentro del proceso de implementación del Esquema Gubernamental de Seguridad de la Información como un Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO/IEC 27001 o bien como documento referencial para instituciones que implementen controles de seguridad de la información comúnmente aceptados. (…)”*

Para dar cumplimiento al Hito 7: *“Seguridad física y del entorno”, Sección 7.2 “Seguridad de los equipos” Subsección 7.2.7 “Seguridad de la reutilización o eliminación segura de dispositivos de almacenamiento”,* descrita en la Declaración de Aplicabilidad o Statement of Applicability (SoA por sus siglas en inglés), la Unidad de Gestión de Tecnologías de la Información y Comunicación en materia de conservación, resguardo y eliminación/destrucción debe asegurar los principios de: integridad, que garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada; disponibilidad, como capacidad de asegurar la fiabilidad y el acceso oportuno a los datos y recursos que los soportan por parte de los individuos autorizados y; confidencialidad, para prevenir su divulgación no autorizada cuando está almacenada o en tránsito.

De igual manera, es de obligatoriedad atender las medidas de conservación, resguardo y eliminación/destrucción contenidas en este documento, de conformidad con las mejores prácticas o estándares en la materia, salvaguardando y efectuando medidas y procedimientos para la conservación, resguardo y eliminación/destrucción de la información.

La Secretaría Técnica Ecuador Crece Sin Desnutrición Infantil y todos sus funcionarios son responsables de resguardar y conservar la información, así como su documentación, en la forma y términos que señale el presente documento, mediante procesos de almacenamiento, mantenimiento y gestión para su disponibilidad permanente.

|  |                |  |
|--|----------------|--|
|  <p><b>Gobierno del Ecuador</b><br/>GUILLERMO LASSO<br/>PRESIDENTE</p> |                | <p><b>SEGURIDAD DE LA INFORMACIÓN</b></p> <p><b>PROCEDIMIENTO DE RESGUARDO, CONSERVACIÓN Y ELIMINACIÓN/DESTRUCCIÓN DE INFORMACIÓN.</b></p> |
| <b>Fecha:</b>  | <b>Página:</b> |  |
| 28/03/2023   | 5 de 11        |  |
| <b>ÁREA REQUIRIENTE:</b>   |                | <b>GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN</b>   |

## 2. Objetivo

Establecer las medidas y procedimientos de conservación y resguardo de la información institucional a través de las mejores prácticas y estándares salvaguardando los principios de integridad, disponibilidad y confidencialidad y acogiendo las recomendaciones del EGSÍ V2 emitido por el MINTEL.

## 3. Medidas generales

La conservación y el resguardo deben asegurar la integridad, disponibilidad y confidencialidad, por lo que se han establecido los siguientes procedimientos:

- a) Proveer los servicios y equipos tecnológicos necesarios para la conservación y resguardo de la información, siendo estos: Servidor NAS (Network Attached Storage), el cual es un dispositivo de almacenamiento conectado a la red para el almacenamiento de datos e información; Duplicati, siendo un software de código abierto que permite realizar copias de seguridad (backups), con cifrado de seguridad AES-256; Discos duros externos independientes de los sistemas de red con el fin de salvaguardar la información ante cualquier intrusión.
- b) Verificar que los contenidos cumplen con los criterios técnicos, conceptuales y estándares definidos para la conservación y resguardo de la información.
- c) Documentar cambios que aseguren la integridad y la correcta actualización de las instancias en la información y los backups como medida de control y seguimiento, ya que al momento de ser exportados almacenan este activo con la fecha de descarga del respaldo, misma que en futuros backups puede ser actualizada.
- d) Implementar procedimientos que permitan controlar el acceso a la información con su respectivo monitoreo, estas medidas pueden ser: mediante previa autorización firmada por el comité CSI (Comité de Seguridad de Información); correos electrónicos para solicitar acceso, formularios, entre otros.
- e) Agendar ventanas de mantenimiento para contar con una copia de seguridad, asimismo, documentar el proceso de backup y archivarlo.

|  |                |  |
|--|----------------|--|
|  <p><b>Gobierno del Ecuador</b><br/>GUILLERMO LASSO<br/>PRESIDENTE</p> |                | <p><b>SEGURIDAD DE LA INFORMACIÓN</b></p> <p><b>PROCEDIMIENTO DE RESGUARDO, CONSERVACIÓN Y ELIMINACIÓN/DESTRUCCIÓN DE INFORMACIÓN.</b></p> |
| <b>Fecha:</b>  | <b>Página:</b> |  |
| 28/03/2023   | 6 de 11        |  |
| <b>ÁREA REQUIRIENTE:</b>   |                | <b>GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN</b>   |

- f) Implementar los procesos para la destrucción de archivos conforme al “Procedimiento de resguardo, conservación y eliminación/destrucción de información” de la Unidad de Gestión de Tecnologías de la Información y Comunicación, este procedimiento debe efectuarse una vez se verifique la vigencia de los datos, por consiguiente, esta debe ser eliminada convenientemente de forma segura y confidencial, potenciando la seguridad e imagen institucional.

#### **4. Seguridad de la información (resguardo - conservación)**

La Seguridad de la Información tiene como fin la protección de la información y de los sistemas de la información del acceso, uso, divulgación, interrupción o destrucción no autorizada, a través de medidas, funciones, procesos y procedimientos que, de manera coordinada, contribuyen a preservar la confidencialidad, integridad y disponibilidad de la información.

Como parte de las medidas para la conservación y resguardo de la información, la Secretaría Técnica Ecuador Crece Sin Desnutrición Infantil deberá tomar en cuenta los siguientes factores:

##### **4.1 Seguridad de comunicaciones y operaciones; acceso lógico y sistemas de información.**

4.1.1 La Unidad de Gestión de Tecnologías de la Información y Comunicación responsable de las comunicaciones (conectividad y servicios), control de accesos lógicos, adquisición de equipos de infraestructura, uso y mantenimiento de los sistemas de información institucionales, debe considerar los siguientes aspectos:

- a) La planificación, adquisición, implementación y adaptación de soluciones de software y cambios en la infraestructura aseguren una alta disponibilidad de las operaciones, seguridad de los activos de TIC's, la confidencialidad, integridad y disponibilidad de la información y documentación (física y digital) de los procesos.
- b) Que los mecanismos para monitoreo, acceso, respaldo y protección de la información, aseguren los principios de la seguridad de la información.

|  |                |  |
|--|----------------|--|
|  <p><b>Gobierno del Ecuador</b><br/>GUILLERMO LASSO<br/>PRESIDENTE</p> |                | <p><b>SEGURIDAD DE LA INFORMACIÓN</b></p> <p><b>PROCEDIMIENTO DE RESGUARDO, CONSERVACIÓN Y ELIMINACIÓN/DESTRUCCIÓN DE INFORMACIÓN.</b></p> |
| <b>Fecha:</b>  | <b>Página:</b> |  |
| 28/03/2023   | 7 de 11        |  |
| <b>ÁREA REQUIRIENTE:</b>   |                | <b>GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN</b>   |

4.1.2 La responsable de la Unidad deberá:

- a) Verificar que todos los equipos (de escritorio o portátiles) que formen parte de paquete tecnológico tengan acceso a los servicios institucionales y cumplan con las siguientes medidas: registro de nombre del equipo y usuario responsable; integración al dominio; antivirus; software actualizado.
- b) Definir protocolos de seguridad para evitar intrusiones externas a la infraestructura, incluyendo ataques externos e internos.
- c) Realizar respaldos de información para conservación, resguardo y archivo cada vez que se actualice o modifique.
- d) Mantener vigencia y actualizar formatos e imagen institucional en todos los servicios y documentación física y digital, siendo esta: formularios para proveer servicios específicos; Intranet; informes técnicos; manuales; entre otros.
- e) Mantener una copia del software, soluciones tecnológicas, aplicativos, parámetros de configuración de los sistemas, estructuras de datos y datos, que aseguren la conservación y resguardo de la información que generada y su recuperación en caso necesario.
- f) Establecer medidas de reemplazo de los medios de almacenamiento de la información generada, con base en la vida útil de éstos, asegurando la destrucción de los medios desechados que contengan información confidencial o reservada.

4.1.3 A su vez tener en cuenta las siguientes recomendaciones:

- a) Documentar los procedimientos de respaldo de la información y llevar un registro de las operaciones de respaldo y recuperación realizadas.
- b) Llevar el registro de los incidentes que hayan afectado la Seguridad de la Información, identificando la causa, qué lo originó, el nivel de gravedad, los alcances, los efectos percibidos, la solución adoptada y las

|  |                |  |
|--|----------------|--|
|  <p><b>Gobierno del Ecuador</b><br/>GUILLERMO LASSO<br/>PRESIDENTE</p> |                | <p><b>SEGURIDAD DE LA INFORMACIÓN</b></p> <p><b>PROCEDIMIENTO DE RESGUARDO, CONSERVACIÓN Y ELIMINACIÓN/DESTRUCCIÓN DE INFORMACIÓN.</b></p> |
| <b>Fecha:</b>  | <b>Página:</b> |  |
| 28/03/2023   | 8 de 11        |  |
| <b>ÁREA REQUIRIENTE:</b>   |                | <b>GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN</b>   |

medidas establecidas para minimizar la posibilidad de que vuelva a presentarse.

- c) Controlar que los cambios en los componentes tecnológicos y de comunicaciones no afecten a la seguridad de los mismos ni de la información a la que dan soporte.
- d) Monitorear necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas, a fin de procurar el procesamiento y almacenamiento adecuados tomando en cuenta los nuevos requerimientos de los sistemas, así como las tendencias proyectadas para el período estimado de vida útil de cada componente.

## 5. Procedimiento para la destrucción de archivos

La protección de la información personal de las personas e instituciones públicas y privadas exigen que, en base a la normativa vigente, los documentos que se eliminan sean destruidos de forma que su reconstrucción y la posterior utilización de la información que contienen sea imposible. Para hacerlo así, el proceso de destrucción debe estar sometido a estrictos controles que garanticen la seguridad, eficacia y confidencialidad.

A efectos de este documento, se emplea el término borrado como el procedimiento de eliminación de los datos o ficheros de un soporte o conjunto de soportes, permitiendo la reutilización de dichos soportes, y el término destrucción como el proceso de inutilización de información almacenada en soportes de almacenamiento que contengan documentos electrónicos, identificando técnicas de borrado/destrucción apropiadas, asimismo, como en cualquier otro proceso de destrucción, es necesario dejar constancia documental de los procedimientos de borrado realizados.

### 5.1 Recomendaciones para la eliminación y destrucción de información.

#### 5.1.2 Eliminación previa autorización:

- a) Se deben eliminar/destruir todas las copias de los documentos, datos o ficheros, archivos previa autorización, dejando constancia exhaustiva/completa de esta destrucción en el expediente de eliminación.

|   |                |  |
|---|----------------|--|
|  <p><b>Gobierno del Ecuador</b><br/>GUILLERMO LASSO<br/>PRESIDENTE</p> |                | <p><b>SEGURIDAD DE LA INFORMACIÓN</b></p> <p><b>PROCEDIMIENTO DE RESGUARDO, CONSERVACIÓN Y ELIMINACIÓN/DESTRUCCIÓN DE INFORMACIÓN.</b></p> |
| <b>Fecha:</b>   | <b>Página:</b> |  |
| 28/03/2023  | 9 de 11        |  |
| <b>ÁREA REQUIRIENTE:</b>  |                | <b>GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN</b>   |

- b) Si es parcial (afecta a una parte del sistema de almacenamiento) o total (afecta a todo el soporte de almacenamiento o sistema de almacenamiento).
- c) Realizar el borrado/destrucción de la información con los medios internos registrando la fecha, el tipo de borrado (eliminación - destrucción), contenido, técnico responsable, asignado y autorizado para la eliminación, ruta en donde se alojaba la información y el motivo para el efecto en una matriz custodiada por la Unidad de Gestión de Tecnologías de la Información y Comunicación y formalizada con las firmas correspondientes.
- d) Hay diversas aplicaciones que proporcionan estos algoritmos de borrado, tales como “Eraser” (aplicación para Windows con licencia GPL desarrollada por Heidi Computers Ltd.) o “EraserIT Loop” (desarrollada por Recovery Labs y certificada por el CCN).
- e) La forma y lugar de realización, el borrado seguro debe realizarse siempre por personal y con medios propios del organismo y en sus instalaciones. Únicamente en los casos en los que la institución se ve en situaciones de riesgo se puede considerar su externalización, dejando evidencia con los parámetros que anteceden.
- f) La Unidad debe emplear métodos de borrado/destrucción y el nivel borrado /destrucción de la información aplicables requerientes para el efecto.

### 5.1.3 Niveles de eliminación/destrucción de la información:

- a) Nivel 0: Borrado usando comandos/utilidades estándar del sistema operativo. Estas técnicas generalmente marcan el espacio ocupado por los archivos a borrar como disponible, pero no eliminan realmente el contenido almacenado. Por este motivo, no impide la recuperación posterior de la información borrada ni proporciona ninguna garantía frente a la revelación no autorizada de la información.
- b) Nivel 1: Borrado usando mecanismos de sobrescritura del espacio ocupado por los archivos a borrar. La recuperación de la información borrada sólo puede realizarse usando técnicas avanzadas.

|  |                |  |
|--|----------------|--|
|  <p><b>Gobierno del Ecuador</b><br/>GUILLERMO LASSO<br/>PRESIDENTE</p> |                | <p><b>SEGURIDAD DE LA INFORMACIÓN</b></p> <p><b>PROCEDIMIENTO DE RESGUARDO, CONSERVACIÓN Y ELIMINACIÓN/DESTRUCCIÓN DE INFORMACIÓN.</b></p> |
| <b>Fecha:</b>  | <b>Página:</b> |  |
| 28/03/2023   | 10 de 11       |  |
| <b>ÁREA REQUIRIENTE:</b>   |                | <b>GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN</b>   |

- c) Nivel 2: Borrado seguro. Impide la recuperación de la información borrada incluso utilizando mecanismos avanzados. Algunas de las técnicas que se pueden utilizar para realizar este borrado son: el borrado seguro mediante firmware; la sobrescritura de la información con protocolos que hagan imposible su reconstrucción (generalmente, mediante una serie consecutiva de sobrescrituras); o el cifrado de la información con criptografía fuerte y ofuscación de la clave de cifrada.
- d) Nivel 3: Destrucción física del soporte (destrucción segura): Se realiza por procesos industriales como: triturado, incineración, pulverización, fusión de los materiales de que constan los soportes y otros de similar naturaleza.

#### 5.1.4 Copias de seguridad o backup:

- a) Una copia de seguridad o respaldo (backup) no es una copia destinada a una actualización o consulta regular (como ocurre con un archivo de oficina), este tipo de archivos se recupera solamente en caso de incidentes de seguridad o pérdidas de información. En la mayoría de estos incidentes se produce la pérdida de la totalidad o la mayoría de la información.
- b) Desde este punto de vista, el que un documento eliminado pueda contener réplicas en varios archivos de respaldo o “backup” no representa un riesgo importante ya que, como se ha indicado, a estas copias se accederá sólo ocasionalmente (cuando se produzcan incidentes) y sin que se efectúen búsquedas selectivas de un archivo o documento concreto.
- c) Además, hay que tener en cuenta que las copias se van sobrescribiendo a medida que se realizan, eliminando las más antiguas de su tipo. En consecuencia, al finalizar un ciclo completo de copiado (por ejemplo, de un año) no quedará ya ninguna réplica de documentos/archivos que se eliminaron durante el año anterior.

## 6. Glosario

| <b>TÉRMINO</b> | <b>SIGNIFICADO</b>  |
|----------------|---|
| Backup         | Un backup es una copia de seguridad de los datos e información que se puede realizar a baja o alta escala.  |
| Firmware       | Se conoce como firmware al conjunto de instrucciones de un programa informático que se encuentra registrado en una memoria ROM, flash o similar.  |
| Sobrescritura  | Se refiere a la sustitución de datos antiguos por datos nuevos.   |
| Cifrado        | El cifrado en ciberseguridad es la conversión de datos de un formato legible a un formato codificado, proceso técnico por el cual la información se convierte en un código secreto que permite ocultar los datos que envías, recibes o almacenas. |
| Licencia GPL   | Licencia Pública General, es una licencia usada en el software libre y código abierto que garantiza a los usuarios libertad de usar, estudiar, compartir, modificar el software.  |
| Algoritmo      | Es un conjunto de instrucciones definidas, ordenadas y acotadas para resolver un problema, realizar un cálculo o desarrollar una tarea.   |
| EGSI           | Esquema Gubernamental de Seguridad de la Información.   |
| MINTEL         | Ministerio de Telecomunicaciones y de la Sociedad de la Información.  |
| NAS            | Dispositivo de Almacenamiento en Red o por sus siglas en inglés (NAS) Network Attached Storage, el cual permite el almacenamiento de archivos e información evitando pérdida de datos.  |
| Duplicati      | Duplicati es un cliente de copia de seguridad que almacena de forma segura copias de seguridad remotas cifradas, incrementales y comprimidas.   |
| TIC's          | Tecnologías de la Información y Comunicación.   |
| Eliminación    | Es un proceso de depuración de archivos, dicho proceso se lleva a cabo cuando el ciclo de vigencia de la información ha concluido.  |
| Destrucción    | Actividad encargada de la suprimir de forma segura toda la información, previa aprobación, en este proceso no se puede recuperar información.   |