POL-SSI-12

POLÍTICA DE RESPALDO DE LA INFORMACIÓN

PRESIDENCIA DE LA REPÚBLICA

Aprobado por: Julio Maiers Hechenleitner

Director Administrativo

NOTA DE SENSIBILIDAD Y PROPIEDAD INTELECTUAL

Tabla de Contenidos:

1. Objetivo.

Establecer los lineamientos que permitan brindar protección contra la pérdida de datos, con el propósito de asegurar la ejecución copias de la información, del software y de cualquier otro elemento del sistema que contenga datos que se consideren relevantes para la continuidad de las actividades institucionales.

2. Alcance.

El alcance de este documento aplica a todos los activos de información de la Presidencia de la República que se hayan determinado como críticos o relevantes en cuanto a la necesidad de disposición e integridad del mismo.

3. Roles y Responsabilidades.

- **Director Administrativo.**
  Responsable de liderar la implantación y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), asignando los recursos técnicos y humanos necesarios para mantener activo dicho sistema, mediante la promulgación de políticas internas que indiquen lineamientos y las obligaciones de las personas (usuarios) de la institución.

- **Integrantes del Comité de Seguridad de la Información.**
  Responsables de apoyar y gestionar la implementación de los requisitos de seguridad de la información del SGSI para el correcto y adecuado uso de los activos de información de la Institución.

- **Encargado de Seguridad de la Información.**
  Responsable de supervisar y coordinar las actividades de monitoreo, control y evaluación del SGSI de la institución para el cumplimiento de los requisitos de seguridad de la información.

- **Encargado de respaldo de datos**
  Responsable de realizar las actividades de respaldo y restauración de información institucional.

- **Coordinadores del SGSI**
  Responsables de gestionar el cumplimiento de los requisitos de seguridad del SGSI vinculados a su Departamento a través de la correcta aplicación de las políticas y procedimientos asociados.

- **Usuarios (personal de institución y personal externo).**
  Responsables de aplicar y cumplir las responsabilidades y/o tareas que tengan definidas en las políticas y procedimientos de seguridad de la información de la institución.

4. Definiciones (contenido).

La Presidencia de la República proporciona los recursos necesarios para la generación de copias de respaldo y posterior almacenamiento de su información crítica, siendo el Departamento de Tecnologías de la Información y la Comunicación (TIC) quien establece los procedimientos y mecanismos para la realización de estas actividades, y define la estrategia a seguir y los periodos de retención para el respaldo y almacenamiento de la información. Además, vela porque los medios que contienen los respaldos de la información crítica, sean almacenados en una ubicación diferente a la de origen. Las Áreas dueñas de la información, son responsables de alojar la información que consideren crítica en los contenedores definidos para tales efectos. Para asegurar el cumplimiento de los puntos anteriores, la Presidencia de la República declara que:

a) Se deben definir los tipos de respaldos a utilizar como estándar para la Institución. Este estándar debe considerar como base la frecuencia del respaldo, los medios de almacenamiento, el tipo de contenido, versiones y periodo de retención. Los procedimientos de respaldos se desarrollan de acuerdo a cada plataforma.

b) Se deben realizar pruebas de recuperación de respaldos en forma periódica, utilizando para ello su correspondiente ambiente de pruebas.

c) Los respaldos de la información crítica existente en los sistemas centrales, se deben realizar en un medio magnético confiable y debidamente rotulado, los que deben ser almacenados de manera segura fuera de las instalaciones donde se originaron.

d) Se deben generar las acciones necesarias de resguardo de la información ante un cambio tecnológico que se produzca en los medios de respaldo y que pueda generar obsolescencia tecnológica en los medios existentes. De la misma forma, los cambios severos en los archivos de sistemas aplicativos, deben necesariamente considerar el análisis de posibles migraciones en la información que se encuentre respaldada.

e) Se debe disponer de un sistema de repositorio centralizado, en el cual los usuarios tendrán espacios de almacenamiento individuales asignados. Cada usuario es responsable de almacenar la información institucional, que éstos administren o generen, en dicho repositorio.

f) Se debe contar con instalaciones de respaldo adecuadas, que permitan garantizar que toda la información y el software relevante o considerado crítico, pueda ser respaldado y en caso de ser necesario, pueda ser recuperado ante desastres o fallas.

g) Se debe definir un procedimiento documentado para el respaldo de información.

h) Se debe monitorear, registrar y documentar diariamente todas las actividades ejecutadas en el servidor de respaldo.

i) Se podrá reutilizar medios de respaldo, siempre y cuando la información almacenada en ellos hubiere cumplido el plazo de retención definido.

j) Se deben desechar los medios de respaldo que generen errores en el proceso o muestren alguna falla física, procediendo a efectuar un proceso de eliminación segura, registrándolo en el medio establecido (ver PRO-SSI-12).

k) Según se considere necesario, ya sea por solicitud de alguna Jefatura de Departamento o según el nivel de riesgos de la información relacionada, se realizan pruebas de restauración de datos de respaldo, asegurándose de no sobrescribir los medios originales, con el objeto de validar la integridad y confiabilidad de dicha información.

l) El periodo de retención de la información digital es de cuatro años.

5. Periodicidad de Evaluación y Revisión.

Los lineamientos y alcances contenidos en esta política son susceptibles de mejorar continuamente, por lo tanto, son factibles de someter a modificaciones, actualizaciones y cambios periódicos tendientes a mantenerla vigente y aplicable de acuerdo con las condiciones en que la institución se encuentre.

Sin perjuicio de lo anterior, se establece que la periodicidad ordinaria de revisión de esta política es **anual.**

6. Difusión.

La presente política y sus lineamientos estratégicos están disponibles al personal bajo el control de la Presidencia de la República y terceros, según corresponda.

El mecanismo de difusión de esta política es:

- Publicación en la Intranet institucional.
- Publicación en el Portal de transparencia institucional.

7. Control de Cambios.

Versión	Fecha	Principales revisiones y/o modificaciones	Nº de revisión	Elaborado por	Revisado por	Aprobado por (responsable del documento)
01	30.12.2015	Resolución Exenta n°2923 - Versión inicial.	01	Encargado de Seguridad de la Información.	Depto. de TIC.	Director Administrativo
02	02.11.2017	-Se actualiza incorpora codificación al presente documento, quedando "POL-SSI-09", producto de una nueva forma de identificar los documentos (todas las páginas, encabezado del documento) -Se incorpora la sección "2. Objetivo Principal" página 3, sección 2. Objetivo Principal. -Se incorporan las tablas "Objetivo y Productos estratégicos y Procesos Críticos en ámbito de aplicación del PMG-SSI PRESIDENCIA)" y "Alcance de Dominios y Controles de Seguridad de la Información asociados a este documento" (página 4, sección 2.-Alcance o Ámbito de Aplicación. -Se incorpora la sección "8. Lineamientos de la Política" página 5, sección 6. Lineamientos de la Política. -Se incorpora la sección Mecanismos de difusión, cambio observado en página 6, sección 8. Mecanismo de Difusión. -Se incorpora la sección Excepciones al cumplimiento, cambio observado en página 7, sección 9. Excepciones al cumplimiento. -Se posiciona al final del documento la tabla de Historial de versiones (control de cambios) incorporando en columna "Principales Modificaciones" el texto (Página / Sección) y se crea una nueva columna denominada "Motivo del Cambio", (página 7, sección 10.-Historial de versiones (control de cambios).	02	Encargado de Seguridad de la Información.	Depto. de TIC.	Director Administrativo
03	19.11.2018	- Se modifica Sección alcance (página 3)	03	Encargado de Seguridad de la Información.	Depto. de TIC.	Director Administrativo
04	13.11.2019	-Se ajusta nombre codificación y contenido de política según los requisitos del control NChISO27001 12.3.1 y un nuevo orden establecido para el SGSI institucional. -El presente documento se aprueba bajo firma electrónica del Director Administrativo.	04	Encargado de Seguridad de la Información.	Jefatura Depto. de TIC.	Director Administrativo