

Ministerio Secretaría General de la Presidencia	POLÍTICA DE RESPALDO DE LA INFORMACIÓN	Versión N° 4.3 Año 2023
		1

Controles NCH ISO 27001:2013 Relacionados

CONTROL	NOMBRE
A.12.03.01	Respaldo de la Información

Nota de confidencialidad

La información contenida en este documento es de uso exclusivo de la Institución y su personal. Cualquier uso no autorizado por terceros, copia o distribución de la información está estrictamente prohibido.

Ministerio Secretaría General de la Presidencia	POLÍTICA DE RESPALDO DE LA INFORMACIÓN	Versión N° 4.3 Año 2023
		2

Control de versiones

FECHA	VERSIÓN	RESPONSABLES	DESCRIPCIÓN
15.06.2016	1.0	Marcelo Aliaga Q. Liliana Reyes G.	Elaboración de documentos.
05.10.2016	1.1	Marcelo Aliaga Q. Liliana Reyes G.	Modificación de texto y configuración de documentos.
17.10.2016	1.2	Marcelo Aliaga Q. Liliana Reyes G.	Modificación formato portada, tabla, control de versiones, marcos de imágenes, objetivo de control.
13.10.2014	2.0	Marcelo Aliaga Q. Liliana Reyes G.	Modificación de contenidos en base a documento "Estrategia de Trabajo SSI 2017". Se incorporan títulos: Alcance, Objetivo, Roles y responsabilidades, Mecanismo de difusión, Evaluación y revisión. Se incorpora en pág.4 punto 6 Evaluación y revisión (...) "No obstante podrá revisarse cuando la situación amerite a la autoridad lo disponga". Se agrega en pág.9 Título "Formato de registro" e imagen.
11.10.2018	3.0	Jorge Romero V. Solange Godoy C.	En Introducción, se eliminaron Controles A.08.03.02, A.11.02.07 y A.18.01.03. Se completan "objetivo" y "alcance". Se desagregan los Roles y se incorpora responsabilidad del Encargado de Seguridad de la Información en sección 4. "Roles y responsabilidades". Actualización de políticas incorporando título Definiciones. Responsabilidad del Encargado de Seguridad de la Información en Sección 6. Se modifica mecanismo de difusión. En "Marco normativo", se eliminó D.S 81/2014 y D.S 77/2014. Sección 9. "Consideraciones Generales", se incorporan 4 puntos.

Ministerio Secretaría General de la Presidencia	POLÍTICA DE RESPALDO DE LA INFORMACIÓN	Versión N° 4.3 Año 2023
		3

11-10-2019	4.0	Jorge Romero Vargas Solange Godoy Carrera	Cambia estructura de acuerdo a guía metodológica. Se mejora redacción a Roles y Responsabilidades. Marco normativo se cambia al final de definiciones. Se elimina: - Numeración a Marco normativo; Medios de respaldo; Especificación de tipo de respaldo. - Se elimina Título Consideraciones Generales. - En definiciones se incorpora; "El largo de los nombres...". "En el nombre de los...". Puede reemplazar los...". Para facilitar la..." - Control, cambia nombre jefatura DAG y Pie de firma de Jefe Departamento de Informática o Unidad de Tecnologías de la Información.
30-11-2021	4.1	Jorge Romero	Actualiza sección firmantes. Menciona privilegiar el almacenamiento en la nube en caso de eventos disruptivos. Incluye días de almacenamiento como política institucional para el almacenamiento de registros de video vigilancia. Actualiza medio de respaldo en la nube.
15-11-2022	4.2	Jorge Romero	Actualización sección firmantes. Incorpora tiempo de retención de respaldos. Especifica el uso de carpetas de usuarios como respaldo en la nube. Incorpora mecanismo de denuncias y notificaciones por incumplimiento.
11-08-2023	4.3	Jorge Romero	Modifica Jefe Unidad de Tecnologías de la Información por Encargado Área de Tecnologías de la Información. Modifica Unidad de Tecnologías de la Información por Área de Tecnologías de la Información. Especifica el tipo de

Ministerio Secretaría General de la Presidencia	POLÍTICA DE RESPALDO DE LA INFORMACIÓN	Versión N° 4.3 Año 2023
		4

			respaldo a realizar en la sección definiciones.
--	--	--	---

1. Introducción

El Ministerio Secretaría General de la Presidencia en adelante “el Ministerio”, dispone del presente documento, “Política de Respaldo de la Información”, como parte integrante del sistema de seguridad de la información. En específico, se enmarca en el cumplimiento de la NCH ISO 27001, que propone como requisito de control:

Control A.12.03.01 Respaldo de la Información

“Se deben hacer copias de respaldo y pruebas de información, del software y de las imágenes del sistema con regularidad, de acuerdo con la política de respaldo acordada”.

- Requisito control A.12.03.01 NCH ISO 27001:2013

2. Objetivo

El objetivo de la Política de Respaldo de la Información, es establecer las directrices que rigen las acciones en la reutilización o descarte de equipos y en el respaldo de la información, para proteger esta información contenida en el Ministerio Secretaría General de la Presidencia. Esta política brinda protección contra la pérdida de datos, softwares contenidos en los dispositivos hardware, entre otras.

3. Alcance

Este documento, se aplicará a todas las cuentas de usuario de este Ministerio, ya sean de funcionarios/as de planta, a contrata, a honorarios, alumnos en práctica y terceras personas que puedan estar prestando servicios en el Ministerio a los que se les asigna equipos y que requieran el uso de sistemas y servicios de información contenida en servidores, estaciones de trabajo y equipos de comunicaciones que incluya datos, configuraciones, aplicativos, sistemas y todo servicio crítico para el Ministerio.

4. Roles y responsabilidades

Independiente del cargo/rol que se desempeñe, del nivel jerárquico del que se goce y de la modalidad bajo la cual se esté contratado, es responsabilidad de todo el personal de este Ministerio conocer y dar debido cumplimiento a la Política de Respaldo de la información. Asimismo, se establecen las siguientes responsabilidades respecto de esta política:

- **Comité de Seguridad de la Información:** Velar por la periodicidad de su revisión, así como su cumplimiento, actualización y difusión.

Ministerio Secretaría General de la Presidencia	POLÍTICA DE RESPALDO DE LA INFORMACIÓN	Versión N° 4.3 Año 2023
		5

- **Encargado/a de Seguridad de la Información:** Monitorear el cumplimiento de esta política, así como promover y supervisar el estricto apego de sus funcionarios/as y trabajadores a esta norma.
- **Jefes/as de División/Comisión/Unidad:** Aplicar, dar cumplimiento, promocionar y supervisar esta norma en las personas a su cargo.

5. Mecanismo de difusión

Es responsabilidad del Comité de Seguridad de la Información, la difusión de la Política de Respaldo de la Información, la que deberá permanecer en la Intranet institucional a disposición de todo el personal del Ministerio.

6. Evaluación y revisión

El/la Encargado/a de Seguridad de la Información, comunicará en la sesión respectiva al Comité de Seguridad de la Información los cambios y/o actualizaciones de esta Política. El Comité de Seguridad de la Información por su parte, revisará, observará y aprobará esta política según la normativa vigente y lineamientos establecidos por la institución.

7. Definiciones

El Ministerio conservará los respaldos de la configuración de los servidores de aplicaciones, bases de datos, correos electrónicos, información de usuarios/as desvinculados/as por el tiempo que sea necesario o a requerimiento de esta Secretaría de Estado.

Para el mejor desarrollo de su función, el Ministerio, asignará un equipo computacional al personal contratado en las diversas modalidades ya sea planta, contrata, honorarios, alumnos en práctica y terceros que presten servicios en la institución, cuando la jefatura directa lo solicite.

Cada equipo contará con una carpeta de trabajo conectada al servicio de computación en la nube de la institución. Esta carpeta será respaldada automáticamente como parte del servicio contratado, permitiendo un manejo de versiones, generar una indexación del contenido para búsquedas, además de mejorar el acceso, disponibilidad de la información desde cualquier lugar y recuperación de información.

Adicionalmente existirán otros respaldos relacionados a:

- Sistemas
- Bases de datos
- Portales web
- Correos electrónicos
- Equipos computacionales

Los respaldos de equipos computacionales se deberán llevar a cabo por las siguientes situaciones:

Ministerio Secretaría General de la Presidencia	POLÍTICA DE RESPALDO DE LA INFORMACIÓN	Versión N° 4.3 Año 2023
		6

- Cambio de equipo de usuario/a, para nueva asignación
- Solicitud de jefatura de el/la usuario/a al Área de Tecnologías de la Información

Es importante considerar los siguientes puntos respecto a los respaldos en esta Secretaría de Estado.

Se deberá realizar un respaldo de tipo completo o total, generando una copia exacta de todo el conjunto de datos.

Cada funcionario/a o colaborador/a deberá contar con una cuenta asociada a una carpeta individual en el servicio de almacenamiento en la nube de la institución, en adelante "Carpeta de trabajo", la que será visible en el directorio de archivos de su equipo computacional.

La referida carpeta de trabajo deberá ser de acceso único por parte de el/la funcionario/a o colaborador/a mediante sus credenciales de acceso al equipo computacional o desde internet accediendo directamente al servicio de almacenamiento en la nube institucional.

Toda información de carácter personal que se encuentre en los equipos computacionales al momento del proceso de respaldo no deberá ser incluida.

La información confidencial que sea respaldada deberá protegerse mediante un mecanismo de cifrado u otra técnica de encriptación.

El Área de Tecnologías de la Información, junto a su jefatura directa, establecerán el tiempo de retención de copia de seguridad y procedimientos a seguir para la destrucción o eliminación de la información contenida en el respaldo. Las jefaturas directas serán responsables de la revisión, valor y utilidad de la información almacenada y/o respaldada.

Cada funcionario/a o colaborador/a deberán contar con un equipo asignado por el Ministerio para desempeñar de mejor forma sus funciones según lo solicitado por su jefatura directa.

Cada funcionario/a o colaborador/a deberán mantener sus archivos de trabajo en la Carpeta de trabajo asignada para tal efecto.

Cada funcionario/a o colaborador/a deberán contar con una casilla de correo electrónico institucional para mejor desempeño de sus labores asociada al servicio de almacenamiento en la nube.

El personal deberá salvaguardar la información que genere en el desarrollo de las actividades propias del cargo, para que esta se encuentre disponible en todo momento.

Ministerio Secretaría General de la Presidencia	POLÍTICA DE RESPALDO DE LA INFORMACIÓN	Versión N° 4.3 Año 2023
		7

El personal del Ministerio deberá conocer y cumplir la política de seguridad de la información, la cual se encuentra publicada en la Intranet Institucional y será dada a conocer junto con las demás políticas y procedimientos relacionados mediante correo electrónico de manera masiva al menos una vez al año, con el fin de resguardar los atributos esenciales de los activos de información institucionales.

Los grupos de trabajo, unidades y otros equipos ad-hoc creadas para una labor específica, podrán contar con carpetas compartidas de acceso grupal, mediante un servicio de almacenamiento en la nube para esos fines. Este espacio de trabajo deberá ser solicitado al Área de Tecnologías de la Información para su configuración, habilitación y establecimiento de permisos. Las ediciones de documentos en carpetas compartidas en el servicio de almacenamiento en la nube podrán ser realizadas de manera directa en este recurso. Será responsabilidad de cada persona usuaria, llevar el debido control de versiones del documento que trabaje de forma local en el equipo computacional y realizar la consolidación de la información trabajada en esta modalidad.

El Área de Tecnologías de la Información es la encargada de dar cumplimiento a este procedimiento de respaldo.

En caso de situaciones excepcionales, como robo de equipamiento o eventualidad técnica, el respaldo deberá corresponder a la última la sincronización de datos desde el equipo local hacia el servicio de respaldo en la nube, para lo cual el equipo computacional deberá estar conectado a internet.

El largo de los nombres de los documentos y carpetas no deberían superar los 30 caracteres.

En el nombre de los documentos y carpetas, no se deberá utilizar tildes, ni espacios entre palabras.

Puede reemplazar los espacios por guion bajo “_”.

Para facilitar la legibilidad, las palabras que no se separen por guion bajo se sugiere utilizar notación CamelCase, que corresponde a poner mayúsculas en cada inicio de palabra (por ejemplo, EsteEsUnDocumento).

Todo lo anterior, con el fin de facilitar las operaciones de respaldo y recuperación de información.

La Carpeta de trabajo, deberá ser un respaldo de la información contenido en su equipo personal designado para sus funciones.

Se deberá almacenar la información en el servicio de respaldo en la nube proporcionado por la institución, con el fin de mitigar riesgos de pérdida de información por eventos disruptivos ya sea por

Ministerio Secretaría General de la Presidencia	POLÍTICA DE RESPALDO DE LA INFORMACIÓN	Versión N° 4.3 Año 2023
		8

daño en hardware o contaminación por virus que puedan provocar daños irreparables en la documentación.

Tiempo de retención

Se deberá establecer un tiempo máximo de retención de respaldo de información histórica, el cual no deberá sobrepasar los 6 años. Esta información deberá ser organizada y resguardada en un repositorio de infraestructura en la nube, aplicable a la siguiente información:

- Respaldo de bases de datos
- Respaldo de sistemas
- Respaldo de portales
- Respaldo de documentos de usuarios/as
- Respaldo de correos electrónicos de usuarios/as

Cumplido el tiempo de retención la información de respaldo deberá ser eliminada por el Área de Tecnologías de la Información, mediante un acto administrativo, especificando el tipo de respaldo y contenido.

El almacenamiento de información, para cámaras de video vigilancia mediante dispositivo DVR de las dependencias de la institución, deberá mantener registros hasta 25 días corridos. El proceso de grabación de video deberá ser realizado de forma continua y sin descanso para todas las entradas de vídeo que reciben en las dependencias de la institución. Una vez que los discos duros que almacenan esta información se encuentran llenos, los registros más antiguos deberán ser sobre escritos automáticamente para dejar espacio a los más actuales.

Medios de respaldo

Los respaldos deberán ser realizados en tres tipos de medios, dependiendo de las necesidades que se requieran y del tiempo en que se necesite resguardar la información:

Disco: Información que no sea necesario mantener el histórico de la información. Posee la capacidad necesaria para almacenar los datos del respaldo como primer destino para respaldar en otro medio.

Almacenamiento en la Nube: Información que se debe mantener por periodos más largos. Este proceso se realiza en un servidor destinado al almacenamiento de respaldos en la nube.

Blue - Ray: Información correspondiente a el/la usuario/a específicamente.

Ministerio Secretaría General de la Presidencia	POLÍTICA DE RESPALDO DE LA INFORMACIÓN	Versión N° 4.3 Año 2023
		9

Los medios de respaldo señalados se deberán mantener en resguardo en el Área de Tecnologías de la Información del Ministerio.

Especificación de Tipo de Respaldo

El Área de Tecnologías de la Información del Ministerio Secretaría General de la Presidencia deberá realizar dos tipos de respaldos asociado a funcionarios/as y equipos, que se detallan a continuación:

- Carpeta de trabajo
- Equipo Computacional

Los tipos de respaldo se detallan a continuación:

Carpeta de trabajo: Cada funcionario/a deberá contar con una Carpeta de trabajo. Esta carpeta deberá contener los documentos que el funcionario/a ha creado o editado referente a sus funciones. Respecto al respaldo de la Carpeta de trabajo cabe consignar que:

- La carpeta deberá estar conectada al servicio de almacenamiento en la nube que dispone la institución.
- Se deberá realizar el respaldo de manera automática
- Una vez finalizado el vínculo con la organización, se podrá disponer si es solicitado una copia del respaldo realizado al superior jerárquico de el/la usuario/a. El cual contendrá, la información almacenada en el equipo computacional al momento de su entrega y correo electrónico institucional. El Área de Tecnologías de la Información deberá almacenar el respaldo en un repositorio de almacenamiento en la nube destinado para este fin.
- Cada funcionario/a o colaborador/a poseerá un espacio de almacenamiento en la nube asociado a su cuenta de correo institucional.
- El/la funcionario/a o colaborador/a podrá realizar un respaldo de información del trabajo diario institucional y/o podrá trabajar directamente desde esta fuente de información.
- Esta información se encontrará respaldada en la nube del proveedor de servicios contratado y será administrado por el Área de Tecnologías de la Información.

Equipo Computacional:

- La jefatura deberá informar tanto al Área de Tecnologías de la Información como a la Unidad de Gestión y Desarrollo de las Personas, el cese de funciones de un/a usuario/a, de modo de iniciar el proceso.
- El Área de Tecnologías de la Información deberá almacenar el respaldo en un repositorio de almacenamiento en la nube destinado para este fin.
- El proceso de respaldo contemplará solo la información existente en el equipo computacional.
- Posterior a la generación del respaldo, se podrá entregar una copia a la jefatura directa de el/la funcionario/a o colaborador/a en caso de ser requerido.

Ministerio Secretaría General de la Presidencia	POLÍTICA DE RESPALDO DE LA INFORMACIÓN	Versión N° 4.3 Año 2023
		10

Formulario de Generación de Respaldo

Para la realización de respaldo de equipos, la acción deberá ser requerida por la jefatura respectiva o por el/la funcionario/a o colaborador/a, a través de solicitud realizada al Área de Tecnologías de la Información. Cada solicitud deberá ser formalizada a través del formulario de Generación de Respaldo. Este formulario deberá contar con la autorización de la jefatura directa de el/la funcionario/a o colaborador/a.

Seguridad en la reutilización o descarte de equipos

Se deberá verificar el equipo para asegurar que no contengan medios de almacenamiento antes de su eliminación o reutilización. Los medios de almacenamiento que contengan información sensible o con derecho de autor se deberá destruir, eliminar o sobrescribir mediante técnicas para hacer que la información original no se pueda recuperar en vez de utilizar la función de eliminación o formateo normal.

Denuncias y notificaciones

Para efectos de denuncias de alguna mala práctica o incumplimiento de esta política podrá enviar un correo electrónico a ssi@minsepres.gob.cl o dirigirse directamente a el/la Encargado/a del Área de Tecnologías de la Información para tomar las acciones pertinentes.

Marco normativo

Este procedimiento se enmarca y considera el siguiente marco normativo.

- Ley N° 19.799, del 2002, Sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, del Ministerio de Economía, Fomento y Reconstrucción.
- Decreto 181/2002, Aprueba Reglamento de la Ley N° 19.799 Sobre documentos electrónicos, firma electrónica y la certificación de dicha firma, del Ministerio de Economía, Fomento y Reconstrucción.
- Ley N° 20.285, del 2008, Sobre acceso a la información pública, del Ministerio Secretaría General de la Presidencia.
- Decreto 13/2009, Reglamento de la Ley N° 20.285, Sobre acceso de la información pública, del Ministerio Secretaría General de la Presidencia.
- Ley 19.628, de 1999, Sobre protección a la vida privada.
- Ley 17.336, de 1970, Sobre propiedad intelectual, y sus actualizaciones, del Ministerio de Educación.
- Ley 21.459, de 2022, Establece normas sobre delitos informáticos, deroga la Ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest, del Ministerio de Justicia y Derechos Humanos.
- Ley N° 21.180, sobre transformación digital del estado.

Ministerio Secretaría General de la Presidencia	POLÍTICA DE RESPALDO DE LA INFORMACIÓN	Versión N° 4.3 Año 2023
		11

- Decreto Supremo 83/2004, Aprueba norma técnica para los Órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos, del Ministerio Secretaría General de la Presidencia.
- Decreto Supremo 93/2006, Aprueba norma técnica para la adopción de medidas destinadas a minimizar los efectos perjudiciales de los mensajes electrónicos masivos no solicitados recibidos en las casillas electrónicas de los organismos de la Administración del Estado y de sus funcionarios/as, del Ministerio Secretaría General de la Presidencia.
- Normas Chilenas ISO 27001 y 27002.

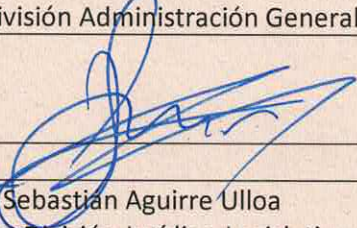
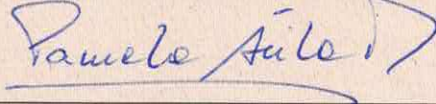
Ministerio Secretaría General de la Presidencia	POLÍTICA DE RESPALDO DE LA INFORMACIÓN	Versión N° 4.3 Año 2023
		12

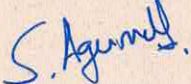
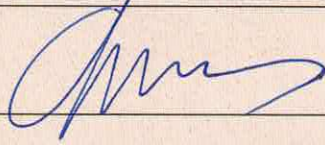
8. Control

Elaborado por: Jorge Romero Vargas

Fecha: 11-08-2023

Comité de Seguridad de la Información, Ministerio Secretaría General de la Presidencia

Samir Toro Garrido Jefe División Administración General	Pamela Ávila Rubio Jefa Unidad de Control de Gestión
	

Sebastián Aguirre Ulloa Asesor División Jurídico-Legislativa	Christian Valenzuela Lorca Jefe Gabinete de la Subsecretaria
	

Fabiola Vidal Oyarzún Asesor Comisión de Integridad y Transparencia	José Inostroza Lara Jefe División de Gobierno Digital
	

Jorge Romero Vargas Oficial de Seguridad de la Información Encargado Área de Tecnologías de la Información


Fecha: 11-08-2023
