

Ministerio Secretaría General de la Presidencia	PROCEDIMIENTO DE CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	Versión N° 1.1 Año 2023
		1

Controles NCH ISO 27001:2013 Relacionados
Derivado de Política de Continuidad de la Seguridad de la Información

CONTROL	NOMBRE
A.17.01.02	Implementación de la continuidad de la seguridad 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	PROCEDIMIENTO DE CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	Versión N° 1.1 Año 2023
		2

Control de versiones

FECHA	VERSIÓN	RESPONSABLES	DESCRIPCIÓN
30-09-2019	1.0	Jorge Romero Vargas Solange Godoy Carrera	Elaboración de documentos
10-11-2023	1.1	Jorge Romero	Actualización sección firmantes. 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. Incorpora lenguaje inclusivo en el documento. Complementa sección definiciones, objetivo, alcance, roles y responsabilidades.

Ministerio Secretaría General de la Presidencia	PROCEDIMIENTO DE CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	Versión N° 1.1 Año 2023
		3

1. Introducción

El Ministerio Secretaría General de la Presidencia dispone del presente documento, “Procedimiento de Continuidad de la Seguridad 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.17.01.02 Implementación de la continuidad de la seguridad de la información

“La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa”.

- Requisito control A.17.01.02 NCH ISO 27001-2013

2. Objetivo

El objetivo de este procedimiento es garantizar en el Ministerio la continuidad de la seguridad de la información. Para ello, se implementarán controles de mitigación ante posibles incidentes, los cuales deberán ser verificados, revisados y evaluados de manera periódica para confirmar su eficacia frente a cualquier situación que comprometa la seguridad de la información.

3. Alcance

El alcance de este procedimiento abarca todos los sistemas operativos y medios tecnológicos de información del Ministerio. Su finalidad es mitigar los daños potenciales de cualquier evento que comprometa la continuidad de la información.

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 al Procedimiento de Continuidad de la Seguridad de la Información, asimismo, es responsabilidad de:

- Encargado/a Área de Tecnologías de la Información

Asegurar que la infraestructura y las soluciones tecnológicas de la institución respalden efectivamente la continuidad de la seguridad de la información. Este procedimiento comienza con la colaboración con el Encargado/a de Seguridad de la Información para integrar las políticas de seguridad con la tecnología. Enfocarse en la implementación y el mantenimiento de sistemas tecnológicos críticos como los de respaldo y recuperación de datos, asegurando que estén actualizados y sean robustos. Realización de pruebas regulares de los sistemas para garantizar su efectividad en situaciones adversas. Paralelamente, gestionar la evaluación de riesgos tecnológicos y coordina la capacitación de funcionarios/as y colaboradores en el uso seguro de la tecnología.

Ministerio Secretaría General de la Presidencia	PROCEDIMIENTO DE CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	Versión N° 1.1 Año 2023
		4

Encargado/a de la Seguridad de la Información

Liderar el desarrollo y la implementación de estrategias de continuidad de la seguridad de la información. Este rol implica la identificación y gestión de riesgos, la supervisión del cumplimiento de estándares, y la coordinación eficaz con otros centros de responsabilidad para garantizar que las medidas de seguridad sean adecuadas y efectivas. Dar respuesta y recuperación ante incidentes, asegurando la resiliencia y la continuidad de las operaciones.

- Comité de Seguridad de la Información

Supervisión y revisión de las políticas y prácticas de continuidad de la seguridad. Participar en la gobernanza y mejora continua de los procesos de seguridad, facilitando la comunicación y concienciación en toda la institución. Coordinación en la respuesta a incidentes y el mantenimiento de una comunicación efectiva con autoridades, asegurando que los enfoques de gestión de riesgos y continuidad estén en línea con los objetivos estratégicos de la institución.

Operador/a

Funcionario/a o Trabajador/a del Área de Tecnologías de la Información quien es destinado para realizar una operación específica.

5. Definiciones y modo de operación

El Procedimiento de Continuidad de Seguridad de la Información contempla los siguientes sub procesos:

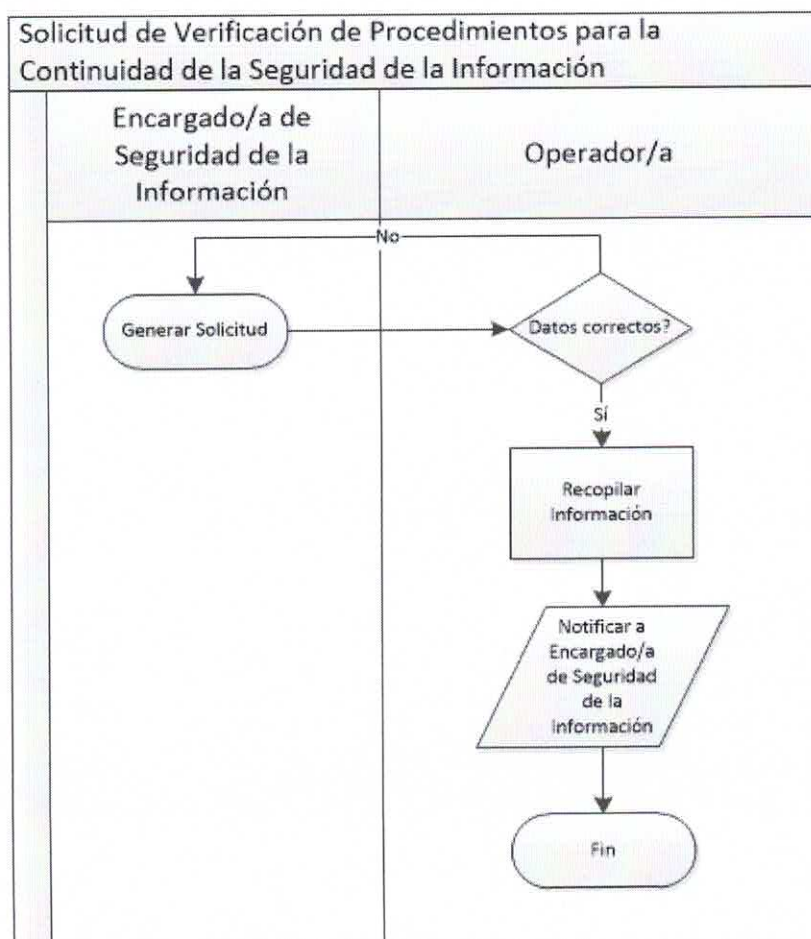
- Solicitud de Verificación de Procedimientos para la Continuidad de la Seguridad de la Información
- Solicitud de Desarrollo o Actualización de Procedimientos para la Continuidad de la Seguridad de la Información

Ministerio Secretaría General de la Presidencia	PROCEDIMIENTO DE CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	Versión N° 1.1 Año 2023
		5

Sub Proceso: Solicitud de Verificación de Procedimientos para la Continuidad de la Seguridad de la Información

Control: A.17.01.02 Implementación de la continuidad de la seguridad de la información

El/la Encargado/a de seguridad de la Información solicitará a el/la operador/a realizar la verificación de procedimientos para asegurar la continuidad de la seguridad de la información. Para ello, deberá indicar el nombre del procedimiento. En base a esto verificar la aplicabilidad para garantizar el nivel necesario para mantener la continuidad y asegurar mantener una estructura de administración con personal que posea la autoridad, experiencia y competencia necesaria. Por otra parte, verificar la nominación de personal de respuesta ante incidentes que posean la responsabilidad, autoridad y competencia necesaria para administrar un incidente manteniendo la seguridad de la información.



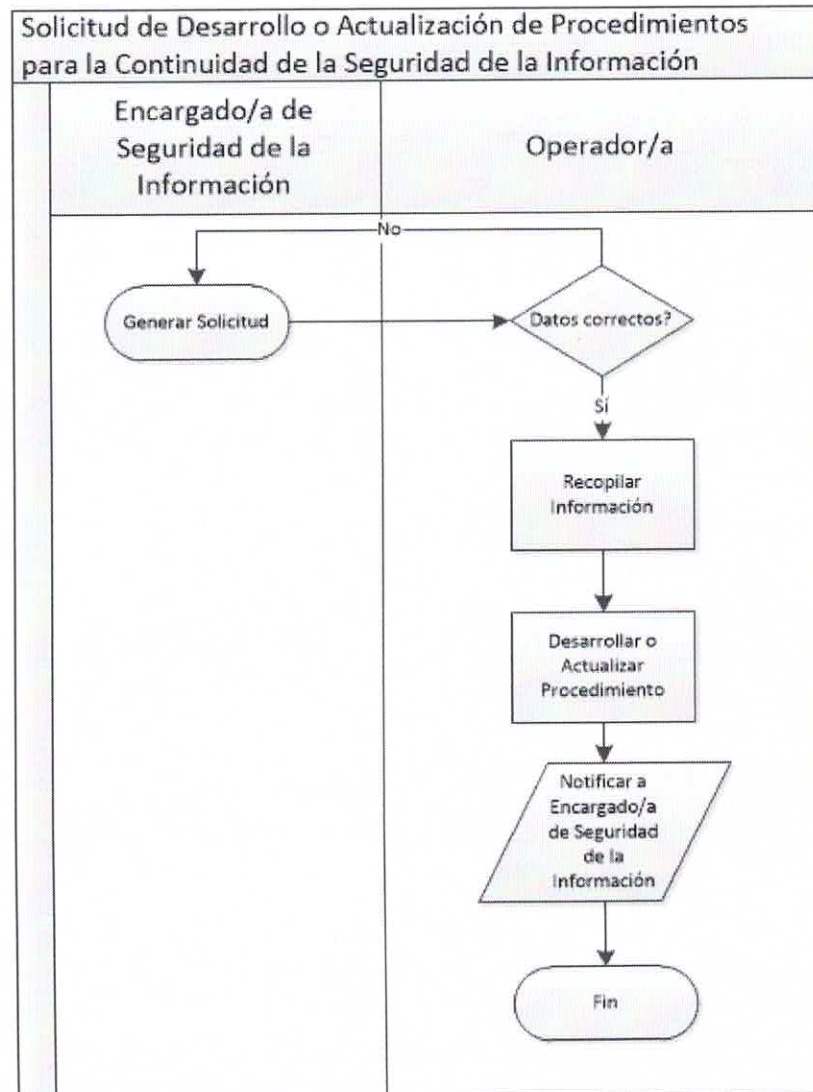
Descripción de actividades: El/la Encargado/a de seguridad de la Información genera una Solicitud de Verificación de Procedimientos para la Continuidad de la Seguridad de la Información, la cual será enviada a el/la operador/a quien validará los datos y realizará la recopilación de información notificando posteriormente al Encargado/a de seguridad de la Información.

Ministerio Secretaría General de la Presidencia	PROCEDIMIENTO DE CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	Versión N° 1.1 Año 2023
		6

Sub Proceso: Solicitud de Desarrollo o Actualización de Procedimientos para la Continuidad de la Seguridad de la Información

Control: A.17.01.02 Implementación de la continuidad de la seguridad de la información

El/la Encargado/a de seguridad de la Información solicitará a el/la operador/a el desarrollo o actualización de procedimientos para la continuidad de la seguridad de la información. Se deberá verificar la aplicabilidad en cómo la organización administra un evento disruptivo, involucra a especialista en seguridad de la información, incorpora los controles de seguridad dentro de los procesos, procedimientos, sistemas y herramientas de apoyo. Evaluar posibilidad de incorporar controles de compensación para otros controles que no se puedan mantener durante situaciones adversas y cómo funcionan en estos ámbitos.



Descripción de actividades: El/la Encargado/a de seguridad de la Información genera una Solicitud de Desarrollo o Actualización de Procedimientos para la Continuidad de la Seguridad de

Ministerio Secretaría General de la Presidencia	PROCEDIMIENTO DE CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	Versión N° 1.1 Año 2023
		7

la Información, la cual será enviada a el/la operador/a quien validará los datos y realizará la recopilación de información, desarrollará o actualizará el procedimiento y finalmente notificará a el/la Encargado/a de seguridad de la Información.

6. Registro de operación

Sub Proceso: Solicitud de Verificación de Procedimientos para la Continuidad de la Seguridad de la Información

Control: A.17.01.02 Implementación de la continuidad de la seguridad de la información

Formulario: CON-01



CON-01
Área de Tecnologías de la Información
**Solicitud de verificación de procedimientos para
la continuidad de la seguridad de la información**
A.17.01.02

Fecha:

Solicitante Encargado/a de Seguridad de la Información

Nombre:

RUT:

Nombre del procedimiento:

Verificar

- ☐ Aplicabilidad de procedimientos para garantizar el nivel necesario para la continuidad de la seguridad de la información.
- ☐ Estructura de administración con personal que posea la autoridad, experiencia y competencia necesaria.
- ☐ Nominación de personal de respuesta ante incidentes con la responsabilidad, la autoridad y la competencia necesaria para administrar un incidente y mantener la seguridad de la información.

Observaciones:

Firma

Operado por

Nombre:

RUT:

Firma

Ministerio Secretaría General de la Presidencia	PROCEDIMIENTO DE CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	Versión N° 1.1 Año 2023
		8

Sub Proceso: Solicitud de Desarrollo o Actualización de Procedimientos para la Continuidad de la Seguridad de la Información

Control: A.17.01.02 Implementación de la continuidad de la seguridad de la información

Formulario: CON-02



CON-02
Área de Tecnologías de la Información
**Solicitud de desarrollo o actualización de procedimientos
para la continuidad de la seguridad de la información**
A.17.01.02

Fecha:

Solicitante Encargado/a de Seguridad de la Información

Nombre:

RUT:

Nombre del procedimiento:

☐ Desarrollo ☐ Actualización

Descripción:

Verificar aplicación de:

- ☐ Como la organización administra un evento disruptivo y mantendrá la seguridad de la información a un nivel predeterminado.
- ☐ Involucrar a especialistas de seguridad de la información.
- ☐ Incorporación de controles de seguridad de la información dentro de la continuidad de los procesos, procedimientos y sistemas y herramientas de apoyo.
- ☐ Incorporación de procesos, procedimientos y cambios de implementación para mantener los controles de seguridad de la información existentes durante una situación adversa.
- ☐ Incorporación de controles de compensación para los controles de seguridad de la información que no se puede mantener durante una situación adversa.
- ☐ Si los controles de seguridad no pueden continuar resguardando la información, se deberían establecer, implementar y mantener otros controles para mantener un nivel aceptable de seguridad de la información.
- ☐ Los controles de seguridad de la información que se han implementado deberían seguir funcionando durante una situación adversa.

Operado por

Nombre:

RUT:

Firma

Ministerio Secretaría General de la Presidencia	PROCEDIMIENTO DE CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	Versión N° 1.1 Año 2023
		9

7. Documentos relacionados

Este procedimiento está relacionado directamente con controles contenidos en la Política de Continuidad de la Seguridad de la Información, documento vigente, del Ministerio Secretaría General de la Presidencia.

8. Indicador

El indicador mide la ejecución del procedimiento y sub procesos en base a las solicitudes que se ingresan y son atendidas en general.

Meta anual: 80%

Fórmula de cálculo:

$$(\text{N}^{\circ} \text{ de solicitudes realizadas} / \text{N}^{\circ} \text{ de solicitud recibidas}) * 100$$

Plazo de ejecución: < 24 horas de recibida la solicitud

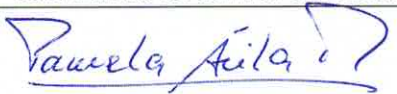
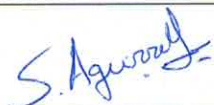
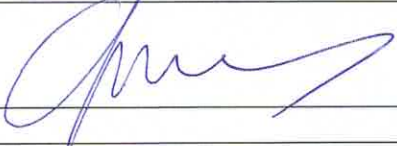
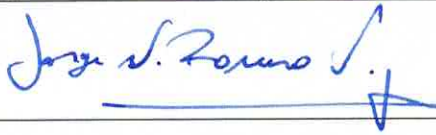
Ministerio Secretaría General de la Presidencia	PROCEDIMIENTO DE CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	Versión N° 1.1 Año 2023
		10

9. Control

Elaborado por: Jorge Romero Vargas

Fecha: 10-11-2023

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: 10-11-2023	