Controles NCH ISO 27001:2013 Relacionados

CONTROL	NOMBRE
A.16.01.01	Responsabilidades y procedimientos
A.16.01.02	Informe de eventos de seguridad de la información
A.16.01.03	Informe de las debilidades de seguridad de la información
A.16.01.04	Evaluación y decisión sobre los eventos de seguridad de la información
A.16.01.05	Respuesta ante incidentes de seguridad de la información
A.16.01.06	Aprendizaje de los incidentes de seguridad de la información
A.16.01.07	Recolección de evidencia

CONTROL DE VERSIONES

CONTROL A.16.01.04 Evaluación y decisión sobre los eventos de seguridad de la información

FECHA	VERSIÓN	RESPONSABLES	DESCRIPCIÓN
16-06-2016	1.0	Marcelo Aliaga Q. Liliana Reyes G.	Elaboración de procedimiento
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
13-10-2017	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. 3 punto 6 Evaluación y revisión (...) "No obstante, podré revisarse cuando la situación amerite o la autoridad lo disponga".
11-10-2018	3.0	Jorge Romero V. Solange Godoy C.	Sección 1 se corrige control mencionado en introducción de A.09.04.02 POR A.16.01.04. Actualización de política incorporando título Definiciones. Se cambió nombre a archivo de política a procedimiento. Se agregó rol de Encargado de Seguridad de la Información. Se complementó sección 3. Sección 4 se desagregaron roles y responsabilidades. Se agrega sección 11 flujograma de registro de incidente.
30-05-2019	4.0	Jorge Romero V. Solange Godoy C.	Se agregan controles A.16.01.01 Responsabilidades y procedimientos A.16.01.02 Informe de eventos de seguridad de la información A.16.01.03 Informe de las debilidades de seguridad de la información A.16.01.05 Respuesta ante incidentes de seguridad de la información A.16.01.06 Aprendizaje de los incidentes de seguridad de la información A.16.01.07 Recolección de evidencia
27-08-2020	4.1	Jorge Romero V.	Mejora en formato de registros.

Introducción

El Ministerio Secretaría General de la Presidencia, dispone del presente documento denominado "Procedimiento Evaluación y Decisión de los Eventos de Seguridad de la Información", como parte integrante del Sistema de Seguridad de la Información. En específico, se enmarca en el cumplimiento de la Norma Chilena ISO 27001, que propone como requisito de control:

Control A.16.01.01 Responsabilidades y procedimientos
"Se deben establecer responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y metódica a los incidentes de seguridad de la información".
- Requisito de control, A.16.01.01 NCH-ISO 27001:2013

Control A.16.01.02 Informe de eventos de seguridad de la información
"Se deben informar lo antes posible, los eventos de seguridad de la información mediante canales de gestión apropiados".
- Requisito de control, A.16.01.02 NCH-ISO 27001:2013

Control A.16.01.03 Informe de las debilidades de seguridad de la información
"Se debe requerir que los empleados y contratistas que usen los sistemas y servicios de información de la organización, observen e informen cualquier debilidad en la seguridad de la información en los sistemas o servicios observada o que se sospeche".
- Requisito de control, A.16.01.03 NCH-ISO 27001:2013

Control A.16.01.04 Evaluación y decisión sobre los eventos de seguridad de la información
"Los eventos de seguridad de la información se deben evaluar y decidir si van a ser clasificados como incidentes de seguridad de la información"
- Requisito de control, A.16.01.04 NCH/ISO 27001:2013

Control A.16.01.05 Respuesta ante incidentes de seguridad de la información
"Los incidentes de seguridad de la información deben ser atendidos de acuerdo a los procedimientos documentados".
- Requisito de control, A.16.01.05 NCH-ISO 27001:2013

Control A.16.01.06 Aprendizaje de los incidentes de seguridad de la información
"Se debe utilizar el conocimiento adquirido al analizar y resolver incidentes de seguridad de la información para reducir la probabilidad o el impacto de incidentes futuros".
- Requisito de control, A.16.01.06 NCH-ISO 27001:2013

Control A.16.01.07 Recolección de evidencia
"La organización debe definir y aplicar los procedimientos para la identificación, recolección, adquisición y conservación de información, que pueda servir de evidencia".
- Requisito de control, A.16.01.07 NCH-ISO 27001:2013

1. Objetivo

Este procedimiento tiene como objetivo, proporcionar directrices e información que van direccionadas a la adopción de procedimientos lógicos, técnicos y administrativos estructurados, con la finalidad de responder de manera rápida y eficiente en situaciones de emergencias y así garantizar la seguridad de la información en el Ministerio, evaluando los eventos de seguridad de la información como incidentes y así, mantener un registro de estos para adoptar medidas eficientes y oportunas para el resguardo de la información.

El presente documento, proporciona directrices e información que tienen como finalidad la adopción de decisiones y así facilitar la respuesta inmediata y eficiente y el registro de los eventos.

2. Alcance

Este documento se aplicará a los sistemas, servicios e instalaciones de procesamiento de la información que utilizan los trabajadores y funcionarios del Ministerio para ejecutar sus funciones y que pueden sufrir incidentes de todos los usuarios de este Ministerio, alumnos en práctica y terceros que puedan estar prestando servicios en el servicio y que requieran el uso de sistemas informáticos y servicios de información.

3. 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 esta política, asimismo, es responsabilidad de:

- **Comité de Seguridad de la Información:** este Comité estará a cargo de la periodicidad de revisión, velar por el cumplimiento, actualización y difusión del "Procedimiento de Evaluación y Decisión de los Eventos de Deguridad de la Información". Además, es de su responsabilidad establecer nexos de coordinación que permitan contacto inmediato en caso de incidentes, como: equipos de seguridad, asesoría legal en delitos informáticos, bomberos, etc.
- **Encargado de seguridad de la información:** su responsabilidad es la aplicación del procedimiento e informar acerca de cualquier evento que se produzca en el Ministerio que tenga directa relación con la seguridad de la información, además, de la revisión periódica del cumplimiento de esta norma.
- **Jefe Unidad de Tecnología de la Información**
  Su responsabilidad es el resguardo de la información ante cualquier evento que se pueda presentar en el Ministerio.
- **Encargado de redes y seguridad**
  Su responsabilidad es contar con planes de acción ante cualquier evento detectado en el Ministerio. Será el responsable de la operación de este procedimiento, generando los registros y medios de verificación indicados en esta norma.

- **Jefes/as de División, Comisión, Unidad:** su responsabilidad es la aplicación de la política, procedimiento y/o instructivos, así también del cumplimiento, promover y supervisar el estricto apego de sus funcionarios a esta norma.

4. Mecanismo de difusión

Es responsabilidad del Comité de Seguridad de la Información, la difusión de este Procedimiento, el que deberá permanecer a disposición de todos los usuarios de este Ministerio en la Intranet institucional.

5. Evaluación y revisión

El tiempo de evaluación y revisión estándar para este documento, será cada dos años. No obstante, podrá revisarse cuando la situación lo amerite o la autoridad así lo disponga. El Encargado de Seguridad de la Información informará en Sesión de Comité de Seguridad de la Información los cambios y/o actualizaciones de este documento. El Comité de Seguridad de la Información lo revisará, observará y aprobará.

6. Definiciones y modo de operación

El Encargado de Seguridad de la Información está a cargo de la protección de la integridad de la información del Ministerio, el que busca resguardarla para la no modificación de datos no autorizados y entregar accesos a la información y sistemas cuando la autoridad lo requiera, siempre resguardando la confidencialidad de la información.

Cualquier evento o situación que comprometa la disponibilidad, confidencialidad e integridad de los activos de información se considerará, igualmente, un incidente de seguridad de la información, así como el no cumplimiento de este procedimiento.

Responsabilidades y evaluación de los incidentes

El Encargado de Seguridad de la Información, el Jefe Unidad de Tecnología de la Información y el Encargado de Soporte y Redes del Ministerio Secretaría General de la Presidencia, evaluarán la información asociada a los eventos reportados como incidentes, la que analizarán y definirán el alcance del incidente (Sistema de información, infraestructura tecnológica, infraestructura física) o la información misma procesada en estos sistemas. Durante la evaluación es necesario solicitar información como:

- En qué consiste el incidente de seguridad de la información, según los eventos identificados
- Ponderación de la gravedad del incidente detectado
- Identificación de los activos afectados (Sistema de Información, Información, Procesos)
- Cómo fue causado, y qué o quién lo causó
- Fecha y hora de ocurrencia. Frecuencia de la ocurrencia
- Impacto real del incidente en el servicio
- Tratamiento temporal del incidente

- Tratamiento temporal del incidente
- Estudio y análisis de las acciones tomadas, para la mejora de los procedimientos para evitar o mitigar un nuevo incidente

Es recomendable que esta información, se suministre a modo de relato o según los criterios que se hayan definido en el formato del reporte de Incidentes de Seguridad de la Información.
Posterior al análisis de la información, el encargado de Seguridad de la Información junto a la Unidad de Tecnología de la Información, determinarán si es un incidente del contexto de Seguridad de la Información, los que deberán promover la respuesta necesaria para la toma de decisión adecuada y actuar ante el incidente de seguridad.
La Unidad de Tecnología de la Información tendrá la obligación de brindar y mantener los registros de los incidentes detectados en el Servicio.
Las jefaturas de la Institución tienen la obligación de reportar el incidente de manera inmediata a los responsables (Unidad de Tecnología de la Información), por los canales definidos para tal situación.

Requisito y comunicación
El Jefe de la Unidad de Tecnología de la Información, deberá informar al Jefe/a de la División de Administración General, acerca del incidente de seguridad detectado. Esta información será entregada trimestralmente, si los hubiera.

Categorización de Eventos e Incidentes de Seguridad de la Información

Categoría	Descripción	Ejemplo
Incidente de daño físico	La pérdida de seguridad de la información es causada por acciones físicas accidentales o deliberadas	Incendio, agua, electrostática, destrucción de equipos, destrucción de medios, robo de equipos, pérdida de equipos, alteración de equipos, etc.
Incidente de fallas de infraestructura	La pérdida de seguridad de la información es causada por fallas en los sistemas y servicios básicos que apoyan el funcionamiento de los sistemas de información	Fallas en la alimentación eléctrica, en las redes, en el aire acondicionado, en el suministro de agua, etc.
Incidente de falla técnica	La pérdida de seguridad de la información es causada por fallas en los sistemas de información o en	Falla de hardware, mal funcionamiento del software, sobrecarga (saturación de la capacidad

	instalaciones no técnicas relacionadas, al igual que problemas humanos no intencionales que dan como resultado la no disponibilidad o destrucción de los sistemas de información	de los sistemas de información), etc.
Incidente de malware	La pérdida de seguridad de la información es causada por programas maliciosos creados y divulgados en forma deliberada. Un programa malicioso se inserta en los sistemas de información para afectar la confidencialidad, la integridad o disponibilidad de los datos, las aplicaciones o sistemas operativos, y/o afectar la operación normal de los sistemas.	Virus informáticos, gusanos de red, troyanos, botnet, ataques combinados, páginas web con códigos maliciosos, apt (advanced persistence threat – amenazas persistentes avanzadas)
Incidente de ataque técnico	La pérdida de seguridad de la información es causada por el ataque a sistemas de información, a través de redes u otros medios técnicos, ya sea mediante el aprovechamiento de las vulnerabilidades de los sistemas de información en cuanto a configuraciones, protocolos o programas, o por la fuerza, lo que da como resultado un estado anormal de los sistemas de información, o daño potencial a las operaciones presentes en el sistema	Escaneo de redes, aprovechamiento de vulnerabilidades, aprovechamiento de puertas traseras (backdoors), intento de ingreso, interferencia, denegación de servicio, etc.
Incidente de puesta en riesgo de la información	La pérdida de seguridad de la información es causada al	Interceptación, espionaje, divulgación,

	poner en riesgo en forma accidental o deliberada la seguridad de la información, por ejemplo, en cuanto a confidencialidad, integridad y disponibilidad	enmascaramiento, ingeniería social, phishing de redes, robo y/o pérdida de datos, alteración de datos, etc.
Otros incidentes	No clasificados en algunas de las anteriores categorías	N/A

Es recomendable que esta información, se suministre a modo de relato o según los criterios que se hayan definido en el formato del reporte de Incidentes de Seguridad de la Información.
Posterior al análisis de la información, el Encargado de Seguridad de la Información junto a la Unidad de Tecnología de la Información, determinarán si es un incidente del contexto de Seguridad de la Información, los que deberán promover la respuesta necesaria para la toma de decisión adecuada y actuar ante el incidente de seguridad.

Criterio de evaluación de riesgo

Alta

El riesgo detectado tiene un impacto y consecuencias graves para la institución o terceros

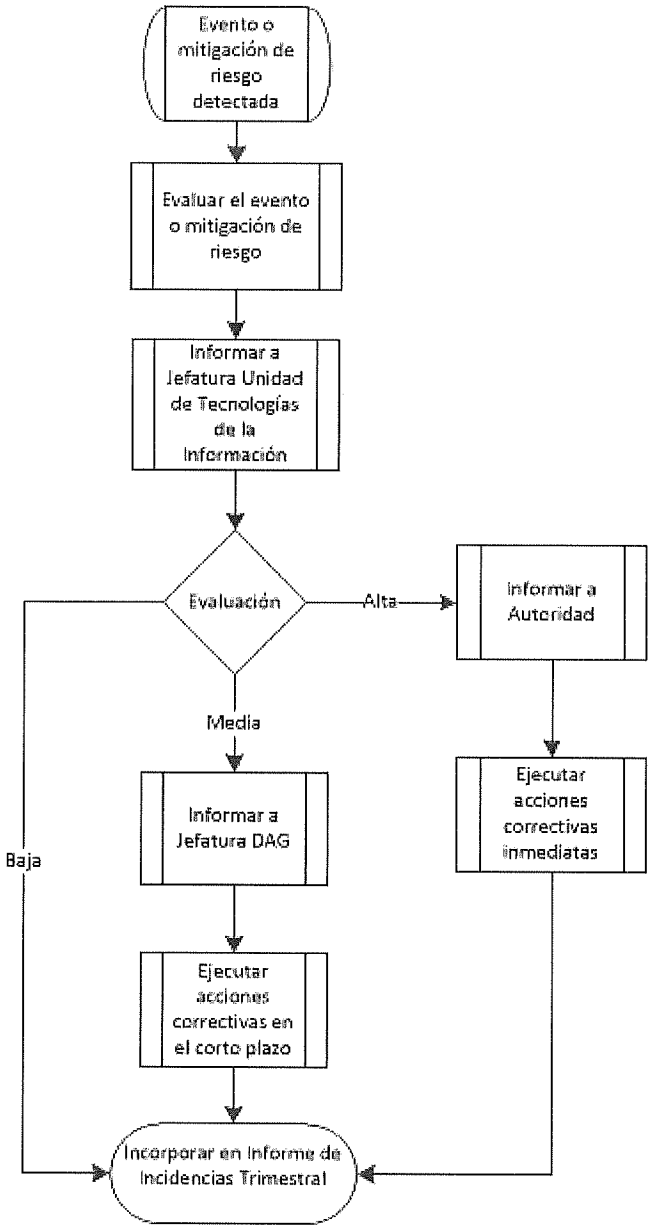
Media

El riesgo detectado tiene un impacto y consecuencias significativas para la institución o tercero

Baja

El riesgo detectado tiene un impacto y consecuencias leves para la institución o terceros

Flujograma de evento o mitigación de riesgo



7. Formato de registro

- Reporte de incidentes de seguridad para el periodo que indica

Ministerio Secretaría General de la Presidencia

Memorándum Electrónico
Administración General/ Unidad de Tecnologías de la Información
[Año - N°]
[Fecha]

De	[Nombre Apellido], Jefe Unidad de Tecnologías de la Información
Para	[Nombre Apellido], Jefa de División Administración General
Antecedentes o materia	Reporte de incidentes [Periodo]
Detalle de Memorándum	Se adjunta reporte de incidentes correspondiente al [Periodo].
Visaciones	Sin visadores
Distribución	Sin Distribución
Derivación	Sin Derivación Asignada

Adjuntos

#	Descripción	
[N°]	MemoReporteIncidentes[Periodo]	🔍
[N°]	ReporteDeIncidentes[Periodo]	🔍

Descargar Memo

Documento generado en Ministerio Secretaría General de la Presidencia.

Reporte de Incidentes de Seguridad

Periodo	
Responsable	

A continuación, exponemos los incidentes de seguridad para el periodo señalado

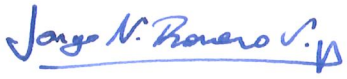
Incidente	Descripción del Incidente	Fecha y hora de ocurrencia	Fecha y hora de término	Impacto	Mitigación

Atentamente,

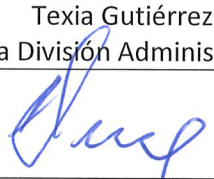
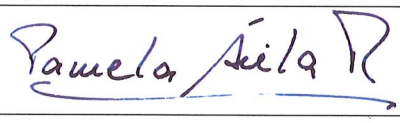
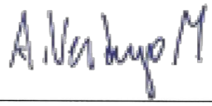
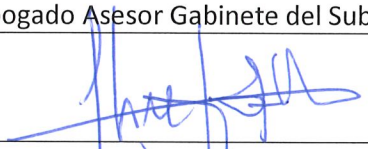
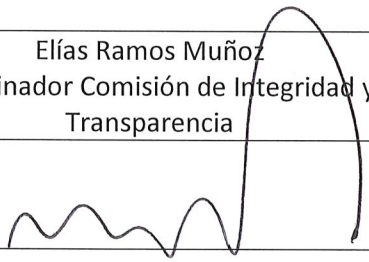
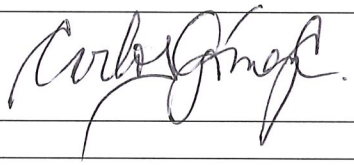
Nombre Apellido
Encargado Área Redes y Seguridad
Ministerio Secretaría General de la Presidencia

DISTRIBUCIÓN:
1. Nombre Apellido – Jefatura DAG
2. Archivos Informática

8. Control

Elaborado por: Jorge Romero Vargas

Fecha: 14-09-2020

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

Texia Gutiérrez Inostroza Jefa División Administración General	Pamela Ávila Rubio Jefa Unidad de Control de Gestión
	
Anamaría Verdugo Marchese Abogada Asesora CSI	Federico Ureta Hurtado Abogado Asesor Gabinete del Subsecretario
	
Elías Ramos Muñoz Coordinador Comisión de Integridad y Transparencia	Carlos Gómez Cruz Jefe División de Gobierno Digital
	

Jorge Romero Vargas Oficial de Seguridad de la Información Jefe Unidad de Tecnologías de la Información

Fecha: 14-09-2020