Controles NCH ISO 27001:2013 Relacionados

Control	Nombre
A.06.01.03	Contacto con autoridades
A.06.01.04	Contacto con grupos especiales de interés

Control de versiones

Fecha	Versión	Responsables	Descripción
15-06-2016	1.0	Marcelo Aliaga Q. Liliana Reyes G.	Elaboración de Procedimiento
05-10-2016	1.1	Marcelo Aliaga Q. Liliana Reyes G.	Modificación del texto y configuración de documentos
17-10-2016	1.2	Marcelo Aliaga Q. Liliana Reyes G.	Modificación del formato de la portada, la tabla de control de versiones, marcos de imágenes, Objetivo de control.
30-10-2017	2.0	Marcelo Aliaga Q. Liliana Reyes G.	Modificación del contenido en base al documento "Estrategia de trabajo SSI 2017": alcance, objetivo, roles y responsabilidades, mecanismos de difusión, evaluación y revisión. Se incorpora en página 4 punto 6. "Evaluación y revisión" (...) "no obstante, podrá revisarse cuando la situación amerite o la autoridad lo disponga". Se agrega en página 5 título "Formato de registro" e imagen.
27-09-2018	3.0	Jorge Romero V. Solange Godoy	Modificación de objetivo y alcance. Se elimina la dependencia de Agustinas N°1291. Incorporación de flujograma contacto con grupos de interés.
19-11-2019	4.0	Jorge Romero V. Solange Godoy	Modificación formato documento: Se eliminó punto 5 Mecanismos de difusión; punto 6 Evaluación y revisión; punto 7 Definiciones. Se agregó punto 5 Definiciones y modo de operación. Se cambión punto 10 por punto 6 registro de operación. Se actualizaron registros de operación. Se desagregó punto 4 roles y responsabilidades. Se actualizaron autoridades y operativos en punto 6. En punto 7 se actualizó nombre Jefa DAG y cargo a Jefe Unidad de Tecnologías de la Información. Mejora en flujogramas y redacción.
18-05-2020	4.1	Jorge Romero V. Solange Godoy C.	Actualización de datos de contrapartes internas. Actualización de formato de registro de operación "Reporte de Incidentes de Seguridad". Cambio de formato de acta de reunión.
14-09-2020	4.2	Jorge Romero V.	Actualización de datos de contraparte internas; Sección firmantes.
29-06-2021	4.3	Jorge Romero V.	Actualización de datos de contraparte internas; Sección firmantes.
31-08-2021	4.4	Jorge Romero V.	Mejoras en la redacción del documento. Actualización de datos de contraparte internas; Sección firmantes.

26-07-2022	4.5	Jorge Romero V.	Actualización de datos de contraparte internas; Sección firmantes.
11-08-2023	4.6	Jorge Romero V.	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.
23-02-2024	4.7	Jorge Romero V.	Modifica Área de Tecnologías de la Información por Departamento de Gestión de Tecnologías de la Información. Modifica mejorar por mejoras. Modifica Edificio Bicentenario por Edificio Moneda Bicentenario. Modifica usuarios por usuarios/as. Modifica Encargado/a del Área de Tecnologías de la Información por Jefe/a de Departamento de Gestión de Tecnologías de la Información. Modifica Jefes/as División, Comisión, Unidad por Jefes/as División, Comisión, Departamento. Modifica Encargado/a del Área de Redes y Seguridad por Encargado/a de la Unidad de Redes y Seguridad. Modifica informe por reporte. Complementa información de contacto de contrapartes externas. Incorpora análisis de nivel de impacto. Mejora de flujograma de Contacto con Autoridades y Flujograma de Contacto con grupos de interés. Incorporar criterios de evaluación de emergencia. Incorporar especificación de tiempos de respuesta en notificaciones a autoridades. Mejoras en la redacción del documento. Incorporar formulario de notificación de incidente y define catálogo de nivel de peligrosidad, clasificación y tipo de Incidente.

1. Introducción

El Ministerio Secretaría General de la Presidencia, dispone del presente documento denominado "Procedimiento de Contacto con Autoridades y Grupos Especiales de Interés", como parte integrante del Sistema de Seguridad de la Información.

Este procedimiento ha sido desarrollado para asegurar el cumplimiento de los estándares definidos por la Norma Chilena ISO 27001:2013, con un enfoque particular en los controles que buscan promover el establecimiento de comunicaciones estratégicas con autoridades relevantes tanto internas como externas. Este documento detalla las directrices y responsabilidades asignadas para asegurar relaciones adecuadas con las autoridades competentes y grupos especializados, foros de seguridad y asociaciones profesionales. Al implementar este procedimiento, el objetivo es promover una gestión proactiva y coordinada de los incidentes de seguridad de la información, así como cultivar un entorno de colaboración continua. Esto nos permite estar siempre al día con las mejores prácticas y avances en el campo de la seguridad de la información, asegurando una mejora constante en nuestras estrategias de protección. Dichos controles son los siguientes:

Control A.06.01.03

"Se deben mantener los contactos apropiados con las autoridades pertinentes".

- Requisito de Control, A.06.01.03 NCh/ISO 27001:2013

Control A.06.01.04

"Se deben mantener los contactos apropiados con los grupos especiales de interés u otros foros especializados en seguridad, así como asociaciones de profesionales".

- Requisito de Control, A.06.01.04 NCh/ISO 27001:2013

2. Alcance

El alcance de este procedimiento se extiende a todas las acciones de comunicación que el Oficial de Seguridad de la Información lleve a cabo en respuesta a incidentes de seguridad, así como a las iniciativas destinadas a enriquecer el conocimiento sobre seguridad de la información y a implementar mejoras en las políticas y procedimientos existentes. Este enfoque estratégico está diseñado para fortalecer la infraestructura de seguridad de la organización de manera integral.

En cuanto a la notificación de incidentes, este procedimiento es de obligatoria aplicación en las áreas designadas a continuación:

Dirección	Piso
Oficinas Edificio Moneda Bicentenario, Teatinos N°92	9
Oficinas, Moneda N°1160	Entrepiso EP, 2, 3, 4, 5, 6
Palacio de La Moneda, Moneda s/n	Gabinete de Ministro, Subsecretaría y División Jurídico Legislativa
Bodega institucional, Compañía de Jesús 1852	1
Congreso Nacional	2

Todas las personas presentes en estas dependencias, ya sea trabajando o visitando, estarán sujetas a las directrices aquí establecidas. Esto incluye a funcionarios/as, personal contratado bajo cualquier modalidad (honorarios, contratistas, subcontratistas), así como a usuarios/as y visitantes, asegurando así una cobertura completa y efectiva ante cualquier incidente de seguridad, independientemente de su relación contractual con la institución.

3. Objetivo

Los objetivos de este procedimiento son los siguientes:

- Mantener comunicación continua con las autoridades correspondientes para reportar de manera inmediata cualquier incidente de seguridad de la información que ocurra.

- Establecer y mantener relaciones constructivas con grupos de interés especializados y otros foros de expertos en seguridad, así como con asociaciones profesionales, con el objetivo de enriquecer nuestro conocimiento sobre las mejores prácticas en seguridad de la información, así como para compartir e intercambiar información acerca de nuevas tecnologías y otros temas relevantes.

4. Roles y responsabilidades

Independiente del cargo/rol que se desempeñe; del nivel jerárquico que se tenga; 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 este procedimiento. Asimismo, es responsabilidad del:

- **Oficial de Seguridad de la Información:** La aplicación de este procedimiento y la revisión del cumplimiento de lo establecido en este documento.

- **Comité de Seguridad de la Información:** La revisión, actualización y difusión de este procedimiento, así como velar por el cumplimiento de este.

- **Jefe/a del Departamento de Gestión de Tecnologías de la Información:** Velar por el debido cumplimiento de este procedimiento.

- **Jefes/as División, Comisión, Departamento:** Tener conocimiento de este procedimiento y su cumplimiento.

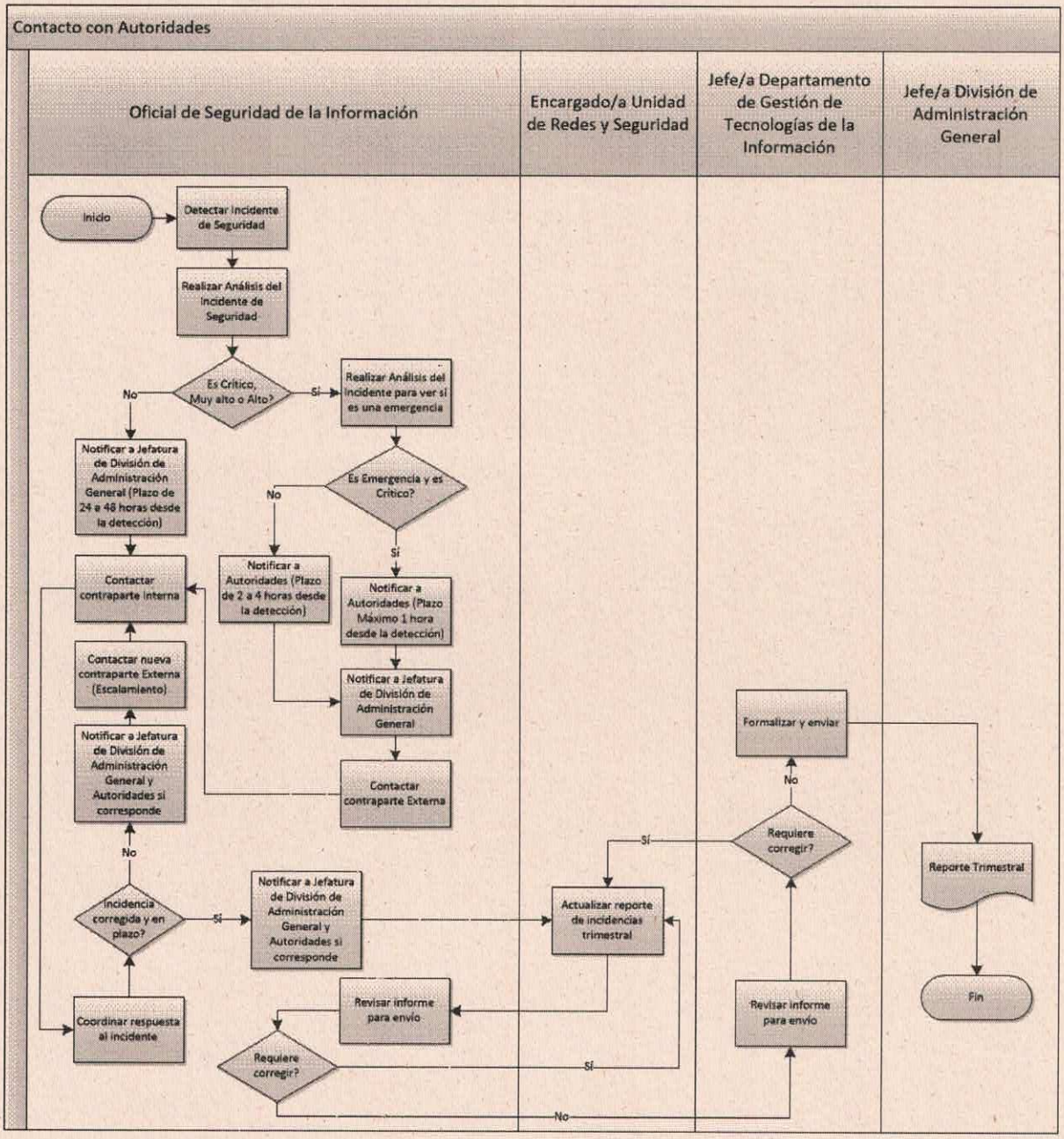
- **Funcionarios/as y Colaboradores:** Tener conocimiento de este procedimiento y su cumplimiento.

- **Encargado/a de la Unidad de Redes y Seguridad:** Gestionar la incorporación de incidentes de seguridad para envío de reporte trimestral.

5. Definiciones y modo de operación

El Ministerio Secretaría General de la Presidencia, específicamente, el/la Oficial de Seguridad de la Información y el/la Encargado/a de la Unidad de Redes y Seguridad mantendrán comunicación periódica con especialistas en tecnologías de la información y seguridad. Esta interacción se realizará a través de una cuenta de correo electrónico dedicada para asegurar un flujo constante y seguro de información relevante: (incidentes@interior.gob.cl, soc@interior.gob.cl) y a través de un chat denominado chat RCE.

5.1. Contacto con Autoridades



Tras la detección de un incidente dentro de la institución, se deberá llevar a cabo un análisis de impacto inicial para clasificar su gravedad. Este análisis determinará si el incidente se categoriza como Crítico, Muy Alto, Alto, Medio o Bajo, basándose en los siguientes criterios preestablecidos.

Análisis de nivel de impacto

Crítico				
Impacto	**Datos sensibles**	**Daño financiero**	**Reputación**	**Cumplimiento legal**
Causa una parálisis total o casi total de las operaciones críticas de la institución.	Implica una exposición masiva de datos confidenciales o regulados, poniendo en riesgo la privacidad de los datos personales, secretos o información gubernamental clasificada.	Provoca pérdidas financieras catastróficas que podrían amenazar la viabilidad de la institución.	Tiene el potencial de causar un daño irreparable a la reputación de la institución.	Incumple de manera significativa con las leyes y regulaciones aplicables, resultando en sanciones severas o litigios de gran envergadura.
Recuperación	La recuperación es extremadamente difícil y requiere una cantidad significativa de tiempo y recursos.			
Ejemplo	Ataques que causan interrupciones masivas de servicios críticos, brechas de seguridad que exponen grandes volúmenes de datos sensibles, incluyendo información financiera o de identificación personal.			
Tiempo de solución	Inmediato a 4 horas.			

Muy alto				
Impacto	**Datos sensibles**	**Daño financiero**	**Reputación**	**Cumplimiento legal**
Interrumpe las operaciones críticas, pero permite cierta capacidad operativa limitada.	Exposición de datos sensibles significativa, pero no a una escala masiva.	Causa pérdidas financieras importantes, pero no catastróficas.	Puede resultar en un daño significativo a la reputación que requerirá esfuerzos considerables para recuperarse.	Resulta en incumplimientos legales o de regulaciones que pueden llevar a sanciones significativas o litigios.

Recuperación	La recuperación es desafiante y requiere recursos considerables y tiempo.
Ejemplo	Ataques que resultan en una pérdida financiera significativa o robo de propiedad intelectual valiosa para la institución.
Tiempo de solución	4 a 8 horas.

Alto				
Impacto	**Datos sensibles**	**Daño financiero**	**Reputación**	**Cumplimiento legal**
Afecta las operaciones no críticas o causa interrupciones temporales en las operaciones críticas.	Involucra una pérdida de datos sensibles limitada o controlada.	Provoca un impacto financiero moderado que la organización puede manejar sin riesgo de viabilidad.	Causa preocupación entre clientes o socios, pero es manejable con esfuerzos de comunicación efectivos.	Implica posibles incumplimientos de leyes o regulaciones que pueden ser rectificados sin sanciones severas.
Recuperación	La recuperación es manejable con los recursos existentes, aunque puede requerir esfuerzos significativos.			
Ejemplo	Ataques que interrumpen servicios no críticos o que conducen a la pérdida de datos no esenciales, pero aún sensibles.			
Tiempo de solución	8 a 24 horas.			

Medio				
Impacto	**Datos sensibles**	**Daño financiero**	**Reputación**	**Cumplimiento legal**
Causa inconvenientes menores en las operaciones, pero no afecta significativamente la continuidad operacional de la institución.	Puede involucrar una exposición mínima de datos sensibles, manejable mediante procedimientos estándar de respuesta.	Tiene un impacto financiero menor, con costos asociados principalmente a la investigación y remedio del incidente.	Puede generar preguntas o preocupaciones menores entre las partes interesadas, pero no afecta significativamente la percepción pública.	Puede requerir revisiones de cumplimiento, pero no se espera que resulte en sanciones o incumplimientos graves.
Recuperación	La recuperación está dentro de las capacidades normales de respuesta y manejo de incidentes.			

Ejemplo	Infecciones por malware que afectan un número limitado de sistemas, incidentes de phishing que no tienen resultados en pérdida de datos sensibles.
Tiempo de solución	1 a 3 días continuos.

Bajo				
Impacto	**Datos sensibles**	**Daño financiero**	**Reputación**	**Cumplimiento legal**
Tiene un impacto insignificante en las operaciones diarias.	No hay pérdida de datos sensibles o la pérdida es insignificante y fácilmente contenible.	El impacto financiero es mínimo, con costos limitados a acciones correctivas menores.	Tiene un impacto despreciable o nulo en la reputación de la institución.	No se espera que viole leyes o regulaciones o que cualquier incumplimiento sea de naturaleza menor y fácilmente corregible.
Recuperación	La recuperación es rápida y requiere recursos mínimos.			
Ejemplo	Ataques fallidos o exitosos que no comprometen datos sensibles ni afectan significativamente las operaciones del negocio.			
Tiempo de solución	3 a 7 días continuos.			

Sin impacto
El incidente de seguridad no presenta impacto apreciable dentro de la institución.

Se informará a las autoridades únicamente en los casos en que el incidente sea clasificado como Crítico, Muy Alto o Alto. Adicionalmente, se deberá determinar si el incidente corresponde o no a una emergencia, considerando el cumplimiento de alguno de los siguientes criterios:

Criterios de evaluación de emergencia

Criterio	**Subcriterio**	**Descripción**
Evaluación del impacto	**Operaciones críticas afectadas**	El incidente afecta las funciones esenciales para la continuidad operativa de la institución. Servicios vitales están comprometidos y requieren restauración inmediata.
	Seguridad de funcionarios/as y colaboradores	Si existe un riesgo inmediato para la seguridad física de funcionarios/as y colaboradores.

	Daño a la infraestructura crítica	Si existen daños a sistemas o infraestructuras críticas que podrían tener un efecto dominó en otras operaciones de la institución o en la seguridad pública.
Análisis de la pérdida de datos	**Exfiltración de datos sensibles**	Si hay evidencia de que datos confidenciales están siendo robados o expuestos públicamente.
	Compromiso de datos regulados	Si el incidente involucra la posible pérdida o compromiso de datos sujetos a regulaciones estrictas como datos personales protegidos.
Potencial de escalada	**Expansión del ataque**	Si el incidente tiene el potencial de expandirse rápidamente, comprometiendo más sistemas o datos de la institución.
	Amenazas activas	La presencia de actores de amenazas activamente explotando vulnerabilidades o realizando ataques dirigidos.
Capacidad de respuesta	**Recursos disponibles**	Falta de recursos para responder al incidente de manera inmediata.
	Tiempo de respuesta	Si el tiempo para mitigar el incidente antes de que se produzcan daños irreparables es extremadamente corto.
Impacto reputacional y financiero	**Daño a la reputación**	El incidente podría dañar significativamente la reputación de la institución de manera inmediata.
	Consecuencias financieras	El incidente conlleva un impacto financiero severo e inmediato.

En caso de determinarse que el incidente constituye una emergencia, se establecerá comunicación con la contraparte externa para coordinar una respuesta conjunta al incidente con el equipo interno de la institución.

Por otro lado, si el incidente no se clasifica como una emergencia, se trabajará en la resolución de este en colaboración con las contrapartes internas pertinentes.

En caso de que el incidente no pueda ser resuelto dentro de los plazos establecidos de su clasificación, deberá ser escalado a una nueva contraparte externa. Se deberá notificar a la Jefatura de la División de Administración General.

Una vez resuelto el incidente, se deberá notificar a la Jefatura de la División de Administración General y Autoridades si corresponde, según clasificación. El incidente será documentado junto con su solución en el reporte trimestral de incidentes de seguridad. Se formalizará a través de un memorándum interno, que posteriormente se remitirá a la Jefatura de la División de Administración General cuando sea programado su envío.

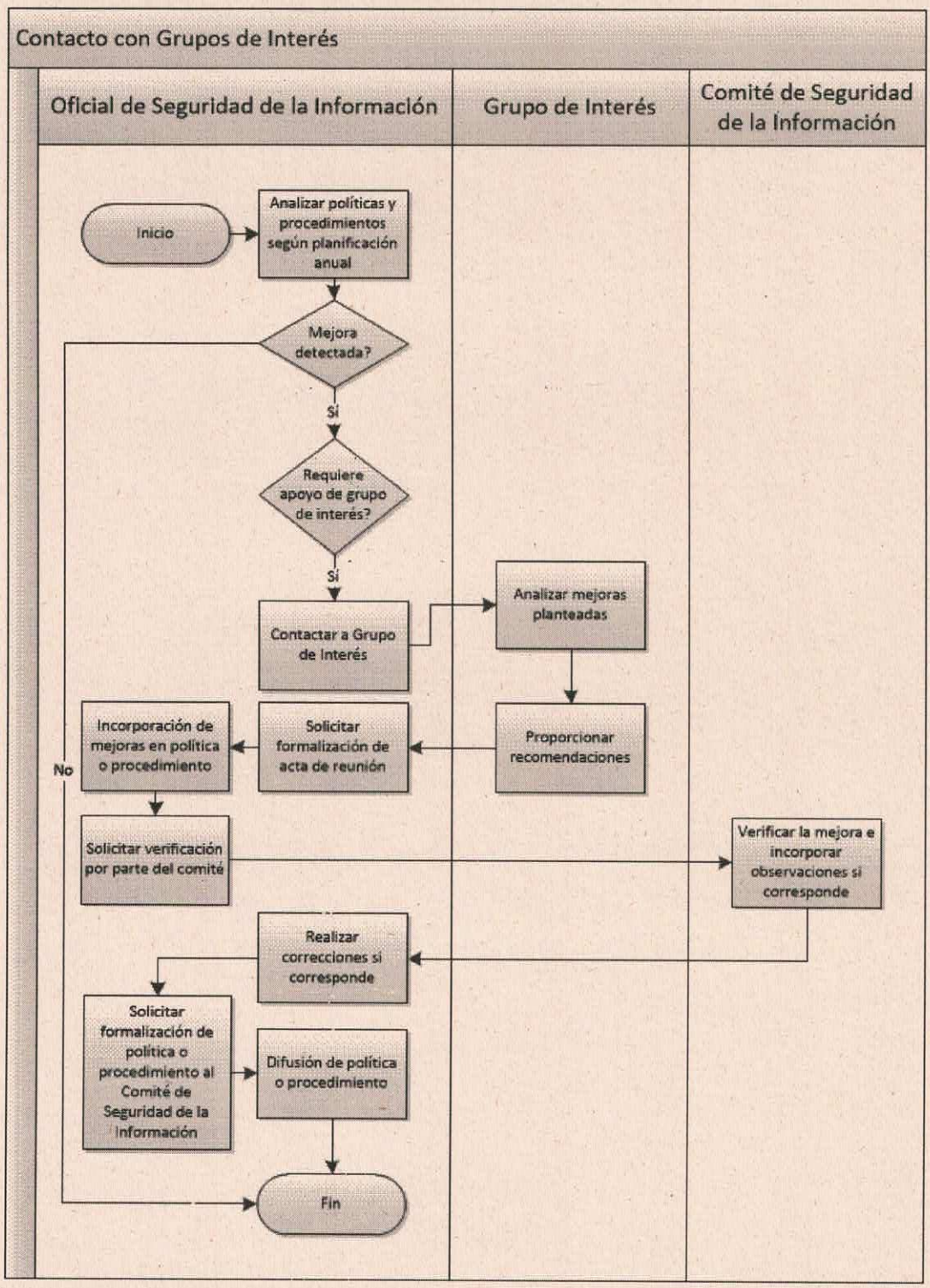
Se deberán considerar los siguientes tiempos de respuesta a notificaciones para Autoridades de la Institución y Jefatura de la División de Administración General:

Incidentes críticos y emergencias	Informar de inmediato o en un plazo máximo de 1 hora, después de la detección.
Incidentes clasificados como muy altos y altos	Informar dentro de las 2 a 4 horas, después de la detección.

Para los casos de incidentes clasificados como medio o bajo se deberá informar a la Jefatura de la División de Administración General dentro de las 24 a 48 horas, después de la detección.

Las notificaciones deberán ser realizadas mediante correo electrónico dirigido a la Jefatura del Gabinete de la Subsecretaría, con copia a la Jefatura de la División de Administración General. El correo deberá acompañar el formulario de notificación de incidente.

5.2. Contacto con grupos de interés



Cuando es detectada una necesidad de mejoramiento en políticas y/o procedimientos del Sistema de Seguridad de la Información SSI dentro del Ministerio Secretaría General de la Presidencia, el/la Oficial de Seguridad de la Información podrá considerar tomar contacto con un grupo especial de interés, con el que podrá reunirse para presentar la necesidad de mejora y obtener recomendaciones. Posteriormente, el/la Oficial de Seguridad de la Información deberá realizar una formalización del acta de la reunión e incorporar las mejoras detectadas en políticas o procedimientos. Una vez finalizada la propuesta, esta será enviada para la evaluación y verificación por parte del Comité de Seguridad de la Información. Realizada la verificación e incorporación de observaciones por parte de dicho Comité, los documentos serán formalizados y difundidos según su indicación.

5.3. Contrapartes Externas

Servicio	Dirección	Distancia	Teléfono	Tiempo de llegada
Equipo de Respuesta ante Incidentes de Seguridad Informática CSIRT	Teatinos 92, Piso 9	300 mts.	1510	5 minutos
Bomberos 5º Compañía	Nataniel Cox Nº85	450 mts.	2 26982161	5 minutos
Bomberos 4º Compañía	Santo Domingo Nº1495	750 mts.	2 26961443	8 minutos
Carabineros 1º Comisaría	Santo Domingo N°714	1000 mts.	2 29223700	10 minutos
Carabineros Palacio de la Moneda	Palacio de la Moneda S/N	100 mts.	2 22690400	2 minutos
Policía de Investigaciones PDI	General Borgoño N°1204	1300 mts.	2 25657424	12 minutos
Policía de Investigaciones PDI	Palacio de la Moneda S/N	100 mts.	2 22690400	2 minutos
Mutual de Seguridad Agustinas	Agustinas Nº1362	200 mts.	2 28765700	5 minutos
Hospital Mutual de Seguridad	Av. Libertador Bernardo O'Higgins Nº4848	3450 mts.	2 26775000	35 minutos
Clínica Dávila	Av. Recoleta Nº464	1750 mts.	2 27308000	18 minutos
Posta Central	Portugal N°125	1250 mts.	2 24633800	12 minutos

5.4. Contrapartes Internas

- **Autoridades y Jefaturas**

Cargo	Nombre Apellido	Teléfono - Correo
Subsecretaria	Macarena Lobos Palacios	2 26946170 - mlobos@minsegpres.gob.cl
Jefe de Gabinete Subsecretario	Christian Valenzuela Lorca	2 26945969 - cvalenzuela@minsegpres.gob.cl
Jefe División de Administración General	Samir Toro Garrido	2 26945862 - storo@minsegpres.gob.cl
Jefa División de Estudios	Javiera Ascencio de la Fuente	2 26945507 - jascencio@minsegpres.gob.cl
Jefa División Jurídico-Legislativa	Francisca Moya Marchi	2 26945964 - fmoya@minsegpres.gob.cl
Jefe División de Coordinación Interministerial	Rodrigo Echecopar Kisic	2 26945339 - rechecopar@minsegpres.gob.cl
Jefe División de Gobierno Digital	José Inostroza Lara	2 22198309 - jinostroza@minsegpres.gob.cl
Secretaria Ejecutiva Comisión Asesora Presidencial para la Integridad Pública y Transparencia	Valeria Lübbert Álvarez	2 22198416 - vlubbert@minsegpres.gob.cl
Jefe División de Relaciones Políticas e Institucionales	Nicolás Facuse Vásquez	226945863 - nfacuse@minsegpres.gob.cl

- **Personal operativo**

Cargo	Nombre Apellido	Teléfono - Correo
Presidenta de CPHS e Integrante Comisión Investigación de Accidente	Schlomit Cordero B.	2 26945803 - scordero@minsegpres.gob.cl
Departamento de Gestión y Desarrollo de Personas Prevencionista de Riesgos	Paul Martínez	2 26945507 - pmartinez@minsegpres.gob.cl
Oficial de Seguridad de la Información Encargado de Ciberseguridad	Jorge Romero V.	2 26945917 - jromero@minsegpres.gob.cl
Departamento de Gestión Estratégica y Operaciones Telefonía/Telefonía Móvil	Juan C. Zúñiga M.	2 26945849 - jzuniga@minsegpres.gob.cl

Departamento de Gestión de Tecnologías de la Información Conectividad	Juan Parra E.	2 26945908 - jparra@minsegpres.gob.cl
Departamento de Gestión de Tecnologías de la Información Seguridad de Accesos	Juan Parra E.	2 26945908 - jparra@minsegpres.gob.cl
Departamento de Gestión de Tecnologías de la Información Soporte Informático de HW y SW	Mesa de Ayuda Informática y soporte técnico en terreno	2 26945800 - soporte@minsegpres.gob.cl
Departamento de Gestión de Tecnologías de la Información Servicio de Impresión	Mesa de Ayuda Informática y soporte técnico en terreno	2 26945800 - soporte@minsegpres.gob.cl
Departamento de Gestión Estratégica y Operaciones Agua, Electricidad y otros servicios básicos	Juan C. Zúñiga M.	2 26945849 - serviciosgenerales@minsegpres.gob.cl

6. Registro de operación

Memorándum "Reporte de Incidentes de Seguridad para el periodo que indica (Ejemplo)

Ministerio Secretaría General de la Presidencia

Memorándum Electrónico

Administración General/ **Departamento de Gestión de Tecnologías de la Información**

Año N°
[Fecha]

De	[Nombre Apellido], **Jefe/a Departamento de Gestión de Tecnologías de la Información**
Para	[Nombre Apellido], **Jefe/a División de 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

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/a Unidad Redes y Seguridad
Ministerio Secretaría General de la Presidencia

DISTRIBUCIÓN:
1. Nombre Apellido – Jefatura DAG
2. Archivos Área Tecnologías de la Información

Acta de Reunión

Acta de Reunión

Lugar	Fecha	Hora	Asistentes
		Inicio: **Término:**	

Objetivo		Organizador

N°	Desarrollo	
1		
2		

N°	Compromisos		Responsable	Plazo
1				
2				

Observaciones	

Nombre	Centro de Responsabilidad	Firma

Formulario de notificación de incidente

Ministerio Secretaría General de la Presidencia
Gobierno de Chile

Notificación de Incidente de Seguridad de la Información
Comité de Seguridad de la Información

Fecha:

Asunto:

Descripción:

Origen del Incidente:

Fecha:
Hora:

Detección del Incidente:

Fecha:
Hora:

Nivel de peligrosidad:

- ☐ Crítico
- ☐ Muy alto
- ☐ Alto
- ☐ Medio
- ☐ Bajo

Clasificación:

Tipo de Incidente:

Nivel de Impacto:

- ☐ Crítico
- ☐ Muy alto
- ☐ Alto
- ☐ Medio
- ☐ Bajo
- ☐ Sin impacto

Recursos tecnológicos afectados:

Plan de acción y contramedida:

Observaciones

Oficial de Seguridad de la Información

Nombre:

Rut:

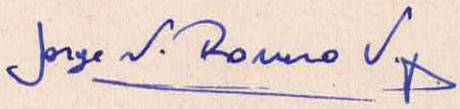
Firma

- Catálogo de Nivel de Peligrosidad, Clasificación y Tipo de Incidente

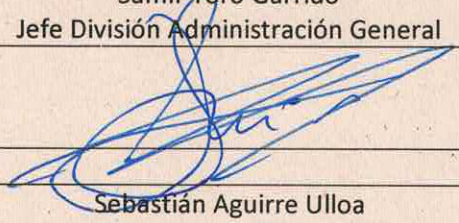
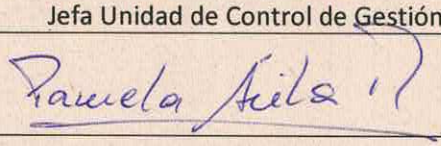
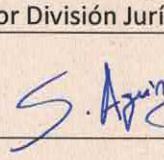
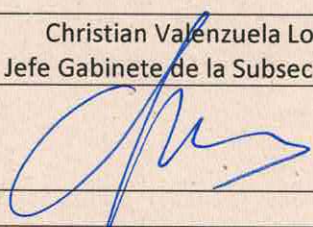
Nivel	Clasificación	Tipo de Incidente
Crítico	**Otros**	APT (Advanced Persistent Threat) Ataque cibernético dirigido
Muy alto	**Código dañino**	Distribución de malware
		Configuración de malware
	Intrusión	Robo
	Disponibilidad	Sabotaje
		Interrupciones
Alto	**Contenido abusivo**	Pornografía infantil, contenido sexual o violento inadecuado
	Contenido dañino	Sistema infectado
		Servidor C&C (Mando y control)
	Intrusión	Compromiso de aplicaciones
		Compromiso de cuentas con privilegios
	Intento de intrusión	Ataque desconocido
	Disponibilidad	DoS (Denegación de Servicio)
		DDoS (Denegación distribuida de servicio)
	Compromiso de la información	Acceso no autorizado a información
		Modificación no autorizada de información
		Pérdida de datos
	Fraude	Phishing
Medio	**Contenido abusivo**	Discurso de odio
	Obtención de información	Ingeniería social
	Intento de intrusión	Explotación de vulnerabilidades conocidas
		Intento de acceso con vulneración de credenciales
	Intrusión	Compromiso de cuentas sin privilegios
	Disponibilidad	Mala configuración
	Fraude	Uso no autorizado de recursos
		Derechos de autor
		Suplantación
	Vulnerable	Criptografía débil
		Amplificador DDoS
		Servicios con acceso potencial no deseado
		Revelación de información

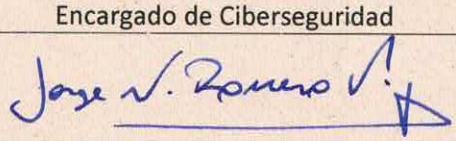
		Sistema vulnerable
Bajo	**Contenido abusivo**	Spam
	Obtención de información	Escaneo de redes (scanning)
		Análisis de paquetes (sniffing)
	Otros	Otros

7. Control

Elaborado por: Jorge Romero Vargas

Fecha: 23-02-2024

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 de Ciberseguridad

Fecha: 23-02-2024