APRUEBA LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DEL MINISTERIO SECRETARÍA GENERAL DE LA PRESIDENCIA Y DEJA SIN EFECTO LA RESOLUCIÓN EXENTA Nº 694, DE 2021, DE ESTE ORIGEN.

RESOLUCIÓN EXENTA Nº 1109 /

SANTIAGO, 23 DIC 2022

V I S T O S:

La Ley Nº 18.993, que crea este Ministerio, y su Reglamento Orgánico, contenido en el Decreto Supremo Nº 7, de 1991, de esta Secretaría de Estado; el Decreto con Fuerza de Ley Nº 1/19.653, de 2000, del Ministerio Secretaría General de la Presidencia, que fija el texto refundido, coordinado y sistematizado de la Ley Nº 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; el Decreto con Fuerza de Ley Nº 29, de 2004, del Ministerio de Hacienda, que fija el texto refundido, coordinado y sistematizado de la Ley Nº 18.834, sobre Estatuto Administrativo; la Ley Nº 19.799, sobre documentos electrónicos, firma electrónica y los servicios de certificación de dicha firma, y su reglamento contenido en el Decreto Supremo Nº 181, de 2002, del Ministerio de Economía, Fomento y Reconstrucción; la Ley Nº 20.285, sobre Acceso a la Información Pública; el Decreto Supremo Nº 83, de 2004, de este origen, que aprueba norma técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos; el Decreto Supremo Nº 12, de 2022, de este Ministerio, que designa a su Subsecretaria; la Resolución Exenta Nº 694, de 2021, que aprueba la política general de seguridad de la información de esta Secretaría de Estado; y la Resolución Nº 7, de 2019, de la Contraloría General de la República, que fija normas sobre exención del trámite de toma de razón.

C O N S I D E R A N D O:

1. Que, según la Ley Nº 18.993, que crea el Ministerio Secretaría General de la Presidencia, establece que dicha Secretaría de Estado estará encargada de realizar funciones de coordinación y de asesoría directa al Presidente de la República, al Ministerio del Interior y Seguridad Pública y a cada uno de los Ministros, especialmente en materias políticas, jurídicas y administrativas, referentes a las relaciones del Gobierno con el Congreso Nacional, los Partidos Políticos y otras organizaciones sociales e instituciones de la vida nacional, así como propender al logro de una efectiva coordinación programática general de la gestión de gobierno.

2. Que, lo indicado precedentemente implica la generación, envío, recepción, almacenamiento y distribución de multiples y diversos activos de información que demandan requisitos de seguridad apropiados para garantizar los atributos esenciales de confidencialidad, integridad y disponibilidad de la misma.

3. Que, en razón de lo anterior, es necesario actualizar periodicamente la Política General de Seguridad de la Información, con el objeto de definir y establecer los lineamientos generales del Sistema de Gestión de la Seguridad de la Información del cual formará parte la presente Política, enmarcándose en el cumplimiento de la Norma Chilena ISO 27001, cuyo objetivo principal es resguardar la seguridad de los activos de información de esta Secretaría de Estado.

4. Que, de acuerdo con lo expuesto, y lo solicitado mediante Memorándum Nº 395, de 2022, del Jefe de la División de Administración General de

este Ministerio, el presente acto administrativo viene en aprobar la Política General de Seguridad de la Información del Ministerio Secretaría General de la Presidencia.

R E S U E L V O:

1º.- APRUÉBASE la Política General de Seguridad de la Información del Ministerio Secretaría General de la Presidencia, cuyo texto es el siguiente:

Controles NCH ISO 27001:2013 Relacionados

Control	Nombre
A.05.01.01	Políticas de seguridad de la información
A.05.01.02	Revisión de las políticas de seguridad de la información
A.06.01.01	Roles y responsabilidades de la seguridad de la información

2022

Control de Versiones

FECHA	VERSIÓN	RESPONSABLES	DESCRIPCIÓN
31-05-2011	1.0	Departamento de Informática	Edición y aprobación R.EX.N°1396
07-12-2012	2.0	Departamento de Informática	Edición y aprobación R.EX.N°2595
31-12-2013	3.0	Departamento de Informática	Edición y aprobación R.EX.N°5196
29-12-2015	4.0	Departamento de Informática	Edición y aprobación R.EX.N°4287
30-11-2016	5.0	Departamento de Informática	Edición y aprobación R.EX.N°1853
22-12-2017	6.0	Departamento de Informática	Edición y aprobación R.EX.N°1323
1-10-2018	7.0	Jorge Romero V. Solange Godoy	1. Cambio de año de política a 2018 en portada 2. Cambios de formato (Indentación en índice, eliminación de fechas en pie de página, viñetas en Sección II y alineación título Sección V-k)) 3. Sección I se agrega descripción de Requisito de Control A.05.01.02 y A.06.01.01 4. Sección II e) se modifica eliminando Decretos Supremos 81, 77 de 2004 y 100 de 2006, los que han sido derogados además de "política nacional de ciberseguridad" y "circular 16 sobre austeridad, probidad y eficiencia en el uso de los recursos públicos" 5. Se agregaron roles de Comisiones, Unidades y Departamento de Recursos Humanos 6. Se eliminó letra g) del punto II "Lineamientos de la política general 7. Sección III, se complementó letra a) y se eliminó párrafo alusivo a aplicaciones 8. Sección IV, se elimina párrafo en letra a) "Perímetro de Seguridad Física" y se eliminaron letras e)" retiro de activos de información" y f)" plan de emergencias para la continuidad del negocio" 9. Sección V b) "Procedimiento de Gestión de Usuarios" cambia a "Procedimiento de Gestión alta modificación y baja de usuarios". Se eliminaron los párrafos "Procedimiento de seguridad informática" y "recuperación en caso de desastres". Además de algunos párrafos específicos en "red computacional" y "herramientas de apoyo a la gestión interna" 10. Sección VI se eliminó párrafo "Incorporación de la política a los actos administrativos y contratos" además de párrafos específicos en "publicación, difusión y obligación de conocimiento", "fomento de su cumplimiento" y "evaluación y actualización" 11. Sección VII, Equipos de informática móvil: cambio "Palmtops" por "Tablets". Eliminación de Smart Cards. 12. Sección VII, Medios Removibles, se agrega tokens de firma

			13.Cambio en sección de firmantes
01-10-2019	8.0	Área de Tecnologías de la Información	1. Punto II, letra e), se incorpora lo establecido en la Política de Lineamientos Normativos. Letra f) se elimina Departamento/Áreas y se cambia Departamento de Personal por Unidad de Gestión y Desarrollo de las personas. 2. Punto III, Se cambia título a Gestión de Activos de Información. Letra a) párrafo 4 se cambia Departamento de Informática, por Unidad de Tecnologías de la Información. Letra c), párrafo 2 cambia Departamento de Informática, por Unidad de Tecnologías de la Información. 3. Punto IV, en título se agrega "y las operaciones". Letra b) párrafo 2 cambia Departamento de Informática, por Unidad de Tecnologías de la Información. 4. Punto V, letra a) cambia Departamento de Informática, por Unidad de Tecnologías de la Información. Letra b), se cambia procedimiento de Gestión, Alta, Modificación y baja de Usuarios, por Procedimiento de Gestión de Activos. Se elimina Departamento/Áreas. Se cambia Departamento de Personal por Unidad de Gestión y Desarrollo de las Personas. Se cambia Departamento de Bienes y Servicios por Unidad de Bienes y Servicios. Se cambia Departamento de Informática, por Unidad de Tecnologías de la Información. Letra c), párrafo 2 cambia Departamento de Informática, por Unidad de Tecnologías de la Información. Letra d) cambia Departamento de Informática, por Unidad de Tecnologías de la Información. Se elimina párrafo que hacía mención a la "Política y Normas de Uso en Materia Informática". Se incorpora punto acerca del patrón del correo institucional. Cambia Departamento de Informática, por Unidad de Tecnologías de la Información. Letra f), Letra e) cambia Departamento de Informática, por Unidad de Tecnologías de la Información. Se elimina "Departamento". Cambia Departamento de Informática, por Unidad de Tecnologías de la Información. Letra i), cambia Departamento de Informática, por Unidad de Tecnologías de la Información. 5. Se Incorpora sección documentos relacionados 6. Cambio en sección firmantes.
17-08-2020	8.1	Área de Tecnologías de la Información	1. Actualización en sección firmantes. 2. Mejoras en la redacción del documento en general. 3. Incorpora lo relativo a convenio de traspaso tecnológico en punto V Normas de Seguridad y Uso en Materia Informática, Letra g. Acceso mediante VPN, registro de operaciones, auditorías y restricción de uso del recurso mediante wifi abiertas.

19-05-2021	8.2	Área de Tecnologías de la Información	1. Actualiza definición de correos electrónicos de la institución, sección uso del correo electrónico.
04-11-2022	8.3	Área de Tecnologías de la Información	1. Actualización en sección firmantes. 2. Remueve dominio de laboratorio de gobierno en uso de correo electrónico. Incorpora prohibición de uso de aplicaciones o servicios gratuitos para información institucional. 3. Establece el alcance de la política para almacenamiento externo en modalidad de computación en la nube. 4. Complementa leyes y decretos 5. Complementa funciones de la institución

I. INTRODUCCIÓN

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

Control A.05.01.01
"La dirección debe definir, aprobar, publicar y comunicar a todos los empleados y a las partes externas pertinentes un grupo de políticas para la seguridad de la información".
– Requisito de Control, A.05.01.01 NCh/ISO 27001:2013

Control A.05.01.02
"Se deben revisar las políticas de seguridad de la información a intervalos planificados, o si se producen cambios significativos, para asegurar su conveniencia, suficiencia y eficacia continuas".
— Requisito de Control, A.05.01.02 NCh/ISO 27001:2013

Control A.06.01.01
"Todas las responsabilidades de la seguridad de la información deben ser definidas y asignadas".
— Requisito de Control, A.06.01.01 NCh/ISO 27001:2013

II. ANTECEDENTES GENERALES

1. Objetivo de la Política General de Seguridad de la Información.

La "Política General de Seguridad de la Información", busca resguardar la seguridad de los activos de información que son de propiedad del Ministerio, relacionados con su envío, recepción, almacenamiento, acceso y distribución.

Esta Política tiene por objeto definir y establecer los lineamientos generales del Sistema de Gestión de la Seguridad de la Información, en adelante e indistintamente "SGSI", a ser implementado y continuamente mejorado en esta Secretaría de Estado.

La información es un activo de gran valor para la Institución, y como tal, debe ser protegida en forma adecuada de las variadas amenazas y vulnerabilidades que traen consigo ambientes de trabajo cada vez más interconectados. A esta política le concierne, por lo tanto, procurar y promover la seguridad de todos los activos de información, sin perjuicio de la forma que adopten en su almacenamiento (electrónica en discos, redes u otros, o en archivos físicos) y comunicación (verbal, impresa o electrónica) de conformidad a la normativa vigente.

2. Justificación del Sistema de Seguridad de la Información.

El Ministerio es la entidad encargada de realizar funciones de coordinación y de asesorar directamente al Presidente de la República, al Ministro del Interior y a cada uno de los Ministros, sin alterar sus atribuciones proveyéndoles, entre otros medios, de las informaciones y análisis político-técnicos necesarios para la adopción de las decisiones que procedan:

a) Prestar asesoría al Presidente de la República, al Ministro del Interior y a cada uno de los Ministros, en materias políticas, jurídicas y administrativas, como asimismo, asesorar al Presidente de la República y al Ministro del Interior y demás Ministros, cuando así lo requieran, en lo que se refiera a las relaciones del Gobierno con el Congreso Nacional; como también con los Partidos Políticos y otras organizaciones sociales e instituciones de la vida nacional, en coordinación con el Ministerio Secretaría General de Gobierno:
b) Propender al logro de una efectiva coordinación programática general de la gestión de Gobierno;
c) Actuar, "Por orden del Presidente de la República", mancomunadamente con otros Ministerios, y a través de ellos, con los Servicios y Organismos de la Administración del Estado;
d) Efectuar estudios y análisis de corto y de mediano plazo relevantes para las decisiones políticas y someterlos a la consideración del Presidente de la República y del Ministerio del Interior, y

e) Informar al Ministro del Interior respecto de la necesidad de introducir innovaciones a la organización y procedimientos de la Administración del Estado

f) Coordinar y asesorar intersectorialmente a los órganos de la Administración del Estado en el uso estratégico de las tecnologías digitales.

En virtud del mandato legal y los productos estratégicos asociados, cada uno de los procesos que tiene lugar en el Ministerio involucra la generación, envío, recepción, almacenamiento y distribución de múltiples y diversos activos de información. Estos activos demandan requisitos de seguridad apropiados para garantizar los atributos esenciales de confidencialidad, integridad y disponibilidad.

La adopción de un SGSI constituye una decisión estratégica, toda vez que proporciona niveles adecuados de resguardo ante la pérdida, manipulación y/o divulgaciones no autorizadas de los activos de información institucionales, protegiendo la continuidad de la organización, gestión institucional, operativa institucional o "gestión y operatividad institucional".

3. Alcance.

Esta Política se aplicará al uso de todos los activos de información que se generen, intercambien, transporten y almacenen de forma interna y externa en modalidad de computación en la nube contratada por la institución, y entre este y los distintos Órganos de la Administración del Estado o con particulares.

De ello se desprende que sus disposiciones regirán para todo el personal del Ministerio, sea cual fuere su nivel jerárquico y/o calidad jurídica, prestadores de servicios, proveedores y cualquier persona o entidad que pueda hacer uso de la información en virtud de una autorización expresa por medio de un vínculo contractual.

4. Principio de Legalidad.

La presente Política se deberá interpretar de manera tal que su aplicación se concilie con las normas legales y constitucionales vigentes, referidas a los derechos y libertades de las personas.

5. Normativa relevante.

A continuación, se presenta el marco aplicable a la Seguridad de la Información de acuerdo con la Política de Lineamientos Normativos:

- Ley Nº 20.478, sobre recuperación y continuidad en condiciones críticas y de emergencia del sistema público de telecomunicaciones.
- Ley Nº 20.285, sobre acceso a la información pública.
- Ley Nº 17.336, sobre propiedad intelectual.
- Ley Nº 19.927, que modifica el código penal, el código de procedimiento penal y el código procesal penal en materia de delitos de pornografía infantil.
- Ley Nº 19.880, que establece bases de los procedimientos administrativos que rigen los actos de los Órganos de la Administración del Estado.
- Ley Nº 19.799, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.
- Ley Nº 19.628, sobre protección de la vida privada.
- Ley Nº 21.459, que 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.
- Ley Nº 21.180, sobre transformación digital del Estado.
- Decreto Nº 1299, de 2005, del Ministerio del Interior y Seguridad Pública, que establece nuevas normas que regulan la red de conectividad del Estado que administra el Ministerio del Interior y fija los procedimientos, requisitos y estándares tecnológicos para la incorporación a dicha red de instituciones públicas.
- Decreto Nº 83, de 2005, del Ministerio Secretaría General de la Presidencia, que aprueba norma técnica para los Órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos.

- Decreto Nº 93, de 2006, del Ministerio Secretaría General de la Presidencia, que 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 Órganos de la Administración del Estado y de sus funcionarios.
- Decreto Nº 181, de 2002, del Ministerio de Economía; Fomento y Reconstrucción que aprueba reglamento de la Ley Nº 19.799, sobre documentos electrónicos, firma electrónica y la certificación de dicha firma,
- Decreto Nº 1, de 2015, del Ministerio Secretaría General de la Presidencia, que aprueba norma técnica sobre sistemas y sitios web de los Órganos de la Administración del Estado.
- Decreto Nº 533, de 2015, del Ministerio del Interior y Seguridad Pública, que crea comité interministerial sobre ciberseguridad.
- Instructivo Presidencial Nº 008, de 2018, que imparte instrucciones urgentes en materia de ciberseguridad, para la protección de redes, plataformas y sistemas informáticos de los Órganos de la Administración del Estado
- Política Nacional de Ciberseguridad, 2018.
- Instructivo Presidencial Nº 006, de 2004, que imparte instrucciones sobre implementación y uso de la firma electrónica en los actos, contratos y cualquier tipo de documento de la Administración Central del Estado.
- Instructivo Presidencial Nº 001, de 2017, que instruye implementación de la Política Nacional sobre Ciberseguridad.

6. Roles y responsabilidades de seguridad de la información.

Esta Secretaría de Estado ha designado mediante Resolución Exenta Nº 568, de 24 de julio de 2018, al encargado de seguridad del Ministerio y mediante Resolución Exenta Nº 420, de 25 de junio de 2020, se creó y designó a los integrantes del Comité de Seguridad de la Información vinculadas al SGSI, que cumplen un rol fundamental en su diseño, implementación y actualización:

- **Encargado de Seguridad de la Información:** Actúa como asesor del Jefe de Servicio en las materias relativas a la seguridad de los activos de información, teniendo a su cargo el desempeño de las siguientes funciones:
  - Desarrollar las políticas de seguridad al interior de este Ministerio y controlar su implementación, velando por su correcta aplicación;
  - Coordinar la respuesta a incidentes que afecten a los activos de información institucionales; y
  - Establecer puntos de enlace con los Encargados de Seguridad de otros organismos públicos, así como con especialistas externos, que le permitan estar al tanto de las tendencias, normas y métodos de seguridad pertinentes.
- **Comité de Seguridad de la Información:** Tiene a su cargo la gestión de la Política General de Seguridad de la Información del Ministerio. En tal sentido, el Comité será responsable de supervisar la implementación de la presente Política, así como de proponer al Jefe de Servicio aquellas modificaciones tendientes a su actualización y mejoramiento continuo. Asimismo, el Comité estará encargado de proponer estrategias e implantar los controles que sean necesarios, para dar debida solución a las situaciones de riesgo que sean detectadas en relación con los activos de información institucionales.

Sin perjuicio del rol que cumplirán dichas entidades, es importante reconocer que el SGSI se fundamenta en una adecuada combinación entre seguridad física, seguridad lógica y –ante todo- estrategia organizacional, por lo que todo el personal de este Ministerio deberá cumplir un rol en torno al fortalecimiento del SGSI institucional.

Es por esta razón que, no obstante, los perímetros de seguridad y los procesos de seguridad informática existentes en la Institución, la responsabilidad respecto de la confidencialidad, integridad y disponibilidad de los activos de información del Ministerio residirán en cada una de las personas que trabajan en la Institución, quienes deberán encontrarse plenamente integrados al Sistema para que éste sea exitoso en

su implementación, monitoreo y actualización. De esta forma, se deberán cumplir también en el Ministerio los siguientes roles:

- **Personal del Ministerio:** Deberán conocer y cumplir la Política General de Seguridad de la Información, resguardando los atributos esenciales de los activos de información institucionales: confidencialidad, disponibilidad e integridad. Asimismo, deberán reportar al Encargado o Comité de Seguridad de la Información los incidentes o eventos que comprometan la seguridad de los activos de información.
- **Jefaturas (Divisiones/Comisiones/Unidades):** Deberán, además de cumplir con el rol que les corresponde como cualquier otro integrante del Ministerio, velar por el cumplimiento de la Política General de Seguridad de la Información en sus equipos de trabajo.
- **Unidad de Gestión y Desarrollo de las Personas:** La función de esta Unidad dentro del Ministerio será velar por la correcta inducción de los funcionarios que ingresan respecto de la seguridad de la información.

III. NORMAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN

1. Confidencialidad, integridad y disponibilidad de la información.

La información constituye un activo de valor para la Institución, razón por la cual es deber del personal resguardar el acceso por parte de personas no autorizadas y guardar reserva de la información y documentos que revistan carácter de confidenciales.

El personal deberá procurar no alterar o manipular los activos de información a los que tenga acceso, protegiendo su exactitud, a no ser que se encuentre habilitado para ello.

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

Por su parte, el Área de Tecnologías de la Información deberá garantizar y mantener la confidencialidad, integridad y disponibilidad de la información y datos de los usuarios a los que tengan acceso con ocasión de la administración de sistemas informáticos y servicios de red.

Se prohíbe la utilización de aplicaciones y servicios gratuitos para almacenamiento de información institucional. Deberá llevarse a cabo una contratación del servicio según lo que estable la ley Nº 19.886 de compras públicas, lo que deberá en cualquiera de sus formas de contratación asegurar la confidencialidad, integridad y disponibilidad de la información.

2. Clasificación de la información.

La clasificación de la información es un proceso que ordena o dispone los activos de información por categorías que implican diferentes niveles de protección y requisitos de seguridad.

Los activos de información institucionales se deberán clasificar conforme al grado de sensibilidad y criticidad de su contenido, estableciendo de esta forma los niveles de protección apropiados en relación con los atributos esenciales de la información, confidencialidad, integridad y disponibilidad.

La clasificación que se debe seguir es la que establece la Ley Nº 20.285, Sobre Acceso a la Información Pública.

3. Gestión de Activos de Información.

Se identificarán los activos de información relevantes vinculados a los procesos de provisión de este Ministerio, precisando los riesgos asociados a cada uno de ellos y los controles mitigadores aplicados. Este inventario y análisis de riesgos, permitirá al Ministerio disponer de un instrumento para diagnosticar el SGSI, sus avances, los resultados y las brechas en términos de seguridad.

Como entidad vinculada al SGSI, es responsabilidad del Comité de Seguridad de la Información la confección y actualización del inventario de activos de información, sin perjuicio de la responsabilidad que tienen los

Jefes de División/Comisión/Unidad y/o encargadas/os de cada uno de los procesos estratégicos ministeriales, de proveer la asistencia necesaria para desarrollar esta labor en óptimas condiciones.

El inventario se mantiene actualizado en virtud de las modificaciones que surgen en relación con las definiciones estratégicas de la Institución, sus procesos de provisión y demás componentes. Por esta razón, el Comité de Seguridad de la Información revisará anualmente el inventario.

IV. NORMAS DE SEGURIDAD FÍSICA Y DEL AMBIENTE

1. Perímetro de seguridad física.

El Ministerio resguardará que las instalaciones de procesamiento de información (datacenter, estaciones de trabajo, entre otros) estén ubicadas en áreas protegidas por un perímetro de seguridad definido, que incluya barreras de seguridad (paredes, puertas, accesos con llave, clave o huella digital, etc.) y controles de acceso (portería, secretarias, cámaras de seguridad, alarmas, etc.), evitando accesos físicos no autorizados, daños e interferencias.

El datacenter deberá contar con acceso restringido mediante huella digital, una bitácora de control de acceso, monitoreo continuo por medio de cámaras de seguridad y registro de grabación de video.

Todas las áreas de trabajo deberán estar protegidas por controles de entrada y salida adecuados, que aseguren el acceso sólo al personal debidamente autorizado.

2. Seguridad del equipamiento y las operaciones.

Ante los riesgos de pérdida, hurto y daños asociados a amenazas físicas y ambientales, se deberán considerar mecanismos para proteger el equipamiento que es de propiedad ministerial.

Se velará porque la ubicación de los equipos reduzca los riesgos ambientales y las oportunidades de acceso no autorizado, respetando siempre los criterios del perímetro de seguridad física detallados en el literal anterior. No estará permitida la instalación de equipos en lugares que no cumplan con las condiciones físicas y ambientales adecuadas, lo que estará sujeto a la verificación del equipo de Soporte Técnico, dependiente del Área de Tecnologías de la Información, conforme al procedimiento de gestión de usuarios que defina el Ministerio.

Los usuarios serán responsables y deberán tener la precaución necesaria en el uso cotidiano del equipamiento asignado. No se permitirá el consumo de alimentos y bebidas en la cercanía de los equipos, ni tampoco el traslado del equipamiento por parte de personal no autorizado.

3. Deber del personal ante riesgo de acceso no autorizado.

El personal del Ministerio tiene el deber de proteger las oficinas de los accesos no autorizados. Esto implica mantener las puertas de acceso cerradas si no se está circulando, no permitir la entrada y circulación de personas que no se encuentran autorizadas o que no cuentan con una justificación formal, informar a la jefatura si se detecta la presencia de una persona externa al Ministerio, entre otros.

4. Escritorio y Pantallas Limpios.

Se adoptarán buenas prácticas para el uso de equipamiento orientado a Escritorio y Pantalla Limpios dentro de la institución, a fin de promover el resguardo de los activos de información de tipo documentos, en formato papel o digital que utiliza el personal en el desarrollo de sus procesos de trabajo, reduciendo los riesgos de acceso no autorizado, pérdida o daño de los activos.

V. NORMAS DE SEGURIDAD Y USO EN MATERIA INFORMÁTICA

1. Rol Área de Tecnologías de la Información.

El Área de Tecnologías de la Información será responsable de la administración y buen funcionamiento de la red computacional del Ministerio, que considera las dependencias de Moneda 1160, del Palacio de la Moneda, del Edificio Moneda Bicentenario, además de las dependencias del Ministerio en el edificio del

Congreso Nacional ubicado en la ciudad de Valparaíso, y demás unidades que se integren posteriormente al Ministerio.

Como encargada de la administración y buen funcionamiento de la red computacional ministerial, dicha Área implementará los controles y mecanismos necesarios para proporcionar seguridad lógica a los sistemas de información institucionales.

2. Gestión alta modificación y baja de usuarios

Se establecerá en esta Secretaría de Estado, un Procedimiento que defina las responsabilidades y la secuencia de actividades a seguir en el Ministerio frente al ingreso, modificación de funciones y/o cargo y desvinculación, en términos de la habilitación/deshabilitación de oficinas, la asignación / devolución de recursos informáticos, la habilitación/deshabilitación de cuentas de usuario, la entrega/remoción de permisos de acceso, entre otros.

Esta norma, perteneciente a la Política General de Seguridad de la Información, formalizará y regulará la coordinación estratégica que debe existir entre cada una de las Divisiones/Comisiones/Unidades del Ministerio, la Unidad de Gestión y Desarrollo de Personas, el Área de Bienes y Servicios, y el Área de Tecnologías de la Información, para la oportuna instalación/desinstalación de las estaciones de trabajo y los recursos informáticos, asegurando la creación, actualización y eliminación de los privilegios de acceso de usuarios, teniendo como finalidad el resguardo de la seguridad de los activos de información institucionales.

3. Responsabilidad de los usuarios.

Los usuarios del Ministerio tendrán a su disposición el acceso a equipos de uso personal, diversos recursos de la red computacional y uso del correo electrónico, como una forma de facilitar el cumplimiento de sus funciones.

Por esta razón, el uso de los servicios y sistemas suministrados por el Ministerio, incluyendo redes de datos, correo electrónico, sistemas de almacenamiento de datos, software de gestión y productividad, sistema de impresión y otros, debe enmarcarse en el ámbito de competencia de este, y tener como finalidad el ejercicio de las funciones propias e inherentes para las cuales el usuario ha sido contratado o se ha convenido su prestación de servicios. En consecuencia, no estará permitida la utilización de los recursos con fines comerciales o recreativos (Juegos, chat o conversación electrónica en tiempo real, redes sociales, telefonía por internet, etc.).

El usuario deberá cumplir con las normas dispuestas por el Área de Tecnologías de la Información en relación con el uso de los servicios que requiera para cumplir con su función, así como seguir los instructivos de buenas prácticas que emanen de la mencionada Área. En este sentido, el usuario será responsable de:

- Brindar un cuidado razonable al equipo que le ha sido asignado para el desempeño de sus labores. No estará permitido el consumo de alimentos y bebidas en la cercanía de los equipos, ni tampoco el traslado del equipamiento por parte de personal no autorizado para ello.
- Aceptar las actualizaciones del sistema operativo y aplicaciones instaladas en el equipo asignado, proceso que se realizará habitualmente. Para ello deberá seguir paso a paso las instrucciones que se indican de forma automática.
- Bloquear el equipo al ausentarse de su puesto de trabajo durante la jornada laboral, en periodos extensos.
- Apagar el equipo al finalizar su jornada laboral (CPU, Monitor, Parlantes, etc.) si las funciones que se realizan lo permiten.

4. Sobre la red computacional.

El servicio de red es una herramienta importante para el normal y óptimo funcionamiento del Ministerio, por lo que su incorrecta utilización por parte de algunos usuarios no sólo puede perjudicar las tareas de otros usuarios, sino que también puede comprometer la seguridad de la información que diariamente se

transmite, comparte y almacena a través de este recurso. El Área de Tecnologías de la Información tendrá las facultades para monitorear permanentemente el tráfico que producen los usuarios en la red.

Ante hallazgos importantes o reiterativos, el Área de Tecnologías de la Información reportará al Comité de Seguridad de la Información, entidad que propondrá las medidas que estime convenientes a fin de corregir la situación.

Queda estrictamente prohibido la utilización de redes ministeriales para tener acceso a pornografía, juegos de azar y actividades ilícitas.

5. Uso del correo electrónico.

Para la utilización del correo electrónico, deberá tenerse en consideración los siguientes criterios básicos asociados a su uso seguro:

- El sistema de correo electrónico es una herramienta de trabajo que el Ministerio pone a disposición de los usuarios. Por esta razón, la información intercambiada por este medio deberá restringirse a propósitos institucionales.
- El Área de Tecnologías de la Información no realizará respaldos de los correos en las carpetas locales de los usuarios, siendo responsabilidad de éstos hacerlo.
- Cada usuario deberá mantener bajo reserva su clave de acceso a la red institucional, la que permitirá el ingreso al correo electrónico, entre otros recursos.
- El usuario deberá abstenerse de transmitir información confidencial o reservada por este medio, dado que no está garantizada la confidencialidad de los textos enviados a Internet, a menos que estos sean encriptados.
- Los correos electrónicos de la institución serán administrados por el Área de Tecnologías de la Información siguiendo el patrón de creación: "[InicialPrimerNombre][PrimerApellido]@[dominio].gob.cl" y en casos de duplicidad de cuentas "[InicialPrimerNombre][PrimerApellido][InicialSegundoApellido]@[dominio].gob.cl". Este patrón de correo será considerado como el oficial de la Institución, manteniendo su debida disponibilidad, resguardo y respaldo de la información.
- Las personas que ingresan a realizar su práctica profesional al Ministerio se les creará un correo electrónico de "practica[NúmeroCorrelativoDeCreación]@[dominio].gob.cl", el cuál será para ser utilizado en la institución. El Área de Tecnologías de la Información deberá restringir el envío de información fuera de la institución.
- Los dominios oficiales de la institución serán los siguientes:
  - @minsegpres.gob.cl
  - @consejodeauditoria.gob.cl
  - @digital.gob.cl

El uso del listado de direcciones de correos electrónicos es para consulta y uso exclusivo dentro del Ministerio, y está prohibido difundir este listado por cualquier medio electrónico o impreso para propósitos que no sean de uso institucional.

6. Servicio de impresión y fotocopia.

Como norma general de seguridad de la información, se establece que la utilización de las impresoras y fotocopiadoras será controlada a través de claves asignadas por el Área de Tecnologías de la Información u otro mecanismo de autenticación personal, a cada uno de los usuarios de la institución.

Estas claves serán personales e intransferibles, al estar vinculadas al ID único de usuario, el que deberá considerar todas las precauciones necesarias para mantener la confidencialidad de la contraseña asignada y velar por su correcto uso.

7. Herramientas de apoyo a la gestión interna.

En virtud de la creciente demanda por herramientas que favorezcan y faciliten la gestión interna, el Área de Tecnologías de la Información está facultada para desarrollar, mantener, operar y adquirir aplicaciones o sistemas según requerimiento.

El proceso de desarrollo, implementación y mantención de estas aplicaciones será responsabilidad del Área de Tecnologías de la Información, y su correcto uso será responsabilidad de la División/Comisión/Unidad para la cual fue diseñada e implementada cada herramienta. No obstante, los centros de responsabilidad que requieran llevar a cabo su propia línea de adquisición deberán canalizar sus solicitudes de igual forma mediante la División de Administración General.

En relación con el intercambio de sistemas de información entre el Ministerio y entidades externas, se adoptarán los protocolos existentes en la Administración Pública, de modo que los acuerdos o solicitudes de intercambio deberán ser formalizados mediante un convenio de traspaso tecnológico el cual establezca obligaciones de las partes, confidencialidad de la información, protección de los datos personales, propiedad intelectual, contrapartes técnicas de ambas partes y costos asociados.

8. Uso y acceso a redes virtuales privadas.

Para las necesidades de trabajo remoto y acceso a la red del Ministerio fuera de las dependencias institucionales, el Área de Tecnologías de la Información podrá autorizar, a ciertos usuarios, el uso de redes virtuales privadas (en adelante, "VPN" – Virtual Private Network). Sólo usarán las conexiones VPN los usuarios aprobados por el Área de Tecnologías de la Información que cuenten con computadores con un antivirus actualizado. El uso de este recurso como cualquier equipo proporcionado por la institución para trabajo de forma remota será susceptible a auditoría. Se encuentra prohibido hacer uso de este recurso hacia la institución mediante conexiones wifi-abiertas proporcionadas de forma gratuita en lugares públicos. Deberá hacer uso de redes privadas con modalidad de cifrado de forma mínima en WPA2-PSK y WPA/WPA2-PSK.

El Área de Tecnologías de la Información es responsable de los accesos de usuarios autorizados a ingresar a la red del Ministerio a través de VPN. Asimismo, es responsabilidad de aquellos usuarios autorizados a ingresar a través de VPN contar con el enlace internet apropiado y mantener de manera segura sus datos de conexión proporcionados.

En lo que respecta al uso de infraestructuras tecnológicas en la nube, será obligatorio el uso de VPN propias de cada plataforma para acceder a los recursos y se deberá llevar un control de la asignación y revocación de los permisos, siendo responsabilidad de cada centro de responsabilidad encargado de la administración del recurso hacerlo.

9. Servicio de soporte técnico e informático.

El Área de Tecnologías de la Información, a través de su Área de Soporte Técnico, realiza servicios de soporte únicamente respecto de los servicios y equipamiento proporcionados por el Área de Tecnologías de la Información: correo electrónico, programas, portales web, sistemas informáticos, redes, equipos e impresoras.

En caso de dificultades técnicas u operacionales, el usuario deberá comunicarse con la Mesa de Ayuda Informática a través de la dirección de correo soporte@minsegpres.gob.cl o al anexo 5800. El horario de atención de la Mesa de Ayuda Informática es de lunes a viernes de 07:30 a 20:00 horas. Ante una eventualidad de alguna División/Comisión/Unidad fuera de este horario, deberá ser comunicada al Área de Tecnologías de la Información con la debida anticipación.

10. Acciones especiales de seguridad (obtención de pruebas).

Con motivo de una investigación sumaria o sumario administrativo, el/la Jefe/a de Servicio podrá autorizar al Área de Tecnologías de la Información, en forma escrita, sobre procesos definidos para obtener la información necesaria, garantizando afectar en el menor grado la privacidad del usuario involucrado.

VI. DISPOSICIONES FINALES

1. Publicación, difusión y obligación de conocimiento.

El/la Encargado/a de Seguridad de la Información es responsable de mantener publicada en la intranet del Ministerio la Política General de Seguridad de la Información, en forma permanente.

Sin perjuicio de lo anterior, el personal de este Ministerio deberá conocer y dar fiel cumplimiento a la Política General de Seguridad de la Información. Para lo anterior, el Ministerio publicitará esta política a través de la intranet institucional y se enviará una vez al año un correo masivo informando esta política a todos los funcionarios del Ministerio.

2. Fomento de su cumplimiento y supervisión.

Sin perjuicio de las responsabilidades de publicación y difusión mencionadas, todas las jefaturas deberán fomentar y supervisar el cumplimiento de la presente Política en sus equipos de trabajo.

El/la Encargado/a de Seguridad de la Información y el Comité de Seguridad de la Información estarán facultados para revisar y evaluar el nivel de cumplimiento de la Política y sus normas anexas, cuando lo estimen necesario y/o conveniente.

El incumplimiento de la Política General de Seguridad de la Información y normas anexas puede dar origen a la consiguiente responsabilidad y eventuales sanciones administrativas, conforme a la legislación vigente.

3. Evaluación y actualización.

Con el fin de asegurar su continua idoneidad, eficiencia y eficacia, la Política General de Seguridad de la Información será evaluada y actualizada cada dos años. Asimismo, el enfoque de seguridad de la información implementado en el Ministerio deberá ser revisado por el Comité de Seguridad de la Información cuando ocurran cambios significativos en el Ministerio.

VII. DOCUMENTOS RELACIONADOS

- Política de Continuidad de la Seguridad de la Información
- Política de Desarrollo
- Política de Gestión de Proveedores
- Política de Lineamientos Normativos
- Política de Gestión de Medios Removibles
- Política de Segregación de Funciones
- Política de Seguridad de la Información en la Gestión de Proyectos
- Política de Seguridad de las Operaciones
- Política de Seguridad en las Redes y Comunicaciones
- Política de Seguridad Perimetral
- Política de Selección
- Política de Uso de Equipamiento
- Política Dispositivos Móviles
- Política de Acceso a la Información
- Política Gestión de Operaciones
- Política de Respaldo de Información
- Política de Datos de la Organización
- Política de Seguridad de la Información para las Relaciones con el Proveedor
- Procedimiento contacto con autoridades y grupos especiales de interés
- Procedimiento de Gestión de Activos
- Procedimiento de sensibilización de Seguridad de la Información
- Procedimiento de Sincronización de Relojes
- Procedimiento Evaluación y Decisión de los Eventos de Seguridad de la Información
- Procedimiento de Controles para Código Malicioso
- Procedimiento de Acceso a la Información
- Procedimiento de Seguridad Perimetral
- Procedimiento de Separación de las Redes
- Procedimiento Retiro de Activos

- Procedimiento Mensajería Electrónica
- Procedimiento Controles de Red
- Procedimiento Seguridad de Servicios de Red
- Procedimiento de Seguridad en la Gestión de Proyectos
- Procedimiento de Medios Removibles
- Procedimiento de Segregación de Funciones
- Procedimiento de Mantenimiento de Equipos
- Procedimiento de Uso de Equipamiento
- Procedimiento de Instalación de Software
- Procedimiento de Gestión de Operaciones
- Procedimiento de Selección
- Procedimiento de Desarrollo
- Procedimiento de Continuidad de la Seguridad de la Información
- Procedimiento de Lineamientos Normativos

VIII. GLOSARIO

Para los propósitos de la presente Política, normas asociadas y el SGSI en su conjunto, se entenderá por:

A	
Activos de información	Todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de la información que es de valor para la Institución. Se distinguen tres niveles básicos de activos de información: 1. La información propiamente tal, en sus múltiples formatos (papel, digital, texto, imagen, audio, video, etc.); 2. Los equipos/sistemas/infraestructura que soportan esta información; y 3. Las personas que utilizan la información y que tienen el conocimiento de los procesos institucionales. Conforme a estos antecedentes es posible observar que activos de información son, por ejemplo: bases de datos, software especializado, equipos computacionales, respaldos en los servidores, las personas que trabajan diariamente en la ejecución de cada uno de los procesos de la Institución, archivos y documentos en formato digital o papel, entre muchos otros.
C	
Confidencialidad	Propiedad de resguardar los activos de información del acceso no autorizado.
Continuidad del negocio	Continuidad de las operaciones del Ministerio.
Control	Medio para manejar el riesgo.
Correo electrónico	Transmisión electrónica de información a través de un protocolo de correo como SMTP o IMAP.
D	
Disponibilidad	Propiedad que determina el acceso oportuno a los activos de información por parte de las personas autorizadas, toda vez que lo requieran.
Documento electrónico	Toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior.
Documento electrónico institucional	Documento electrónico creado, enviado, comunicado o recibido por los usuarios del Ministerio, en ejercicio de las funciones propias de la institución.
E	

Evento de seguridad de la información	Situación que indica una posible violación de la Política de Seguridad de la Información, la falta de salvaguardas o una situación previamente desconocida que pueda ser relevante para la seguridad de los activos de información.
Equipos de informática móvil	Equipos informáticos transportables, que tienen la funcionalidad de mantener al usuario comunicado a través de conexiones de red informáticas o telefónicas. Entre este tipo de recursos se encuentran: notebooks, tablets, laptops, teléfonos móviles y otros que posean la misma funcionalidad.
F	
Factibilidad de autenticación	Propiedad que establece la posibilidad de verificar o confirmar la identidad digital del usuario que generó un documento electrónico y/o que utiliza un sistema informático.
I	
Incidente de seguridad de la información	Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de amenazar o poner en riesgo uno o varios activos de información, y con ello, comprometer la continuidad del negocio.
Integridad	Propiedad de salvaguardar la veracidad y exactitud de los activos de información y sus modificaciones (las que sólo pueden ser efectuadas por entes debidamente autorizados).
M	
Medios Removibles	Dispositivos en los que se puede almacenar información para ser transportada, como cintas, discos, memorias flash, discos duros externos, CDs, DVDs, tokens de firma, medios impresos y otros.
N	
Negocio	Función o servicio prestado por el Ministerio.
P	
Política de Seguridad de la Información	Intención y dirección general que reúne un conjunto de normas y buenas prácticas, declaradas formalmente por la dirección y aplicadas por el Ministerio, cuyo objetivo es disminuir el nivel de riesgo al que están expuestos los activos de información, con el fin de garantizar la continuidad del negocio.
Procesos de provisión	Procesos destinados a proveer los productos estratégicos de la Institución y dar cumplimiento a la misión institucional. Corresponden a los procesos del negocio.
Procesos de soporte	Procesos de apoyo al negocio de la Institución.
R	
Red Computacional	Conjunto de hardware (computadores, impresoras, etc.) y software intercomunicados entre sí para compartir información, recursos y servicios.
Riesgo	Combinación entre la probabilidad de ocurrencia de un acontecimiento y su consecuencia o impacto, que se constituye como una vulnerabilidad o amenaza ante los atributos esenciales de un activo de información.
S	
Seguridad de la información	Preservación de la confidencialidad, integridad y disponibilidad de los activos de información. Además, en el caso de los activos de información en formato electrónico, la seguridad de la información involucra la propiedad de factibilidad de autenticación.
Seguridad física	Aspecto de la seguridad de la información que consiste en la aplicación de perímetros y condiciones ambientales de seguridad, para resguardar

	la confidencialidad, integridad y disponibilidad de los activos de información.
Seguridad lógica	Aspecto de la seguridad de la información que consiste en la aplicación de procedimientos de protección y restricción de acceso a datos y programas, para resguardar la confidencialidad, integridad y disponibilidad de los activos de información contenidos en sistemas informáticos.
Sistema de Gestión de la Seguridad de la Información	Parte del sistema de gestión global del Ministerio, basada en un enfoque de riesgos del negocio, cuyo fin es establecer, implementar, operar, monitorear, revisar, mantener y mejorar una Política de Seguridad de la Información.
Sistema informático	Uno o más computadores, software asociado, periféricos, terminales, procesos físicos, medios de transferencia de información y otros, que forman un todo autónomo capaz de realizar procesamiento de información y/o transferencia de información.
U	
Usuario	Funcionario del Ministerio o cualquier persona o institución autorizada, que utiliza un sistema informático, correo electrónico o red de conectividad proporcionado o administrado por el Ministerio, ya sea que lo utilice en virtud de un empleo, de una función o de cualquier prestación de servicio, sin importar la naturaleza jurídica de esta o del estatuto que lo rija.

2º.- DÉJASE sin efecto la Resolución Exenta Nº 694, de 27 de agosto de 2021, de esta Secretaría de Estado, que aprobó la Política General de Seguridad de la Información del Ministerio Secretaría General de la Presidencia.

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE

REPÚBLICA DE CHILE MINISTERIO SECRETARÍA GENERAL DE LA PRESIDENCIA

MACARENA LOBOS PALACIOS
Subsecretaria General de la Presidencia

CFS/STG/JDE/VVH
DISTRIBUCIÓN:
1. MINSEGPRES (Gabinete Subsecretaria)
2. MINSEGPRES (Unidad de Fiscalía Interna)
3. MINSEGPRES (División de Administración General:
   - Área de Tecnologías de la información)
4. MINSEGPRES (Oficina de Partes)