Ministerio Secretaría General de la Presidencia

Gobierno de Chile

APRUEBA POLÍTICA DE SEGURIDAD PERIMETRAL DEL MINISTERIO SECRETARÍA GENERAL DE LA PRESIDENCIA.

RESOLUCIÓN EXENTA Nº 276 /

SANTIAGO, 20 MAR 2023

VISTOS:

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; la ley N° 19.880, que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del 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; el Decreto Supremo Nº 12, de 2022, de este Ministerio, que designa a su Subsecretaria; 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.

CONSIDERANDO:

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 múltiples y diversos activos de información que demandan requisitos de seguridad apropiados con el objeto de que el personal interno y externo de la institución tengan un control de acceso físico a cada una de las dependencias del Ministerio.

3.- Que, en razón de lo anterior, es necesario establecer una Política de Seguridad Perimetral como parte integrante del Sistema de Seguridad de la Información, enmarcándose en el cumplimiento de la Norma Chilena ISO 27001:2013, cuyo objetivo principal es la protección de la información de esta Secretaría de Estado.

4.- Que, de acuerdo con lo expuesto, y lo solicitado mediante Memorándum Nº 00078, de 2023, del Jefe de la División de Administración General de este Ministerio, el presente acto administrativo viene en aprobar la "Política de Seguridad Perimetral del Ministerio Secretaría General de la Presidencia".

RESUELVO:

ARTÍCULO ÚNICO.- APRUÉBASE la "Política de Seguridad Perimetral del Ministerio Secretaría General de la Presidencia", de fecha 26 de julio de 2022, cuyo texto es el siguiente:

"Controles NCH ISO 27001:2013 Relacionados

Control	*Nombre*
A.11.01.01	*Perímetro de seguridad física*
A.11.01.02	*Controles de acceso físico*
A.11.01.04	*Protección contra amenazas externos del ambiente*
A.11.02.01	*Ubicación y protección del equipamiento*
A.11.02.02	*Elementos de soporte*
A.11.02.04	*Mantenimiento del equipamiento*
A.11.02.05	*Retiro de activos*
A.11.02.07	*Seguridad de la reutilización o descarte de equipos*

Nota de confidencialidad

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

2022

Control de versiones

Fecha	*Versión*	*Responsables*	*Descripción*
30-05-2019	*1.0*	*Jorge Romero Vargas* *Solange Godoy Carrera*	*Elaboración de Documento*
14-09-2020	*1.1*	*Jorge Romero Vargas*	*Mejoras en la redacción del documento*
29-06-2021	*1.2*	*Jorge Romero Vargas*	*Incorpora nueva dependencia Laboratorio de Gobierno. Mejoras en la redacción. Actualización en sección firmantes.*
31-08-2021	*1.3*	*Jorge Romero Vargas*	*Mejoras en la redacción del documento. Se incluye forma de entrega del equipamiento para funcionarios/as y colaboradores/as en trabajo remoto. Actualización en sección firmantes.*
26-07-2022	*1.4*	*Jorge Romero Vargas*	*Se remueve dependencia de Laboratorio de Gobierno. Actualización en sección firmantes.*

Introducción

El Ministerio Secretaría General de la Presidencia, dispondrá de la presente política, denominada "Política de Seguridad Perimetral", 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 27001:2013, cuyo objetivo principal es la protección de la información, permitiendo a la organización evaluar los riesgos de

información a los que se encuentra expuesta, así como a la aplicación de controles para mitigarlos, para alcanzar un sistema de información en el que se dé la confidencialidad, integridad y disponibilidad de los activos de información. Dichos controles son los siguientes:

Control A.11.01.01 Perímetro de seguridad física

"Se deben definir y utilizar perímetros de seguridad para proteger las áreas que contienen, ya sea información sensible o crítica, y las instalaciones de procesamiento de información".

- *Requisito de control, A.11.01.01 NCH – ISO 27001:2013*

Control A.11.01.02 Controles de acceso físico

"Las áreas seguras deben estar protegidas por controles de entrada apropiados que aseguren que solo se permite el acceso a personal autorizado".

- *Requisito de control, A.11.01.02 NCH – ISO 27001:2013*

Control A.11.01.04 Protección contra amenazas externas del ambiente

"Se debe diseñar y aplicar la protección física contra daños por desastre natural, ataque malicioso o accidentes".

- *Requisito de control, A.11.01.04 NCH – ISO 27001:2013*

Control A.11.02.01 Ubicación y protección del equipamiento

"El equipamiento se debe ubicar y proteger para reducir los riesgos ocasionados por amenazas y peligros ambientales, y oportunidades de acceso no autorizado".

- *Requisito de control, A.11.02.01 NCH – ISO 27001:2013*

Control A.11.02.02 Elementos de soporte

"Se debe proteger el equipamiento contra fallas en el suministro de energía y otras interrupciones causadas por fallas en elementos de soporte".

- *Requisito de control A.11.02.02 NCH – ISO 27001:2013*

Control A.11.02.04 Mantenimiento del equipamiento

"El equipamiento debe recibir el mantenimiento correcto para asegurar su permanente disponibilidad e integridad".

- *Requisito A.11.02.04 NCH – ISO 27001:2013*

Control A.11.02.05 Retiro de activos

"El equipamiento, la información o el software no se deben retirar del local de la organización sin previa autorización".

- *Requisito de control A.11.02.05, NCH – ISO 27001:2013*

Control A11.02.07 Seguridad de la reutilización o descarte de equipos

"Todos los elementos del equipamiento que contenga medios de almacenamiento deben ser revisados para asegurar que todos los datos sensibles y software licenciado que se hayan removido o se haya sobrescrito con seguridad antes de su descarte o reutilización".

- *Requisito de control A.11.02.07, NCH – ISO 27001:2013*

1. Alcance

Esta política se aplicará en todas las instalaciones y equipamiento que sean utilizados para el funcionamiento de la seguridad perimetral de este Ministerio, así como de todos los trabajadores, alumnos en práctica y terceros que puedan estar realizando funciones para el Ministerio y que requieran autorización para el acceso físico a las dependencias de la Institución, ubicadas en el Palacio de La Moneda, Edificio Moneda Bicentenario, Edificio Moneda N° 1160, en Santiago, Región Metropolitana de Santiago, y en el Congreso Nacional, en Valparaíso, Región de Valparaíso.

2. Objetivo

Proteger la información de la institución, asegurando que el personal interno y externo tengan un control de acceso físico a cada una de las dependencias del Ministerio. Las dependencias de la institución se encontrarán resguardadas, llevando un registro de ingreso y un ambiente adecuado para la seguridad del equipamiento institucional.

Se mantendrán controles preventivos contra cualquier amenaza que pueda perjudicar el normal funcionamiento de los equipos, manteniéndolos en un lugar adecuado para la protección de éstos, contando con elementos y mantenimiento, el cual deberá realizar el Área de Soporte Técnico y el Área de Redes y Seguridad del Ministerio.

3. Roles y responsabilidades

Independiente del cargo/rol que se desempeñe, nivel jerárquico y de la modalidad bajo la cual se encuentre contratado, será responsabilidad de todo el personal de este Ministerio conocer y dar el debido cumplimiento a esta norma. Asimismo, será responsabilidad de:

- ***Del Encargado del Área de Tecnologías de la Información***
  Delimitar las áreas de seguridad perimetral de la institución, realizando revisiones periódicas a cada uno de los perímetros, identificando oportunidades de mejora.
- ***Del Encargado del Área de Redes y Seguridad***
  El monitoreo constante de las cámaras de seguridad de las dependencias de la institución, así como llevar a cabo planes de acción frente a cualquier evento que interrumpa o deteriore la calidad del servicio que proporciona el Área de Tecnologías de la Información.
- ***Del Encargado de Seguridad de la Información***
  La elaboración de esta norma, su actualización y velar por su cumplimiento, así como la realización de revisiones periódicas del cumplimiento de esta.
- ***De los/las Jefes/as de División, Comisión, Unidades***
  Difundir y concientizar a los trabajadores a su cargo del cumplimiento de esta norma.

4. Mecanismo de difusión

Es responsabilidad del Comité de Seguridad de la Información, la difusión de esta política, la que deberá ser enviada por correo electrónico a cada trabajador y 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 lo disponga.
El Encargado de Seguridad de la Información, deberá informar en sesión del Comité de Seguridad de la Información, los cambios y/o actualizaciones de esta política. El Comité de Seguridad de la Información deberá revisarla, observarla y aprobarla según corresponda.

6. *Definiciones*

Las dependencias del Ministerio Secretaría General de la Presidencia deberán contar con protección adecuada que permita garantizar la disponibilidad y seguridad de la información en un funcionamiento óptimo.

- ***Control A. 11.01.01 Perímetro de seguridad física***

  Los perímetros de seguridad física de la institución son los siguientes:
  - *Palacio de La Moneda, Santiago*
  - *Edificio Moneda 1160, piso EP, 2,3,4,5,6, Santiago*
  - *Edificio Moneda Bicentenario, piso 9, Santiago*
  - *Congreso Nacional, piso 2, Cámara de Diputados, Valparaíso*
  - *Congreso Nacional, piso 4, Senado, Valparaíso*

- ***Control A.11.02.02 Controles de acceso físico***

  Palacio de La Moneda:
  - *Vigilancia policial en la entrada*
  - *Credenciales de acceso para transito*
  - *Recepción en la entrada al Palacio*

  Edificio Moneda 1160, piso EP, 2, 3, 4, 5 y 6

  - *Ingreso a cada uno de los pisos con claves de acceso o huella dactilar*
  - *Conserjería externa*
  - *Cámaras de seguridad en todas las entradas de los pisos y acceso principal*

  Edificio Moneda Bicentenario, piso 9
  - *Recepción en la entrada del edificio*
  - *Torniquetes de acceso al edificio con credencial*
  - *Ingreso al piso, con credencial, clave y/o huella dactilar*
  - *Cámaras de seguridad en las entradas del piso y espacios de trabajo para seguridad de los bienes*

  Congreso Nacional, piso 2 y 4
  - *Recepción puertas de acceso*
  - *Credenciales de acceso y transito*
  - *Torniquetes de acceso*
  - *Vigilancia policial de entrada*

  Área de Tecnologías de la Información, sala de servidores
  - *Cámaras de seguridad en salas de servidores y espacios de trabajo para seguridad de los bienes*
  - *Moneda 1160. Puerta de acceso al Área de Tecnologías de la Información y Sala de Servidores con clave de acceso y huella dactilar.*
  - *Edificio Moneda Bicentenario Piso 9. Puerta de acceso a la Sala de Servidores con clave de acceso y huella dactilar.*

- ***Control A.11.01.04 Protección contra amenazas externas del ambiente***

  Los equipos de comunicaciones y sala de servidores estarán ubicados en espacios seguros en los que se deberá mantener un control de acceso.

  Se deberá realizar una planificación de acciones preventivas y de mitigación de riesgos asociados a cualquier amenaza que se pudieran presentar en las salas ubicadas en el Área de Tecnologías de la Información, Moneda 1160 - piso 6 y Edificio Moneda Bicentenario - piso 9.

- ***Control A.11.02.01 Ubicación y protección del equipamiento***

El Área de Redes y Seguridad deberá monitorear constantemente la temperatura y humedad de las salas de servidores.

Los equipos deberán estar en un ambiente libre de polvo, materias contaminantes, interferencias electromagnéticas y dentro de los siguientes rangos de temperatura y humedad:

Temperatura: 20 ±5ºC

Humedad: Entre 20 y 80% sin condensación.

Las salas de servidores deberán contar con cámaras de vigilancia y control de acceso mediante clave y/o huella dactilar. El acceso a las áreas de trabajo y sala de servidores que contengan información deberá ser restringido sólo a las personas autorizadas y con su debida justificación.

Cuando el equipamiento computacional esté en uso no se deberá consumir ningún tipo de alimento o líquido.

No se deberán colocar objetos de ningún tipo sobre el equipamiento, tampoco cubrir o tapar los orificios de ventilación de estos, incorporar material adhesivo o adornos de ningún tipo.

Los cables de conexión eléctrica o comunicaciones deberán estar en un lugar seguro en el que no sean pisados, ni se pueda poner objetos sobre ellos. Todo cable dañado deberá ser reemplazado de forma inmediata por uno nuevo. Está prohibido el uso de cables añadidos o con adaptaciones.

Los equipos portátiles deberán contar con candado de seguridad o en caso de no uso ser guardado bajo llave, para minimizar la probabilidad de robo o extravío.

No se deberán mantener sistemas o equipos de red sin el aseguramiento correspondiente cuando se encuentren en oficinas o lugares abiertos.

El equipamiento computacional deberá ser limpiado con un paño levemente humedecido, sin utilizar ningún tipo de líquido que pueda dañar o dejar inhabilitado para su funcionamiento. El área encargada de dar las directrices para la limpieza del equipamiento será el área de soporte técnico.

El equipamiento tecnológico de acceso biométrico a las dependencias deberá ser revisado de forma periódica. En caso de cumplir su vida útil, deberá ser reiniciado su sistema operativo, verificada la unidad de respaldo y reemplazada. Además, deberán ser verificados los sensores y alarmas de apertura de puertas.

El equipamiento computacional solo debe ser utilizado en las dependencias de la institución a excepción del equipamiento portátil.

Está absolutamente prohibido intercambiar o hacer uso de equipamiento de otro funcionario/a. Los equipos son de uso exclusivo del funcionario/a asignado. Ante daño, pérdida o robo, el funcionario/a deberá informar inmediatamente a su jefatura y el Área de Tecnologías de la Información.

- ***Control A.11.02.02 Elementos de soporte***

El Ministerio deberá contar con el equipamiento necesario para la protección de los equipos ante eventuales cortes de suministros eléctrico, o por otras eventualidades que surjan en los servicios básicos de apoyo, por cuanto, el servicio deberá mantener a lo menos:

- *Buenas condiciones de iluminación de emergencia y de todo artefacto de respaldo para las comunicaciones y continuidad del servicio en caso de emergencias.*
- *Visibilidad y fácil acceso a las válvulas de cortes de suministro de luz, agua y gas.*
- *Extintores de incendio adecuados a cada necesidad, ya sea para equipamiento computacional en sala de servidores u otros espacios dentro de las dependencias.*

- ***Control A.11.02.04 Mantenimiento del equipamiento***

  El Área de Soporte Técnico se encargará del mantenimiento del equipamiento computacional de la institución, los que deberán mantenerse en buenas condiciones de uso, realizando pruebas, inspecciones, ajustes, reemplazo, reinstalaciones, calibración y/o reparaciones. Se deberá realizar una planificación para el mantenimiento de los equipos, recuperación de la información que se pueda encontrar almacenada en estos, así como también la eliminación de software maliciosos, archivos temporales y eliminación de registros que se encuentren dañados.

  Esta planificación deberá contar con una programación de mantenimiento preventivo de equipos computacionales e impresoras, para lo cual, se deberá tomar contacto con los servicios externos que sean necesarios o que tengan contrato vigente con el Ministerio para la mantención preventiva.

  El encargado de redes y seguridad estará a cargo de la mantención del equipamiento ubicado en las salas de servidores de la institución, las que deberán contar con un mantenimiento adecuado para su funcionamiento. Deberá mantener una constante coordinación con personal especializado ya sea de equipamiento como control del aire acondicionado o climatización.

- ***Control A.11.02.05 Retiro de activos***

  El retiro de activos del Ministerio Secretaría General de la Presidencia deberá contar con la autorización de la jefatura correspondiente, la que deberá comunicar al Área de Tecnologías de la Información, el motivo por el cual debe ser retirado.

  Sólo el personal del Área de Soporte Técnico, correspondiente al Área de Tecnologías de la Información podrá hacer retiro de los equipos. Cabe destacar que los funcionarios/as y colaboradores/as que se encuentren realizando trabajo remoto, deberán acercarse a las dependencias del Área de Tecnologías de la Información para poder hacer entrega del equipamiento asignado. En esa instancia, el equipo será revisado y se generará un acta de entrega conforme del bien.

  Las bajas de equipamiento computacional deberán contar con una resolución asociada para su retiro.

  Ante un cese de funciones se debe devolver el equipamiento en las mismas condiciones que fue entregado por el Área de Tecnologías de la Información, la que deberá realizar una revisión del quipo, generando un acta de recepción conforme.

- ***Control A.11.02.07 Seguridad de la reutilización o descarte de equipos***

  El equipamiento computacional del Ministerio Secretaría General de la Presidencia deberá ser revisado y analizado exclusivamente por el Área de Tecnologías de la Información con su Área de Soporte Técnico. Este equipamiento sólo podrá ser retirado de las dependencias del Ministerio con la autorización del Área de Tecnologías de la Información, siendo el área de Soporte Técnico la encargada de realizar el respaldo, formateo y/o eliminación segura de información de la institución contenida en el equipamiento, ya sea para una reutilización o descarte para baja. El área de Soporte Técnico es la única área a nivel institucional autorizada para formatear y reinstalar equipamiento computacional. Asimismo tendrá bajo su cargo el control de la vida útil del equipamiento tecnológico de la institución, el cual será evaluado para garantizar su óptimo funcionamiento y realizar la correspondiente baja cuando este se encuentre obsoleto o haya cumplido su función de manera óptima y segura. De igual forma, el área de Soporte Técnico en conjunto con el área de Redes y Seguridad, evaluarán las condiciones de funcionamiento del equipamiento de redes y comunicaciones, el cual deberá prestar servicios de la forma óptima y en caso de no cumplir las condiciones

mínimas deberá ser dado de baja y reemplazado. Los elementos tecnológicos dados de baja deberán estar ingresados en el sistema de inventario y activo fijo. Finalmente, los registros de estado de estos elementos serán actualizados en la aplicación con su respectiva resolución de baja.

Constan firmas de los miembros del Comité de Seguridad de la Información."

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE

REPÚBLICA DE CHILE
MINISTERIO
SECRETARIA GENERAL DE LA PRESIDENCIA

MACARENA LOBOS PALACIOS
Subsecretaria General de la Presidencia

RSA/CPS/STG/JRV
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)