Ministerio Secretaría General de la Presidencia

Gobierno de Chile

APRUEBA POLÍTICA DE USO DE EQUIPAMIENTO COMPUTACIONAL DEL MINISTERIO SECRETARÍA GENERAL DE LA PRESIDENCIA.

RESOLUCIÓN EXENTA Nº 398 /

SANTIAGO, 15 JUN 2020

V I S T O S:

La Ley Nº 18.993, que crea este Ministerio; el Decreto Supremo Nº 7, de 1991, de esta Secretaría de Estado, que aprueba su Reglamento Orgánico; 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 83, de 2004, 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; la Resolución Exenta Nº 1003, de 2019, que aprueba nueva Política General de Seguridad de la Información del Ministerio Secretaría General de la Presidencia; el Decreto Supremo Nº 12, de 2019, del Ministerio Secretaría General de la Presidencia, que designa a su Subsecretario; 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 relación a lo anterior, mediante Resolución Exenta Nº 1003, de 20 de noviembre de 2019, se aprobó una nueva Política General de Seguridad de la Información de este Ministerio, estableciendo los lineamientos generales de implementación del Sistema de Gestión de Seguridad de la Información, con el objeto de resguardar la seguridad de los activos de información de propiedad de esta Secretaría de Estado.

4. Que, por su parte, el uso de equipamiento computacional de este Ministerio, forma parte de la Política General de Seguridad de la Información, indicada en el considerando anterior. En específico, se enmarca en el cumplimiento de la Norma Chilena ISO 27001, la cual permite garantizar la confidencialidad e integración de la información que manipulan los organismos, llevando a cabo una evaluación del riesgo y adoptando los controles indispensables para lograr mitigarlos.

5. Que, en concordancia con lo anterior, es necesario promover una segura administración y utilización del equipamiento proporcionado por el Ministerio a su personal, en donde almacenan los activos de información, para el desempeño de sus funciones, con el fin de reducir los riesgos de pérdida y acceso no autorizado.

6. Que, de acuerdo a lo expuesto, el presente acto administrativo viene en aprobar la Política de Uso de Equipamiento Computacional del Ministerio Secretaría General de la Presidencia.

R E S U E L V O:

ARTÍCULO ÚNICO.- APRUÉBASE la Política de Uso de Equipamiento Computacional del Ministerio Secretaría General de la Presidencia, cuyo texto es el siguiente:

APRUEBA POLÍTICA DE USO DE EQUIPAMIENTO COMPUTACIONAL

DEL

MINISTERIO SECRETARÍA GENERAL DE LA PRESIDENCIA

Controles NCH ISO 27001:2013 Relacionados

CONTROL	NOMBRE
A.11.02.08	Equipo del usuario desatendido
A.11.02.09	Política de escritorio y pantalla limpios

1. Introducción

El Ministerio Secretaría General de la Presidencia, en adelante el "Ministerio", dispone del presente documento, denominado "Política de uso de equipamiento", como parte integrante del Sistema de Seguridad de la Información. En específico, se enmarca en el cumplimiento de la Norma Chilena ISO 27001, cuyo objetivo es la seguridad de la información, proponiendo como requisitos de control:

Control A.11.02.08 Equipo del usuario desatendido

"Los usuarios se deben asegurar de que a los equipos desatendidos se les da protección apropiada".

- Requisito de control, A.11.02.08 NCH-ISO 27001:2013

Control A.11.02.09 Política de escritorio y pantalla limpios

"Se debe adoptar una política de escritorio limpio para papeles y medios de almacenamiento removibles y una política de pantalla limpia para las instalaciones de procesamiento de información".

- Requisito de control, A.11.02.09 NCH-ISO 27001:2013

2. Alcance

Este documento debe aplicarse a todos los funcionarios/as y servidores/as públicos del Ministerio o a cualquier tercero que pueda estar prestando servicios, todos en conjunto denominados "usuario o usuarios", a los que se les asignará un escritorio de trabajo, equipos computacionales (fijo/portátil), el

manejo de documentación física y/o digitales y que requieran el uso de sistemas y servicios de información.

3. Objetivo

El objetivo de la "Política de uso de equipamiento", es promover una segura administración y utilización del equipamiento proporcionado por el Ministerio, para la ejecución de sus labores, en donde los usuarios almacenen los activos de información, para el desempeño de sus funciones y en virtud de las actividades propias del cargo, con el fin de reducir los riesgos de pérdida y acceso no autorizado.

Cada usuario será responsable del buen uso y resguardo del equipamiento proporcionado al finalizar la jornada laboral, asegurando la protección física de cada equipo desatendido.

Esta política protege la información del Ministerio que esté contenida en la pantalla de un equipo computacional o medios removibles, así como cualquier otra información impresa o escrita que se encuentre en las estaciones de trabajo, salas de reuniones, impresoras o que se encuentre expuesta en otros medios.

4. Roles y responsabilidades

Independiente del cargo o rol que se desempeñe, del nivel jerárquico del que se goce y de la modalidad bajo la cual se esté contratado, es responsabilidad de todo el personal de este Ministerio conocer y dar debido cumplimiento a este documento, asimismo, es responsabilidad:

- Del Encargado de Seguridad de la Información, la revisión periódica y el cumplimiento, actualización y difusión de esta Política.
- De los Jefes/as de División, Comisión y Unidades, la promoción y supervisión del estricto apego a esta política por parte de su personal a cargo.
- De la Oficina de Computación, en adelante "Unidad de Tecnología de la Información", velar por el debido cumplimiento de esta norma.
- Del Comité de Seguridad de la Información, la revisión periódica, cumplimiento, actualización y difusión de esta Política.

5. Mecanismos de difusión

Es responsabilidad del Comité de Seguridad de la Información la difusión de la "Política de uso de equipamiento", la que deberá permanecer en la Intranet institucional a disposición de todo el personal del Ministerio.

6. Evaluación y revisión

El tiempo de evaluación y revisión estándar para esta política, será cada dos años. No obstante, podrá revisarse cuando la situación lo amerite o la autoridad así lo disponga.

El encargado de seguridad de la información propondrá en Sesión del Comité de Seguridad de la Información los cambios y/o actualizaciones que sean necesarios para la presente política, quien los revisará, observará y aprobará para su correspondiente envió al Jefe de Servicio.

7. Definiciones

a) Control A.11.02.09 Política de escritorio y pantalla limpios

Toda información sensible, confidencial y/o crítica del Ministerio contenida en medios de almacenamiento removibles y/o en papel, debe estar asegurada en muebles de seguridad bajo llave (cajoneras, estantes, etc.) especialmente cuando no esté siendo utilizada y/o el usuario no se encuentre en la institución.

Asimismo, se debe prevenir el acceso no autorizado a la información, retirando la documentación inmediatamente de las impresoras y fotocopiadoras, teniendo la precaución de no dejar documentación visible de ser copiada.

Además, no se deben mantener papeles con información privada y de uso personal (como nombres de usuario y/o contraseñas de acceso), adheridos a los artefactos de oficina como escritorio, pantalla, teclado, teléfono u otros; ni tampoco deben estar visibles documentos con información sensible al momento de recibir a terceros en la oficina.

Los equipos computacionales que se encuentren desatendidos deben ser protegidos con el mecanismo de bloqueo de pantalla controlado por contraseña personal (mecanismo de autenticación de usuario), especialmente cuando la estación de trabajo esté vacía. Asimismo, es responsabilidad del usuario apagar el equipo al finalizar su jornada laboral.

Además, se recomienda mantener los archivos digitales organizados en carpetas que no estén visibles directamente en el escritorio del computador. De la misma forma, cuando se recibe a terceros en la oficina o escritorio de trabajo, se debe tener precaución respecto del contenido que se muestra en pantalla. De ser información sensible esta debe ser cerrada y mantenida en confidencialidad. Adicionalmente se sugiere lo siguiente:

- Prevenir el uso no autorizado de las impresoras y fotocopiadoras, manteniendo la reserva absoluta del código de uso personal y no dejando archivos abiertos en el computador, susceptibles de ser impresos sin la debida autorización.
- El computador asignado no se debe encontrar conectado a medios de almacenamientos fácilmente removibles (pendrives, discos duros externos, etc.)
- La pantalla del computador se debe encontrar bloqueada por un mecanismo de autenticación de usuario o bien se debe encontrar apagado.

b) Control A.11.02.08 Equipo del usuario desatendido

Los equipos que sean instalados necesitarán la protección que corresponda contra los accesos no autorizados. Debido a esto, los usuarios son los que deben asegurar que sus equipos sean protegidos apropiadamente en su ausencia:

- Bloqueando su computador a través de contraseñas de acceso cuando éste no esté siendo utilizado.
- Realizar el cierre de sesión de sus tareas cuando su equipo no cuente con supervisión.
- Los equipos portátiles (telefonía móvil, notebooks, etc.) deberán contar con la protección necesaria cuando éstos sean desatendidos evitando la manipulación de información que contengan.

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE

JUAN JOSÉ OSSA SANTA CRUZ
Subsecretario General de la Presidencia

FGR/MCC/TGI/JRV/vvh
DISTRIBUCIÓN:
1. MINSEGPRES (Gabinete Subsecretario)
2. MINSEGPRES (División Jurídico-Legislativa:
   - Unidad de Asesoría Jurídica - Administrativa)
3. MINSEGPRES (División de Administración General:
   - Unidad de Tecnología de la Información)
4. MINSEGPRES (Oficina de Partes)