Superintendencia de Seguridad Social

Gobierno de Chile

HGL/LBA/pac

REF.: Aprueba Política de Seguridad de la Información de la Superintendencia de Seguridad Social y deja sin efecto la Resolución Exenta que indica

==========

TRAMITADO

Stgo.

RESOLUCIÓN EXENTA Nº 848 /

SANTIAGO, 21 DIC 2018

VISTO:

Las atribuciones que me confieren la Ley N° 16.395, Texto Refundido de la Ley de Organización y Atribuciones de la Superintendencia de Seguridad Social; lo señalado en su Reglamento Orgánico, contenido en el D.S. N° 1, de 1972, del Ministerio del Trabajo y Previsión Social; el artículo 5º del D.F.L. N° 1-19.653, de 2001, del Ministerio Secretaría General de la Presidencia, que fija el texto refundido, coordinado y sistematizado de la Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; lo previsto en la Ley N° 19.880, que establece las bases de los procedimientos administrativos que rigen los actos de los Órganos de la Administración del Estado; en la Ley Nº 19.799, sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha Firma; en la Ley Nº 19.628, sobre Protección de la Vida Privada; en la Ley Nº 19.223, sobre Delitos Informáticos; en la Ley Nº 20.285, sobre Acceso a la Información Pública; en el Decreto Supremo Nº 83, de 2005, de la 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; lo dispuesto en la Norma Chilena NCh-ISO 27001/2013 Tecnología de la Información - Técnicas de Seguridad - Sistemas de Gestión de la Seguridad de la Información - Requisitos, especialmente en el punto 5.2; en la Norma Chilena NCh-ISO 27002/2013, Tecnología de la Información - Técnicas de Seguridad - Código de Prácticas para los Controles de Seguridad de la Información, especialmente en el punto 5.1.1; y en la Resolución Nº 1.600, de 2008, de la Contraloría General de la República que fija normas sobre exención del trámite de toma de razón, y

TENIENDO PRESENTE:

Que la Superintendencia de Seguridad Social debe regular y fiscalizar el cumplimiento de la normativa de seguridad social y garantizar el respeto de los derechos de las personas, especialmente de los trabajadores, pensionados y sus familias, resolviendo con calidad y oportunidad sus consultas, denuncias y apelaciones, proponiendo las medidas tendientes al perfeccionamiento del Sistema Chileno de Seguridad Social.

Que dentro de los objetivos estratégicos vigentes de este Organismo se encuentra el incorporar tecnologías de información y nuevas metodologías de gestión, que permitan a la ciudadanía garantizar un mejor acceso a los beneficios de Seguridad Social.

Que este Servicio debe cumplir con las normas que regulan los Procedimientos de Seguridad de la Información, de conformidad con los requisitos establecidos en el Decreto Supremo N° 83, de 2005, que aprueba la Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los

Documentos Electrónicos, así como en las Normas Chilenas NCh-ISO 27001/2013 y NCh-ISO 27002/2013.

Que considerando los requerimientos de Seguridad de la Información, así como la reciente implementación del Procedimiento Administrativo Electrónico (PAE) por parte de esta Superintendencia, se hace necesario derogar la Resolución Exenta N° 360, de 21 de diciembre de 2016.

Que este Servicio ha actualizado su Política General de Seguridad de la Información, con la finalidad de facilitar su implementación y aplicación por parte de sus funcionarios, y de terceros externos que prestan servicios y que tengan acceso a los activos de información de la Institución.

Los acuerdos tomados en Reunión del Comité de Seguridad de la Información de fecha 20 de noviembre de 2018, en el sentido de atender la necesidad y el compromiso de revisar y actualizar la Política de Seguridad de la Información en la Institución.

RESUELVO:

1. Déjese sin efecto la Resolución Exenta Nº 360 de 21 de diciembre de 2016, que Aprueba la Política General de Seguridad de la Información de la Superintendencia de Seguridad Social.

2. Apruébese la Política de Seguridad de la Información de la Superintendencia de Seguridad Social, cuyo texto se transcribe a continuación:

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

I. DECLARACIÓN INSTITUCIONAL

La Superintendencia de Seguridad Social está comprometida en proteger la confidencialidad, integridad y disponibilidad de los activos de información con que cuenta para el desarrollo de sus funciones, a través de la implementación, mantención y mejora continua de un Sistema de Seguridad de la Información.

Para ello, dispone de mecanismos administrativos, físicos y técnicos apropiados al grado de sensibilidad de la información que maneja, orientados a asegurar la continuidad operacional de la Institución, proveer un servicio de calidad a sus usuarios, y proteger la información que administra en el desempeño de sus funciones.

II. OBJETIVOS

El objetivo general de esta política es proveer un marco de trabajo en materia de seguridad de la información, orientado a proteger los activos de información de la Superintendencia de Seguridad Social de acceso no autorizado, pérdida o daño, al tiempo que permita la entrega de servicios de calidad a sus clientes, usuarios y beneficiarios.

Adicionalmente, se definen los siguientes objetivos específicos:

a) Definir e implementar un conjunto de políticas, instructivos, procedimientos y controles orientados a garantizar la confidencialidad, integridad y disponibilidad de todo activo de información que sea responsabilidad de la Institución.

b) Definir e implementar un sistema de seguridad de la información que permita una gestión adecuada sobre el control, monitoreo y evaluación periódica de los puntos críticos en el resguardo de los activos de información, mediante una gestión por riesgos.
c) Contar con una estructura organizacional de soporte al Sistema de Seguridad de la Información, que entregue lineamientos y directrices para su adecuada gestión y mejora continua.
d) Establecer un marco de responsabilidades, deberes y niveles de protección de la información, bajo el concepto de activo de información, que rijan el comportamiento de todo funcionario de planta o a contrata de esta Superintendencia, así como del personal contratado a honorarios y de terceros que presten servicios a esta Institución.
e) Asegurar el conocimiento y acceso, a través de los medios con que cuente la Institución, a la Política de Seguridad de la Información y sus instrumentos asociados, de manera comprensible y pertinente a la labor de todas las personas mencionadas en la letra d) precedente.

III. PRINCIPIOS ORIENTADORES

La Política de Seguridad de la Información de la Superintendencia de Seguridad Social se basa en los siguientes principios orientadores:

a) Confidencialidad: se debe asegurar la privacidad de la información, aplicando los controles necesarios para resguardar los activos de información de cualquier acceso no autorizado, revelaciones accidentales, espionaje y otras acciones similares.
b) Integridad: se debe asegurar la exactitud, completitud y consistencia de la información, aplicando los controles necesarios para resguardar los activos de información de cualquier degradación por efectos de agentes internos o externos, efectos ambientales o manipulación no deseada.
c) Disponibilidad: se debe asegurar que la información sea accesible y esté preparada para su uso, aplicando los controles necesarios para evitar interrupciones que afecten a los activos de información, de manera que se preserve la continuidad operacional.
d) Autorización: se deben establecer los privilegios para acceder o gestionar información, aplicando los controles necesarios para resguardar los activos de información de cualquier consulta, revisión, copia, modificación, eliminación, análisis, o manejo, otorgando autorización sólo cuando existan necesidades asociadas al cumplimiento de funciones institucionales.

IV. SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN

La Superintendencia de Seguridad Social considera que los activos de información comprenden tanto los equipos, sistemas e infraestructura tecnológica que soportan la información (sean de propiedad de la Superintendencia o externalizados), las personas que la utilizan y que tienen el conocimiento de los procesos institucionales (sean de la institución o externas a ella), así como la información propiamente tal (sea en formato físico o electrónico).

Por lo anterior, el objetivo es proteger aquellos activos de información considerados relevantes para la Superintendencia de Seguridad Social, de manera que se resguarde su confidencialidad, integridad y disponibilidad, asegurando que puedan acceder a la información sólo aquellos usuarios autorizados para hacerlo, a objeto de mantener y asegurar la continuidad operacional de la Institución.

V. ÁMBITO DE APLICACIÓN

La Política de Seguridad de la Información comprende todos los ámbitos de operación de la Superintendencia de Seguridad Social, incluyendo sus recursos y procesos, sean éstos internos, externos o gestionados a través de contratos o acuerdos con terceros.

Todos los funcionarios de la Institución (planta, contrata y honorarios), así como terceros que se vinculen con ella en el desarrollo de sus funciones deben atenerse al cumplimiento de esta Política de Seguridad de la Información. De igual forma, esta Política aplica también a todos los individuos y entidades a quienes se les haya otorgado acceso a información seleccionada, incluyendo pero sin limitarse a, proveedores, investigadores, trabajadores temporales, así como cualquier empresa o entidad pública o privada con que se relacione.

VI. ROLES Y RESPONSABILIDADES

En el contexto del Sistema de Seguridad de la Información, la Superintendencia de Seguridad Social establece los siguientes roles y responsabilidades:

- Comité de Gestión de Seguridad de la Información: debe revisar la presente Política con una periodicidad máxima de tres años, procurando mantenerla actualizada y relevante al quehacer institucional, incorporando las modificaciones necesarias en función de los cambios que pudiesen afectar su definición.
- Encargado de Seguridad de la Información: debe velar por la seguridad de los activos de información, incluyendo la supervisión de todos los aspectos tratados en la presente Política.
- Funcionarios(as) de planta y contrata, personal a honorarios y terceros externos contratados que prestan servicios y que tengan acceso a los activos de información de la Institución: deben dar cumplimiento a la presente Política y a otras políticas, instructivos, procedimientos o controles asociados al Sistema de Seguridad de la información.

Las funciones del Comité de Gestión y del Encargado de Seguridad de la Información, se encuentran descritas en detalle en sus respectivas resoluciones de creación o designación. Adicionalmente, se establecen las siguientes responsabilidades:

a) Las Jefaturas y/o dueños de activos o procesos, deben procurar que el personal de su dependencia conozca y cumpla la presente Política así como todas las normas, procedimientos y prácticas asociadas al Sistema de Seguridad de la información. Asimismo, son responsables de clasificar los activos de información respectivos según su grado de sensibilidad y criticidad, debiendo documentar y mantener actualizada la clasificación efectuada, y definir a los usuarios que tendrán acceso a la información de acuerdo a su función y competencia. Por otra parte, están encargados de la inclusión y el monitoreo de las medidas de seguridad en los sistemas a su cargo en todas sus fases.
b) Los usuarios de la información y de los sistemas utilizados en su procesamiento son responsables de conocer, aplicar y hacer cumplir la Política de Seguridad de la Información vigente, así como de notificar oportunamente acerca de la ocurrencia de cualquier incidente de seguridad de la información.
c) Los administradores/ coordinadores de contrato, deben velar porque los terceros externos (proveedores) contratados que presten servicios y que tengan acceso a los activos de información de la Institución, den cumplimiento a la presente Política y a otras políticas, normas, procedimientos o prácticas asociadas al Sistema de Seguridad de la información, así como asegurar que en los respectivos contratos de provisión de servicios externos, se incluyan cláusulas de confidencialidad, integridad y disponibilidad de la información a la que tengan acceso a propósito de la ejecución de los mismos.
d) La Unidad de Desarrollo de las Personas informará a todo el personal que ingresa a la institución sobre su obligación de cumplir la Política de Seguridad de la Información Institucional, así como todas las normas, procedimientos y prácticas que de ella surjan.
e) La Unidad de Infraestructura y Soporte cumplirá la función de implementar los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos tecnológicos transversales de la Institución.

VII. DIRECTRICES GENERALES

La Política de Seguridad de la Información establece que se debe:

a) Velar porque los funcionarios de planta y contrata y el personal a honorarios de la Institución, cuenten con las competencias y conocimiento en materias concernientes a la presente Política y a otra normativa asociada al Sistema de Seguridad de la Información.
b) Asegurar que toda la información y los medios que la contienen, procesen, almacenen, emitan y/o transporten, cumplan con las regulaciones legales vigentes.
c) Fomentar que el procesamiento y almacenamiento de la información se realice mediante una óptima utilización de los recursos disponibles en la Institución.
d) Promover condiciones de ambiente seguro en los lugares de procesamiento y almacenamiento de los activos de información.
e) Garantizar que todos los medios de procesamiento y/o almacenamiento de información cuenten con medidas de protección física que eviten el acceso y/o utilización indebida por personas no autorizadas.
f) Registrar todas las operaciones realizadas mediante sistemas de información, controlando el acceso físico/ lógico a los activos de información.
g) Comprobar y validar periódicamente el funcionamiento seguro de los sistemas de información.
h) Garantizar que la información y la capacidad de procesamiento manual o automático, sean resguardados y recuperados de manera que se mantenga la continuidad operacional.
i) Asegurar que todos los derechos de propiedad sobre los activos de información que sean utilizados, estén legalmente establecidos en favor de la Institución.
j) Canalizar los incidentes de seguridad de los activos de información al responsable competente para su conocimiento, evaluación y resolución.

VIII. INCUMPLIMIENTO DE LAS POLÍTICAS DE SEGURIDAD

El incumplimiento de la presente Política o de otras normas, procedimientos y prácticas que de ella surjan en el marco del Sistema de Seguridad de la Información, ya sea por parte del personal del Servicio o de externos, podrá traer como consecuencia la aplicación de las sanciones administrativas, civiles o penales establecidas en la legislación vigente y en los procedimientos internos de la Institución.

Es deber de todo el personal de la Superintendencia de Seguridad Social y de terceros externos, informar a la brevedad a su jefatura directa si se tiene conocimiento del incumplimiento de la normativa vigente en esta materia. Estos antecedentes deberán reportarse al Encargado de Seguridad de la Información a través de los medios formales disponibles.

3. Evalúese anualmente el cumplimiento de la Política de Seguridad de la Información por el Comité de Gestión Seguridad de la Información.

4. Analícese y evalúese el contenido de la Política de Seguridad de la Información por el Comité de Gestión de Seguridad de la Información con una periodicidad máxima de tres años, contados desde la fecha de su aprobación, o cuando se produzca un cambio o incidente significativo que la impacte.

5. Difúndase el presente documento a los funcionarios de planta y contrata de la Superintendencia de Seguridad Social, al personal contratado a honorarios y a los terceros que interactúen de manera habitual u ocasional con la Institución, mediante su publicación en la Intranet y el sitio web Institucional www.suseso.cl.

ANÓTESE, REGÍSTRESE, COMUNÍQUESE Y ARCHÍVES

CLAUDIO REYES BARRIENTOS
SUPERINTENDENTE DE SEGURIDAD SOCIAL

A: Fiscalía
Intendenta de Seguridad y Salud en el Trabajo
Intendente de Beneficios Sociales
Departamentos y Unidades
Unidad de Desarrollo de las Personas
Unidad de Gestión de Correspondencia y Archivo Central