



APRUEBA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA SUBSECRETARÍA DE DESARROLLO REGIONAL Y ADMINISTRATIVO, EN EL MARCO DEL SISTEMA DE MEJORA DE LA GESTIÓN Y DEJA SIN EFECTO LA RESOLUCIÓN EXENTA N° 14.185, DEL AÑO 2016, DE ESTA SUBSECRETARÍA. (E20571/2018)  
RESOLUCION EXENTO N°: 8328/2018  
Santiago25/07/2018

DOCUMENTO ELECTRONICO

**VISTOS:**

Lo dispuesto en la Ley N° 18.359, de 1984, que crea el cargo de Subsecretario de Desarrollo Regional y Administrativo; en el D.F.L. N° 1-18.359, de 1985, del Ministerio del Interior, que traspasa y asigna funciones a la Subsecretaría de Desarrollo Regional y Administrativo; en el Decreto Supremo N° 77, de 2004, y el Decreto Supremo N° 83, de 2004, ambos del Ministerio Secretaría General de la Presidencia; en la Resolución Exenta N° 13.187, de 2011, de la Subsecretaría de Desarrollo Regional y Administrativo, y en la Resolución N° 1.600, de 2008, de la Contraloría General de la República.

**CONSIDERANDO:**

1.- Que el Programa de Mejoramiento de la Gestión de Seguridad de la Información tiene por objetivo contar con un sistema de gestión de seguridad de la información que permita lograr niveles adecuados de integridad, confidencialidad y disponibilidad para todos los activos de información institucional considerados relevantes, de manera tal que se asegure la continuidad operacional de los procesos institucionales y la entrega de productos y servicios a los usuarios, funcionarios y beneficiarios de SUBDERE.

2.- Que, la Subsecretaría de Desarrollo Regional y Administrativo del Ministerio del Interior y Seguridad Pública, en el Marco del citado Programa requiere actualizar su Política de Seguridad de la Información.

**RESUELVO:**

Artículo 1°.- Apruébese la revisión y actualización de la Política General de Seguridad de la Información de la Subsecretaría de Desarrollo Regional y Administrativo del Ministerio del Interior y Seguridad Pública, que se establece seguidamente:

**POLÍTICA GENERAL DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Subsecretaría de Desarrollo Regional y Administrativo (SUBDERE)**

1. Objetivo: El propósito de esta Política es definir el objetivo, dirección, principios y reglas básicas para la gestión de la seguridad de la información en la Subsecretaría de Desarrollo Regional y Administrativo. La Autoridad del servicio reconoce la importancia y el valor de los activos de información como un elemento crítico al proceso de toma de decisiones para el cumplimiento de su Misión Institucional y, por tanto, establece la Política del Sistema De Seguridad de la Información.

En el marco de este Objetivo, la SUBDERE establece las características mínimas obligatorias de seguridad y confidencialidad que deben cumplir los documentos electrónicos, como también, estándares mínimos de seguridad en el uso, almacenamiento, acceso y distribución del documento electrónico; facilitar la relación electrónica al interior de esta Subsecretaría, con otros órganos de la Administración del Estado, la ciudadanía y el sector privado.

**2. Documentos de Referencia:**

- i) Decreto Supremo 83, de 2004, del Ministerio Secretaría General de la Presidencia, Aprueba Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos.
- ii) Ley 20.285, de 2008, Ministerio Secretaría General de la Presidencia, Sobre Acceso a la Información Pública.
- iii) Ley 19.223, de 1993, Tipifica Figuras Relativas a la Informática.
- iv) Ley 19.927, de 2004, Modifica código de procedimiento penal y el código procesal penal en materia de delitos de pornografía Infantil.
- v) DFL 29 Fija texto refundido, coordinado y sistematizado de la ley N°18.834
- vi) Norma NCh-ISO 27001 y 27002 Segunda edición 2013.10.25

**3. Definiciones.**

a) Sistema de Gestión de la Información. Parte del sistema de gestión, basada en un enfoque hacia los riesgos de una institución, cuyo fin es establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión considera la estructura organizacional, políticas, actividades de planificación, responsabilidad, prácticas, procedimientos, procesos y recursos.

b) Comité de Calidad, Gestión de Riesgos y Seguridad de la Información. Entidad aprobada por Resolución Exenta N°15387, de fecha 29/12/2014. Este Comité es presidido por el Jefe de la División de Administración y Finanzas.

c) Activo de Información. Aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información, de valor para la Institución. Se distinguen 3 niveles básicos de activos de información:

c.1) La Información propiamente tal, en sus múltiples formatos, a modo de ejemplo, papel, digital, texto, imagen, audio, video.

c.2) Los Equipos, Sistemas de Información e Infraestructura que soportan esta información.

c.3) Las Personas que utilizan la información, y que tienen el conocimiento de los procesos institucionales.

d) Seguridad de la Información. Es el nivel de certeza y confianza que la organización desea tener de su capacidad para preservar la confidencialidad, factibilidad de autenticación, integridad y disponibilidad de la información. De esta forma, proteger el recurso o activo de información de una amplia gama de amenazas, asegurando la continuidad de las operaciones de la Subsecretaría, minimizando el daño y cumpliendo su misión y objetivos estratégicos.

e) Sistema de Información. Conjunto de uno o más computadores, software asociado, periféricos, terminales, usuarios, procesos físicos, medios de transferencia de información y otros, que forman un todo autónomo capaz de obtener, almacenar, tratar, administrar, controlar, procesar, transmitir o recibir datos, para satisfacer una necesidad de información.

f) Autenticación. Proceso de confirmación de la identidad del usuario que generó un documento electrónico y/o que utiliza un sistema informático.

g) Confidencialidad. Aseguramiento de que el documento electrónico sea conocido sólo por quienes están autorizados para ello.

h) Contenido del documento electrónico. Información, ideas y conceptos que un documento expresa.

i) Continuidad del negocio. Continuidad de las operaciones de la institución.

j) Disponibilidad. Aseguramiento de que los usuarios autorizados tengan acceso oportuno al documento electrónico y sus métodos de procesamiento.

k) 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.

l) Documentos públicos. Aquellos documentos que no son ni reservados ni secretos, cuyo conocimiento no está circunscrito.

m) Documentos reservados. Aquellos documentos cuyo conocimiento está circunscrito al ámbito de la respectiva unidad del órgano a que sean remitidos, en virtud de una ley o de una norma administrativa dictada en Conformidad a ella, que les confiere tal carácter.

n) Documentos secretos. Los documentos que tienen tal carácter de conformidad al artículo 13 de la Ley Orgánica Constitucional de Bases Generales de la Administración del Estado y su Reglamento.

ñ) Ejecutivo. Autoridad dentro de la institución.

o) Identificador formal de autenticación. Mecanismo tecnológico que permite que una persona acredite su identidad utilizando técnicas y medios electrónicos.

p) Incidentes de seguridad. Situación adversa que amenaza o pone en riesgo un sistema informático.

q) Integridad. Salvaguardia de la exactitud y totalidad de la información y de los métodos de procesamiento del documento electrónico, así como de las modificaciones realizadas por entes debidamente autorizados.

r) Negocio. Función o servicio prestado por la organización.

s) Política de seguridad. Conjunto de normas o buenas prácticas, declaradas y aplicadas por una organización, cuyo objetivo es disminuir el nivel de riesgo en la realización de un conjunto de actividades de interés, o bien garantizar la realización periódica y sistemática de este conjunto.

t) Repositorio. Estructura electrónica donde se almacenan documentos electrónicos.

v) Riesgos. Amenazas de impactar y vulnerar la seguridad del documento electrónico y su posibilidad de ocurrencia.

w) Usuario. Entidad o individuo que utiliza un sistema informático.

4. Contexto General. La Subsecretaría de Desarrollo Regional y Administrativo tiene, por mandato legal, las funciones de coordinar, impulsar y evaluar el desarrollo regional. A la vez, debe colaborar en las funciones de modernización y reforma administrativa del Estado, estas políticas de seguridad de la información estarán alineadas con la misión de la Subsecretaría de Desarrollo Regional y Administrativo.

Las leyes o decretos que rigen a SUBDERE son las siguientes:

• Ley N°18.359, que Crea el cargo de Subsecretario de Desarrollo Regional y Administrativo del

Ministerio del Interior y Seguridad Pública.

- D.F.L. N°1 - 18.359, de 1985, que Traspasa funciones a la Subsecretaría de Desarrollo Regional y Administrativo del Ministerio del Interior y Seguridad Pública.
- Ley N° 19.602, artículos 2° y 3°, que modifican la Ley N°18.695, Orgánica Constitucional de Municipalidades, en materia de Gestión Municipal.

5. Alcance de la presente Política. La Política de Seguridad de la Información se aplica a todo el personal que se desempeña en la SUBDERE, cualquiera sea su condición jurídica laboral, personas naturales y a las entidades externas que tengan acceso a los activos de información de la SUBDERE, para cuyo efecto deberán suscribirse los acuerdos correspondientes, además a todos los procesos de la SUBDERE, los cuales se incorporarán anualmente y en forma gradual al SGSI, conforme a las prioridades que establezca el Comité de Calidad, Gestión de Riesgos y Seguridad de la Información, incluyen las unidades dependientes que participan en el desarrollo de sus actividades y los recursos utilizados, salvo en aquellos casos en que explícitamente se indique lo contrario. Además, la presente Política General de Seguridad de la Información podrá ser complementada con Políticas sobre aspectos específicos de la Seguridad de la Información, Manuales de Procedimientos, Procedimientos y/o Instructivos de Trabajo, que podrán incluir las siguientes áreas:

- i) Organización de la Seguridad, que busca establecer un modelo de gerenciamiento para controlar la implementación del sistema y la definición clara de funciones y responsabilidades.
- ii) Gestión de Activos, destinado a mantener una adecuada protección de los activos, con base en los niveles requeridos y tratamiento especial de acuerdo a su clasificación.
- iii) Seguridad de los Recursos Humanos, orientado a reducir los riesgos en el manejo de información y el establecimiento de compromisos y mecanismos necesarios para fortalecer las debilidades en materia de seguridad a este respecto.
- iv) Seguridad Física y del Entorno, destinado a impedir accesos no autorizados, daños o alteraciones en la infraestructura que posee a la SUBDERE.
- v) Gestión de las Comunicaciones y las Operaciones, dirigido a mantener disponible y en correcto funcionamiento de las instalaciones de la SUBDERE.
- vi) Control de Acceso, orientado a validar, verificar y proveer el acceso lógico y físico a la información (aplicaciones, bases de datos y servicios en general) de forma adecuada.
- vii) Desarrollo y Mantenimiento de los Sistemas de Información, en donde se definirán las medidas necesarias para crear ambientes propios de desarrollo, implementación y mantenimiento de los sistemas de información y los controles de seguridad de cada uno.
- viii) Gestión de Incidentes de Seguridad de la Información, con el objeto de establecer los lineamientos generales para la gestión de incidentes de seguridad de la información, con el fin de prevenir y limitar el impacto de los mismos.
- ix) Gestión de la Continuidad del Negocio, orientado a minimizar el impacto causado por interrupciones en las actividades ejecutadas dentro del proyecto, protegiendo los procesos críticos de eventos significativos funestos que pudieran presentarse.
- x) Cumplimiento, destinado a impedir posibles infracciones o violaciones a las normas, reglamentos, contratos y requisitos de seguridad de información que se establezcan como parte de la implementación del SGSI de la SUBDERE.

5.1 Norma Chilena –ISO 27002. La Subsecretaría de Desarrollo Regional y Administrativo – SUBDERE- se compromete a contar con un Sistema de Gestión de Seguridad de la Información que permita lograr niveles adecuados de confidencialidad, integridad, disponibilidad y factibilidad de autenticación para todos los activos de información relacionados con los procesos de negocio considerados relevantes y de los procesos de tecnologías de la información y la comunicación (TIC) que los soportan, de acuerdo a la Declaración de Aplicabilidad vigente, de manera tal que se asegure la continuidad operacional de los procesos así como la entrega de productos y servicios a sus clientes /Usuarios/beneficiarios.

La SUBDERE, se compromete revisar a intervalos regulares el SGSI, disponer los recursos necesarios para su operación, mantención, mejora continua, tomar decisiones en relación a la gestión de riesgos en materias del SGSI acorde con el rol de la institución y de los recursos disponibles. La SUBDERE se compromete además a través de su Comité de Calidad, Gestión de Riesgos y Seguridad de la Información, revisar de forma periódica, la política y objetivos del Sistema de Gestión de Seguridad de la Información con el fin de asegurar su pertinencia y adecuación. Se promueve la toma de conciencia por parte de los funcionarios, comunicando la importancia de cumplir con la política de seguridad de la Información, los requisitos legales, y la mejora continua del SGSI, para lo cual se desarrollará un Plan de Difusión, (publicación en Intranet SUBDERE y envío de correos masivos con las políticas generales de seguridad de la información Previamente sancionada por la autoridad del servicio mediante el acto administrativo firmada por el jefe de servicio), sensibilización y capacitación para los funcionarios de SUBDERE.

5.2 Objetivos del Sistema de Gestión de Seguridad de la Información.

i) Objetivo General del SGSI. Lograr niveles adecuados de integridad, confidencialidad y disponibilidad para toda la información institucional relevante, con el objeto de asegurar continuidad operacional de los procesos críticos que desarrolla la SUBDERE, mediante el resguardo de los activos de información asociados a los procesos críticos del negocio y su soporte.

ii) Objetivo Específico del SGSI. Los objetivos del Sistema de Gestión de Seguridad de la Información se organizan en las siguientes categorías: INVENTARIO Y CLASIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN.

Por tanto, el SGSI deberá asegurar el cumplimiento de las siguientes acciones:

- Contar con el inventario de los activos de información más importantes de la organización, que incluya al menos las siguientes características: tipo de activo, formato, ubicación e importancia.

- Identificar propietarios o responsables de cada uno de los activos de información.
- Clasificar los activos de información, según la importancia y la sensibilidad de la información, bajo el modelo de ANÁLISIS DE RIESGO.
- Elaborar o adoptar una metodología de análisis de riesgo de los activos de información.
- Realizar un análisis de riesgo de los activos de información, según la metodología seleccionada. POLÍTICAS, ESTÁNDARES, MANUALES Y PROCEDIMIENTOS.
- Generar diferentes documentos tales como: Políticas Específicas, Estándares, Manuales de Procedimientos, Procedimientos e Instructivos de Trabajo de Seguridad de la Información que incluyan los aspectos más relevantes, acordes a las necesidades de la organización y al análisis de riesgos.
- Definir mecanismos de Control y de Actualización Periódica de estos documentos.
- Diseñar procedimientos frente a la posibilidad de ocurrencia de eventos o incidentes que afecten la seguridad de la información. CAPACITACIÓN DEL PERSONAL
- Establecer responsabilidades respecto a los activos de información dentro de las diferentes unidades de la SUBDERE.
- Capacitar a los responsables de los activos de información, en temáticas relacionadas a la generación, manejo y resguardo de los activos de información, de acuerdo a su nivel de importancia.
- Proporcionar al personal material de apoyo relacionados con la seguridad de la información.
- Poner a disposición del personal toda la documentación relativa a la seguridad de la información.

### 5.3 Roles y Responsabilidades.

i) Subsecretario. En su calidad de Jefe de Servicio, es el responsable del Sistema de Gestión de la Seguridad Institucional, provee evidencia de su compromiso con el desarrollo y la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), así como la mejora continua y su efectividad mediante:

- La autorización para que se implemente el SGSI en la SUBDERE.
- Establecer los objetivos del SGSI.
- Asignar roles y responsabilidades en seguridad de la información.
- Establecer un Comité de Calidad, Gestión de Riesgos y Seguridad de la Información.
- Proporcionar todos los recursos necesarios para una adecuada implementación del SGSI.
- Le corresponde revisar a intervalos regulares el SGSI, disponer los recursos necesarios para su operación, mantención y mejora.
- Es responsable, además, del nombramiento del Encargado de Seguridad de la Información, como del nombramiento del Comité de Calidad, Gestión de Riesgos y Seguridad de la información. Información del cual deberá participar o nombrar un representante que actuará en su nombre, que en este caso esta nombrado el jefe de la División de Administración y Finanzas.

- Comunicar a la SUBDERE la importancia de lograr los objetivos de seguridad, de cumplir sus responsabilidades y de buscar el mejoramiento continuo en el área de seguridad de la información.

ii) Comité de Calidad, Gestión de Riesgos y Seguridad de la Información. Le corresponderá proponer y revisar las Políticas SGSI y de la documentación que de ella se desprenda, monitorear y evaluar los riesgos que afecten a los activos críticos de información, tomar conocimiento y supervisar la investigación y monitoreo de incidentes de seguridad, dar curso a las propuestas para mejorar la seguridad de la SUBDERE, promover la difusión de las Políticas de Seguridad de la Información y de la documentación relacionada al SGSI.

iii) Encargado de Seguridad de la Información. Será el encargado de las funciones relativas a la seguridad de los sistemas de información, lo que incluye supervisión de todos los aspectos relativos a los temas tratados en la presente Política. Lo anterior sin perjuicio de las actividades y responsabilidades dispuestas en la resolución de nombramiento vigente.

iv) Departamento de Informática. Unidad encargada de cubrir los requerimientos de seguridad establecidos para la operación, administración, y comunicación de los sistemas y recursos tecnológicos de la Subsecretaría. Además efectuará las tareas de desarrollo y mantenimiento de sistemas siguiendo una metodología de ciclo de vida de sistemas apropiada y que contemple la inclusión de medidas de seguridad en cada una de sus fases.

v) El Departamento de Informática y Recursos Humanos. Unidad encargada de notificar al personal que ingrese a la SUBDERE de sus obligaciones respecto del cumplimiento de las Políticas de Seguridad de la Información y de las normas y procedimientos que a partir de ella se generen. También estará a cargo de la notificación de la presente Política y de los cambios que en ella se produzcan, al personal de la Subsecretaría, como del ajuste de los contratos de honorarios a los nuevos requerimientos de seguridad de la información, de la implementación de acuerdos de confidencialidad y no divulgación, como también de las tareas de capacitación continua en materia de seguridad, Generar propuestas en materias de seguridad de la información relacionadas con temáticas asociadas de Recursos Humanos.

vi) La Fiscalía de SUBDERE , deberá asesorar a la Subsecretaría de Desarrollo Regional en materias de carácter legal, en lo relativo a la seguridad de la información y aplicar sanciones administrativas en la eventualidad de detectar Violaciones o alteraciones al no acatar lo indicado en los documentos que sustentan el sistema de seguridad de información, (políticas, procedimientos, instructivos generales particulares relativos a la seguridad de la Información).

vii) Unidad de Auditoría Interna. Estará a cargo de verificar el avance y cumplimiento por parte de las distintas áreas de la institución, de las políticas y procedimientos desarrollados por el Comité de Calidad, Gestión de Riesgos y Seguridad de la Información, así como de la normativa vigente en materia de seguridad de la información.

viii) Dueño de Activo(s) de Información. Es el funcionario que debe velar dentro de su respectivo proceso porque el/los activo/s de información a su cargo cumpla/n con las políticas, que para este efecto SUBDERE establezca.

## 6. Criterios generales de aplicación de la Política del SGSI.

6.1 De la Información Institucional. La información es un activo vital y todos sus accesos, usos y procesamiento, deberán ser consistentes con las políticas y estándares establecidos por SUBDERE en cada ámbito de la seguridad de la información. La información debe ser protegida, por sus dueños de los activos de información, de una manera consistente con su importancia, valor y criticidad, siguiendo las reglas establecidas en las políticas específicas de seguridad de la información, sus procedimientos asociados y recomendaciones establecidas por SUBDERE. Para ello, la Dirección del Servicio deberá proveer los recursos que permitan implementar los controles necesarios para otorgar el nivel de protección acorde al valor de los activos.

Toda la información creada o procesada por el servicio será considerada como "Pública", a menos que se considere que el acceso no autorizado a la información podría ocasionar daños y/o inconvenientes menores a la organización, en cuyo caso la información podrá ser clasificada como "Uso Interno", en dicho caso la información podrá ser divulgada con la autorización del propietario del activo. Se clasificará como "Reservada", la información que tenga esa clasificación dentro del marco de la Ley N° 20.285, o información cuya divulgación podría implicar un impacto no deseado para la SUBDERE. Periódicamente cada encargado de proceso deberá revisar la clasificación, con el propósito de mantenerla o modificarla según se estime apropiado. SUBDERE proveerá los mecanismos para que la información sea accedida y utilizada por el personal que de acuerdo a sus funciones así lo requiera. Sin embargo, se reserva el derecho de revocar al personal, el privilegio de acceso a la información y tecnologías que la soportan, si la situación y las condiciones así lo ameritan.

6.2 Gestión del riesgo. Los criterios de estimación del riesgo para el Sistema de Gestión de la Seguridad de la Información corresponden a los establecidos por el Consejo de Auditoría Interna General de Gobierno (CAIGG), mediante la metodología COSO II – ERM, y lo estipulado en la "Guía Metodológica del Programa de Mejoramiento de la Gestión – Sistema de Seguridad de la Información" - vigente, ambos documentos de aplicación a los Servicios de la Administración Pública Chilena. SUBDERE y su Comité de Calidad, Gestión de Riesgos y Seguridad de la Información declaran, conforme a lo establecido en la metodología internacional COSO II – ERM y su adaptación por parte del Consejo de Auditoría Interna General de Gobierno (CAIGG), el siguiente "Nivel de Aceptación del Riesgo" que puede afectar a sus activos de información:

i) Severidad del Riesgo. Baja probabilidad por Impacto del Riesgo.

ii) Exposición Final al Riesgo. Menor. Riesgo residual, después de aplicar los controles definidos. Los riesgos que sean evaluados en un nivel superior a lo señalado precedentemente deben ser mitigados, compartidos o eliminados.

6.3 Documentación del Sistema de Gestión de Seguridad de la Información. Además de los documentos obligatorios del SGSI establecidos en la norma NCh-ISO 27002, segunda edición, de fecha 25 de octubre de 2013, de la presente Política, se desprenden Políticas Específicas de SI, Manuales de Procedimientos, Procedimientos y/o Instructivos de Trabajo, un listado con de toda la documentación relacionada con el SGSI deberá ser mantenido, actualizado y aprobado por el Comité de Calidad, Gestión de Riesgos y Seguridad de la Información cada vez que exista una actualización derivado de cambios el SGSI. Así mismo el Comité de Calidad, Gestión de Riesgos y Seguridad de la Información deberá mantener un catastro actualizado de la legislación aplicable a la institución y que incluya aspectos relacionados con Seguridad de la Información.

6.4 Deberes y derechos de los funcionarios. Los funcionarios están obligados a alertar, de manera oportuna y adecuada, cualquier evento y/o incidente que atente contra lo establecido en esta política. Está absolutamente prohibido al personal de la organización divulgar cualquier información de clasificación "Reservada", salvo que sea explícitamente autorizado por el dueño de la información, quien deberá hacerse responsable de esta divulgación.

Los funcionarios tienen el derecho que se les informe mediante los medios adecuados y de forma oportuna cualquier cambio en las políticas general de seguridad.

6.5 Violación de las políticas de seguridad de la información. Cualquier incumplimiento o violación de la Política General de Seguridad de la Información, Políticas Específicas o Estándares, se atiene a las sanciones establecidas para los funcionarios del Sector Público, dispuestas en la Ley 18.834 "Estatuto Administrativo" y cuyo texto se refunde en el Decreto con Fuerza de Ley N° 29, de fecha de promulgación 16 de junio de 2004 (fecha de publicación 16 de marzo de 2005).

6.6 Auditorías al SGSI. Con el fin de velar por el correcto uso de los recursos de su propiedad, la SUBDERE se reserva el derecho de solicitar inspecciones y/o auditorías relacionadas con el cumplimiento de las políticas vigentes.

6.7 Revisión del presente documento. La presente Política y todas aquellas que de aquí se desprendan deberán ser revisadas y de ser necesario actualizadas al menos una vez cada 2 años, o cuando ocurran cambios que pudieran afectar el enfoque de la Subsecretaría para la gestión de la Seguridad de la Información. Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

i) Cantidad de funcionarios y participantes externos que cumplen una función en el SGSI pero que no

están familiarizados con el presente documento.

- ii) No conformidad del SGSI con las leyes y normas, las obligaciones contractuales y con los demás documentos internos de la organización.
- iii) Ineficacia de la implementación y mantenimiento del SGSI.
- iv) Responsabilidades ambiguas para la implementación del SGSI.

7.- Actualización del documento,

7.1.- Punto uno En objetivo se agrega la frase "La autoridad del servicio".

7.2.- Documento de Referencia se actualizan los puntos.-

ii) Ley 20.285, de 2008, Ministerio Secretaria General de la Presidencia, Sobre Acceso a la Información Pública.

iii) Ley 19.223, de 1993, Tipifica Figuras Relativas a la Informática.

iv) Ley 19.927, de 2004, Modifica código de procedimiento penal y el código procesal penal en materia de delitos de pornografía Infantil.

v) DFL 29 Fija texto refundido, coordinado y sistematizado de la ley N°18.834

vi) Norma NCh-ISO 27001 y 27002 Segunda edición 2013.10.25

Artículos 2° Se deja constancia que las actualizaciones que considera la presente resolución respecto de la política general de seguridad de la información definida por la Resolución Exenta N°14.185, de 2016, de , de esta Subsecretaría, que por este acto se deja sin efecto, dicen relación con lo siguiente:

7.3.- Punto 5 "Alcance de la presente Política" numeral 5.1., se agrega la frase "mediante el acto administrativo firmada por el jefe de servicio"

7.4.- Punto 5.3 Roles y Responsabilidades, numeral v se cambió Recurso de Humano por Departamento de Informática.

7.5.- Punto 5.3 Roles y Responsabilidades, numeral vi y vii se redacta y se mejora la redacción de los puntos.

Asimismo se incorpora un nuevo artículo tercero relativo a la difusión de la política de seguridad de la Información.

Artículo 3° Difusión de la política.

La Difusión de las políticas de Seguridad de la Información será responsabilidad del Departamento de Informática de SUBDERE,

quien realizara todas las gestiones y acciones que requiera esta política, la que debe ser conocida y asumida por todos los funcionarios de la SUBDERE a quienes se les aplica.

Para ello, se utilizará para este medio Correo Masivos institucionales (solosubdere) y la publicación de la presente resolución en la intranet Institucional.

Artículo 4°.- Dejase sin efecto la Resolución Exenta N° 14.185, del año 2016, de esta Subsecretaría sobre la misma materia, a contar de la fecha de total tramitación de la presente resolución.

ANÓTESE, COMUNÍQUESE Y PUBLÍQUESE EN LA INTRANET INSTITUCIONAL



MARIA EUGENIA MARTINEZ BOLZONI

Subsecretaria(S)

Gabinete

MEM/ / SSG/ CAC/ JHN/ IAO/ JHR/ CUG/ jrmd

DISTRIBUCION:

Jefe Departamento - Departamento Informatica

JESSICA DEL GONZALEZ - Secretaria - Fiscalia

JOSE ROBERTO DURANA - Asesor - Fiscalia

NIEVES DURAN - Jefa Unidad - Oficina de Partes, Archivo y Centro Documental  
RODRIGO ZUÑIGA - Encargado(a) Unidad - Unidad de Proyectos y Desarrollo

Firmado Electrónicamente en Conformidad con el Artículo 2º letra F y G de la Ley 19.799