Mat.: Actualización de la Política General de Seguridad de la Información de los Servicios Administrativos del Gobierno Regional de Antofagasta y deja sin efecto Resolución Exenta N° 1175 de fecha 06 de noviembre de 2017 que aprobó la Política General de Seguridad de la Información del Servicios Administrativos del Gobierno Regional de Antofagasta.

Resolución Exenta N° 000268

Antofagasta, 29 MAR. 2019

VISTOS

Constitución Política de la República; Ley N° 18.575, sobre Bases Generales de la Administración del Estado; Ley N° 19.880, que Establece Bases de los Procedimientos Administrativos que rigen los actos de los órganos de la Administración del Estado; Instructivo Presidencial N° 4, junio 2003.: Imparte instrucciones sobre aplicación de la ley de Bases de Procedimientos Administrativos; Ley que Aprueba el Presupuesto para el Sector Público para el año; Decreto Ley N° 1.263, decreto ley orgánica de administración financiera del Estado; Ley N° 18.091, establece normas complementarias de incidencia presupuestaria, de personal y de administración financiera; Decreto Ley N° 3.001, normas complementarias de administración financiera y de incidencia presupuestaria; Ley Nº 19.886 de Bases sobre Contratos Administrativos de Suministro y Prestación de Servicios y su respectivo Reglamento contenido en el Decreto (H) N° 250 del año 2004;Resolución Nº 1.600 de 05 noviembre de 2008, fija normas sobre exención del tramité de TOMO RAZÓN; Instructivo Presidencial N°002 del 04 de abril del 2018, sobre Austeridad y eficiencia en el uso de los recursos públicos; Ley N° 19.553, febrero 1998, concede asignación de modernización y otros beneficios que indica. Ministerio de Hacienda; Decreto N° 475. Reglamento Ley N° 19.553 para la aplicación del incremento por Desempeño Institucional del artículo 6° de la Ley y sus modificaciones; Ley N° 20.212, agosto 2007. Modifica las leyes N° 19.553, N° 19.882, y otros cuerpos legales, con el objetivo de incentivar el desempeño de los funcionarios públicos. Ministerio de Hacienda; Ley 21.050, otorga reajuste de remuneraciones a los trabajadores del sector público, concede aguinaldos que señala, concede otros beneficios que indica, y modifica diversos cuerpos legales; Ley N° 19.799 sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de Firma Electrónica. Ministerio de Economía; Decreto Supremo N° 181. Reglamento de la Ley N° 19.799 sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de Firma Electrónica. Ministerio de Economía; Instructivo Presidencial N° 5, mayo 2001. Define el concepto de Gobierno electrónico. Contiene la mayor parte de las instrucciones referidas al desarrollo de Gobierno electrónico en Chile; Instructivo Presidencial N° 6, junio 2004. Imparte instrucciones sobre la implementación de la firma electrónica en los actos, contratos y cualquier tipo de documento en la administración del Estado, para dotar así de mayor grado de seguridad a las actuaciones gubernamentales que tiene lugar por medio de documentos electrónicos y dar un mayor grado de certeza respecto de las personas que suscriben tales documentos; Decreto Supremo N° 158. Modifica Decreto Supremo N° 81 sobre norma técnica para la interoperabilidad de los instrumentos electrónicos; Decreto Supremo N° 83. Norma técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos; Decreto Supremo N° 93. Norma técnica para minimizar la recepción de mensajes electrónicos masivos no deseados en las casillas electrónicas de los órganos de la Administración del Estado y de sus funcionarios; Decreto Supremo N° 14, febrero 2014., Ministerio de Economía, Fomento y Turismo. Modifica Decreto Supremo N° 181 de 2002; Ley N° 20.285, agosto 2008. Regula el principio de transparencia de la función pública y el derecho de acceso a la información de los órganos de la Administración del Estado. Ministerio Secretaria General de la Presidencia; Decreto N° 13 de 2009 que aprueba Reglamento de Ley N° 20.285; Instructivo General N° 2, mayo 2009, del Consejo para la Transparencia: Designación de Enlaces con el Consejo para la Transparencia; Instructivo General N° 3, mayo 2009, del Consejo para la Transparencia: Índice de Actos o Documentos calificados como secretos o reservados; Ley 18.845, establece sistemas de microcopia o micrograbación de documentos; Circular N°28.704 de 1981, de la Contraloría General de la República sobre disposiciones y recomendaciones referentes a la eliminación de documentos; Instructivo Presidencial N° 8, diciembre 2006. Imparte instrucciones sobre Transparencia activa y Publicidad de la Información de la Administración del Estado; Circular N° 3, enero de 2007: Detalla las medidas específicas que deben adoptar los servicios y disponer los materiales necesarios para facilitar la implementación del instructivo presidencial sobre transparencia

activa y publicidad de la información de la Administración del Estado; Instructivo General N° 11 del 2014 sobre Transparencia Activa del Consejo para la Transparencia; Ley Nº 20.730, que regula el Lobby y las gestiones que representen intereses particulares ante las autoridades y funcionarios; Decreto N° 71 de 2014 sobre Reglamento de Ley Nº 20.730; Decreto Supremo N° 533, abril 2015. Crea el comité Interministerial sobre Ciberseguridad, Ministerio del Interior y Seguridad Pública; subsecretaria del Interior; Instructivo de Presidencial N°1 del 27 de abril del 2017, que instruye implementación de la Política Nacional sobre Ciberseguridad; Decreto N° 1 de 11 de junio de 2015 Norma técnica sobre sistemas y sitios web de los órganos de la administración del Estado; Ley N°20.422, Establece Normas sobre Igualdad de Oportunidades e Inclusión Social de Personas con Discapacidad; Ley 21.096, consagra el derecho a protección de los datos personales; Ley N° 19.268 sobre Protección de la vida privada; Decreto N° 779 de 11 de noviembre de 2000 sobre Registro de Banco de datos personales a cargo de organismos públicos; Ley N° 19.175 Orgánica Constitucional sobre Gobierno y Administración Regional promulgada el año 2005 del Ministerio del Interior y Seguridad Pública y modificada *a través de la Ley Nº 20.035 Estructura y Funciones de los Gobiernos Regionales y Ley N° 21.074 Fortalecimiento de la Regionalización del País*; Decreto Supremo N°415 del 11 de marzo de 2018 del Ministerio del Interior y Seguridad Pública, que nombra Intendente de la Región de Antofagasta; y

CONSIDERANDO

1. Que, en el cumplimiento de sus obligaciones legales, el Servicio Administrativo del Gobierno Regional de Antofagasta debe tener las normas adecuadas que regulen los distintos aspectos involucrados en materia de seguridad de la información.

2. Que el Decreto Supremo N° 83_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. Al respecto, la norma técnica tiene por objetivo garantizar estándares mínimos de seguridad en el uso, almacenamiento, acceso y distribución de documentos electrónicos, junto con facilitar la relación electrónica entre los órganos del Estado y entre éstos y la ciudadanía.

3. Que, el Estado a través de las políticas gubernamentales de los últimos años ha complementado la norma técnica del Decreto Supremo N° 83_2004, implementando el sistema de gestión de seguridad de la información en los órganos administrativos del Estado, basándose en la Norma ISO/IEC 27001:2013.

R E S U E L V O

1. **DEJASE SIN EFECTO** la Resolución Exenta N° 1175 de fecha 06 de noviembre de 2017 que aprobó la Política General de Seguridad de la Información del Servicio Administrativo del Gobierno Regional de Antofagasta.

2. **APRUÉBESE** la actualización de la Política General de Seguridad de la Información del Servicio Administrativo del Gobierno Regional de Antofagasta, la cual se transcribe íntegramente en la presente Resolución:

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN
SERVICIO ADMINISTRATIVO DEL GOBIERNO REGIONAL DE ANTOFAGASTA

NOTA DE CONFIDENCIALIDAD

La Política General de Seguridad de la Información para el Servicio Administrativo del Gobierno Regional de Antofagasta (en adelante el Servicio), se rige por los términos y condiciones que en este documento se establecen. Su uso está dirigido a todos los funcionarios de esta institución sin distinción de su condición contractual, los que podrán acceder a ella, previo a su conocimiento, de entendimiento y de la aceptación de los términos relativos a su utilización.

CONTROL DE VERSIONES

N° Versión	Fecha Aprobación	Modificación	Páginas o Secciones modificadas	Autor
1	30/03/2011	Elaboración inicial	Todas.	Encargado S.I.
2	14/09/2011	Se mejoran Punto I, Punto III y Punto IV.	Puntos: I, III y IV.	Encargado S.I.

3	07/10/2015	Se agrega Punto V Componentes de la Política de Seguridad de la Información, según actualización norma NCh-ISO 27001_2013.	Punto V.	Encargado S.I.
4	04/12/2015	Se modifica Punto VII letra g, sobre revisión de una política.	Punto VII.	Encargado S.I.
5	17/10/2017	✓Se complementa el Punto2. ✓Desde Punto 4 se extrae un nuevo punto independiente para la Difusión de la Política de Seguridad de la Información y otro punto parta la Revisión de la Política de Seguridad de la Información y se complementa Punto 4. ✓Se renumeran los contenidos desde punto 5 al 10. ✓Se modifica Punto 6 (actual 8) sobre Roles y responsabilidades. ✓Se modifica Punto 7 (actual 9) en Letra g (actual 9.10) sobre Revisión de una Política y Letra a (actual 9.1) en respuesta ante un incidente yen Uso de Recursos. ✓Se agrega a Punto 6 (actual 8) el Rol de Oficial de Seguridad.	Puntos: 2, 4,6 y 7.	Oficial S.I.
6	25/01/2019	✓Se complementa Sección 1. ✓Se complementa Sección 2. ✓Se complementa Sección 4. ✓Se complementa Sección 5. ✓Se complementa Sección 6. ✓Se complementa Sección 7. ✓Se complementa Sección 8. ✓Se complementa Sección 9.	Sección: 1, 2, 4, 5, 6, 7, 8,9.	Encargado S.I.

CONTROLES NORMA NCh-ISO 27001_2013 ABORDADOS

Control	Objetivo del control
A.05.01.01	Políticas de Seguridad de la Información
A.05.01.02	Revisión de las Políticas de Seguridad de la Información

FIRMAS RESPONSABLES

Elaborado por:	Revisado por:	Aprobado por:
Fecha:25/01/2019	Fecha:05/03/2019	Fecha:08/03/2019
Miguel Lagos Covarrubias	**Luis Colman Vega**	**Marco Antonio Díaz Muñoz**
Encargado Seguridad de la Información	Encargado Unidad Jurídica	Jefe Superior del Servicio

TABLA DE CONTENIDO

1. OBJETIVO

El presente documento de Política General de Seguridad de la Información establece el marco de referencia, a través del cual el Servicio, fija los estándares de seguridad de la información a aplicar para proteger adecuadamente sus activos de información, según lo establece el Decreto Supremo Nº 83 sobre Seguridad y Confidencialidad que aprobó la "**Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos**".

Su objetivo es garantizar estándares mínimos de Seguridad de los Activos de información entendiéndose por tal:

- ✓ La disponibilidad, integridad, confidencialidad, legalidad y confiabilidad de la información.
- ✓ La implementación, mantención, monitoreo y mejoramiento continuo de la aplicación de la presente política.
- ✓ Los procedimientos para asegurar la continuidad del negocio.
- ✓ La detección y la comunicación oportuna de vulnerabilidades y eventos de riesgos que afecten a los activos de información.
- ✓ El acceso amplio, pero controlado a los activos de información.
- ✓ La operación correcta y segura de las instalaciones de procesamiento de información.
- ✓ La seguridad física y del entorno donde se encuentran y operan los activos de información.
- ✓ Los roles, responsabilidades y competencias de los funcionarios del Gobierno Regional de Antofagasta que tengan relación con los activos de información.
- ✓ La identificación de los responsables de la seguridad de los activos de información.
- ✓ La relación con los proveedores y usuarios externos.

2. DECLARACION INSTITUCIONAL

La protección de los activos de información y de la tecnología para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, es una responsabilidad de todos y cada uno de los Funcionarios del Servicio, extendiendo esta responsabilidad a nuestros proveedores externos, con el propósito principal de mantener la continuidad de la provisión de los productos estratégicos a nuestros clientes y mantener el soporte a nuestros clientes internos.

3. DEFINICIÓNES

- ✓ Proteger, resguardar y asegurar la disponibilidad, integridad y confidencialidad de los activos de información y tecnologías para su procesamiento a efecto de garantizar la continuidad de los procesos de negocio del Servicio.
- ✓ Identificar y clasificar los activos de información de la institución para la operación y continuidad del negocio, considerando la Matriz de Riesgo.
- ✓ Detectar, eliminar o mitigar las vulnerabilidades y los riesgos que amenacen los activos de información que afecten la operación y continuidad del negocio.
- ✓ Establecer políticas, normas, procedimientos o instructivos para la manipulación, uso y resguardo adecuado de los activos de información.
- ✓ Difundir la Política de Seguridad de la Información y capacitar a todos los (las) funcionarios (as) del Servicio sobre los alcances y buenas prácticas que se establezcan en relación al resguardo de los activos de información y las tecnologías para su procesamiento.

- ✓ Establecer los mecanismos de auditoría y control de los activos de información y tecnologías de procesamiento.

4. AMBITO DE APLICACIÓN

La Política General de Seguridad de la Información del Servicio es única y aborda el marco normativo vigente y los siguientes controles de la Norma Chilena ISO 27001_2013:
A.05.01.01: Políticas de Seguridad de la Información
A.05.01.02: Revisión de las Políticas de Seguridad de la Información

Esta política es extensible a todos los procesos estratégicos establecidos en cada una de las divisiones que conforman el Servicio:

- ✓ División de Administración y Finanzas.
- ✓ División de Presupuesto e Inversión Regional.
- ✓ División de Planificación y Desarrollo Regional.
- ✓ División de Fomento e Industria.
- ✓ División de Infraestructura y Transportes.
- ✓ División de Desarrollo Social y Humano.

Esta política general aplica y es extensible a todo el personal, independiente de la modalidad de su contratación, ya sea planta, contrata, Código del Trabajo u honorario a suma alzada, así también a todas las personas naturales o jurídicas que presten servicios en forma permanente o temporal en el Servicio.

Esta política general es aplicable sobre todos los activos de información propios o administrados por el servicio, considerando toda forma de soporte, almacenamiento, transporte y/o transmisión, sea en formato electrónico, virtual o cualquier otro tipo de formato.

Además, su ámbito de aplicación se extiende a los proveedores externos que interactúan con la información del Servicio (bases de Datos, Archivos físicos, etc.), independientemente de la localización donde desarrollen su actividad. Los contratos que se suscriban deberán contener los respectivos Acuerdo de Confidencialidad de la información y respectar y cumplir las políticas de seguridad.

5. DIFUSIÓN

Se establece que la difusión de la Política de Seguridad de la Información es responsabilidad del Jefe del Servicio, a través del Departamento de Gestión y Desarrollo de Personas para todo el personal independiente de la modalidad de su contratación, ya sea planta, contrata, Código del Trabajo u honorario a suma alzada, así también a todas las personas naturales o jurídicas que presten servicios en forma permanente o temporal en el Servicio.

Los mecanismos de difusión a emplear, a lo menos deben considerar la publicidad en los espacios de intranet y el envío de correos a los funcionarios con el contenido de las políticas vigentes y reiterar el procedimiento cada vez que se modifique la Política de Seguridad de la Información.

El Departamento de Gestión y Desarrollo de Personas programara en el año calendario las Capacitaciones de Difusión de la Política General de Seguridad de la Información y de las políticas específicas que estén vigentes, de acuerdo a los requerimientos que le efectué el Encargado de la Seguridad de la información del Servicio.

A los proveedores externos que interactúan con la información del Servicio (bases de Datos, Archivos físicos, etc.), la difusión se efectuará a través de la publicación de las Políticas que estén vigentes en el sitio web Institucional.

Estos procedimientos se deberán reiterar cada vez que se modifiquen las políticas de la seguridad de la información.

6. REVISIÓN Y ACTUALIZACIÓN

Las directrices y alcances contenidos en esta política son objeto de mejoras continuas, por lo tanto, se entiende que son factibles de someter a modificaciones, actualizaciones y cambios periódicos tendientes a mantenerla vigente y aplicable de acuerdo con las condiciones en que el Servicio se encuentre. Sin perjuicio de lo anterior, se establece que cada 2 años, a lo más, esta política será sometida a revisión y actualización.

La revisión de la política, requiere definir los siguientes aspectos:

- ✓ Será responsabilidad del Encargado de Seguridad del Servicio, analizar y proponer al Comité de Seguridad de la Información, los cambios a la Política General de Seguridad de la Información del Servicio.
- ✓ La propuesta de cambios a la Política General de Seguridad de la Información del Servicio, debe ser sancionada por el Comité de Seguridad de la Información.
- ✓ Será responsabilidad del Encargado de Seguridad del Servicio, la tramitación de la respectiva Resolución Exenta que aprueba la Actualización de la Política General de Seguridad de la Información aprobada por el Comité de Seguridad de la Información, para la aprobación final del Jefe Superior del Servicio.
- ✓ La revisión de la Política General de Seguridad de la Información se efectuará considerando:
  - ❖ Retroalimentación entre las partes interesadas.
  - ❖ Revisiones efectuadas por terceras partes.
  - ❖ Resultado del análisis de acciones correctivas y preventivas.
  - ❖ La legislación que puede modificar los procesos administrativos del Gobierno Regional de Antofagasta.
  - ❖ Nueva legislación sobre Seguridad de la Información.
  - ❖ Nuevos procesos tecnológicos informáticos que hay que adoptar en el trabajo administrativo del Gobierno Regional de Antofagasta.

7. COMPONENTES

La política general de seguridad de la información del Servicio esta complementada por políticas específicas acorde con los dominios de seguridad que establece el DS-83 y Norma Chilena Oficial NCh-ISO 27001:2013 y la Resolución Exenta N° 125 de fecha 20 de febrero de 2019, que actualiza la norma para el funcionamiento y atribuciones del Comité de Seguridad de la Información del Servicio.

Organización de la Seguridad de la Información
Comité de Seguridad de la Información
Establecer un marco referencial a nivel directivo para la implantación del sistema de la seguridad de la información para el Servicio Administrativo del Gobierno Regional de Antofagasta. Este marco se estableció a través de la Resolución Exenta N° 125 de fecha 20 de febrero de 2019 que define las atribuciones del Comité de Seguridad de la Información y deja sin efecto Resoluciones: N° 1275 de fecha 03 noviembre de 2015; N° 1276 de fecha 03 noviembre de 2015; N° 1448 de fecha 17 diciembre de 2015 y N° 1210 de fecha 20 noviembre de 2017, las cuales se refunden en el texto de la Resolución Exenta N° 125.

Encargado de Seguridad de la Información
Mediante Resolución Exenta N° 1173 de fecha 06 de noviembre de 2017, se nombra el Encargado de Seguridad del Servicio Administrativo del Gobierno Regional de Antofagasta, según lo establece el DS-83. Lo anterior, para la implantación del sistema de la seguridad de la información, el desarrollo de las políticas de seguridad y su correcta aplicación, dejando sin efecto la Resolución Exenta N° 340 del 2011.

POLÍTICAS ESPECÍFICAS POR DOMINIO

- **Política para la seguridad de la información**
  Proporcionar orientación y apoyo de la dirección para la seguridad de la información, de acuerdo con los requisitos del negocio y con las regulaciones y leyes pertinentes.
- **Política de gestión de los activos**
  Implementar y mantener una apropiada protección de los activos de información institucionales. Todos los activos deben ser inventariados, catalogados y contar con un responsable identificado, y se debe velar por su uso aceptable.
- **Política de seguridad de los recursos humanos**
  Asegurar que todo el personal independiente de su modalidad de contratación, ya sea planta, contrata, código del trabajo u honorario y a personas naturales o jurídicas que presten servicios en forma permanente o temporalmente en el Servicio y proveedores externos, conozcan la política y normas, entiendan sus responsabilidades y sean idóneos en los roles para los cuales son considerados. También debe considerar la capacitación regular de éstos, en materia relacionadas a la seguridad de la información.
- **Política de seguridad física y del ambiente**
  Prevenir o resguardar los activos de información del acceso no autorizado a los activos de información o a los recintos donde estos se almacenan, operan o trasmiten y protegen de daños, interferencias, o eventos de índole ambiental que afecten negativamente la integridad y disponibilidad de los activos de información del Servicio.

- **Política de seguridad de las operaciones**
  Asegurar la operación correcta y segura de los medios de procesamiento, almacenamiento y transmisión de los activos de información, a través de la creación de procedimientos y definición de responsabilidades operacionales.
- **Política de control de acceso**
  Asegurar que el acceso de los usuarios sea debidamente autorizada y evitar el acceso no autorizado a los sistemas de información. Se deben establecer procedimientos formales para controlar la asignación y retiro de los derechos de acceso y servicios de información.
- **Política de seguridad de las comunicaciones**
  Asegurar la protección de la información en las redes y sus instalaciones de procedimiento de información de apoyo.
- **Política de adquisición, desarrollo y mantenimiento de sistemas de información**
  Garantizar que la seguridad sea una parte integral de los sistemas de información y se incluya en la etapa de formulación del software, tanto para los sistemas que se desarrollen internamente, como para los que se encargue su elaboración a un proveedor calificado.
- **Política de controles criptográficos**
  Asegurar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad o integridad de la información.
- **Política de seguridad de la información en las relaciones con los proveedores**
  Asegurar la protección de los activos de información del Servicio a los que tienen acceso los proveedores y mantener un nivel acordado de seguridad de la información y entrega del servicio, en línea con los acuerdos adquiridos con el proveedor.
- **Política de gestión de incidentes de seguridad de la información**
  Asegurar que las vulnerabilidades y eventos que afecten negativamente la integridad, disponibilidad y confidencialidad de los activos de información asociados a sistemas o procesos de negocio sean comunicados, registrados y gestionados de manera de permitir la adopción de acciones correctivas en forma oportuna.
- **Política de gestión de la continuidad del negocio**
  Contar con planes de contingencia para contrarrestar las interrupciones en los procesos críticos del negocio y minimizar los efectos de fallas significativas que afecten a los activos de información.
- **Política de cumplimiento**
  Evitar los incumplimientos de cualquier ley, estatuto, regulación u obligación contractual y de cualquier requisito de seguridad a los cuales puede estar sujeto el diseño, operación, uso y gestión de los procesos del negocio y/o activos de información que los apoyan.

8. ROLES Y RESPONSABILIDADES

Para cumplir los objetivos de la Política de Seguridad de la Información del Servicio, se establecen los siguientes roles y responsabilidades:

- ✓ **Jefe Superior del Servicio Administrativo Gobierno Regional de Antofagasta**
  Responsable de aprobar la política y sus futuras modificaciones con la Asesoría del Comité de Seguridad de la Información.
- ✓ **Jefes de División**
  Son responsables de la aplicación de las políticas de seguridad de la información al interior de la División a su cargo, así como del cumplimiento de dicha política por parte de sus funcionarios.
- ✓ **Encargado de Seguridad de la Información**
  Corresponde al cargo / persona del Servicio, la cual cumplirá la función de supervisar el cumplimiento de la presente política y de asesorar en materia de Seguridad de la Información al Jefe Superior del Servicio, a los Jefe de División y a los integrantes del Comité de Seguridad de la Información.
  Sus funciones principales corresponden a liderar el establecimiento, implementación y mantenimiento de un sistema de seguridad de la información, gestionar la respuesta ante incidentes de seguridad, mantener puntos de enlace con especialistas y otros organismos y presidir el Comité de Seguridad de la Información del Servicio.
- ✓ **Oficial de Seguridad de la Información**
  Corresponde al cargo / persona del Servicio, la cual cumplirá la función de apoyar profesionalmente y técnicamente al Encargado de Seguridad de la Información en las materias relativas a la implantación de una Política de Seguridad de la Información.
- ✓ **Unidad de Auditoria Interna**
  Responsable de practicar auditorías sobre el cumplimiento de las especificaciones, las medidas de seguridad de la información establecidas por esta política, las normas, los procedimientos y prácticas que de ella surjan, debiendo informar al Jefe Superior del Servicio y al Comité de Seguridad de la Información .

  Funcionarios Usuarios(as)
  Son las personas que usan los activos de información y los sistemas para su procesamiento. Son responsables de conocer, dar a conocer, cumplir y hacer cumplir la política de seguridad de la

información vigente y además tienen la obligación de reportar cualquier incidente de seguridad del que tengan conocimiento.

✓ **Terceros**
Son las personas que a través de los respectivos contratos (entendido como acuerdo de voluntades) se vinculan con el Servicio, son responsables de conocer y cumplir las políticas de seguridad de la información vigente, obligación que se expresara en el respectivo contrato.
Los Consejeros Regionales son responsables de conocer y cumplir las políticas de seguridad de la información vigente, obligación que se expresa cada vez que interactúan con el Servicio Administrativo del Gobierno Regional de Antofagasta.

9. MARCO GENERAL PARA LAS POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

La Seguridad de la Información, se entenderá como todas aquellas medidas preventivas y reactivas que permitan resguardar y proteger la información de la organización de riesgos que puedan afectar la confidencialidad, disponibilidad e integridad de la misma.
A continuación se establece una pauta para la elaboración de las políticas específicas que se desprenden de la política general.

9.1 OBJETIVOS DE LA POLÍTICA

El cumplimiento del marco legal vigente.- Evidentemente, una política debe cumplir con la normativa vigente de nuestro país; para esto se deberán establecer las relaciones que cada ley establece con la Seguridad de la Información, tales como: los derechos de la propiedad intelectual, tratamiento de datos de carácter personal, exportación de información, etc., junto a todos los aspectos relacionados con los registros de eventos y sus respectivas soluciones permanentes y los recursos involucrados y su mantenimiento en el tiempo, para asegurar la continuidad del negocio.

Manejo de información sensible.-El manejo de la información sensible, deberá tener un tratamiento especial al interior del servicio, aplicando toda la normativa usada a la información normal, más la seguridad especial para este caso.

Respuesta ante incidentes.-En caso de incidentes se deberá constituir el comité de seguridad de la información, previo al análisis e informe de sus respectivas dependencias y deberes. La continuidad del negocio, se realizara a través de la creación de planes de continuidad y de análisis de impacto y por otro lado con la aplicación de simulacros de catástrofes.

Control de acceso físico/lógico.- Se debe definir y gestionar los puntos de control de acceso a los recursos informáticos y otros; y para esto se implementaran sistemas de contraseña, seguridad perimetral, monitorización de accesos, etc.

Gestión comunicacional.- La gestión comunicacional se realizara a través de la intranet y también a través de charlas informativas y formativas, en relación a los temas de la seguridad de la información.

Segregación de funciones.- La segregación de funciones al interior de la institución, se realizara en forma descendente, partiendo por el jefe superior, siguiendo con los jefes de División, los jefes de departamento, luego los jefes de unidad y por último los funcionarios.

Uso de recursos.- Los recursos disponibles por el servicio, abarcan los recursos humanos financieros y de gestión y se busca hacer uso de ellos en forma racional y gradual, dependiendo del tipo de incidente a abordar.

9.2 ESTRUCTURA Y CONTENIDO DE LAS POLÍTICAS DE SEGURIDAD

La Estructura y contenido de las Políticas de Seguridad específicas de la Información, deberán contener como mínimo:
- Objetivo
- Alcance o Ámbito de Aplicación
- Roles y Responsabilidades
- Definiciones
- Difusión
- Revisión y Actualización

9.3 GESTACIÓN DE LA POLÍTICA

Cada una de las políticas de seguridad de la información a implementar en el servicio, tendrá como base la matriz de diagnóstico efectuada por el servicio. Los criterios de selección de controles serán definidos y priorizados por el Comité de Seguridad de la Información, conforme a priorización de brechas.

9.4 APROBACIÓN DE LA POLÍTICA

Se aprobarán por el Comité de Seguridad de la Información todos los documentos y productos elaborados para la implementación del sistema de seguridad de la información. La aprobación quedara registrada en el acta de la reunión que aprobó el documento y/o productos elaborados por el centro de responsabilidad del respectivo control.
En el caso de la Política General de Seguridad de la Información, esta se aprobará mediante la aprobación y dictación de la respectiva Resolución Exenta.

9.5 DIFUSIÓN DE LAS POLÍTICAS

La difusión de las políticas de seguridad de la información se efectuará a través de charlas de capacitación a todos los funcionarios del servicio. No obstante lo anterior, dichas políticas serán públicas en la intranet del servicio. En lo que dice relación con la publicación con políticas relacionas con externos, se difundirá en la página web del Gobierno Regional.

9.6 REVISIÓN DE UNA POLÍTICA

La revisión normal de las políticas de seguridad de la información, se realizará en forma periódica, a lo más cada dos (2) años, y frente a eventos que afecten o tengan impacto en los riesgos previamente identificados por el servicio (tales como: cambios legales, cambios de autoridades, surgimiento de nuevas tecnologías, cambios en el entorno ambiental, etc.), se impondrá una revisión adicional.

9.7 SANCIONES POR IMCUMPLIMIENTO

El incumplimiento de las políticas de seguridad de la información u otros documentos, tales como procedimientos, Instructivos, etc., del Servicio Administrativo del Gobierno Regional de Antofagasta, serán sancionados los funcionarios infractores en los términos que establece el Estatuto Administrativo.

10. GLOSARIO DE TÉRMINOS

Para los propósitos de esta Política, se entenderá por:

a) **Activo de Información**: Sistemas de información, aplicación o herramientas de tipo software, bases de datos, equipos computacionales, dispositivos móviles, archivos físicos, documentos electrónicos, personas o cualquier otro activo que por su naturaleza registre, procese, almacene o transmita información considerada relevante para los procesos del negocio de los Servicios Administrativos del Gobierno Regional de Antofagasta.

b) **Administración de Riesgos**: Se entiende por administración de riesgos al proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a los activos de información.

c) **Confidencialidad**: Se entiende por confidencialidad a la característica o propiedad que determina que la información no esté disponible ni se revela a personas, entidades o procesos no autorizados.

d) **Disponibilidad**: Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

e) **Evaluación de Riesgos**: Se entenderá por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatoria del Organismo.

f) **Evento de seguridad de la información**: Ocurrencia identificada de un estado de un sistema, servicio o red que indica una posible violación de la política de la seguridad de la información o falla de salvaguardas, o una situación previamente desconocida que puede ser pertinente a la seguridad.

g) **Incidente de Seguridad**: Un incidente de seguridad es uno o varios eventos que afecta la seguridad de la información y que tienen una probabilidad significativa de comprometer la continuidad operacional de los Servicios Administrativos del Gobierno Regional de Antofagasta en sus procesos de negocio.

h) **Integridad de la información**: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

i) **Seguridad de los Activos de Información**: Es proteger, resguardar y asegurar la disponibilidad, confidencialidad e integridad de los activos de información y tecnologías para su procesamiento a

efecto de garantizar la continuidad operativa de los Servicios Administrativos del Gobierno Regional de Antofagasta

j) **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.

k) **Amenazas**: Cualquier acción o evento que puede ocasionar consecuencias adversas.

l) **Riesgo**: La explotación de una vulnerabilidad por parte de una amenaza.

m) **Controles**: Cualquier acción o proceso que se utiliza para mitigar el riesgo.

n) **Sensibilidad**: El nivel de impacto que tendría una divulgación no autorizada.

o) **Criticidad**: La importancia que tiene un recurso para el negocio.

p) **Normas:** Establecer los límites permisibles de acciones y procesos para cumplir con las políticas.

3. PUBLÍQUESE la presente resolución exenta en el sitio web Institucional www.goreantofagasta.cl, para difundir entre los proveedores externos la actualización de la Política General de Seguridad de la Información del Servicio Administrativo del Gobierno Regional de Antofagasta.

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE

GOBIERNO REGIONAL II REGION ANTOFAGASTA

MARCO ANTONIO DÍAZ MUÑOZ
Intendente
Región de Antofagasta

LUIS COLMAN VEGA
Abogado
Gobierno Regional de Antofagasta

MADM/LCV/YTP/PZC/MLC/mlc

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN GOBIERNO REGIONAL DE ANTOFAGASTA

NOTA DE CONFIDENCIALIDAD

La Política General de Seguridad de la Información para los Servicios Administrativos del Gobierno Regional de Antofagasta, se rige por los términos y condiciones que en este documento se establecen. Su uso está dirigido a todos los funcionarios de esta institución sin distinción de su condición contractual, los que podrán acceder a ella, previo a su conocimiento, de entendimiento y de la aceptación de los términos relativos a su utilización.

CONTROL DE VERSIONES

N° Versión	Fecha Aprobación	Modificación	Páginas o Secciones modificadas	Autor
1	30/03/2011	Elaboración inicial	Todas.	Encargado S.I.
2	14/09/2011	Se mejoran Punto I, Punto III y Punto IV.	Puntos: I, III y IV.	Encargado S.I.
3	07/10/2015	Se agrega Punto V Componentes de la Política de Seguridad de la Información, según actualización norma NCh-ISO 27001_2013.	Punto V.	Encargado S.I.
4	04/12/2015	Se modifica Punto VII letra g, sobre revisión de una política.	Punto VII.	Encargado S.I.
5	17/10/2017	✓ Se complementa el Punto2. ✓ Desde Punto 4 se extrae un nuevo punto independiente para la Difusión de la Política de Seguridad de la Información y otro punto parta la Revisión de la Política de Seguridad de la Información y se complementa Punto 4. ✓ Se renumeran los contenidos desde punto 5 al 10. ✓ Se modifica Punto 6 (actual 8) sobre Roles y responsabilidades. ✓ Se modifica Punto 7 (actual 9) en Letra g (actual 9.10) sobre Revisión de una Política y Letra a (actual 9.1) en respuesta ante un incidente yen Uso de Recursos. ✓ Se agrega a Punto 6 (actual 8) el Rol de Oficial de Seguridad.	Puntos: 2, 4,6 y 7.	Oficial S.I.
6	25/01/2019	✓ Se complementa Sección 1. ✓ Se complementa Sección 2. ✓ Se complementa Sección 4. ✓ Se complementa Sección 5. ✓ Se complementa Sección 6. ✓ Se complementa Sección 7. ✓ Se complementa Sección 8. ✓ Se complementa Sección 9.	Sección: 1, 2, 4, 5, 6, 7, 8,9.	Encargado S.I.

CONTROLES NORMA NCh-ISO 27001_2013 ABORDADOS

Control	Objetivo del control
A.05.01.01	Políticas de Seguridad de la Información
A.05.01.02	Revisión de las Políticas de Seguridad de la Información

FIRMAS RESPONSABLES

Elaborado por:	**Revisado por:**	**Aprobado por:**
Fecha:25/01/2019	Fecha:05/03/2019	Fecha:08/03/2019
Miguel Lagos Covarrubias	**Luis Colman Vega**	**Marco Antonio Díaz Muñoz**
Encargado Seguridad de la Información	Encargado Unidad Jurídica	Jefe Superior del Servicio

GOBIERNO REGIONAL II REGION ANTOFAGASTA

TABLA DE CONTENIDO

1. OBJETIVO

El presente documento de Política General de Seguridad de la Información establece el marco de referencia, a través del cual el Servicio, fija los estándares de seguridad de la información a aplicar para proteger adecuadamente sus activos de información, según lo establece el Decreto Supremo Nº 83 sobre Seguridad y Confidencialidad que aprobó la "**Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos**".

Su objetivo es garantizar estándares mínimos de Seguridad de los Activos de información entendiéndose por tal:

- ✓ La disponibilidad, integridad, confidencialidad, legalidad y confiabilidad de la información.
- ✓ La implementación, mantención, monitoreo y mejoramiento continuo de la aplicación de la presente política.
- ✓ Los procedimientos para asegurar la continuidad del negocio.
- ✓ La detección y la comunicación oportuna de vulnerabilidades y eventos de riesgos que afecten a los activos de información.
- ✓ El acceso amplio, pero controlado a los activos de información.
- ✓ La operación correcta y segura de las instalaciones de procesamiento de información.
- ✓ La seguridad física y del entorno donde se encuentran y operan los activos de información.
- ✓ Los roles, responsabilidades y competencias de los funcionarios del Gobierno Regional de Antofagasta que tengan relación con los activos de información.
- ✓ La identificación de los responsables de la seguridad de los activos de información.
- ✓ La relación con los proveedores y usuarios externos.

2. DECLARACION INSTITUCIONAL

La protección de los activos de información y de la tecnología para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, es una responsabilidad de todos y cada uno de los Funcionarios del Servicio, extendiendo esta responsabilidad a nuestros proveedores externos, con el propósito principal de mantener la continuidad de la provisión de los productos estratégicos a nuestros clientes y mantener el soporte a nuestros clientes internos.

3. DEFINICIÓNES

- ✓ Proteger, resguardar y asegurar la disponibilidad, integridad y confidencialidad de los activos de información y tecnologías para su procesamiento a efecto de garantizar la continuidad de los procesos de negocio del Servicio.
- ✓ Identificar y clasificar los activos de información de la institución para la operación y continuidad del negocio, considerando la Matriz de Riesgo.
- ✓ Detectar, eliminar o mitigar las vulnerabilidades y los riesgos que amenacen los activos de información que afecten la operación y continuidad del negocio.
- ✓ Establecer políticas, normas, procedimientos o instructivos para la manipulación, uso y resguardo adecuado de los activos de información.
- ✓ Difundir la Política de Seguridad de la Información y capacitar a todos los (las) funcionarios (as) del Servicio sobre los alcances y buenas prácticas que se establezcan en relación al resguardo de los activos de información y las tecnologías para su procesamiento.
- ✓ Establecer los mecanismos de auditoría y control de los activos de información y tecnologías de procesamiento.

4. AMBITO DE APLICACIÓN

La Política General de Seguridad de la Información del Servicio es única y aborda el marco normativo vigente y los siguientes controles de la Norma Chilena ISO 27001_2013:

A.05.01.01: Políticas de Seguridad de la Información
A.05.01.02: Revisión de las Políticas de Seguridad de la Información

Esta política es extensible a todos los procesos estratégicos establecidos en cada una de las divisiones que conforman el Servicio:

- ✓ División de Administración y Finanzas.
- ✓ División de Presupuesto e Inversión Regional.
- ✓ División de Planificación y Desarrollo Regional.
- ✓ División de Fomento e Industria.
- ✓ División de Infraestructura y Transportes.
- ✓ División de Desarrollo Social y Humano.

Esta política general aplica y es extensible a todo el personal, independiente de la modalidad de su contratación, ya sea planta, contrata, Código del Trabajo u honorario a suma alzada, así también a todas las personas naturales o jurídicas que presten servicios en forma permanente o temporal en el Servicio.

Esta política general es aplicable sobre todos los activos de información propios o administrados por el servicio, considerando toda forma de soporte, almacenamiento, transporte y/o transmisión, sea en formato electrónico, virtual o cualquier otro tipo de formato.

Además, su ámbito de aplicación se extiende a los proveedores externos que interactúan con la información del Servicio (bases de Datos, Archivos físicos, etc.), independientemente de la localización donde desarrollen su actividad. Los contratos que se suscriban deberán contener los respectivos Acuerdo de Confidencialidad de la información y respectar y cumplir las políticas de seguridad.

5. DIFUSIÓN

Se establece que la difusión de la Política de Seguridad de la Información es responsabilidad del Jefe del Servicio, a través del Departamento de Gestión y Desarrollo de Personas para todo el personal independiente de la modalidad de su contratación, ya sea planta, contrata, Código del Trabajo u honorario a suma alzada, así también a todas las personas naturales o jurídicas que presten servicios en forma permanente o temporal en el Servicio.

Los mecanismos de difusión a emplear, a lo menos deben considerar la publicidad en los espacios de intranet y el envío de correos a los funcionarios con el contenido de las políticas vigentes y reiterar el procedimiento cada vez que se modifique la Política de Seguridad de la Información.

El Departamento de Gestión y Desarrollo de Personas programara en el año calendario las Capacitaciones de Difusión de la Política General de Seguridad de la Información y de las políticas específicas que estén vigentes, de acuerdo a los requerimientos que le efectué el Encargado de la Seguridad de la información del Servicio.

A los proveedores externos que interactúan con la información del Servicio (bases de Datos, Archivos físicos, etc.), la difusión se efectuará a través de la publicación de las Políticas que estén vigentes en el sitio web Institucional.

Estos procedimientos se deberán reiterar cada vez que se modifiquen las políticas de la seguridad de la información.

6. REVISIÓN Y ACTUALIZACIÓN

Las directrices y alcances contenidos en esta política son objeto de mejoras continuas, por lo tanto, se entiende que son factibles de someter a modificaciones, actualizaciones y cambios periódicos tendientes a mantenerla vigente y aplicable de acuerdo con las condiciones en que el Servicio se encuentre. Sin perjuicio de lo anterior, se establece que cada 2 años, a lo más, esta política será sometida a revisión y actualización.

La revisión de la política, requiere definir los siguientes aspectos:

- ✓ Será responsabilidad del Encargado de Seguridad del Servicio, analizar y proponer al Comité de Seguridad de la Información, los cambios a la Política General de Seguridad de la Información del Servicio.
- ✓ La propuesta de cambios a la Política General de Seguridad de la Información del Servicio, debe ser sancionada por el Comité de Seguridad de la Información.
- ✓ Será responsabilidad del Encargado de Seguridad del Servicio, la tramitación de la respectiva Resolución Exenta que aprueba la Actualización de la Política General de Seguridad de la Información aprobada por el Comité de Seguridad de la Información, para la aprobación final del Jefe Superior del Servicio.
- ✓ La revisión de la Política General de Seguridad de la Información se efectuará considerando:
  - ❖ Retroalimentación entre las partes interesadas.
  - ❖ Revisiones efectuadas por terceras partes.
  - ❖ Resultado del análisis de acciones correctivas y preventivas.
  - ❖ La legislación que puede modificar los procesos administrativos del Gobierno Regional de Antofagasta.
  - ❖ Nueva legislación sobre Seguridad de la Información.
  - ❖ Nuevos procesos tecnológicos informáticos que hay que adoptar en el trabajo administrativo del Gobierno Regional de Antofagasta.

7. COMPONENTES

La política general de seguridad de la información del Servicio esta complementada por políticas específicas acorde con los dominios de seguridad que establece el DS-83 y Norma Chilena Oficial NCh-ISO 27001:2013 y la Resolución Exenta N° 125 de fecha 20 de febrero de 2019, que actualiza la norma para el funcionamiento y atribuciones del Comité de Seguridad de la Información del Servicio.

Organización de la Seguridad de la Información
Comité de Seguridad de la Información
Establecer un marco referencial a nivel directivo para la implantación del sistema de la seguridad de la información para el Servicio Administrativo del Gobierno Regional de Antofagasta. Este marco se estableció a través de la Resolución Exenta N° 125 de fecha 20 de febrero de 2019 que define las atribuciones del Comité de Seguridad de la Información y deja sin efecto Resoluciones: N° 1275 de fecha 03 noviembre de 2015; N° 1276 de fecha 03 noviembre de 2015; N° 1448 de fecha 17 diciembre de 2015 y N° 1210 de fecha 20 noviembre de 2017, las cuales se refunden en el texto de la Resolución Exenta N° 125.

Encargado de Seguridad de la Información
Mediante Resolución Exenta N° 1173 de fecha 06 de noviembre de 2017, se nombra el Encargado de Seguridad del Servicio Administrativo del Gobierno Regional de Antofagasta, según lo establece el DS-83. Lo anterior, para la implantación del sistema de la seguridad de la información, el desarrollo de las políticas de seguridad y su correcta aplicación, dejando sin efecto la Resolución Exenta N° 340 del 2011.

POLÍTICAS ESPECÍFICAS POR DOMINIO

- **Política para la seguridad de la información**
  Proporcionar orientación y apoyo de la dirección para la seguridad de la información, de acuerdo con los requisitos del negocio y con las regulaciones y leyes pertinentes.
- **Política de gestión de los activos**
  Implementar y mantener una apropiada protección de los activos de información institucionales. Todos los activos deben ser inventariados, catalogados y contar con un responsable identificado, y se debe velar por su uso aceptable.
- **Política de seguridad de los recursos humanos**
  Asegurar que todo el personal independiente de su modalidad de contratación, ya sea planta, contrata, código del trabajo u honorario y a personas naturales o jurídicas que presten servicios en forma permanente o temporalmente en el Servicio y proveedores externos, conozcan la política y normas, entiendan sus responsabilidades y sean idóneos en los roles para los cuales son considerados. También debe considerar la capacitación regular de éstos, en materia relacionadas a la seguridad de la información.
- **Política de seguridad física y del ambiente**
  Prevenir o resguardar los activos de información del acceso no autorizado a los activos de información o a los recintos donde estos se almacenan, operan o trasmiten y protegen de daños, interferencias, o eventos de índole ambiental que afecten negativamente la integridad y disponibilidad de los activos de información del Servicio.

- **Política de seguridad de las operaciones**
  Asegurar la operación correcta y segura de los medios de procesamiento, almacenamiento y transmisión de los activos de información, a través de la creación de procedimientos y definición de responsabilidades operacionales.
- **Política de control de acceso**
  Asegurar que el acceso de los usuarios sea debidamente autorizada y evitar el acceso no autorizado a los sistemas de información. Se deben establecer procedimientos formales para controlar la asignación y retiro de los derechos de acceso y servicios de información.
- **Política de seguridad de las comunicaciones**
  Asegurar la protección de la información en las redes y sus instalaciones de procedimiento de información de apoyo.
- **Política de adquisición, desarrollo y mantenimiento de sistemas de información**
  Garantizar que la seguridad sea una parte integral de los sistemas de información y se incluya en la etapa de formulación del software, tanto para los sistemas que se desarrollen internamente, como para los que se encargue su elaboración a un proveedor calificado.
- **Política de controles criptográficos**
  Asegurar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad o integridad de la información.
- **Política de seguridad de la información en las relaciones con los proveedores**

Asegurar la protección de los activos de información del Servicio a los que tienen acceso los proveedores y mantener un nivel acordado de seguridad de la información y entrega del servicio, en línea con los acuerdos adquiridos con el proveedor.

- **Política de gestión de incidentes de seguridad de la información**
  Asegurar que las vulnerabilidades y eventos que afecten negativamente la integridad, disponibilidad y confidencialidad de los activos de información asociados a sistemas o procesos de negocio sean comunicados, registrados y gestionados de manera de permitir la adopción de acciones correctivas en forma oportuna.
- **Política de gestión de la continuidad del negocio**
  Contar con planes de contingencia para contrarrestar las interrupciones en los procesos críticos del negocio y minimizar los efectos de fallas significativas que afecten a los activos de información.
- **Política de cumplimiento**
  Evitar los incumplimientos de cualquier ley, estatuto, regulación u obligación contractual y de cualquier requisito de seguridad a los cuales puede estar sujeto el diseño, operación, uso y gestión de los procesos del negocio y/o activos de información que los apoyan.

8. ROLES Y RESPONSABILIDADES

Para cumplir los objetivos de la Política de Seguridad de la Información del Servicio, se establecen los siguientes roles y responsabilidades:

- ✓ **Jefe Superior del Servicio Administrativo Gobierno Regional de Antofagasta**
  Responsable de aprobar la política y sus futuras modificaciones con la Asesoría del Comité de Seguridad de la Información.
- ✓ **Jefes de División**
  Son responsables de la aplicación de las políticas de seguridad de la información al interior de la División a su cargo, así como del cumplimiento de dicha política por parte de sus funcionarios.
- ✓ **Encargado de Seguridad de la Información**
  Corresponde al cargo / persona del Servicio, la cual cumplirá la función de supervisar el cumplimiento de la presente política y de asesorar en materia de Seguridad de la Información al Jefe Superior del Servicio, a los Jefe de División y a los integrantes del Comité de Seguridad de la Información.
  Sus funciones principales corresponden a liderar el establecimiento, implementación y mantenimiento de un sistema de seguridad de la información, gestionar la respuesta ante incidentes de seguridad, mantener puntos de enlace con especialistas y otros organismos y presidir el Comité de Seguridad de la Información del Servicio.
- ✓ **Oficial de Seguridad de la Información**
  Corresponde al cargo / persona del Servicio, la cual cumplirá la función de apoyar profesionalmente y técnicamente al Encargado de Seguridad de la Información en las materias relativas a la implantación de una Política de Seguridad de la Información.
- ✓ **Unidad de Auditoria Interna**
  Responsable de practicar auditorías sobre el cumplimiento de las especificaciones, las medidas de seguridad de la información establecidas por esta política, las normas, los procedimientos y prácticas que de ella surjan, debiendo informar al Jefe Superior del Servicio y al Comité de Seguridad de la Información .

  Funcionarios Usuarios(as)
  Son las personas que usan los activos de información y los sistemas para su procesamiento. Son responsables de conocer, dar a conocer, cumplir y hacer cumplir la política de seguridad de la información vigente y además tienen la obligación de reportar cualquier incidente de seguridad del que tengan conocimiento.
- ✓ **Terceros**
  Son las personas que a través de los respectivos contratos (entendido como acuerdo de voluntades) se vinculan con el Servicio, son responsables de conocer y cumplir las políticas de seguridad de la información vigente, obligación que se expresara en el respectivo contrato.
  Los Consejeros Regionales son responsables de conocer y cumplir las políticas de seguridad de la información vigente, obligación que se expresa cada vez que interactúan con el Servicio Administrativo del Gobierno Regional de Antofagasta.

9. MARCO GENERAL PARA LAS POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

La Seguridad de la Información, se entenderá como todas aquellas medidas preventivas y reactivas que permitan resguardar y proteger la información de la organización de riesgos que puedan afectar la confidencialidad, disponibilidad e integridad de la misma.
A continuación se establece una pauta para la elaboración de las políticas específicas que se desprenden de la política general.

9.1 OBJETIVOS DE LA POLÍTICA

El cumplimiento del marco legal vigente.- Evidentemente, una política debe cumplir con la normativa vigente de nuestro país; para esto se deberán establecer las relaciones que cada ley establece con la Seguridad de la Información, tales como: los derechos de la propiedad intelectual, tratamiento de datos de carácter personal, exportación de información, etc., junto a todos los aspectos relacionados con los registros de eventos y sus respectivas soluciones permanentes y los recursos involucrados y su mantenimiento en el tiempo, para asegurar la continuidad del negocio.

Manejo de información sensible.-El manejo de la información sensible, deberá tener un tratamiento especial al interior del servicio, aplicando toda la normativa usada a la información normal, más la seguridad especial para este caso.

Respuesta ante incidentes.-En caso de incidentes se deberá constituir el comité de seguridad de la información, previo al análisis e informe de sus respectivas dependencias y deberes. La continuidad del negocio, se realizara a través de la creación de planes de continuidad y de análisis de impacto y por otro lado con la aplicación de simulacros de catástrofes.

Control de acceso físico/lógico.- Se debe definir y gestionar los puntos de control de acceso a los recursos informáticos y otros; y para esto se implementaran sistemas de contraseña, seguridad perimetral, monitorización de accesos, etc.

Gestión comunicacional.- La gestión comunicacional se realizara a través de la intranet y también a través de charlas informativas y formativas, en relación a los temas de la seguridad de la información.

Segregación de funciones.- La segregación de funciones al interior de la institución, se realizara en forma descendente, partiendo por el jefe superior, siguiendo con los jefes de División, los jefes de departamento, luego los jefes de unidad y por último los funcionarios.

Uso de recursos.- Los recursos disponibles por el servicio, abarcan los recursos humanos financieros y de gestión y se busca hacer uso de ellos en forma racional y gradual, dependiendo del tipo de incidente a abordar.

9.2 ESTRUCTURA Y CONTENIDO DE LAS POLÍTICAS DE SEGURIDAD

La Estructura y contenido de las Políticas de Seguridad específicas de la Información, deberán contener como mínimo:

- Objetivo
- Alcance o Ámbito de Aplicación
- Roles y Responsabilidades
- Definiciones
- Difusión
- Revisión y Actualización

9.3 GESTACIÓN DE LA POLÍTICA

Cada una de las políticas de seguridad de la información a implementar en el servicio, tendrá como base la matriz de diagnóstico efectuada por el servicio. Los criterios de selección de controles serán definidos y priorizados por el Comité de Seguridad de la Información, conforme a priorización de brechas.

9.4 APROBACIÓN DE LA POLÍTICA

Se aprobarán por el Comité de Seguridad de la Información todos los documentos y productos elaborados para la implementación del sistema de seguridad de la información. La aprobación quedara registrada en el acta de la reunión que aprobó el documento y/o productos elaborados por el centro de responsabilidad del respectivo control.
En el caso de la Política General de Seguridad de la Información, esta se aprobará mediante la aprobación y dictación de la respectiva Resolución Exenta.

9.5 DIFUSIÓN DE LAS POLÍTICAS

La difusión de las políticas de seguridad de la información se efectuará a través de charlas de capacitación a todos los funcionarios del servicio. No obstante lo anterior, dichas políticas serán públicas en la intranet del servicio. En lo que dice relación con la publicación con políticas relacionas con externos, se difundirá en la página web del Gobierno Regional.

9.6 REVISIÓN DE UNA POLÍTICA

La revisión normal de las políticas de seguridad de la información, se realizará en forma periódica, a lo más cada dos (2) años, y frente a eventos que afecten o tengan impacto en los

riesgos previamente identificados por el servicio (tales como: cambios legales, cambios de autoridades, surgimiento de nuevas tecnologías, cambios en el entorno ambiental, etc.), se impondrá una revisión adicional.

9.7 SANCIONES POR IMCUMPLIMIENTO

El incumplimiento de las políticas de seguridad de la información u otros documentos, tales como procedimientos, Instructivos, etc., del Servicio Administrativo del Gobierno Regional de Antofagasta, serán sancionados los funcionarios infractores en los términos que establece el Estatuto Administrativo.

10. GLOSARIO DE TÉRMINOS

Para los propósitos de esta Política, se entenderá por:

a) **Activo de Información**: Sistemas de información, aplicación o herramientas de tipo software, bases de datos, equipos computacionales, dispositivos móviles, archivos físicos, documentos electrónicos, personas o cualquier otro activo que por su naturaleza registre, procese, almacene o transmita información considerada relevante para los procesos del negocio de los Servicios Administrativos del Gobierno Regional de Antofagasta.

b) **Administración de Riesgos**: Se entiende por administración de riesgos al proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a los activos de información.

c) **Confidencialidad**: Se entiende por confidencialidad a la característica o propiedad que determina que la información no esté disponible ni se revela a personas, entidades o procesos no autorizados.

d) **Disponibilidad**: Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

e) **Evaluación de Riesgos**: Se entenderá por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatoria del Organismo.

f) **Evento de seguridad de la información**: Ocurrencia identificada de un estado de un sistema, servicio o red que indica una posible violación de la política de la seguridad de la información o falla de salvaguardas, o una situación previamente desconocida que puede ser pertinente a la seguridad.

g) **Incidente de Seguridad**: Un incidente de seguridad es uno o varios eventos que afecta la seguridad de la información y que tienen una probabilidad significativa de comprometer la continuidad operacional de los Servicios Administrativos del Gobierno Regional de Antofagasta en sus procesos de negocio.

h) **Integridad de la información**: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

i) **Seguridad de los Activos de Información**: Es proteger, resguardar y asegurar la disponibilidad, confidencialidad e integridad de los activos de información y tecnologías para su procesamiento a efecto de garantizar la continuidad operativa de los Servicios Administrativos del Gobierno Regional de Antofagasta

j) **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.

k) **Amenazas**: Cualquier acción o evento que puede ocasionar consecuencias adversas.

l) **Riesgo**: La explotación de una vulnerabilidad por parte de una amenaza.

m) **Controles**: Cualquier acción o proceso que se utiliza para mitigar el riesgo.

n) **Sensibilidad**: El nivel de impacto que tendría una divulgación no autorizada.

o) **Criticidad**: La importancia que tiene un recurso para el negocio.

p) **Normas:** Establecer los límites permisibles de acciones y procesos para cumplir con las políticas.