MAT.: Aprueba Política de Seguridad de la Información.

RESOLUCIÓN EXENTA N° 000369 /

ANTOFAGASTA, 30 MAR 2011

VISTOS:

Lo dispuesto en la Ley N° 18.575, sobre Bases Generales de la Administración del Estado; Ley N° 19.175 Orgánica Constitucional sobre Gobierno y Administración Regional; Ley N° 20.035 que modifica la Ley N° 19.175 Orgánica Constitucional sobre Gobierno y Administración Regional; Ley N° 19.799, sobre documentos electrónicos, firma electrónica y la certificación de dicha firma, DS N° 181 de 2002 del Ministerio de Economía, Fomento y Reconstrucción; DS N° 83 de 2004 del Ministerio Secretaría General de la Presidencia; y Resolución N° 1.600/2008 de la Contraloría General de la República; Ley de Presupuesto Sector Público Nº 20.481 año 2011.

CONSIDERANDO:

1. Que el Decreto Supremo N° 83 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 establece en su artículo N° 12 existencia de un Encargado de Seguridad.

2. Que la Resolución Exenta Nº 353 del 28 de marzo de 2011, aprueba la Creación del Comité de Seguridad de la Información y designa responsables del Sistema de Gestión de Seguridad de la Información.

3. Que la Resolución Exenta Nº 340 del 23 de marzo de 2011, nombre al Encargado del Sistema de Seguridad de la Información.

R E S U E L V O

1. **APRUEBASE,** la Política General de Seguridad de la Información del Gobierno Regional de Antofagasta, la cual se transcribe íntegramente en la presente Resolución:

POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION
GOBERNO REGIONAL DE ANTOFAGASTA

NOTA DE CONFIDENCIALIDAD:

Esta Política General de Seguridad de la Información para los Servicios Administrativo del Gobierno Regional de Antofagasta, se rige por los términos y condiciones que en este documento se establecen. Su uso está dirigida 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.

Firmas de los responsables.

ELABORADO POR	REVISADO POR	APROBADO POR
Cesar Peñafiel Núñez	Hernán Flores Arrouch	Álvaro Fernández Slater
Representante del Comité Operativo de Seguridad	Encargado de Seguridad Gobierno Regional de Antofagasta	Intendente Región de Antofagasta Jefe del Servicio

I. INTRODUCCION

El 03 de junio del 2004 el Ministerio Secretaría General de la Presidencia del Gobierno de Chile, promulgó el Decreto Supremo N° 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 en el uso, almacenamiento, acceso y distribución del documento electrónico; además de facilitar la relación electrónica entre los órganos del Estado y entre éstos y la ciudadanía.

En su contenido se plantea la obligación de que las entidades regidas por el decreto adopten políticas de seguridad permanente, que incluyan planes de contingencia frente a fenómenos de toda índole que pudieran poner en riesgo la continuidad operacional de los sistemas de información.

Con todo lo anterior, surge la necesidad de que cada institución gubernamental cuente con un Sistema de Seguridad de la Información adecuado que permita asegurar la calidad, *disponibilidad* y oportunidad de la información respectos de los procesos institucionales y que abarque no solamente a los documentos electrónicos, sino a todos los activos de información *conforme a los* alcances señalados por la Red de Expertos en la guía metodológica del Sistema de Seguridad de la Información.

En consecuencia se elaboró el presente documento, que es una Declaración de Política General de Seguridad de la Información, que se concretó con el trabajo de los integrantes del Comité de

Seguridad de la Información, y servirá como punto de partida para la elaboración de las políticas específicas correspondientes para cada ámbito de acción.

II. DECLARACION INSTITUCIONAL

En cuanto al sistema de seguridad de la información para la organización, la evaluación interna sobre la internalización de la seguridad permite concluir que adolece de una cultura organizacional de seguridad de la información, Esta apreciación se observa tanto en los niveles directivos como operativos, por cuanto puede resultar difícil alcanzar un avance mínimo esperado en cuanto a la valorización de la seguridad y la organización de la institución para asumir la implantación de un sistema de gestión de seguridad como un proceso continuo.

Sin embargo, existe una importante valorización de parte del Jefe del Servicio frente al aseguramiento de los procesos de negocios y el uso de tecnologías para el mejoramiento de la gestión, lo que posibilita que la instalación de un sistema de seguridad en la organización cuente con el respaldo y la supervigilancia del Jefe del Servicio.

III. OBJETIVOS DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

Las acciones a realizar para la clasificación y catastro de activos de información se llevaran a cabo realizando un inventario de ellos con la definición de los datos a considerar relevantes.

Las acciones necesarias para el análisis de riesgo tendrán que ser concordantes respecto de la normativa vigente en la institución (matriz de riesgo institucional / matriz de Riesgos de PMG SSI).

Será responsabilidad del Comité de Seguridad de la Información y/o Encargado de Seguridad de la Información, reunirse (en el caso del Comité) y/o informar directamente al Jefe Superior del Servicio (Encargado de Seguridad de la Información), según sea la urgencia y posibilidad de impacto, la necesidad de analizar riesgos que afecten al servicio, conforme a las políticas de seguridad de la información vigentes en este.

Con respecto a la capacitación dirigida y destinada a todos los funcionarios del Gobierno Regional de Antofagasta, se realizará a través de exposiciones y charlas educativas e instructivas. Por expertos que se encuentran en nuestro servicio y por externos. Es necesario destacar, que estas actividades, formaran parte del Programa Anual de Capacitación, el cual es validado y aprobado por el Comité Bipartito de Capacitación de nuestro servicio.

Con respecto a la estructura institucional para el desarrollo de las políticas, estándares y procedimientos en materia de seguridad de la información, durante el presente año, se ha formalizado y definido las funciones, roles, tareas y deberes de los funcionario que integran el Comité de Seguridad de la Información y el Sistema de Mejoramiento de Seguridad de la Información. Siendo el medio de asignación de lo expresado, a través de la emisión de Resoluciones, estas son, la Número 340 de fecha 23 de marzo del 2011, la cual nombra al Encargado de Sistema de Seguridad de la Información. La Número 353 de fecha 28 de Marzo de 2011, que aprueba la creación del Comité de Seguridad de la Información y designa responsables del Sistema de Gestión de Seguridad de la Información. Con respecto al responsable operativo del Sistema de Seguridad de la Información, que forma parte de la ejecución del Programa de Mejoramiento de la Gestión a nivel institucional esta se encuentra en la Resolución Número 304, de fecha 16 de Marzo de 2011.

IV. AMBITO DE APLICACIÓN DE LA POLITICA DE SEGURIDAD DE LA INFORMACION

Esta Política se debe aplicar en todo el ámbito del **Gobierno Regional de Antofagasta**, a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

V. ROLES Y RESPONSABILIDADES.

El rol del Comité de Seguridad de la Información, será Gestionar la Política de seguridad del servicio, entre las cuales se incluyen supervisar la implementación de procedimientos y estándares, proponer estrategias y soluciones específicas, arbitrar conflictos en materias de seguridad y coordinarse con el Comité de Riesgos de la institución, entre otros.

Será responsabilidad de cada uno de los integrantes del Comité de Seguridad participar activamente en las reuniones del Comité y cumplir cada una de las misiones encargadas a éste y ser agentes de transmisión al personal a su cargo de las políticas de seguridad de la información.

Será responsabilidad de cada uno de los funcionarios del servicio cumplir con cada una de las políticas de seguridad de información del servicio.

VI. MARCO GENERAL PARA LAS POLÍTICAS 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. OBJETIVOS POLITICAS DE SEGURIDAD.

El cumplimiento del marco legal vigente.- Evidentemente, una política debe cumplir con la normativa vigente de nuestro país; para esto se deberá establecer las relaciones con cada ley, 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 registros de eventos en los recursos y su mantenimiento.

Tipo de 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 mas 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 departamento, luego los jefes de unidad y por último los empleados u operarios.

Uso de recursos.- El uso de recursos son los disponibles por el servicio, y se buscaran recursos adicionales en la medida de las necesidades.

b. ESTRUCTURA Y CONTENIDO DE LAS POLITICAS DE SEGURIDAD

La Estructura y contenido de las Políticas de Seguridad especificas de la Información, deberá contener los siguientes aspectos:

- Definición, objetivos y alcance de la política especifica
- La Declaración institucional del Gobierno Regional de Antofagasta
- El Cumplimiento legal
- Controles a implementar
- Difusión de la política específica.

c. GESTACION DE UNA POLITICA

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.

d. APROBACION DE UNA POLITICA

La aprobación de una política, será revisada y pre aprobada por el comité de seguridad de la información de los servicios administrativos del Gobierno Regional de Antofagasta, y su aprobación definitiva se realizada mediante Resolución Exenta firmada por el jefe superior del servicio.

e. DIFUSION DE LAS POLITICAS

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 publicas 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.

f. FORMATO DE LAS POLITICAS

Los formatos para almacenar información, de las políticas responderá a los diferentes tipos de formato institucional utilizado y que se encuentran disponible en el mercado.

g. REVISION DE UNA POLITICA

Para una revisión normal de esta política de seguridad de la información, esta se realizara en forma periódica, a lo menos cada tres (03) 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.

VII. GLOSARIO DE TERMINOS

Para los propósitos de esta Política, se entenderá por:

a) **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.

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

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

d) **Confidencialidad:** La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

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

f) **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.

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

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

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

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

ANOTESE, COMUNIQUESE Y ARCHIVESE

GOBIERNO REGIONAL II REGION ANTOFAGASTA

ALVARO FERNANDEZ SLATER
Intendente Región de Antofagasta

DANIELLA PIANTINI MONTIVERO
Asesora Jurídica

AFS/DPM/HFA/vms

DISTRIBUCIÓN:
- División de Administración y Finanzas
- División de Análisis y Control de Gestión, Coordinador PMG institucional
- División de Planificación y Desarrollo Regional
- Asesoría Jurídica
- Auditora Interna
- Encargado de Seguridad
- Encargado del Sistema de Seguridad de la Información del PMG
- Oficina de Partes