

# resolución

La Serena, 02 de noviembre de 2017

## *visto*

- La Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado y sus modificaciones;
- La Ley N° 19.175, Orgánica Constitucional sobre Gobierno y Administración Regional y sus modificaciones;
- El Decreto N° 83 de 2.005, 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;
- El Decreto N° 973 de fecha 13 de Julio de 2015 del Ministerio de Interior y Seguridad Pública;
- La Resolución Exenta N° 2.028, de fecha 02 de diciembre de 2.010, que aprobó la Política de Seguridad de Sistemas de Información y la Definición de Responsables y Roles para la correcta aplicación de la Política de Seguridad de la Información del Servicio Administrativo del Gobierno Regional de Coquimbo;
- La Resolución Exenta N° 1778, de fecha 30 de diciembre de 2.013, que derogó las resoluciones (e) N° s 663 y N° 865, ambas del 2.011, del Gobierno Regional de Coquimbo y aprobó la Política de Sistemas de Seguridad de la Información;
- La Resolución Exenta N° 1511, de fecha 30 de diciembre de 2.015, que modificó la Resolución (e) N° 1778, de fecha 30 de diciembre de 2.015, del Gobierno Regional de Coquimbo;
- La Resolución N° 1.600 de 2.008 de la Contraloría General de la República;

## *teniendo presente:*

- El Memorándum Electrónico N° 2670 de fecha 30 de octubre de 2.017, del Jefe de la División de Administración y Finanzas, mediante el cual solicita la aprobación de la Política de Seguridad de la Información actualizada;
- Que, en virtud de lo señalado precedentemente se hace necesario que este Gobierno Regional reformule la Política de Seguridad de la Información en cumplimiento de las exigencias que la legislación contempla; se dicta la siguiente

**resolución (e) N° 888**

# resolución (e) N°888

1. **DERÓGASE**, las Resoluciones Exenta N° 1103, de fecha 20 de diciembre de 2016 del Gobierno Regional de Coquimbo.
2. **APRUÉBASE**, la Política de Seguridad de la Información del Servicio Administrativo del Gobierno Regional de Coquimbo, cuyo texto es el siguiente:

## Política de Seguridad de la Información del Servicio Administrativo del Gobierno Regional de Coquimbo

### Control de Versiones

Versión	Fecha revisión	Sección	Resumen de modificaciones	Elaborado por	Revisado por	Fecha Autorización
1.0	18/11/2010	Todas	Creación	Equipo de Trabajo Comité de Seguridad de la información	Comité de Seguridad de la información	02/12/2010
2.0	10/12/2013	Alcance, difusión y revisión y monitoreo.	Se incorpora alcance, forma tiempos de difusión, revisión y monitoreo. Se corrigen errores de puntuación.	Equipo de Trabajo Comité de Seguridad de la información	Comité de Seguridad de la información	30/12/2013
2.1	20/10/2017	Control de Versiones	Se incorpora cuadro de control de versiones Se elimina la palabra sistemas del título de la Política. Se corrigen errores de puntuación.	Lorena Encargada Seguridad Baez, de	Comité de Seguridad de la información	26/10/2017

### Introducción

Considerando que la misión del Servicio Administrativo del Gobierno Regional de Coquimbo es: "Apoyar al órgano ejecutivo del Gobierno Regional de Coquimbo con el fin de alcanzar el Desarrollo Estratégico Sustentable Regional en los ámbitos social, cultural y económico, coordinando a los actores públicos y privados en la ejecución de las iniciativas de inversión pública de la Región de Coquimbo", se hace necesario definir una Política de Seguridad de la Información que permita disponer de estos recursos en todo momento, para cumplir con sus propósitos institucionales.

### Objetivos de la Seguridad de la Información

La Seguridad de la Información está concebida para proteger los activos de información de la organización, entre los que se encuentran:



## resolución (e) N° 888

### **La información**

Hoy en día la información se ha convertido en uno de los activos más importantes y valiosos dentro de una organización. La seguridad informática debe velar porque ésta sea administrada según los criterios establecidos por los administradores y supervisores, evitando que usuarios externos y no autorizados puedan acceder a ella sin autorización previa, de lo contrario, la organización corre el riesgo de que la información se pierda, o sea utilizada maliciosamente para obtener ventajas de ella o que sea manipulada, ocasionando lecturas erradas o incompletas de la misma. Otra función de la seguridad de la información en esta área, es la de asegurar el acceso a la información en el momento oportuno, incluyendo respaldos de la misma en caso de que ésta sufra daños o pérdida producto de accidentes, atentados o desastres.

### **La infraestructura computacional**

Es una parte fundamental para el almacenamiento y gestión de la información, así como para el funcionamiento mismo de la organización. La función de la Seguridad de la Información en esta área es velar porque los equipos funcionen adecuadamente y prever en caso de falla, planes de contingencia que permitan su rápida reposición. También debe asegurar que la conectividad de red y toda la infraestructura funcionen correctamente; para ello se deben realizar mantenciones periódicas para detectar posibles fallas en la misma, estableciendo horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos. Por último, la Seguridad de la Información debe asegurar planes de contingencia en caso de robos, incendios, boicot, desastres naturales, fallas en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática.

### **Las Personas**

Son aquellos activos de información que, por un lado, dominan la gestión del negocio y su información; y por otro lado, utilizan la estructura tecnológica y de comunicaciones. La Seguridad de la Información debe establecer procedimientos y/o normas que minimicen los riesgos de pérdida, robo, mal uso, deterioro de los activos de la información. Estas normas deben considerar una gestión del conocimiento que posee cada una de las personas que manejan información, junto con velar por su integridad física y psicológica, y todo lo necesario que permita un buen nivel de seguridad de la información, minimizando el impacto en el desempeño de los funcionarios y de la organización.

### **Importancia de los Activos de Información del Servicio**

Para el Gobierno Regional de Coquimbo, la información, la infraestructura computacional y las personas, constituyen un pilar fundamental para la gestión y el desarrollo de sus procesos y productos estratégicos, por tanto, deben ser protegidos porque son parte fundamental para el logro de los objetivos de la institución.

Por lo anterior, el Gobierno Regional de Coquimbo protegerá los recursos de información y la tecnología usada para su procesamiento de las amenazas internas o externas, deliberadas o accidentales; con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad de la información. Además de poder garantizar la continuidad de los sistemas de

## resolución (e) N° 888

información, minimizar riesgos de daño y asegurar el eficiente cumplimiento de sus objetivos estratégicos.

### **Documento Electrónico**

Se entiende por 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.

Es así como, la seguridad del documento electrónico deberá estar garantizada por la:

- Confidencialidad, esto es, asegurar que la información sea accesible sólo para aquellos usuarios autorizados a tener acceso;
- Integridad, esto es, salvaguardar que la información y los métodos de procesamiento sean exactos y completos; y
- Disponibilidad, esto es, asegurar que los usuarios autorizados tengan acceso a la información y bienes asociados cuando lo requieran.

### **Objetivos de la Política de Seguridad del Servicio Administrativo del Gobierno Regional de Coquimbo:**

Considerando que los objetivos de la Seguridad de la Información son proteger nuestros activos de información: la información propiamente tal, la infraestructura computacional y las personas que manejan la información, nuestra política de seguridad de la información estará basada en disponer de una arquitectura de seguridad basada en soluciones tecnológicas, así como el desarrollo de un plan de acción para el manejo de incidentes y recuperación que disminuya, al máximo, el impacto que éste pudiera ocasionar en caso de ocurrir cualquier tipo de contingencia con los activos de información.

Por lo anterior, las políticas, de nuestra institución, tendrán los siguientes objetivos:

- Identificar y seleccionar lo que se debe proteger (información sensible),
- Establecer niveles de prioridad e importancia sobre esta información,
- Conocer las consecuencias que traería a la compañía, en lo que se refiere a costos y productividad, la pérdida de datos sensibles,
- Identificar las amenazas, así como los niveles de vulnerabilidad de la red,
- Realizar un análisis de costos en la prevención y recuperación de la información, en caso de sufrir un ataque y perderla, y por último
- Implementar respuesta a incidentes y recuperación para disminuir el impacto.

El Intendente Regional como Jefe Superior del Servicio, coordinará la gestión de la Seguridad de la Información y de los sistemas de información, de manera corporativa a través de un Comité de Seguridad de la Información, y dispondrá la revisión periódica de la política y los procedimientos de Seguridad Informática, en el tercer trimestre de cada año, o a consecuencia de incidentes



# resolución (e) N°888

significativos que se relacionen con ella, o por nuevas vulnerabilidades o cambios en la infraestructura técnica u organizacional.

## **Alcance**

La política mencionada en el presente documento, contempla a todo el Gobierno Regional de Coquimbo y aplica a todos los funcionarios y personal a honorarios permanente, proveedores, contratistas, personal que esté vinculado con las firmas que presten los servicios al Gobierno Regional de Coquimbo o que estén relacionados. Se incluye además, todas las dependencias que son parte de la institución o que transite por la red del Gobierno Regional de Coquimbo.

## **Roles y Responsabilidades**

### **Encargado de Seguridad de la Información**

- Velar por el cumplimiento de la presente política.
- Mantener y administrar el sistema de gestión de seguridad de la información.
- Promover la concientización y difusión de la institución en los aspectos de la seguridad de la información.
- Promover la importancia y tratamiento adecuado de los activos de información.
- Coordinar todos los aspectos de la seguridad de la información con los responsables de los distintos departamentos y con el Comité de Seguridad de la Información.
- Establece puntos de enlace con los Encargados de Seguridad de la Información de otros organismos públicos.

### **Comité de Seguridad de la Información (CSI)**

- Apoyar la gestión realizada por el Encargado de Seguridad de la Información.
- Definir, implementar y difundir las Políticas, Normas y Estándares Institucionales en materia de seguridad de la información.
- Promover la concientización y difusión de la institución en los aspectos de la seguridad de la información.
- Promover la importancia y tratamiento adecuado de los activos de información.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.

### **Personal de Planta, Contrata y Honorarios**

- Conocer y respetar las directrices de la presente política

## **Difusión**

La Política de Seguridad de Información será difundida a todos los funcionarios mediante capacitaciones presenciales, correo electrónico e intranet. Además debe incorporarse en el proceso de inducción de funcionarios que ingresen al Servicio, con el objeto de internalizar esta política.

## **Aceptación**

Todo personal del Gobierno Regional de Coquimbo, en cualquier calidad jurídica (planta, contrata u honorario), acepta la política general de seguridad de la información, las políticas específicas y los documentos relacionados.



## resolución (e) N°888

En el caso de terceros, por el solo hecho de participar en una licitación, celebrar un trato directo o suscribir un contrato con el Gobierno Regional de Coquimbo, se presume que el oferente, adjudicatario o contratista conoce, acepta, entiende los términos y condiciones de la política de seguridad de la información publicada en la página web [www.gorecoquimbo.gob.cl/transparencia/web](http://www.gorecoquimbo.gob.cl/transparencia/web)

### Sanciones aplicables

El incumplimiento o violación, debidamente acreditado, a la política general de seguridad de la información, políticas específicas o cualquier otro documento que se derive de ella, conlleva la aplicación de medidas disciplinarias previstas en el Estatuto Administrativo, respecto a los funcionarios del Gobierno Regional de Coquimbo o al término anticipado del contrato, por incumplimiento de obligaciones, cuando se trate de personas que no tengan responsabilidad administrativa o empresas que se encuentren dentro del alcance de ésta, sin perjuicio de las responsabilidades civiles y penales que deriven de tales infracciones.

### Revisión y Monitoreo

El Comité de Seguridad de la Información es el responsable de revisar periódicamente la correcta implementación de esta política en la organización. El monitoreo será incorporado como acciones de aseguramiento en los Planes Anuales de Auditoría Interna de Seguridad de la información, y sus resultados serán revisados por el Comité de Seguridad de la Información. Cuando sea necesario el Comité elaborará planes acción para abordar las brechas y será responsable de su seguimiento y cierre.

***anótese, comuníquese, registrese y publíquese***



ALV/LRH/JPL/FFP/PFC/MTGC/CCS/IGI/bhg



**CLAUDIO IBÁÑEZ GONZÁLEZ**

Intendente Regional

Gobierno Regional - Región de Coquimbo

