APRUEBA POLITICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

RESOLUCIÓN EXENTA Nº 2139.-

VALDIVIA, 18 DE NOVIEMBRE DE 2019.

VISTOS:
Lo dispuesto en la Ley N° 18.575, de Bases Generales de la Administración del Estado, cuyo texto refundido, coordinado y sistematizado se fijó por D.F.L. N° 1 (19.653) de 2000, del Ministerio Secretaría General de la Presidencia; la Ley Orgánica Constitucional N°19.175, sobre Gobierno y Administración Regional; la Ley N° 19.880 de 2003, de Bases de Procedimiento Administrativos que rigen los actos de los órganos de la Administración del Estado; la Ley 20.285, Sobre Transparencia y Acceso a la Información Pública; la Ley 19.553 de 1998 modificada por la Ley 19.618 y 19.882; las resoluciones N°7 y 8, ambas de 2019, de la Contraloría General de la Republica y en el Decreto Nº 421 de 11 de marzo de 2018 de Ministerio de Interior, que nombra al Intendente Titular del Gobierno Regional de Los Ríos.

TENIENDO PRESENTE:
1. Que mediante Resolución N° 1675 de 2018, se aprobó la actualización de el documento "Política de Seguridad de la Información", indicando que fue elaborada en base a la NCh ISO27002 y designa integrantes del comité de seguridad de la información del Gobierno Regional de Los Ríos

2. Qué de acuerdo a lo establecido en la Norma Chilena NCh-ISO 27001 y NCh-ISO 27002, donde se indica los requisitos para establecer y mantener un sistema de seguridad de la información.

3. Qué en reunión de comité de seguridad realizada el 24 de octubre de 2019, de acuerdo a ACTA N° 16 SESIÓN COMITÉ DE SEGURIDAD, se acordó la elaboración de la "Política de Gestión de incidentes de seguridad de la información" del Gobierno Regional de Los Ríos.

RESUELVO:
1° **APRUÉBASE** a contar de esta fecha, la **GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN** que regirá para todas las personas que integren este Gobierno Regional de Los Ríos, cuyo texto íntegro es el siguiente:

GOBIERNO REGIONAL DE LOS RÍOS

POLÍTICA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
Sistemas de Gestión de Seguridad de la Información
(SGSI- ISO/IEC 27001-27002)
A.16.01.01
A.16.01.02
A.16.01.03
A.16.01.04
A.16.01.05
A.16.01.06
A.16.01.07

Contenido

I. Control de cambios

Fecha	Versión	Creador	Modificación o actualización
Noviembre de 2019	1.0	Patricio Acum S.	Primera Versión

II. Introducción

El Gobierno Regional de Los Ríos, es un organismo autónomo con personalidad jurídica de derecho público, que tiene por objetivo la administración, el desarrollo social, cultural y económico de la región, su principal herramienta de inversión el F.N.D.R. (Fondo Nacional de Desarrollo Regional) y su misión como institución pública es "Liderar de manera integrada el desarrollo de la Región de Los Ríos, acorde a principios de participación, equidad, integración territorial y sustentabilidad, con el fin de mejorar la calidad de vida y bienestar de sus habitantes, mediante la formulación e implementación de instrumentos de planificación, coordinación y gestión de la inversión pública."

Durante el desarrollo de los procesos tendientes al logro de los objetivos y misión institucional, se ve involucrada una gran cantidad de información, de medios y sistemas en los que ésta se procesa y de funcionarios y personas que prestan servicios a la institución y/o externos que se relacionan con la institución en las distintas etapas de los procesos. Todo lo anterior forma parte de los ***"Activos de Información del Gobierno Regional de Los Ríos",*** *dichos activos requieren de un adecuado resguardo ante posibles amenazas o incidentes que afecten a la seguridad de los mismos.*

El Gobierno Regional de Los Ríos, en cumplimiento con el Sistema de Gestión de Seguridad de la Información, mediante el presente documento establece la **Política de Gestión de incidentes de seguridad de la información,** *que, en adelante, será el documento guía para el tratamiento de los incidentes de seguridad de la información del Gobierno Regional de Los Ríos.*

III. Objetivo

El presente documento tiene por objeto establecer directrices del tratamiento de los incidentes de seguridad de la información del Gobierno Regional de Los Ríos, de tal modo de administrar eficaz y eficientemente los incidentes relacionados con la seguridad de la información y sus medios de procesamiento, incluyendo cualquier tipo de medio de almacenamiento de información, como plataforma tecnológica, sistemas de información, medios físicos de almacenamientos y las personas, que afecten la continuidad operacional de los procesos críticos del Gobierno Regional de Los Ríos.

Esto, de acuerdo al control establecido en la norma chilena ISO 27001 :2013:

- *A.16.01.01 Responsabilidades y procedimientos*
- *A.16.01.02 Informe de eventos de seguridad de la información*
- *A.16.01.03 Informe de las debilidades de seguridad de la información*
- *A.16.01.04 Evaluación y decisión sobre los eventos de seguridad de la información*
- *A.16.01.05 Respuesta ante incidentes de seguridad de la información*
- *A.16.01.06 Aprendizaje de los incidentes de seguridad de la información*
- *A.16.01.07 Recolección de evidencia*

IV. Alcance

El presente documento es aplicable a todas las áreas del Gobierno Regional de Los Ríos y a todos los procesos de provisión de bienes y servicios utilizados por los funcionarios del Gobierno Regional de Los Ríos independiente de su calidad jurídica y proveedores de servicios al Gobierno Regional de Los Ríos, que afecten por cualquier incidente que comprometa la confidencialidad, integridad o disponibilidad de la información o de los sistemas, detectados en forma interna o externa.

1. Roles y responsabilidades

Responsable	*Rol*	*Funciones*
Jefe de Servicio	*Liderar la implementación del presente Procedimiento*	▪ *Aprobar el documento* ▪ *Autorizar los recursos necesarios para su implementación, así como el nombramiento de funcionarios coordinadores y/o encargados de seguimiento.* ▪ *Liderar su implementación*
Comité de seguridad de la Información	*Revisar, coordinar y controlar la implementación del documento.*	▪ *Revisar y/o proponer mejoras al documento de acuerdo al nivel de implementación* ▪ *Gestionar recursos necesarios para dictar charlas informativas* ▪ *Coordinar y materializar la difusión del procedimiento.*
Encargado de Seguridad de la Información	*Gestionar e informar al comité acerca de la implementación del procedimiento*	▪ *Realizar control y seguimiento de la implementación del documento.* ▪ *Informar de manera periódica al comité de seguridad de la información del grado de avance en la implementación.* ▪ *Proponer mejoras y/o cambios en la implementación* ▪ *Mantener registro actualizado de los resultados del seguimiento y control*
Jefes de División	*Colaborar en la implementación del procedimiento*	▪ *Promover y ejecutar lo establecido en el procedimiento entre todos quienes dependan de sus respectivas divisiones, departamentos y unidades.*
Encargado Unidad de Informática	*Dar cumplimiento a lo establecido en el documento*	▪ *Coordinar que se ejecute correcta y periódicamente lo dispuesto* ▪ *Evaluar el conocimiento adquirido respecto al trabajo y designar al personal idóneo para la ejecución del mismo.*
Funcionarios	*Dar cumplimiento a lo establecido en el documento*	▪ *Declarar cualquier evento sospechoso que pudiera desencadenar un incidente de*

		Seguridad de la Información.

2. Referencias

- ✓ *Ley 19223 Delitos Informáticos*
- ✓ *NCh ISO 27001 – 27002-2013*
- ✓ *Guía Metodológica 2019 (SGSI)*
- ✓ *Política de Seguridad de la Información del Gobierno Regional de Los Ríos*

3. Definiciones

- ***Integridad:*** *Es la propiedad que busca proteger que no se modifiquen los datos de forma no autorizada.*
- ***Disponibilidad:*** *Es el acceso autorizado a la información y a los sistemas en el momento que se requiera por una persona autorizada.*
- ***Confidencialidad:*** *Es la propiedad que impide la divulgación a individuos, entidades o procesos no autorizados. Es decir, asegurar el acceso únicamente a aquellas personas que cuenten con una debida autorización.*
- ***Incidente de seguridad:*** *Cualquier evento o situación que comprometa de manera importante la disponibilidad, integridad y/o confidencialidad de los activos de información. También puede ser la violación o no cumplimiento de una política o procedimiento.*
- ***Incidente de Alto impacto:*** *Interrupción de los procesos de la institución que afecta a un número significativo de usuarios.*
- ***Urgencia Alta:*** *Tiempo máximo de demora que puede aceptar el proceso para la resolución de incidente.*

4. Modo de Operación

4.1. Reporte de eventos y debilidades en la Seguridad de la Información.

Todo el personal del Gobierno Regional de Los Ríos, en coordinación con su Jefatura, es responsable de notificar cualquier tipo de evento que pueda afectar el normal funcionamiento del sistema de seguridad de la información del servicio. Esta notificación se realizará a través del sistema OsTicket seleccionando el ítem "Reporte de incidentes de seguridad de la información" o a través de un correo electrónico al encargado de la seguridad de la información del servicio, indicando todos los antecedentes del evento, el cual deberá clasificar y derivar según su criticidad, además deberá en lo posible evitar realizar acciones sin el apoyo técnico correspondiente.

Una vez realizado el análisis inicial de los antecedentes recopilados, se debe establecer si el evento corresponde a un requerimiento, una debilidad del sistema o un incidente de seguridad de la información.

4.2. Gestión de incidentes de seguridad

4.2.1. Registro y clasificación del incidente

a. Registro:

A través de la plataforma informática se debe registrar el incidente describiendo el máximo de detalles de este.

b. Clasificación:

El Encargado de seguridad de la información deberá clasificar el incidente de acuerdo al origen, tipo y nivel de criticidad.

4.3. Análisis y Gestión de riesgos

Con los antecedentes recopilados se realizará un análisis respecto del tipo de incidente,

alcance y nivel de criticidad y se determinará el tratamiento al riesgo, se asume, se transfiere, se mitiga o se elimina.

4.3.1. Mitigar el riesgo

Reducirlo mediante la implantación de controles que reduzcan el riesgo a un nivel aceptables, implica seleccionar dichos controles, definir y documentar los métodos para ponerlos en marcha y gestionarlos.

4.3.2. Asumir el riesgo

El servicio asume el riesgo ya que está por debajo de un valor de riesgo aceptable, simplemente se requiere que quede documentado que el Servicio cono y acepta estos riesgos. Los riesgos que se han asumido han de ser controlados y revisados periódicamente de cara a evitar que evolucionen y se convierten en riesgos mayores.

4.3.3. Transferir el riesgo

Asegurando el activo que tiene el riesgo o subcontratando el servicio. Deben evaluarse las opciones y tomar las acciones pertinentes para ejecutar la opción escogida, en función del valor del activo y del costo de realizar esta transferencia (no solo el costo económico).

4.3.4. Eliminar el riesgo

Aunque no suele ser la opción más viable, ya que puede resultar difícil o demasiado costoso, si se cree posible o necesario, habrá que establecer los pasos para conseguirlo: eliminar el activo, eliminar el proceso o incluso el área del servicio que es la fuente del riesgo.

4.4. Escalamiento

Si el Encargado de la Unidad de informática, determinará si el incidente detectado requiere tratamiento urgente, de ser así, debe proceder con la mayor celeridad posible e informar al Encargado de la seguridad de la información del servicio quien instruirá la respuesta inmediata.

Cada vez que se registre un incidente de Seguridad de la Información, se debe informar a los responsables de ejecutar las acciones inmediatas según sea el tipo de incidentes para su rápida resolución y respuesta.

En caso de que no se pueda resolver el problema, se realiza un escalamiento interno. Para cada tipo de incidente se avisa a la persona correspondiente. El criterio principal del escalamiento es el de transferencia a una persona de soporte más elevado, que tenga mayor conocimiento o experiencia, recursos para solucionar situaciones complejas y mayor poder en la toma de decisiones.

4.5. Respuesta inmediata

La Jefatura designada para la respuesta inmediata al incidente, es responsable del desarrollo de las siguientes acciones inmediatas: Registro de actividades de gestión de incidentes:

Actividad	*Descripción*
Contener el daño y minimizar el riesgo	*Evitar que se propaguen los daños o efectos del incidente, coordinando las actividades necesarias para su disminución, probabilidad y consecuencia.*
Reclasificar el incidente	*Si es necesario, reclasificar según corresponda al evaluar el incidente de seguridad de la información.*
Proteger las evidencias	*Resguardar las evidencias recopiladas durante la gestión del incidente.*
Notificar a terceros relevantes	*Cuando sea necesario, notificar a organismos externos (carabineros, bomberos, PDI, etc) según lo descrito en el procedimiento de contacto con Autoridades.*
Compilar y organizar la documentación del incidente	*Recopilar todos los antecedentes y evidencias relacionadas con el incidente y entregarlos al Encargado de Seguridad de la Información*
Entregar lineamientos para la respuesta al	*En encargado de la Seguridad de la Información, debe apoyar a la jefatura correspondiente en esta etapa,*

incidente	*para responder de manera adecuada al incidente detectado.*

4.6. Continuidad de operaciones y servicio

En caso de que el incidente no pueda ser controlado y ponga en riesgo las operaciones y entrega de servicios del Gobierno Regional de Los Ríos, el Encargado de seguridad de la Información, el Encargado de la Unidad de Informática y el comité de seguridad de la información evaluarán la pertinencia de activar el Plan de continuidad de operaciones.

4.7. Recolección de evidencia

La recolección de evidencia es responsabilidad del Encargado de Seguridad de la información. Está debe ser clara y suficiente para respaldar el incidente, para ello debe considerar lo siguiente:

***Información en formato a papel:** El original se debe guardar de manera segura con información del individuo que encontró el documento, donde y cuándo fue encontrado y quién fue testigo del descubrimiento. Se debe procurar que el documento original no sea adulterado intencional o accidentalmente.*

***Información formato digital:** Las imágenes o copias de cualquier medio removible, la información contenida de discos duros o en memorias, deben ser retenidas de manera segura para garantizar su disponibilidad. El registro de todas las acciones durante el proceso de copiado, se debe guardar y el proceso se debe realizar en presencia de testigos. Los medios originales y el registro se deben guardar de manera segura, evitando la adulteración de la evidencia.*

Cualquier trabajo forense se debe realizar sólo sobre copias de material de evidencia. Se debe supervisar y registrar cuándo y donde fue ejecutado el proceso, quién lo ejecutó y qué herramientas y/o programas se utilizaron.

Esta información es entregada al comité de seguridad de la información, para la evaluación y aprendizaje del incidente y eventuales acciones legales y disciplinarias.

4.8. Resolución del incidente

La resolución de un incidente de seguridad de la información, se realizará de acuerdo a los procedimientos específicos para cada caso.

4.9. Comunicación

Aquellos incidentes clasificados como de Alto Riesgo o Urgencia Alta, deben ser gestionados, informados a todos los involucrados durante el proceso de resolución y cierre del mismo.

4.10. Análisis de causa y cierre

En esta etapa el Encargado de Seguridad de la información debe:

a) Realizar un análisis de la causa del incidente.
b) En caso de ser necesario, debe diseñar e implementar un plan de acción adecuado que prevenga incidentes futuros.
c) Registrar el cierre del incidente en sistema de gestión de incidentes.
d) Aplicar lecciones aprendidas y ajustar los procedimientos y vías de comunicación con el objeto de contar con mejores herramientas para un eventual futuro incidente.
e) Tomar las medidas para que se cuantifiquen las pérdidas económicas, si las hubiere.
f) Preparar un informe ejecutivo al comité de seguridad de la información, dependiendo de la magnitud e impacto del incidente.

5. Periodicidad de Evaluación y Revisión

Esta Política Gestión De Incidentes De Seguridad De La Información, tendrá una vigencia de tres años calendario desde su aprobación; no obstante, el comité de seguridad de la información del Gobierno Regional de Los Ríos podrá revisar y modificar antes el periodo de vencimiento.

Para asegurar la correcta implementación de la Política a través del tiempo, se definen los siguientes controles, actualización del documento y responsables. Estos son:

CONTROL	*ACTUALIZACIÓN*	*MEDIOS DE VERIFICACIÓN*	*RESPONSABLE*

Inspeccionar la correcta implementación de la Política Gestión De Incidentes De Seguridad De La Información	*La revisión del documento se realizará anualmente, sin perjuicio de las eventuales modificaciones que requiera el instrumento tras su implementación*	*Acta de revisión de la Política Gestión De Incidentes De Seguridad De La Información, validada por el comité de seguridad de la información.*	*Encargado (a) de la seguridad de la información.*

6. *Mecanismos de difusión*

El presente procedimiento será difundido de manera constante, a través de las plataformas tecnológicas de uso frecuente por los funcionarios del Gobierno Regional de Los Ríos.

- *Publicación en Intranet del Gobierno Regional de Los Ríos*
- *Jornada de difusión y sensibilización a los funcionarios del Gobierno Regional de Los Ríos*

2° **DIFÚNDASE,** a todos los funcionarios del Gobierno Regional de Los Ríos la política de **GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN** aprobada en el resuelvo anterior, mediante los medios electrónicos intranet y correo electrónico.

ANÓTESE, COMUNÍQUESE, PUBLÍQUESE EN LA PÁGINA WEB DEL GOBIERNO REGIONAL Y ARCHÍVESE.

GOBIERNO REGIONAL ★ INTENDENTE ★ REGION DE LOS RIOS

CESAR ASENJO JERÉZ
INTENDENTE
GOBIERNO REGIONAL DE LOS RÍOS

COH/ JAS/ PAS

DISTRIBUCION:
- Funcionarios Gobierno Regional de Los Ríos.
- División de Administración y Finanzas.
- Departamento Jurídico.
- Arch. Encargado de Seguridad de la Información.
- Oficina de Partes.