Gobierno de Chile

Región de Los Ríos
GOBIERNO REGIONAL

APRUEBA POLÍTICA DE CONTROL DE ACCESO.

RESOLUCIÓN EXENTA Nº 2315.-

VALDIVIA, 23 DE DICIEMBRE 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", donde se dispone el funcionamiento del comité de seguridad de la información, además de la elaboración de documentos asociados al resguardo de la 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 13 de diciembre, de acuerdo a ACTA N° 17 SESIÓN COMITÉ DE SEGURIDAD, se acordó la elaboración de la "Política de control de acceso" del Gobierno Regional de Los Ríos.

RESUELVO:
1° **APRUÉBASE** a contar de esta fecha, la Política de control de acceso 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 DE CONTROL DE ACCESO
Sistemas de Gestión de Seguridad de la Información
(SGSI- NCh-ISO 27001-27002)
A.09.01.01

Contenido

I. Control de cambios

Fecha	Versión	Creador	Modificación o actualización
Diciembre 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 control de acceso, que, en adelante, será el documento base para el tratamiento de la continuidad de la seguridad de la información del Gobierno Regional de Los Ríos.

III. Objetivo

El presente documento tiene por objeto establecer directrices del tratamiento de la continuidad de la 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.

Este documento presenta los lineamientos necesarios en temas de control de acceso lógico, postulando que todo usuario interno de la institución deberá poseer una cuenta de usuario personal, que actuará como credencial que lo identifique inequívocamente y que le permitirá tener acceso a los recursos de la red corporativa del Gobierno Regional de Los Ríos.

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

- ***A.09.01.01 Política de control de acceso***

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 de la presente Política*	▪ *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 de la Política.*	▪ *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 documento*
Encargado de Seguridad de la Información	*Gestionar e informar al comité acerca de la implementación de la Política*	▪ *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 de la Política*	▪ *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 la Política*	▪ *Coordinar que se ejecute correcta y periódicamente lo dispuesto*
Funcionarios	*Dar cumplimiento a lo establecido en la Política*	▪ *Tomar las acciones necesarias para dar cumplimiento a lo dispuesto en la Política.*

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.*

4. Modo de Operación

La presente política aborda lineamientos de Control de Acceso Lógico del Sistema de seguridad de la información, en tópicos de:

- *Lineamientos generales de control de acceso*
- *Acceso a redes y a los servicios de red*
- *Registro y cancelación de registros de usuarios*
- *Gestión de asignación de acceso a usuarios*
- *Gestión de acceso privilegiados*
- *Revisión de los accesos de los derechos a usuarios*
- *Eliminación o ajuste de los derechos de acceso*
- *Uso de información de autenticación secreta*
- *Restricción de acceso a la información*
- *Procedimiento de inicio de sesión seguro*
- *Uso de programas utilitarios privilegiados*
- *Control de acceso al código fuente de programas*

4.1. Lineamientos de control de acceso lógico

Las reglas de acceso a la red estarán basadas en el principio de negación por omisión, todo está restringido, a menos que esté expresamente permitido.

Las reglas especificas para el control de acceso, estarán documentadas a través de los diferentes procedimientos de control de acceso a los recursos tecnológicos correspondientes.

Se establecerá, documentará y revisará los lineamientos de control de acceso lógico en base a necesidades de seguridad y de servicio de la institución.

4.2. Acceso a las redes y los servicios de redes.

El acceso a redes desde y hacia afuera de la Institución cumplirá con los lineamientos de "Responsabilidad de los usuarios" y adicionalmente se utilizarán métodos como autenticación de protocolo por enrutamiento, rutas estáticas, NAT (Network Address Translation), ACL (listas de control de acceso).

Se desarrollarán procedimientos para la activación y desactivación de derechos de acceso a las redes, las cuales comprenderán, al menos:

- *Controlar el acceso a los servicios de red tanto internos como externos.*
- *Identificar las redes y servicios de red a los cuales se permite el acceso.*
- *Establecer normas, controles y procedimientos de administración para proteger el acceso a la red de datos de la institución.*

4.3. Registro y cancelación de registro de usuario

Se mantendrán protocolos de registro (alta y cancelación (baja) de usuarios con objeto de habilitar la asignación de derechos de acceso.

4.4. Gestión de asignación de acceso de usuarios

Se deben establecer procedimientos que controlen la asignación y revocación de derechos de acceso o privilegios de acceso a los servicios y sistemas del Gobierno Regional de Los Ríos

Se establecerán los procedimientos de registro, modificación y borrado de usuario.

4.5. Gestión de acceso privilegiados

La asignación y uso de derechos de acceso con privilegios especiales o de administrador, debe ser restringido y controlado, dado su alto riesgo en la continuidad operacional de las plataformas tecnológicas

4.6. Gestión de información secreta de autenticación de usuarios

La asignación de información confidencial, como parte de la autenticación del usuario, debe ser controlada mediante un proceso seguro y auditable

4.7. Revisión de los derechos de accesos de usuarios

Los propietarios de los activos deben poder revisar los derechos de acceso asignados o en curso, de todos los usuarios de los sistemas o plataformas a su cargo.

4.8. Eliminación o ajuste de los derechos de accesos

Se deben retirar los derechos de acceso a la información y a las instalaciones del procesamiento de la información para todos los funcionarios, proveedores o usuarios, de terceros, a la finalización del empleo, contrato o acuerdo, o ser revisados en caso de cambio.

Al momento del cese de labores de un funcionario del área tecnologías de información se deberá modificar contraseñas de los equipos de producción y acceso remotos.

4.9. Uso de contraseñas y de cualquier información de autenticación secreta

Se exige a los usuarios el uso de las mejores prácticas de seguridad en el uso y protección de información confidencial de sus contraseñas e información adicional usada para la autenticación.

4.10. Restricción de acceso a la información

Se debe controlar el acceso de los usuarios y personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, según rol y perfil de cada uno.

4.11. Procedimiento de inicio de sesión seguro

Cuando sea requerido por la Política de control de accesos se debe controlar el acceso a los sistemas y aplicaciones mediante un procedimiento seguro.

4.12. Sistema de gestión de contraseñas

Emplear un identificador formal de autenticación único, con una estructura definida y contraseñas configuradas con mayúsculas y minúsculas, con dígitos y con al menos 8 caracteres.

La contraseña asignada a una nueva cuenta de usuario, debe crearse expirada, de modo de obligar a ser cambiada por éste durante su primera conexión.

Las contraseñas son confidenciales, personales e intransferibles y no deben ser enviadas por email, ni por ningún tipo de formulario electrónico.

Las contraseñas de usuarios de la red deben caducar cada 3 meses.

Las contraseñas de acceso a los computadores de la red del Gobierno Regional de Los Ríos, se deberán controlar por un dominio que autentifique las credenciales y el acceso

Uso de programas utilitarios privilegios

Se debe restringir y controlar estrechamente el uso de los Software utilitarios que poseen la capacidad de sobrepasar los controles de acceso a los sistemas y aplicaciones. Debe existir un procedimiento de identificación, autorización, y autenticación para este tipo de software, además, se debe asegurar que:

- *Exista una segregación entre los Sistemas en Producción y los softwares utilitarios*
- *Existe un límite en el uso de softwares utilitarios a un número mínimo y práctico de funcionarios autorizados expresamente por el Encargado de la Unidad de Informática del Gobierno Regional de Los Ríos.*

5. Control de acceso al código fuente de los programas

Se debe restringir el acceso al código fuente de las aplicaciones de software.

6. Periodicidad de Evaluación y Revisión

Esta Política de planificación de la continuidad de la 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 de control de acceso	*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 de control de acceso, validada por el comité de seguridad de la información.*	*Encargado (a) de la seguridad de la información.*

7. 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 de la Unidad de Informática del Gobierno Regional de Los Ríos*

2° **DIFÚNDASE,** a todos los funcionarios del Gobierno Regional de Los Ríos la **POLÍTICA DE CONTROL DE ACCESO,** 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/ JHS/ PAS

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