GOBIERNO REGIONAL DE LOS RÍOS

PROCEDIMIENTO DE ADMINISTRACIÓN DE USUARIOS Y EQUIPOS CONECTADOS A LA RED DEL GOBIERNO REGIONAL DE LOS RÍOS

Sistemas de Gestión de Seguridad de la Información
(SGSI- ISO/IEC 27001-27002)
A.09.04.01
a.09.04.02
A.09.04.03
A.09.04.04
A.09.04.05

Contenido

I. Control de cambios

Fecha	Versión	Creador	Modificación o actualización
Noviembre de 2016	1.0	Sandra Pérez G.	Primera versión
Septiembre de 2019	2.0	Patricio Acum S.	Segunda Versión - Actualización

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 el **Procedimiento de Administración de Usuarios y Equipos Conectados a la Red del Gobierno Regional de Los Ríos** que, en adelante, será la guía para la creación de perfiles de usuarios y asignaciones de privilegios o restricciones en el acceso y uso de los recursos de red institucional.

II. Objetivo y alcance

El objetivo del presente documento es asegurar que se tome las decisiones adecuadas respecto de la seguridad de la información en cuanto a la gestión de usuarios que tendrán acceso a la red institucional tanto a nivel de conexión vía equipo de trabajo como de conexión a la red mediante otros dispositivos electrónicos, así como la asignación de perfiles y privilegios de acuerdo a la responsabilidad y área de desempeño de cada uno.

Junto con lo anterior, se busca establecer de manera procedimental el uso de las herramientas tecnológicas y actos administrativas con el fin sujetar dichos procesos a reglamentos internos institucionales.

El alcance del presente documento involucra a todos los funcionarios o terceros que por la naturaleza de su trabajo o la relación contractual que mantengan con la institución, tengan acceso a la red y sus servicios ya sea de manera permanente o temporal.

III. 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 procedimiento 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 procedimiento. ▪ 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
Encargado de Unidad de Informática	Analizar, coordinar y supervisar la materialización de los cambios.	▪ Recibir las solicitudes de cambios en TI por parte de los funcionarios. ▪ Analizar la factibilidad de los cambios de acuerdo a las necesidades del servicio. ▪ Proponer mejoras y/o cambios en la implementación ▪ Coordinar y supervisar la materialización de los cambios
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.
Funcionarios	Dar cumplimiento a lo	▪ Dar cumplimiento a lo

del Gobierno Regional de Los Ríos	establecido en el procedimiento	establecido en el procedimiento. ▪ Informarse, asistir a charlas o reuniones relacionadas con la difusión del contenido del documento.

IV. Referencias

- ✓ NCh ISO 27001 - 27002
- ✓ Guía Metodológica 2019 (SGSI)
- ✓ Política de Seguridad de la Información
- ✓ Manual de Procedimientos del Usuario

V. Definiciones

1. Gestión de derechos de acceso privilegiados

La gestión de los derechos de acceso privilegiados y en general todos los accesos a los sistemas informáticos institucionales radica en los usuarios administradores de los sistemas de información, las jefaturas de división correspondientes, y el encargado de recursos humanos de la institución, quienes deberán mantener una comunicación fluida respecto de la asignación, eliminación o modificación de dichos derechos de acceso en base a la información de cada usuario y las labores que desarrolla.

2. Asignación de acceso de usuario

La asignación de acceso de los usuarios se realizará en base a la información proporcionada por el Jefe de División respectivo al Encargado de Recursos Humanos, quien, a su vez, debe informar al Encargado de Unidad de Informática a fin de que éste en base a los antecedentes recibidos, gestione la asignación de acceso a los sistemas del usuario de acuerdo al perfil, competencias y labores a desarrollar por el usuario.
Lo anterior, se basará de acuerdo a los siguientes lineamientos:

✓ Acceso restringido:

- Usuarios que desarrollan labores no relacionadas con el área informática.
- Usuarios que por la naturaleza de su trabajo no requieren accesos a sitios restringidos por normas de seguridad institucionales.
- Usuarios que no realizan labores mediante conexiones a sistemas o aplicaciones especiales y que para establecer la conexión requieren de privilegios especiales.

✓ Acceso avanzado:

- Usuarios que por la naturaleza de sus labores requieren de ciertos accesos a programas, aplicaciones y sistema especiales más allá de los disponibles.
- Jefes de división.
- Jefes de departamentos y/o unidades con justificación de la necesidad de dichos accesos por parte de los jefes de división respectivos.

✓ Acceso liberado:

- Administradores de red con la experiencia y capacidad necesarias para dichos accesos, lo anterior, debe ser analizado por el Encargado de Unidad de informática.

3. Uso de programas utilitarios, aplicaciones y sistemas de acceso privilegiado

El uso de programas utilitarios, aplicaciones y sistemas internos de acceso privilegiados se realizará de acuerdo al perfil del usuario y tal como se señala en el ítem precedente, corresponderá al tipo de acceso privilegiado al cuál tendrán acceso los usuarios de tipo avanzado y administrador.

4. Revisión de los derechos de acceso de usuarios

El encargado de seguridad de la información, es responsable de que se efectúe la revisión de derechos de acceso de acuerdo a los siguientes parámetros:

- ✓ Revisar los derechos de acceso de usuarios al menos una vez por año.
- ✓ Los derechos de acceso con privilegios especiales serán revisados cada seis meses.
- ✓ Revisión de derechos de acceso cada vez que se produzca un cambio de labores, ascenso, retiro, término de funciones.

5. Cuentas y grupos de cuentas de usuarios

Debido a la naturaleza de las labores que se desarrollan diariamente y las competencias de cada usuario, en pos de la protección de la red y sus servicios, el Gobierno Regional de Los Ríos mantiene la administración de los usuarios y equipos conectados a la red mediante el servidor de dominio Active Directory, esta herramienta informática se utiliza en función de la correcta asignación de privilegios o restricción según corresponda además de asegurar el uso correcto de contraseñas.

Definir grupos de seguridad es una premisa para asegurar la red institucional, sus componentes y servicios, de acuerdo a anterior, se debe trabajar en base a un mínimo de tres grupos de usuarios clasificados de la siguiente forma:

- **Usuario administrador**
- **Usuario avanzado**
- **Usuario restringido**

6. Usuario administrador

Las cuentas de usuario administrador poseen control total sobre la administración del dominio y control de acceso al resto de los usuarios, es por ello que sólo deben contar con este tipo de cuenta los usuarios calificados y pertenecientes a la unidad de informática del Gobierno Regional.
El encargado de unidad deberá asumir o en su defecto asignar dicha responsabilidad a quién determine siempre y cuando se cumpla con los requisitos mínimos de competencia establecidos para ello.
Las credenciales de acceso a la cuenta de administrador son de exclusiva responsabilidad del funcionario a cargo.
En cumplimiento con el sistema de gestión de seguridad de la información, el encargado de sistema debe hacer entrega de un documento en formato papel o digital con la información actualizada de credenciales de acceso de carácter crítico y relevante para asegurar la continuidad de los procesos al encargado institucional de seguridad o en du defecto al coordinador de sistemas. Esto se revisará y actualizará – al menos – una vez cada año y/o cuando las circunstancias así lo requieran.

7. Usuario avanzado

Los usuarios avanzados son aquellos que debido al trabajo que desarrollan requieren de mayor acceso a sistemas o a la red.

La clasificación del tipo de usuario será determinada por el encargado de la unidad de informática una vez conocido el perfil y tipo de labor a desarrollar por el nuevo funcionario.

8. Usuario restringido

En este grupo se centrarán la mayor parte de los usuarios ya que, debido al perfil, competencias y a la orientación del trabajo que se realiza mayormente en la institución, se justifica la creación de usuarios con accesos restringidos a la red y sus servicios.
Forman parte de este grupo los usuarios a los que se les aplica restricción de accesos a sitios web no relacionados con su labor mediante firewall.

9. Políticas de grupo y restricciones

La creación e implementación de políticas de grupo (GPO) es fundamental para la protección y control de accesos a los equipos de la red del gobierno regional, aplicables tanto a equipos como a usuarios.
En este sentido y en resguardo de los sistemas y la información contenida en ellos, se debe crear y mantener activas ciertas políticas como base de forma estricta y permanente, en adelante y en la medida que el resultado del análisis y comportamiento del usuario así lo requiera, se debe sumar a aquellas políticas de base todas aquellas que sean consideradas necesarias para el resguardo de los activos de información.
De acuerdo al resultado y/o conclusiones emanadas de la información que se obtenga a través del Procedimiento de Incidentes de Seguridad de la Información, el encargado de sistema deberá exponer al comité de seguridad – al menos una vez cada año - sobre la posible necesidad de aumentar o mantener las restricciones existentes, nunca eliminar, particularmente a aquellas que se establecen como de base.

1.1. GPO de base y permanentes:

- Ocultar panel de control para usuarios restringidos; evita el acceso a los programas y actualizaciones instaladas en PC.

- Deshabilitar el uso de REGEDIT.EXE y REGEDT32.EXE; evita el acceso al registro del sistema.
- Uso de claves seguras; obliga al usuario a generar claves de acceso seguras y al cumplimiento de lo dispuesto a través de la política, es decir, **entre seis y diez caracteres, alfanumérica, al menos un carácter mayúsculo, cambio de clave cada ciento veinte días**.
- Bloqueo de usuario; ante intentos reiterados y fallidos de acceso se produce el bloqueo del usuario por lo que se deberá solicitar soporte a la unidad de informática para el desbloqueo.

El funcionario responsable de la administración de dominio deberá asegurar la operatividad y buen funcionamiento tanto del administrador de dominio como de las políticas de grupo implementadas.

10. Gestión de información secreta de autenticación de usuarios

Las contraseñas son las llaves de acceso a los distintos sistemas y por ende a la información que cada usuario maneja, almacena y distribuye a través de su equipo de trabajo, así como a través de los medios y sistemas en los que ésta se procesa, de ahí radica la importancia de aplicar el máximo de seguridad a la hora de generar y resguardar las mismas.

1.2. Contraseñas de usuario de dominio

El administrador de dominio institucional trabaja bajo una rigurosa política de seguridad en la generación de las contraseñas, siendo responsabilidad de cada usuario generarlas cumpliendo los estándares establecidos y mantenerlas fuera del alcance de terceros.
Para la generación de contraseñas se debe cumplir con las siguientes exigencias de seguridad:

- **Entre seis y diez caracteres**
- **Alfa numéricas**
- **Al menos un carácter mayúsculo**
- **No relacionada con datos de usuario (nombre, apellido, etc)**
- **Evitar números descendientes o crecientes fáciles de deducir**

- **No repetidas**
- **Cambiarlas cada ciento veinte días.**

1.3. Contraseñas de correo institucional

Para la creación de contraseñas de correo institucional se aplicará los estándares de seguridad descritos anteriormente, diferenciándose sólo en el sentido que el usuario administrará sus datos de acceso pudiendo mantener o cambiar la contraseña de acceso al correo a discreción, sin perjuicio de lo anterior, se mantiene como único responsable del resguardo de sus datos de acceso.

1.4. Contraseñas para conexión de red inalámbrica

El Gobierno Regional de Los Ríos mantiene disponible conexión de red inalámbrica en cada piso del edificio a través de router, lo anterior en los casos en que terceros tengan la necesidad de conexión a internet, estos aparatos son administrados por los funcionarios de la unidad de informática y se debe cumplir rigurosamente con los siguientes estándares de seguridad.

- **Conexión mediante contraseña proporcionada por el funcionario a cargo.**
- **Generación de contraseña de acuerdo a los estándares establecidos.**
- **Acceso limitado a internet o estrictamente de acuerdo a la necesidad del usuario.**

11. Control de acceso al código fuente

Las credenciales de acceso a servidores y todo tipo software, sistemas, aplicaciones, código fuente, etc., pertenecientes a la institución se consideran como críticos para la continuidad de los procesos y de acuerdo a ello, el Encargado de la Unidad de Informática es responsable de la administración de accesos y mantener una planilla actualizada con la información de acceso proporcionando esta información al presidente del comité de seguridad o en su defecto, a quién lo subrogue, esto deberá realizarse al menos una vez cada año o cuando se produzca algún cambio en la información tanto de nombre de usuario o contraseñas. Lo

anterior se debe cumplir en forma irrestricta para asegurar la disponibilidad de la información a todo evento.
Se establece mediante el presente documento que el acceso al código fuente de los programas queda restringido para todos aquellos usuarios que no califiquen con el perfil de administrador.
Se establece, además, que se debe mantener un registro con los accesos, cambios o eliminación de códigos fuente, lo que se debe realizar bajo estrictas medidas de seguridad que permitan entre otros lo siguiente:

- ✓ En los casos de cambio de sistema, realizar las pruebas correspondientes antes del cambio definitivo.
- ✓ Contar con sistema de reversa en caso de fallas del nuevo sistema.
- ✓ Respaldar antes de iniciar cualquier intervención tanto de sistemas como de códigos.
- ✓ Mantener respaldos durante periodo de marcha blanca y hasta – al menos un año – luego del cambio.

12. Eliminación o ajuste de los derechos de acceso

La eliminación o ajuste de los derechos de acceso se realizará en base a la información que proporcione el Jefe de División correspondiente al Encargado de Recursos Humanos, quién a su vez, enviará dicha información al encargado de la unidad de informática a fin de solicitar que se gestione la eliminación o ajuste de los derechos de acceso de acuerdo a los parámetros establecidos precedentemente.

13. Registro y cancelación de registro de usuario

Ante el cambio o cese de funciones de un usuario, el encargado de la unidad de informática deberá gestionar el bloqueo temporal de las credenciales otorgadas a dicho usuario, ya sea con el fin de habilitar el nuevo perfil y los accesos correspondientes de acuerdo a la nueva función, o para la generación del respaldo correspondiente y la posterior eliminación definitiva de usuario.
Ello aplicará para todo tipo de credenciales de acceso que mantenga el usuario en caso de cese de funciones y para las necesarias en caso de cambio de funciones.

Lo anterior asegura que se tomen las medidas de seguridad correspondientes ante posibles accesos no autorizados e intervenciones no autorizadas.

VI. Registros de Operación

Este documento será revisado en su texto por los miembros del comité de seguridad, una vez aprobado será difundido a los usuarios/funcionarios y puesto a disposición en el repositorio web de intranet denominado PMG-SSI dispuesto para ello y en el cuál se mantiene toda la documentación generada a partir de la implementación del Sistema de Gestión de Seguridad de la Información en la institución.

Las revisiones relativas al cumplimiento efectivo de las directrices y lineamientos que dicta el procedimiento serán realizadas por el encargado de sistema de forma permanente e informado al presidente del comité de seguridad o en su defecto a quién subrogue y al coordinador de PMG institucional acerca de la eventual necesidad de realizar correcciones o modificaciones al mismo.

El profesional de la Unidad de Informática responsable de la administración del dominio deberá entregar al encargado de la seguridad de la información del servicio, quién a su vez deberá presentar al comité de seguridad de la información del Gobierno Regional de Los Ríos para el análisis y la definición de la actualización del presente procedimiento.

- ✓ Informe de implementación de GPO con restricciones mencionadas en este procedimiento.
- ✓ Informe de la asignación de nuevas cuentas a nuevos funcionarios o modificaciones de permisos a usuarios existentes.
- ✓ Informe de administración de cuentas de usuarios en la red del Gobierno regional de Los Ríos.

Validado por:		
Funcionario	**Cargo de integrante de comité de SGSI**	**Firma**
Luis Patricio Acum Salinas	Encargado de Unidad de Informática	
Paola Hermosilla Bucarey	Encargada Departamento Jurídico	
Cesar Pérez Sepúlveda	Encargado Departamento de Finanzas	
Wilson Monzón Riquelme	Jefe División de Presupuesto Inversión Regional	
Heidi Machmar Hernández	Jefa de División de Planificación y Desarrollo Regional	
Carlos Ovando Hernández	Jefe de División de Administración y Finanzas	
Eduardo Fagalde Ampuero	Jefe de División de Desarrollo Social y Humano.	
Ernesto Espinoza Navarrete	Jefe de División de Fomento e Industria	
Alejandro Paredes Zieballe	Administrador Regional	
Rodrigo Aravena Bustamante	Coordinador PMG de la institución	

CESAR ASENJO JERÉZ
INTENDENTE
GOBIERNO REGIONAL DE LOS RÍOS