




**GOBIERNO
REGIONAL DE
LOS LAGOS**

Acción de Futuro

SISTEMA DE SEGURIDAD DE LA INFORMACIÓN


PROCEDIMIENTO "SEGURIDAD DE LOS SERVICIOS DE REDES"

CÓDIGO	SSI-A.13.01.02	CLASIFICACIÓN INFORMACIÓN		Reservada
			X	Uso Interno
				Pública
VERSIÓN	1.0	FECHA DE LA VERSIÓN	04-07-2019	
RESPONSABLE	Encargado de la Unidad de Informática.			


Código : SSI-A.13.01.02	PROCEDIMIENTO SEGURIDAD DE LOS SERVICIOS DE REDES	
Versión: 1.0		
Fecha : 04-07-2019		
Página : 2 de 7		

Historial de modificaciones


Creación/Modificaciones del Documento

Versión	Fecha de modificación	Autor	Motivo	Páginas modificadas	Firma
1.0	04-07-2019	Eduardo Madrid Osorio, Encargado Unidad de Informática	Creación de la primera versión del procedimiento	Todas	

Revisiones


Versión	Fecha	Autor	Observación	Páginas	Firma
1.0	22-07-2019	Javier Soto Mancilla, Apoyo Profesional DAF	Sin observaciones	Todas	

Visto Bueno

Versión	Fecha	Encargado	Firma
1.0	14-08-2019	Oscar Alejandro Oyarzo Pérez, Encargado de Seguridad de la Información	
1.0	14-08-2019	Alejandro Montaña Ampuero, Administrador Regional del Gobierno Regional de Los Lagos	 


Distribuciones

Versión	Fecha	Encargado	Observaciones
1.0	26-11-2019	Oscar Alejandro Oyarzo Pérez, Encargado de Seguridad de la Información	Enviado por correo electrónico e instruida la publicación en intranet a la Unidad de Informática

Código : SSI-A.13.01.02	PROCEDIMIENTO SEGURIDAD DE LOS SERVICIOS DE REDES	
Versión: 1.0		
Fecha : 04-07-2019		
Página : 3 de 7		

Contenido

1. Objetivo	4
2. Alcance o ámbito de aplicación interno	4
3. Roles y Responsabilidades.	4
4. Procedimiento	5
4.1. Documentos de referencia	6
4.2. Registros de control del procedimiento.....	7
5. Validez y gestión de documentos.....	7

Código : SSI-A.13.01.02	PROCEDIMIENTO SEGURIDAD DE LOS SERVICIOS DE REDES	
Versión: 1.0		
Fecha : 04-07-2019		
Página : 4 de 7		

1. Objetivo

Asegurar la protección de información en las redes y sus instalaciones de procesamiento de la información de apoyo y mantener la seguridad de la información transferida dentro del GORE Los Lagos y con cualquier entidad externa.


2. Alcance o ámbito de aplicación interno

El presente procedimiento, establecerá el derecho de acceso a la información que puedan afectar los activos de información del GORE Los Lagos y a todas sus relaciones con terceros que impliquen el acceso a sus datos, recursos y/o a la administración y control de sus sistemas de información.

Este procedimiento es aplicable a todos los funcionarios (planta, contrata, reemplazos y suplencia), personal a honorarios y terceros, es decir, proveedores, que presten servicios al Gobierno Regional de Los Lagos.

3. Roles y Responsabilidades.

ROLES	RESPONSABILIDADES
Jefe Depto. Gestión y Desarrollo de Personas	<ul style="list-style-type: none"> • Informar ingreso y salida del personal de planta, contrata y honorarios, de acuerdo con lo señalado con la política de control de acceso y los procedimientos del área.
Encargado de Seguridad de la Información	<ul style="list-style-type: none"> • Supervisar la implementación del presente control. • Difundir el presente control entre los funcionarios planta, contrata y/u honorarios.
Encarado Unidad de Informática	<ul style="list-style-type: none"> • Implementación de la configuración, monitoreo y controles correspondientes a las redes y los servicios de red en el servicio. • Aprobar o rechazar las solicitudes de permisos especiales de acceso a los servicios de red. • Mantener activo todos los registros (LOGS) que las políticas, procedimientos e instructivos indican. • Mantener respaldo e integridad de los registros activos. • Resguardar que los registros no sobrepasen los límites definidos. • Revisar si las solicitudes de nuevos permisos se acogen a los procedimientos vigentes. • Crear, supervisar y administrar el buen uso de las cuentas genéricas y listas de distribución requeridas por el Servicio.
Funcionarios de Planta, Contrata y Honorarios	<ul style="list-style-type: none"> • Es el único responsable de las acciones que se realizan con su cuenta.

Código : SSI-A.13.01.02	PROCEDIMIENTO SEGURIDAD DE LOS SERVICIOS DE REDES	
Versión: 1.0		
Fecha : 04-07-2019		
Página : 5 de 7		

	<ul style="list-style-type: none"> • Mantener la confidencialidad de sus contraseñas. • Actualizar su clave de acceso periódicamente y antes de que venza. • Almacenar la información relevante en carpetas de trabajo creadas directamente en su equipo y/o servidor de archivos.
--	---

4. Procedimiento

En cuanto a la autorización para permitir acceder a redes y servicios de red: todos los computadores del GORE Los Lagos se configuran para acceder a los servicios de red. Todos los funcionarios tienen sus cuentas de red debidamente configuradas para acceder a los distintos servicios de red, de acuerdo con su perfil (cargo), el que es informado por el departamento de gestión de personas al momento de ingreso de un nuevo funcionario. Las solicitudes de permisos especiales o adicionales para utilizar redes o servicios de red deben ser aprobados por la jefatura directa de cada funcionario a través de correo electrónico al Encargado de la Unidad de Informática, la cual revisará si se acoge a los procedimientos o instructivos vigentes, de lo contrario, escalará la solicitud al Encargado de la Unidad de Informática quién determina si la solicitud no vulnera la Política de Control de accesos del GORE Los Lagos, sopesando los criterios de facilidad de operación y protección de la información.

En cuanto a controles de seguridad a la red y a los servicios de red: las conexiones de red y servicios de red del GORE Los Lagos están configurados para registrar todas las actividades que se realizan, manteniendo estos registros disponibles por un mes.

Los datos que se registran de los usuarios que utilizan redes o servicios de red del servicio son los siguientes:

- Dirección IP origen
- Nombre del dispositivo origen
 - Puertos utilizados
 - Dirección IP destino
 - URL destino
 - Tráfico de red

Para minimizar las fallas y dar respuesta oportuna a incidentes, se debe monitorear los servicios de red del GORE Los Lagos, alertando a los responsables de manera automática.

Para utilizar servicios de red, todos los usuarios deben iniciar sesión en Active Directory. Para usuarios que requieren acceso remoto, se aceptarán conexiones VPN autorizadas por el Encargado de la Unidad de Informática.


Todos los usuarios que utilizan servicios de red desde dispositivos que no estén incorporados al dominio (Active Directory) del Servicio deben cumplir con la Política para el uso de dispositivos móviles.

Las redes inalámbricas (WIFI), debe cumplir con permisos restringidos para las visitas o proveedores externos que solicitan conectarse a la red institucional. Esta conexión es temporal.

Los usuarios con computadores personales que desean utilizar servicios de red en ellos deben ajustarse a los requisitos de la Política para el uso de dispositivos móviles y deberán solicitar su acceso al Encargado de la Unidad de Informática.

Queda prohibido que los usuarios accedan a redes o a servicios de redes no permitidos, sin la autorización correspondiente.

El servicio de red de acceso a internet es restringido con un sistema de filtro de contenidos. Los usuarios tienen prohibición de conectar algún dispositivo que permita compartir acceso a redes o a servicios de red, tales como Router, Switch, o equivalente.

Código : SSI-A.13.01.02	PROCEDIMIENTO SEGURIDAD DE LOS SERVICIOS DE REDES	
Versión: 1.0		
Fecha : 04-07-2019		
Página : 6 de 7		

Todo servicio de red que consuma ancho de banda excesivo (transferencia de videos, o archivos de gran tamaño) será restringido, salvo a usuarios que lo requieran para el

cumplimiento de sus funciones, en cuyo caso, la jefatura del usuario debe solicitar a la mesa de ayuda el acceso a un servicio en particular.

En cuanto a seguridad en los perímetros de la red: El GORE Los Lagos cuenta con equipos del tipo firewall propios y/o de terceros que al menos tienen las siguientes funcionalidades:

- Establecer reglas de filtro y navegación para los usuarios internos (LAN)
- Permitir configurar publicaciones de servicios internos hacia internet (DMZ) en forma segura.
- Filtro de correo (Antispam), bloqueo de mensajes no deseados en tiempo real.
- Filtro de Navegación, restricción de accesos WEB de usuarios, de acuerdo al contenido de los sitios, protección contra sitios maliciosos.
- Filtro antivirus, revisión de tráfico WEB y email de protección perimetral contra spyware, virus y otros.
- Servicio de conectividad remota segura a través de VPN.
- Sistema de prevención de intrusos (IPS), que posibilite en tiempo real, identificar, detectar y/o bloquear ataques o actividades sospechosas sobre la red de la Subsecretaría, complementando los dispositivos de seguridad del firewall.
- Integración con Active Directory, para controlar y agrupar por tipo los diferentes niveles de acceso a Internet por parte de los usuarios.

Por otra parte, al Unidad de Informática, gestiona, a través de recursos propios o de terceros, las siguientes tareas en orden de mantener la Seguridad Perimetral en permanente operación:


- Resumen de incidentes y requerimientos críticos (Informes trimestrales).
- Principales eventos críticos, si los hubieran, de seguridad detectados, criticidad, origen de los mismos y recomendaciones.
- Registro y Reportes de Eventos ocurridos en el firewall y en el acceso bajo supervisión durante el período.

En cuanto a acuerdos de servicios de red: entre la documentación que la Unidad de Informática genera y mantiene permanentemente actualizada en la respectiva carpeta de red está la lista de los Servicios de Red, incluyendo en esta, los mecanismos de seguridad empleados para otorgar el servicio en forma segura, los niveles de servicio y reportes que son solicitados a través de contratos o bien solicitados por GORE Los Lagos.

4.1. Documentos de referencia

En la siguiente tabla, se presentan los documentos que se han utilizado como referencia, para la formulación del presente manual de procedimientos.

Código	Descripción
SSI-A.05.01.01	Política de Seguridad de la Información
SSI-A.13.01.01	Controles de red
SSI-A.13.02.04	Acuerdos de confidencialidad o no divulgación
SSI-A.13.02.01	Políticas y procedimientos de transf. de información
NCh-ISO 27001	Tecnologías de la información – Técnicas de seguridad – Sistemas de gestión de la seguridad de la información.

Código : SSI-A.13.01.02	PROCEDIMIENTO SEGURIDAD DE LOS SERVICIOS DE REDES	
Versión: 1.0		
Fecha : 04-07-2019		
Página : 7 de 7		

NCh-ISO 27002	Tecnologías de la información – Técnicas de seguridad – Código de prácticas para los controles de seguridad de la información.
---------------	--




4.2. Registros de control del procedimiento.

- a) Informes trimestrales de eventos críticos detectados por antivirus.
- b) Informes trimestrales de eventos críticos detectados por el firewall.
- c) Informes trimestrales de eventos críticos detectados por el antispam.
- d) Informes trimestrales de eventos críticos detectados por el registro de eventos de Windows server.

5. Validez y gestión de documentos

Este documento es válido desde la fecha de su aprobación.

El responsable de este documento es el Encargado de la Unidad de Informática, que debe verificar, y si es necesario actualizar el documento, por lo menos una vez cada tres años.

	Aprobado Por	
		
Oscar Alejandro Oyarzo Pérez Encargado de Seguridad de la Información		
14 de Agosto de 2019		