PROCEDIMIENTO DE GESTIÓN Y CONTROL DE REDES

Nch 27001/2013 Control	A.13.01.01	CONTROLES DE RED
Nch 27001/2013 Control	A.13.01.02	SEGURIDAD DE LOS SERVICIOS DE RED
Nch 27001/2013 Control	A.13.01.03	SEPARACIÓN EN LAS REDES
Nch 27001/2013 Control	A.13.02.04	ACUERDOS DE CONFIDENCIALIDAD O NO DIVULGACIÓN
Nch 27001/2013 Control	A.14.01.02	ASEGURAMIENTO DE SERVICIOS DE APLICACIÓN EN REDES PÚBLICAS

CONTROL DE CAMBIOS:

Versión	Fecha	Responsable	Acción
1.0	Diciembre de 2018	ACUM SALINAS LUIS PATRICIO	Elaborado
1.1	Octubre-2019	SANDRA PÉREZ GUZMÁN	Actualizado

Validado:

Comité Seguridad de La Información

Funcionario	Integrante Comité	Firma
Luis Patricio Acum Salinas	Encargado de Unidad de Informática	
Paola Hermosilla Bucarey	Encargado de Departamento Jurídico	
Cesar Pérez Sepúlveda	Encargado de Dep. de Finanzas	
Wilson Monzón Riquelme	Jefe Div. de Presupuesto e Inversión Regional	
Heidi Machmar Hernández	Jefe Div. Planificación y Desarrollo Regional	
Carlos Ovando Hernández	Jefe Div. de Administración y Finanzas	
Eduardo Fagalde Ampuero	Jefe Div. de Desarrollo Social y Humano	
Ernesto Espinoza Navarrete	Jefe Div. de Fomento Productivo e Industria	
Alejandro Paredes Zieballe	Administrador Regional	
Rodrigo Aravena Bustamante	Coordinador de PMG de la Institución.	

GOBIERNO REGIONAL INTENDENTE REGION DE LOS RIOS

CESAR ASENJO JERÉZ
INTENDENTE
GOBIERNO REGIONAL DE LOS RÍOS

Contenido

1. DECLARACIÓN INSTITUCIONAL

El **Gobierno Regional de Los Ríos**, expresa por medio del presente documento su convicción y compromiso de resguardar los activos de información con los que cuenta la institución, conociendo la importancia de dichos activos en el cumplimiento de la relevante misión que desempeña. Es por ello que se crea el **PROCEDIMINETO DE GESTIÓN Y CONTROL DE REDES DEL GOBIERNO REGIONAL DE LOS RÍOS** basado en Sistemas de Gestión de Seguridad de la Información, el que debe garantizar el correcto funcionamiento del servicio, el cumplimiento de metas y la prevención de riesgos y/o amenazas referidas a los Activos de Información al momento del uso de los servicios, la tecnología e infraestructura de red de acuerdo a las necesidades del servicio.

2. ALCANCE O ÁMBITO DE APLICACIÓN DEL PROCEDIMIENTO

El presente Procedimiento de Gestión y Control de Redes es de uso interno y aplicable a todos los funcionarios del Gobierno Regional de Los Ríos y a quienes prestan servicios externos tanto de desarrollo como de soporte de sistemas, especialmente aquellos funcionarios que ejercen sus labores en el área de Tecnologías de la Información de la Institución.

3. OBJETIVO GENERAL

Preservar la disponibilidad de los servicios soportados por la Infraestructura tecnológica institucional.

Establecer los métodos, pasos y medidas a utilizar para la conexión remota a la infraestructura (redes, servidores, etc.) desde fuera de la red de comunicaciones, así como el intercambio de información entre las ubicaciones externas a las oficinas principales.

Salvaguardar la información en tránsito a través de las redes y equipos institucionales, los sistemas soportados y la infraestructura de red.

4. ROLES Y RESPONSABILIDADES

Responsable	Rol	Funciones
Jefe de Servicio	Liderar la implementación del presente	✓ Aprobar el documento. ✓ Autorizar los recursos necesarios para

	procedimiento.	su implementación, así como el nombramiento de funcionarios coordinadores y/o encargados de su 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 Unidad de Informática	Analizar, coordinar y supervisar las solicitudes de conexión.	✓ Recibir y coordinar las conexionas remotas a la red. ✓ Analizar la factibilidad de las solicitudes de conexión remota. ✓ Proponer mejoras y/o cambios en la implementación.
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 del Gobierno Regional de Los Ríos	Dar cumplimiento a lo establecido en el procedimiento.	✓ Dar cumplimiento a lo establecido el procedimiento. ✓ Informarse, asistir a charlas o reuniones relacionadas con la difusión del contenido del documento.

5. DEFINICIONES

Datos: Son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos. En su forma más amplia los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y bases de datos, texto (colección de palabras), hojas de cálculo (datos en forma matricial), imágenes (lista de vectores o cuadros de bits), video (secuencia de tramas), etc.

Privacidad: Es el derecho que tienen los individuos y organizaciones para determinar, ellos mismos, a quién, cuándo y qué información referente a ellos será difundidas o transmitida.

IP: Dirección de 32 bits definida por el Protocolo Internet en STD 5, RFC 791. Se representa usualmente mediante notación decimal separada por puntos.

Soporte: Objeto físico susceptible de ser tratado en un sistema informático y sobre el cual se pueden grabar o recuperar datos.

Usuario: Sujeto o proceso autorizado para acceder a datos u otros recursos.

Activos de información: Corresponde a elementos tales como bases de datos, documentación, manuales de usuarios, planes de continuidad, etc.

Autorización: Proceso por el que se acredita a un individuo para realizar una acción determinada, como el acceso a los recursos una vez que el usuario ha sido autenticado con éxito.

Control de Acceso: Mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

6. CONTROLES DE RED CORPORATIVA

El edificio principal del Gobierno Regional de Los Ríos, actualmente se encuentra conectado a una Red Independiente.

Las medidas de seguridad establecidas en el presente procedimiento están orientadas a proteger el acceso remoto no autorizado a los sistemas como trampolín para realizar ataques a otros sistemas y como protección adicional a los datos y servicios que en ellos residen, independientemente de que estos últimos dispongan de mecanismos específicos de protección.

Los equipos de redes son administrados por el Profesional de la Unidad de Informática del Gobierno Regional de Los Ríos, quien los administra bajo las normativas y procedimientos establecidos en; el Procedimiento de Inventario de Activos; el Procedimiento de Protección de Equipos y Procedimiento de Mantención de Equipos. Sin perjuicio de que el Profesional de la Unidad de Informática es responsable de los equipos bajo su control, los funcionarios y funcionarias son responsables del cuidado y protección de equipos portátiles u otros equipos Institucionales que por el adecuado desarrollo de sus funciones se les ha proporcionado.

6.1. Tipos de Redes

En el Gobierno Regional de Los Ríos se contemplan los siguientes tipos de accesos a través de redes:

- ✓ Acceso Correo: acceso remoto al correo electrónico corporativo desde el exterior, de forma restringida a los empleados del organismo. Este tipo de acceso se realizará cifrando la información que circula por la red mediante mecanismos de autenticación que garantizan los mismos controles de acceso con los que se cuenta en la red interna de las instalaciones del Gobierno Regional de Los Ríos.

- ✓ Acceso a la administración de los sistemas de información desde los puestos del departamento de informática, o remotamente a través de VPN.

Para el acceso a los sistemas de información se establecerán los mecanismos de seguridad suficientes que permitan garantizar que sólo el personal autorizado pueda acceder a los mismos. Los mecanismos que se implanten permitirán la identificación inequívoca de cada usuario que puede acceder al sistema.

Mecanismos de Seguridad

- ✓ Restringir el acceso a los sistemas desde las ubicaciones de los usuarios autorizados (a través de IPs concretas), de forma que no existe la posibilidad de identificarse desde una ubicación distinta.
- ✓ Impedir que la Información usada en la identificación, así como en las operaciones de administración pueda ser capturada por terceros (https, VPNSSL, etc.).
- ✓ Regularizar los accesos remotos mediante autorizaciones expresas.

6.2. Equipos Accesibles

Para las funciones de administración de sistemas se definirán grupos de personas diferentes, a los cuales se les asignará rangos de direcciones de red diferenciados, con objeto de facilitar las medidas de control.

6.3. Acceso Remoto para Administración de Sistemas

La administración de sistemas se podrá realizar, en general, de forma local (desde la consola del sistema) o remota. La entrada directa en la cuenta *root / administrador* de los sistemas solo se podrá efectuar localmente, desde la consola del sistema. Para el acceso remoto será preciso entrar en una cuenta puente y desde allí entrar en *root / administrador.*

La administración remota estará protegida por las medidas que se detallan a continuación, siendo aplicable a cualquier forma de administración remota, desde una red o subred distinta a la red donde se encuentran los servidores del Gobierno Regional de Los Ríos.

Cualquier intento de acceso que no cumpla todas las condiciones no será factible;

- ✓ Ninguna conexión de administración desde una red distinta a la local de servidores será posible sin pasar por una autenticación.

- ✓ La conexión remota debe ser cifrada y suficientemente autenticada. En todo caso no se permite el envío de contraseñas en claro por Red.

- ✓ No se establecen restricciones de horario para la conexión remota para la administración de sistemas.

6.4. Administración Basada en Navegador Web

Para los servicios administrados desde un navegador web, se utilizará una conexión cifrada mediante SSL con cifrado mínimo de 128 bits. El servidor Web de administración debe configurarse para restringir las direcciones IP que se puedan conectar al servicio. El acceso al servidor de administración debe configurarse para que exija contraseña.

6.5. Flujos de Administración

Todos los flujos de administración entrarán exclusivamente a través de los cortafuegos corporativos.

6.6. Acceso Remoto a la Red Corporativa por Parte de Funcionarios(as)

Se considera aquí el acceso a los funcionarios y funcionarias del Gobierno Regional de Los Ríos a los servicios de Red utilizando como acceso Internet.

El acceso de un usuario desde fuera de las instalaciones del Gobierno Regional de Los Ríos debe estar especialmente protegido para impedir que se ponga en riesgo los contenidos sensibles que pueda haber en la Red interna o corporativa.

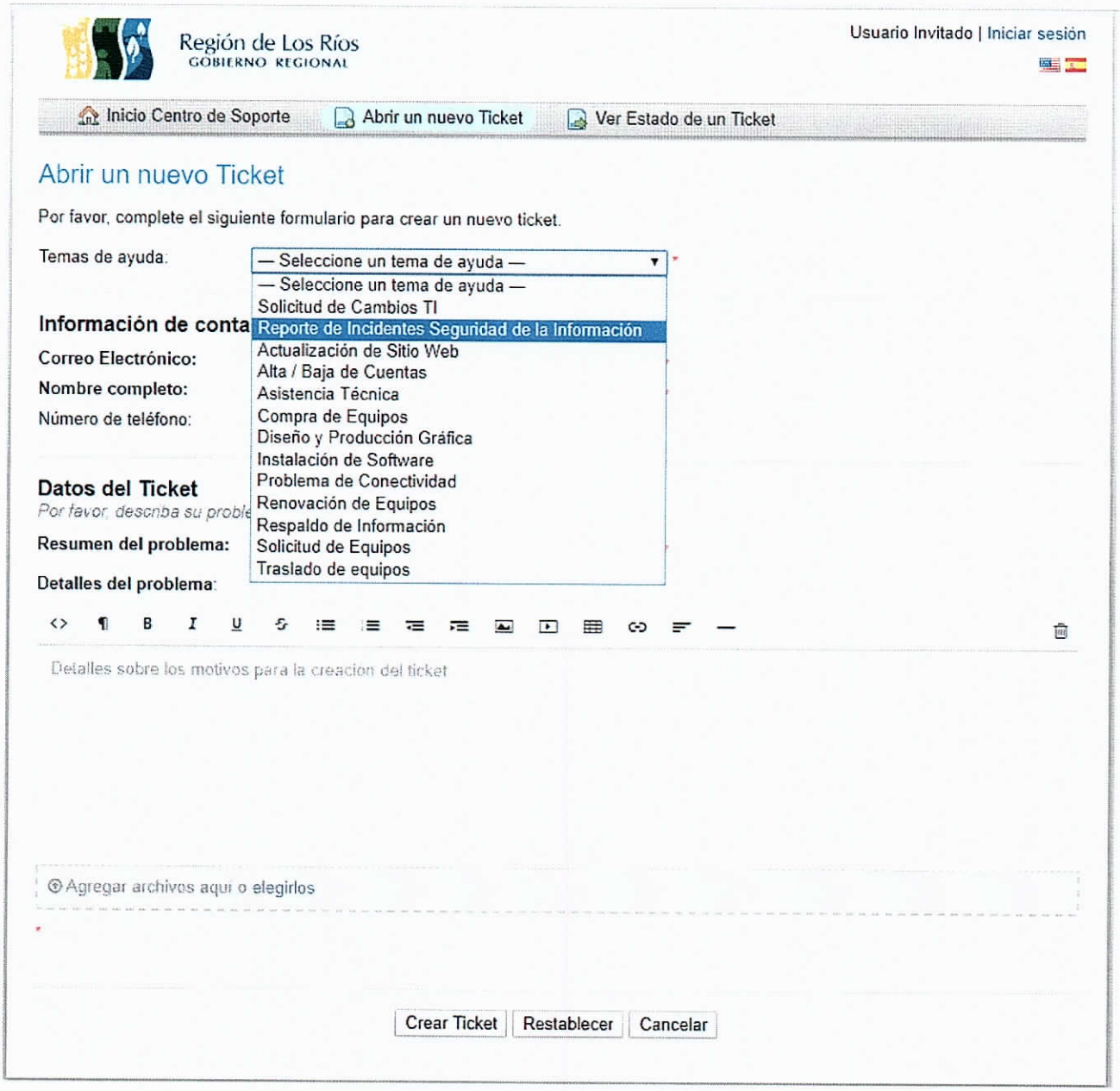
Los servicios a los que un funcionario(a) remotamente puede acceder son los siguientes:

- ✓ Servicio de Correo electrónico
- ✓ Intranet Institucional

6.7. Acceso al Correo Electrónico Web

El acceso se realiza contra el servidor Web de Correo Electrónico, mediante el protocolo HTTP seguro (HTTPS), estableciéndose así una conexión segura de acceso al mismo.

En el caso de que un funcionario(a) alerte o tenga constancia de que su correo podría haber sido vulnerado, así como su certificado de acceso, notificará inmediatamente de la incidencia mediante el Procedimiento de Gestión de Incidentes a través de la opción "Reporte de Incidentes Seguridad de la Información" en la plataforma OsTicket, tal como se demuestra a continuación.



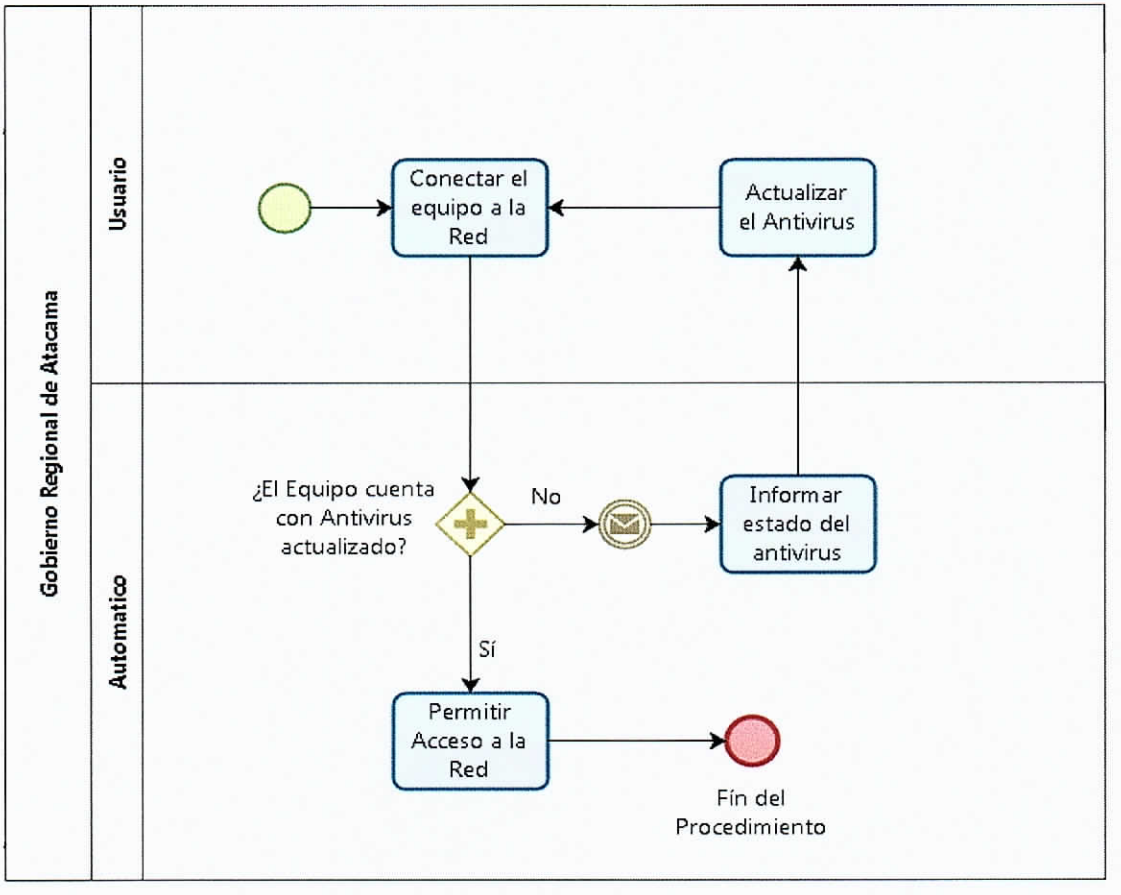
6.8. Registro

Todas las conexiones remotas a la Red y Sistema del Gobierno Regional de Los Ríos serán registradas. Se configurarán los servidores a los que se conectan los usuarios para guardar, adicionalmente la siguiente información específica, tanto de conexiones fallidas como exitosas:

- ✓ Dirección de IP de origen de conexión
- ✓ Dirección de IP de destino de conexión
- ✓ Hora de conexión
- ✓ Hora de desconexión
- ✓ Duración de la conexión
- ✓ Usuario con el que ha sido validada la conexión

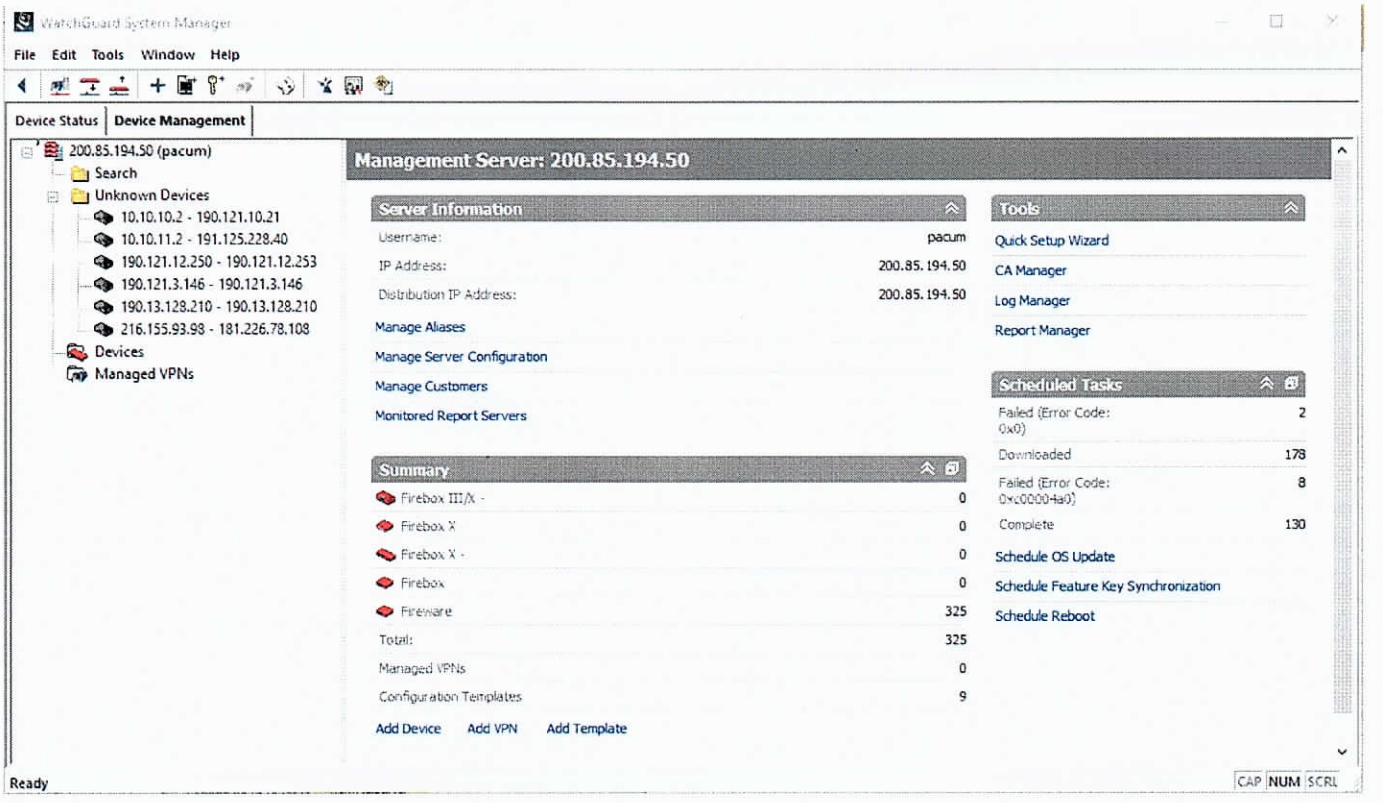
6.9. Requerimientos de Seguridad para el Equipo Remoto de Usuario

Los equipos conectados remotamente deberán cumplir, en general, los mismos requerimientos de seguridad que cualquier otro equipo que se conecte directamente (en las propias instalaciones) a la red de comunicaciones interna de la organización y en particular deberá tener implementadas las medidas de seguridad indicadas en la normativa de uso de computadores portátiles.



7. Seguridad en los servicios de redes.

La seguridad para los servicios de red del Gobierno Regional, son provistos por un proveedor externo mediante un firewall "WatchGuard", el que impide y bloquea los intentos de acceso a la red tanto internos como externos, todo ello de acuerdo a la configuración de seguridad recomendada y solicitada de parte del funcionario a cargo de la unidad de informática de la institución, además, internamente se impide todo acceso mediante restricción de usuarios administrados de forma centralizada a través de ActiveDirectory.



8. Segregación de la red Gore.

La red del Gobierno Regional, se encuentra segregada a nivel físico y lógico tal que cumple con las normas de seguridad de red establecidas por las normas que nuestro país ha suscrito en esta materia, **la topología y sus características no deben ser modificadas en forma arbitraria o intervenida por personas internas o externas sin el conocimiento técnico necesario para ello, en los casos en que estan modificaciones correspondan a mejoras, reparaciones o cambios a nuevas tecnologías, deben realizarse bajo la supervisión del encargado de la unidad de informática o en su defecto de quien sea designado para ello manteniendo el criterio de cumplimiento de las normas técnicas y de seguridad recomendadas y vigentes**.

los tipos de segregación y sus características son las siguientes:

8.1. Segregación Física

La segregación física se define por los Rack de Comunicaciones ubicados en cada piso del edificio, que a su vez se comunican con la central de la sala de servidores, esta topología de red es de carácter lineal (topología de Bus), con ello se separan en tres sub-redes que proveen del servicio de internet a cada piso del edificio.

Debido a lo anterior, en caso de fallos es posible monitorear, revisar y aislar el switch que presente problemas o sea objeto de algún ataque tanto interno como externo, evitando así la contaminación de la red completa.

8.2. Segregación Lógica

- La segregación lógica permite, a través de configuraciones del switch el paso o habilitación de enlaces dedicados o especiales para la conexión de otros dispositivos, con ello se separa los puertos o bocas que proveen a los equipos computacionales del servicio de internet de otros equipos que requieren de IPs externas u otros pools IPs internos distintos de los que proveen servicio a los equipos gore.

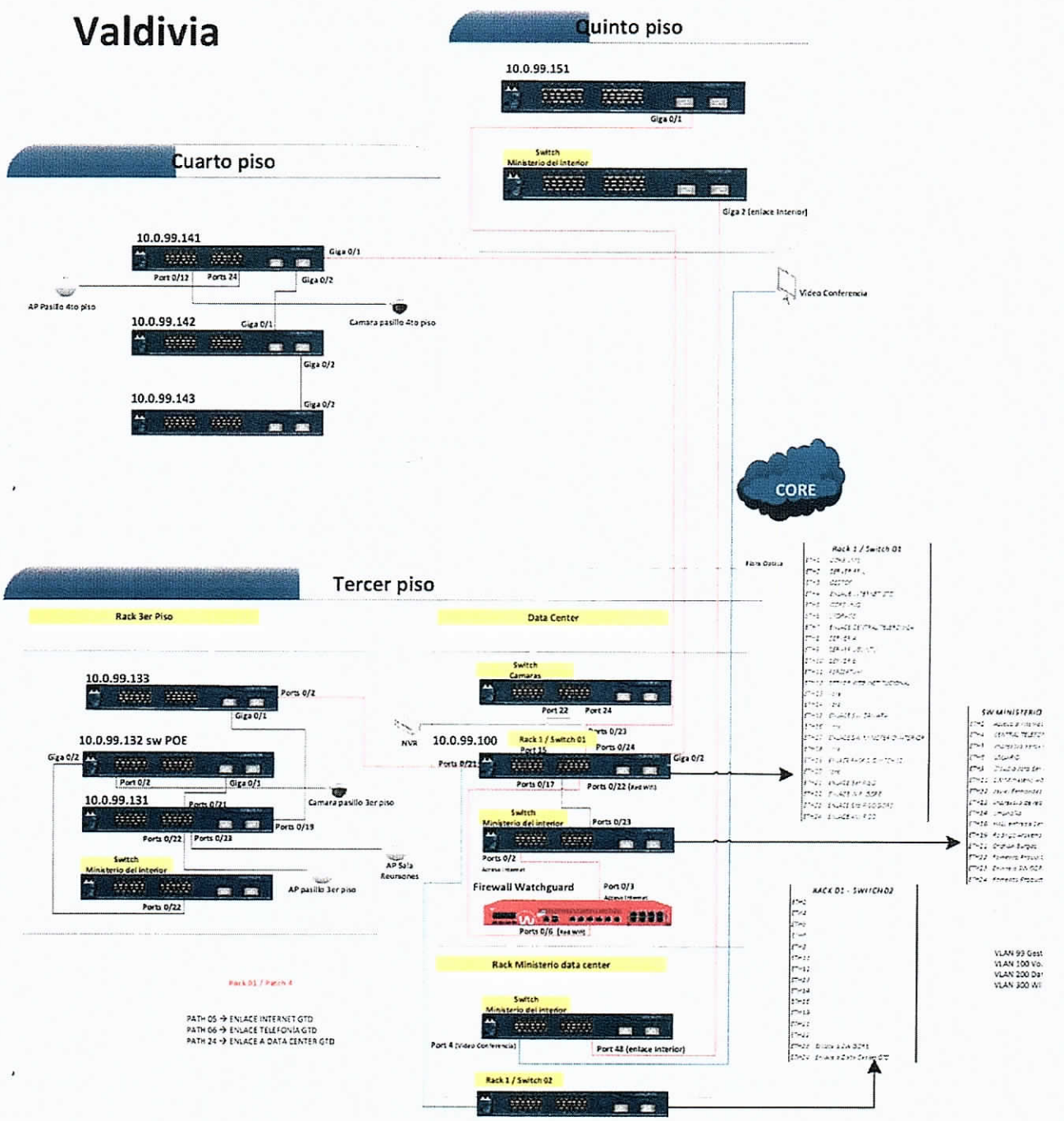
Los siguientes servicios se encuentran separados lógicamente a través de configuraciones de switch:

VLAN 99 gestor
VLAN 100 vos
VLAN 200 datos
VLAN 300 WIFI

Igualmente, todos aquellos servicios diferentes de los estrictamente necesarios para proveer internet a través de cableado y aplicaciones o programas, deben estar separados de forma lógica para evitar que distintos servicios transiten por la misma vía.

La siguiente imagen demuestra la topología de red y sus características:

Red Gore Valdivia



9. Acuerdos de Confidencialidad y/o no Divulgación

Con la finalidad de evitar mal uso, pérdida o modificación de información de carácter sensible a la cual se tenga acceso por parte de funcionarios, además de las restricciones físicas y lógicas de acceso, se debe incorporar a las actas de entrega, un texto referido a la obligación de mantener absoluta confidencialidad respecto a la información que se tenga acceso y que, debido a sus características, no deba ser divulgada. En el caso de terceros, se debe evitar proporcionar accesos a información sin la debida supervisión de un funcionario perteneciente al área de informática de la institución.

Para dar cumplimiento a lo anterior, se solicitará la firma de un documento de compromiso que se detalla en los anexos del presente documento "**Acuerdo de Confidencialidad**".

10. Aseguramiento de Servicios de Aplicación en Redes Públicas

El Gobierno Regional de Los Ríos es una institución que en su naturaleza no mantiene servicios de aplicación disponibles en redes públicas de forma permanente, sin embargo, en ocasiones se debe poner a disposición del público exterior formularios de postulación a los distintos recursos concursables, lo cual esta a cargo de proveedor externo en el caso del sistema de subvenciones, FIC y FRIL.

Las postulaciones a través de dichos sistemas se realizan de tal forma que sea bajo las normas de seguridad establecidas:

- ✓ Protección de la confidencialidad y la integridad de la información.
- ✓ Otorgar confianza sobre la identidad de los postulantes a través de script de verificación de datos.

11. Anexos

Anexo "A" – Solicitud de Acceso Remoto por parte de Terceros

Las solicitudes de Acceso Remoto por parte de terceros deben contener necesariamente la siguiente información:

- **Datos del Solicitante:**

Nombres y Apellidos:	
Rut:	
Email:	
Teléfonos:	
Ubicación Física:	

- **Responsable del Servicio que avala la Solicitud:**

Nombre y Apellido:	
Email:	
Teléfono:	

- **Acceso Solicitado**

Cliente Software	_____	**Cliente Hardware**	_____	**LAN to LAN**	_____	
Justificación del Acceso:						

- **Frecuencia, Temporalidad y Tipo de Soporte:**

¿Acceso ligado a un contrato de soporte?	**Sí** _____	**No** _____
Tipo de Soporte:		
Vigencia del Contrato:		
Franja Horario de los Accesos		
Número Máximo de Conexiones Simultaneas:		

- **Servidores y Servicios para los que solicita Acceso (clientes software y hardware):**

Servidor	**Dirección IP**	**Protocolo de Encapsulado**	**Puertos**

Descripción del Servidor o subred a la que desea acceder

Ubicación de los Servidores (CPD, oficina Externa…)

- **Servidores y Servicios para los que Solicita Acceso (LAN to LAN)**

Sentido: Gobierno Regional de Los Ríos → exterior

Protocolo	Puerto	Protocolo	Puerto

Sentido: Exterior → Gobierno Regional de Los Ríos

Protocolo	Puerto	Protocolo	Puerto

Acuerdo de Confidencialidad

ACUERDO DE CONFIDENCIALIDAD

15 de mayo de 2017

a) Me comprometo a guardar estricta confidencialidad de la información del Gobierno Regional de Los Ríos a la cual tuve acceso con motivo del correcto desarrollo de mis funciones.

b) Guardaré secreto profesional sobre toda la información, documentos y asuntos a los que tuve acceso, estando obligado a no hacer público o transmitir cuantos datos conozca, incluso después de finalizar el plazo o la duración del acceso.

c) La información necesaria para el acceso (identificador de usuario, contraseñas, parámetros de configuración, direcciones IP internas, etc.) no podrá ser divulgada bajo ningún concepto a terceras personas, ajenas o no al Gobierno Regional de Los Ríos, así como tampoco podrá ser utilizada con posterioridad a la finalización de la autorización de acceso, o aun teniendo autorización, en equipamiento diferente al designado.

d) En caso de finalización de mi relación laboral con el Gobierno Regional de Los Ríos, me comprometo a realizar la devolución íntegra de toda la información a la cual tenga acceso con motivo del correcto desarrollo de mis funciones, así como también la devolución de todos los bienes que tuviese bajo mi responsabilidad.

e) El presente acuerdo tendrá vigencia durante y después del transcurso de la vigencia del convenio contractual.

Mediante el presente acepto las condiciones mencionadas en el listado anterior.

_____

Nombre, Firma y Timbre de Encargado de Seguridad de la Información Gobierno Regional de Los Ríos

_____

Nombre y Firma de Funcionario(a)

12. Registros de Control

Para asegurar la correcta implementación del Procedimiento de Control de Red a través del tiempo, se definen los siguientes controles, periodicidad y responsables. Estos son:

CONTROL	MEDIO DE VERIFICACIÓN	PERIODICIDAD	RESPONSABLE
Inspeccionar la correcta Implementación del Procedimiento de Control y Gestión de Red	▪ Informe de Monitoreo de Red Corporativa Edificio. ▪ Solicitud de Acceso Remoto por parte de Terceros ▪ Acuerdo de confidencialidad por parte de Terceros	Anual	Encargado(a) Seguridad de la Información

13. Mecanismos de Difusión

El Procedimiento de Control de Red será difundido de manera constante, a través de las plataformas tecnológicas de uso frecuente por los funcionarios(as) de la Institución, estas son:

CANAL DE COMUNICACIÓN	OBJETIVO	PERIODICIDAD	MEDIO DE VERIFICACIÓN
Intranet del Servicio	Notificar al personal del Servicio a través del correo electrónico institucional sobre la disponibilidad del Procedimiento de Control de Red, periódicamente y toda vez que esta se actualice y que el documento para consulta se encontrará en la intranet.	Anual	Print de pantalla de Intranet del Gobierno Regional de Los Ríos

Además, se realizarán actividades de difusión y sensibilización donde se dará a conocer el Procedimiento de Control y Gestión de Red. El detalle de estas actividades es:

CANAL DE COMUNICACIÓN	OBJETIVO	PERIODICIDAD	MEDIO DE VERIFICACIÓN
Jornada de Difusión/sensibilización (Presencial)	Que funcionarios y funcionarias de la Institución conozcan e internalicen el Procedimiento de Control.	Anual	Registro de participación de funcionarios y Funcionarias Gobierno Regional de Los Ríos.
Campaña Online "Mejoremos Nuestras prácticas en Seguridad de los Activos de la Información"	Entregar recomendaciones en detalles con técnicas de autocuidado en relación a los controles implementados sobre la Seguridad de los Activos de la Información del Gobierno Regional de Los Ríos.	Anual	Correo Electrónico difundiendo Campaña "Mejoremos Nuestras prácticas en Seguridad de los Activos de la Información"; Pantallazos Pagina Web de la Campaña.

Valdivia, octubre del 2019.

PROCEDIMIENTO DE GESTIÓN Y CONTROL DE REDES

Nch 27001/2013 Control	A.13.01.01	CONTROLES DE RED
Nch 27001/2013 Control	A.13.01.02	SEGURIDAD DE LOS SERVICIOS DE RED
Nch 27001/2013 Control	A.13.01.03	SEPARACIÓN EN LAS REDES
Nch 27001/2013 Control	A.13.02.04	ACUERDOS DE CONFIDENCIALIDAD O NO DIVULGACIÓN
Nch 27001/2013 Control	A.14.01.02	ASEGURAMIENTO DE SERVICIOS DE APLICACIÓN EN REDES PÚBLICAS

CONTROL DE CAMBIOS:

Versión	Fecha	Responsable	Acción
1.0	Diciembre de 2018	ACUM SALINAS LUIS PATRICIO	Elaborado
1.1	Octubre-2019	SANDRA PÉREZ GUZMÁN	Actualizado

Validado:

Comité Seguridad de La Información

Funcionario	Integrante Comité	Firma
Luis Patricio Acum Salinas	Encargado de Unidad de Informática	
Paola Hermosilla Bucarey	Encargado de Departamento Jurídico	
Cesar Pérez Sepúlveda	Encargado de Dep. de Finanzas	
Wilson Monzón Riquelme	Jefe Div. de Presupuesto e Inversión Regional	
Heidi Machmar Hernández	Jefe Div. Planificación y Desarrollo Regional	
Carlos Ovando Hernández	Jefe Div. de Administración y Finanzas	
Eduardo Fagalde Ampuero	Jefe Div. de Desarrollo Social y Humano	
Ernesto Espinoza Navarrete	Jefe Div. de Fomento Productivo e Industria	
Alejandro Paredes Zieballe	Administrador Regional	
Rodrigo Aravena Bustamante	Coordinador de PMG de la Institución.	

GOBIERNO REGIONAL ★ INTENDENTE ★ REGIÓN DE LOS RÍOS

CESAR ASENJO JERÉZ
INTENDENTE
GOBIERNO REGIONAL DE LOS RÍOS

Contenido

1. DECLARACIÓN INSTITUCIONAL

El **Gobierno Regional de Los Ríos**, expresa por medio del presente documento su convicción y compromiso de resguardar los activos de información con los que cuenta la institución, conociendo la importancia de dichos activos en el cumplimiento de la relevante misión que desempeña. Es por ello que se crea el **PROCEDIMINETO DE GESTIÓN Y CONTROL DE REDES DEL GOBIERNO REGIONAL DE LOS RÍOS** basado en Sistemas de Gestión de Seguridad de la Información, el que debe garantizar el correcto funcionamiento del servicio, el cumplimiento de metas y la prevención de riesgos y/o amenazas referidas a los Activos de Información al momento del uso de los servicios, la tecnología e infraestructura de red de acuerdo a las necesidades del servicio.

2. ALCANCE O ÁMBITO DE APLICACIÓN DEL PROCEDIMIENTO

El presente Procedimiento de Gestión y Control de Redes es de uso interno y aplicable a todos los funcionarios del Gobierno Regional de Los Ríos y a quienes prestan servicios externos tanto de desarrollo como de soporte de sistemas, especialmente aquellos funcionarios que ejercen sus labores en el área de Tecnologías de la Información de la Institución.

3. OBJETIVO GENERAL

Preservar la disponibilidad de los servicios soportados por la Infraestructura tecnológica institucional.

Establecer los métodos, pasos y medidas a utilizar para la conexión remota a la infraestructura (redes, servidores, etc.) desde fuera de la red de comunicaciones, así como el intercambio de información entre las ubicaciones externas a las oficinas principales.

Salvaguardar la información en tránsito a través de las redes y equipos institucionales, los sistemas soportados y la infraestructura de red.

4. ROLES Y RESPONSABILIDADES

Responsable	Rol	Funciones
Jefe de Servicio	Liderar la implementación del presente	✓ Aprobar el documento. ✓ Autorizar los recursos necesarios para

	procedimiento.	su implementación, así como el nombramiento de funcionarios coordinadores y/o encargados de su 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 Unidad de Informática	Analizar, coordinar y supervisar las solicitudes de conexión.	✓ Recibir y coordinar las conexionas remotas a la red. ✓ Analizar la factibilidad de las solicitudes de conexión remota. ✓ Proponer mejoras y/o cambios en la implementación.
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 del Gobierno Regional de Los Ríos	Dar cumplimiento a lo establecido en el procedimiento.	✓ Dar cumplimiento a lo establecido el procedimiento. ✓ Informarse, asistir a charlas o reuniones relacionadas con la difusión del contenido del documento.

5. DEFINICIONES

Datos: Son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos. En su forma más amplia los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y bases de datos, texto (colección de palabras), hojas de cálculo (datos en forma matricial), imágenes (lista de vectores o cuadros de bits), video (secuencia de tramas), etc.

Privacidad: Es el derecho que tienen los individuos y organizaciones para determinar, ellos mismos, a quién, cuándo y qué información referente a ellos será difundidas o transmitida.

IP: Dirección de 32 bits definida por el Protocolo Internet en STD 5, RFC 791. Se representa usualmente mediante notación decimal separada por puntos.

Soporte: Objeto físico susceptible de ser tratado en un sistema informático y sobre el cual se pueden grabar o recuperar datos.

Usuario: Sujeto o proceso autorizado para acceder a datos u otros recursos.

Activos de información: Corresponde a elementos tales como bases de datos, documentación, manuales de usuarios, planes de continuidad, etc.

Autorización: Proceso por el que se acredita a un individuo para realizar una acción determinada, como el acceso a los recursos una vez que el usuario ha sido autenticado con éxito.

Control de Acceso: Mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

6. CONTROLES DE RED CORPORATIVA

El edificio principal del Gobierno Regional de Los Ríos, actualmente se encuentra conectado a una Red Independiente.

Las medidas de seguridad establecidas en el presente procedimiento están orientadas a proteger el acceso remoto no autorizado a los sistemas como trampolín para realizar ataques a otros sistemas y como protección adicional a los datos y servicios que en ellos residen, independientemente de que estos últimos dispongan de mecanismos específicos de protección.

Los equipos de redes son administrados por el Profesional de la Unidad de Informática del Gobierno Regional de Los Ríos, quien los administra bajo las normativas y procedimientos establecidos en; el Procedimiento de Inventario de Activos; el Procedimiento de Protección de Equipos y Procedimiento de Mantención de Equipos. Sin perjuicio de que el Profesional de la Unidad de Informática es responsable de los equipos bajo su control, los funcionarios y funcionarias son responsables del cuidado y protección de equipos portátiles u otros equipos Institucionales que por el adecuado desarrollo de sus funciones se les ha proporcionado.

6.1. Tipos de Redes

En el Gobierno Regional de Los Ríos se contemplan los siguientes tipos de accesos a través de redes:

- ✓ Acceso Correo: acceso remoto al correo electrónico corporativo desde el exterior, de forma restringida a los empleados del organismo. Este tipo de acceso se realizará cifrando la información que circula por la red mediante mecanismos de autenticación que garantizan los mismos controles de acceso con los que se cuenta en la red interna de las instalaciones del Gobierno Regional de Los Ríos.

- ✓ Acceso a la administración de los sistemas de información desde los puestos del departamento de informática, o remotamente a través de VPN.

Para el acceso a los sistemas de información se establecerán los mecanismos de seguridad suficientes que permitan garantizar que sólo el personal autorizado pueda acceder a los mismos. Los mecanismos que se implanten permitirán la identificación inequívoca de cada usuario que puede acceder al sistema.

Mecanismos de Seguridad

- ✓ Restringir el acceso a los sistemas desde las ubicaciones de los usuarios autorizados (a través de IPs concretas), de forma que no existe la posibilidad de identificarse desde una ubicación distinta.
- ✓ Impedir que la Información usada en la identificación, así como en las operaciones de administración pueda ser capturada por terceros (https, VPNSSL, etc.).
- ✓ Regularizar los accesos remotos mediante autorizaciones expresas.

6.2. Equipos Accesibles

Para las funciones de administración de sistemas se definirán grupos de personas diferentes, a los cuales se les asignará rangos de direcciones de red diferenciados, con objeto de facilitar las medidas de control.

6.3. Acceso Remoto para Administración de Sistemas

La administración de sistemas se podrá realizar, en general, de forma local (desde la consola del sistema) o remota. La entrada directa en la cuenta *root / administrador* de los sistemas solo se podrá efectuar localmente, desde la consola del sistema. Para el acceso remoto será preciso entrar en una cuenta puente y desde allí entrar en *root / administrador*.

La administración remota estará protegida por las medidas que se detallan a continuación, siendo aplicable a cualquier forma de administración remota, desde una red o subred distinta a la red donde se encuentran los servidores del Gobierno Regional de Los Ríos.

Cualquier intento de acceso que no cumpla todas las condiciones no será factible;

- ✓ Ninguna conexión de administración desde una red distinta a la local de servidores será posible sin pasar por una autenticación.

- ✓ La conexión remota debe ser cifrada y suficientemente autenticada. En todo caso no se permite el envío de contraseñas en claro por Red.

- ✓ No se establecen restricciones de horario para la conexión remota para la administración de sistemas.

6.4. Administración Basada en Navegador Web

Para los servicios administrados desde un navegador web, se utilizará una conexión cifrada mediante SSL con cifrado mínimo de 128 bits. El servidor Web de administración debe configurarse para restringir las direcciones IP que se puedan conectar al servicio. El acceso al servidor de administración debe configurarse para que exija contraseña.

6.5. Flujos de Administración

Todos los flujos de administración entrarán exclusivamente a través de los cortafuegos corporativos.

6.6. Acceso Remoto a la Red Corporativa por Parte de Funcionarios(as)

Se considera aquí el acceso a los funcionarios y funcionarias del Gobierno Regional de Los Ríos a los servicios de Red utilizando como acceso Internet.

El acceso de un usuario desde fuera de las instalaciones del Gobierno Regional de Los Ríos debe estar especialmente protegido para impedir que se ponga en riesgo los contenidos sensibles que pueda haber en la Red interna o corporativa.

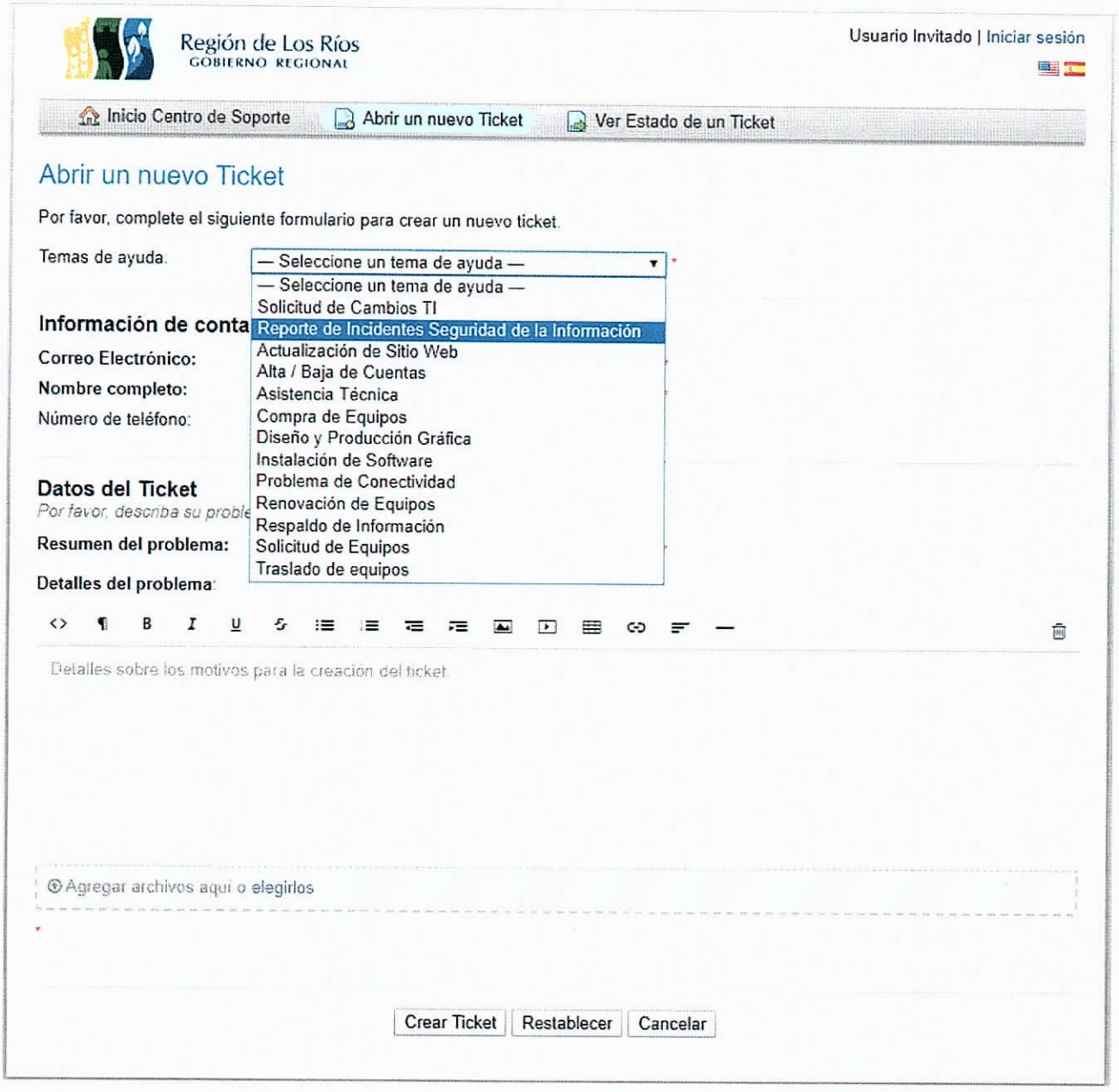
Los servicios a los que un funcionario(a) remotamente puede acceder son los siguientes:

- ✓ Servicio de Correo electrónico
- ✓ Intranet Institucional

6.7. Acceso al Correo Electrónico Web

El ,acceso se realiza contra el servidor Web de Correo Electrónico, mediante el protocolo HTTP seguro (HTTPS), estableciéndose así una conexión segura de acceso al mismo.

En el caso de que un funcionario(a) alerte o tenga constancia de que su correo podría haber sido vulnerado, así como su certificado de acceso, notificará inmediatamente de la incidencia mediante el Procedimiento de Gestión de Incidentes a través de la opción "Reporte de Incidentes Seguridad de la Información" en la plataforma OsTicket, tal como se demuestra a continuación.



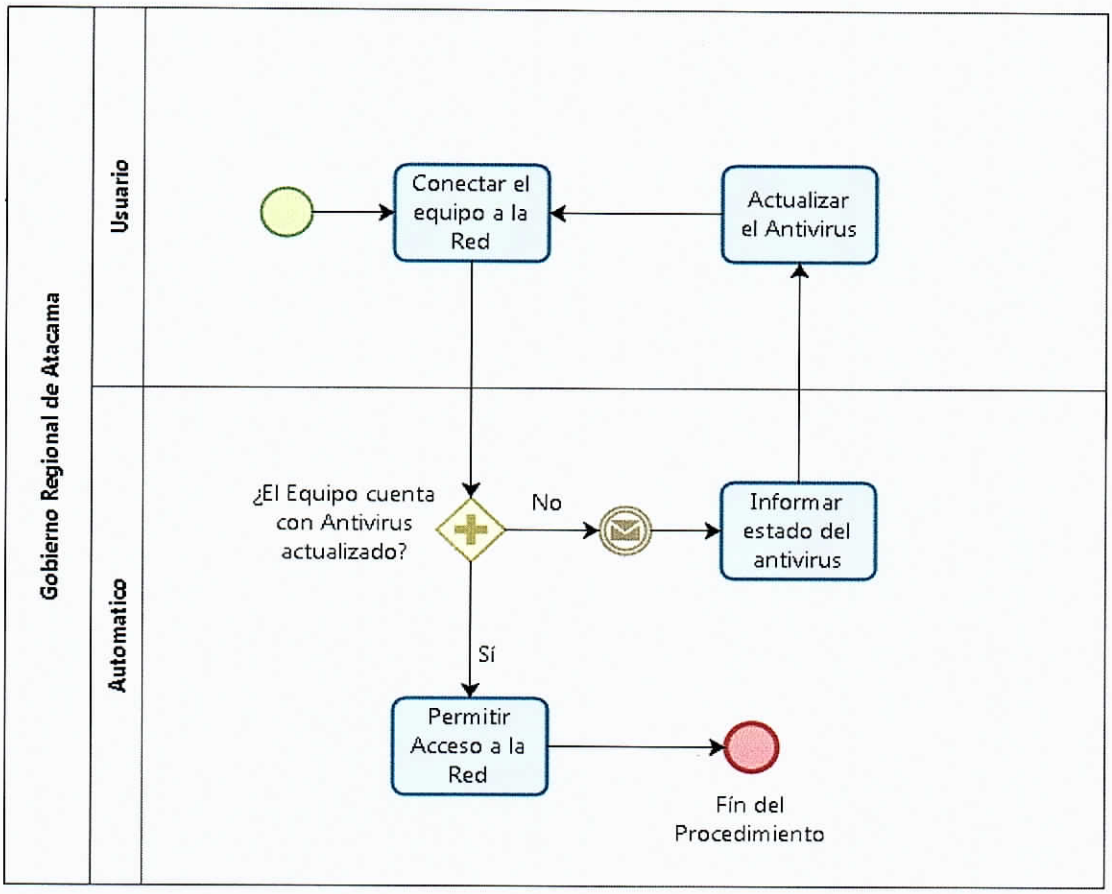
6.8. Registro

Todas las conexiones remotas a la Red y Sistema del Gobierno Regional de Los Ríos serán registradas. Se configurarán los servidores a los que se conectan los usuarios para guardar, adicionalmente la siguiente información específica, tanto de conexiones fallidas como exitosas:

- ✓ Dirección de IP de origen de conexión
- ✓ Dirección de IP de destino de conexión
- ✓ Hora de conexión
- ✓ Hora de desconexión
- ✓ Duración de la conexión
- ✓ Usuario con el que ha sido validada la conexión

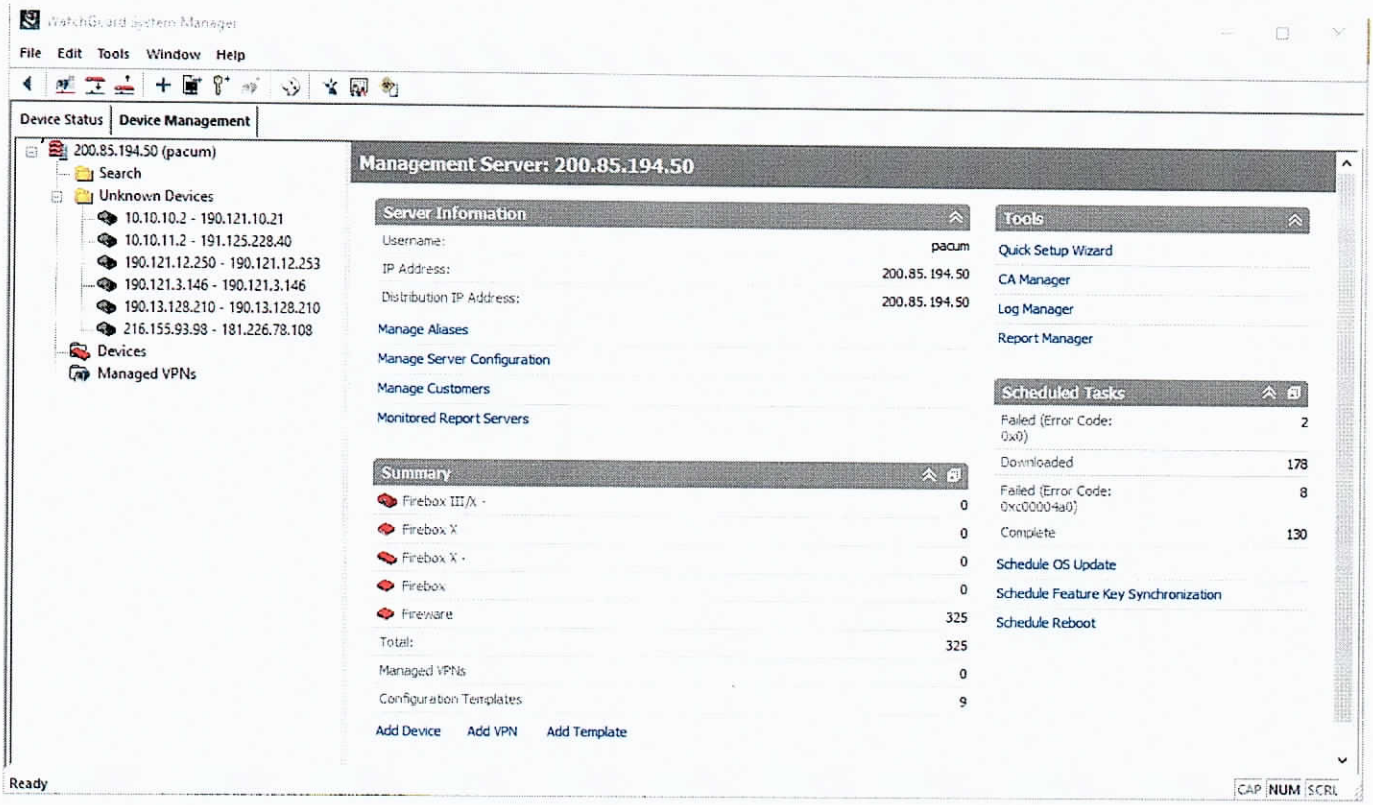
6.9. Requerimientos de Seguridad para el Equipo Remoto de Usuario

Los equipos conectados remotamente deberán cumplir, en general, los mismos requerimientos de seguridad que cualquier otro equipo que se conecte directamente (en las propias instalaciones) a la red de comunicaciones interna de la organización y en particular deberá tener implementadas las medidas de seguridad indicadas en la normativa de uso de computadores portátiles.



7. Seguridad en los servicios de redes.

La seguridad para los servicios de red del Gobierno Regional, son provistos por un proveedor externo mediante un firewall "WatchGuard", el que impide y bloquea los intentos de acceso a la red tanto internos como externos, todo ello de acuerdo a la configuración de seguridad recomendada y solicitada de parte del funcionario a cargo de la unidad de informática de la institución, además, internamente se impide todo acceso mediante restricción de usuarios administrados de forma centralizada a través de ActiveDirectory.



8. Segregación de la red Gore.

La red del Gobierno Regional, se encuentra segregada a nivel físico y lógico tal que cumple con las normas de seguridad de red establecidas por las normas que nuestro país ha suscrito en esta materia, **la topología y sus características no deben ser modificadas en forma arbitraria o intervenida por personas internas o externas sin el conocimiento técnico necesario para ello, en los casos en que estan modificaciones correspondan a mejoras, reparaciones o cambios a nuevas tecnologías, deben realizarse bajo la supervisión del encargado de la unidad de informática o en su defecto de quien sea designado para ello manteniendo el criterio de cumplimiento de las normas técnicas y de seguridad recomendadas y vigentes**.

los tipos de segregación y sus características son las siguientes:

8.1. Segregación Física

La segregación física se define por los Rack de Comunicaciones ubicados en cada piso del edificio, que a su vez se comunican con la central de la sala de servidores, esta topología de red es de carácter lineal (topología de Bus), con ello se separan en tres sub-redes que proveen del servicio de internet a cada piso del edificio.

Debido a lo anterior, en caso de fallos es posible monitorear, revisar y aislar el switch que presente problemas o sea objeto de algún ataque tanto interno como externo, evitando así la contaminación de la red completa.

8.2. Segregación Lógica

La segregación lógica permite, a través de configuraciones del switch el paso o habilitación de enlaces dedicados o especiales para la conexión de otros dispositivos, con ello se separa los puertos o bocas que proveen a los equipos computacionales del servicio de internet de otros equipos que requieren de IPs externas u otros pools IPs internos distintos de los que proveen servicio a los equipos gore.

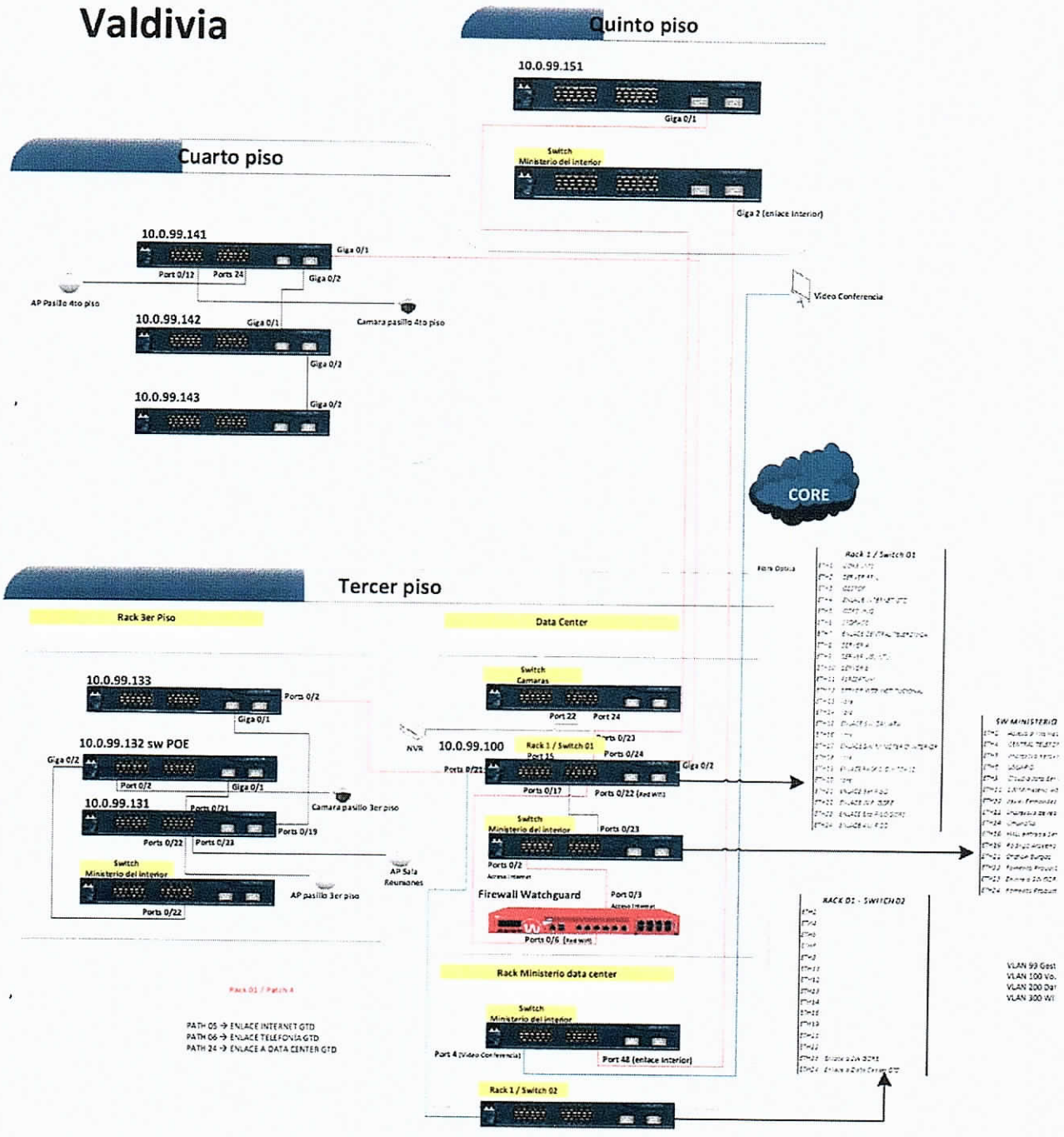
Los siguientes servicios se encuentran separados lógicamente a través de configuraciones de switch:

VLAN 99 gestor
VLAN 100 vos
VLAN 200 datos
VLAN 300 WIFI

Igualmente, todos aquellos servicios diferentes de los estrictamente necesarios para proveer internet a través de cableado y aplicaciones o programas, deben estar separados de forma lógica para evitar que distintos servicios transiten por la misma vía.

La siguiente imagen demuestra la topología de red y sus características:

Red Gore Valdivia



9. Acuerdos de Confidencialidad y/o no Divulgación

Con la finalidad de evitar mal uso, pérdida o modificación de información de carácter sensible a la cual se tenga acceso por parte de funcionarios, además de las restricciones físicas y lógicas de acceso, se debe incorporar a las actas de entrega, un texto referido a la obligación de mantener absoluta confidencialidad respecto a la información que se tenga acceso y que, debido a sus características, no deba ser divulgada. En el caso de terceros, se debe evitar proporcionar accesos a información sin la debida supervisión de un funcionario perteneciente al área de informática de la institución.

Para dar cumplimiento a lo anterior, se solicitará la firma de un documento de compromiso que se detalla en los anexos del presente documento "**Acuerdo de Confidencialidad**".

10. Aseguramiento de Servicios de Aplicación en Redes Públicas

El Gobierno Regional de Los Ríos es una institución que en su naturaleza no mantiene servicios de aplicación disponibles en redes públicas de forma permanente, sin embargo, en ocasiones se debe poner a disposición del público exterior formularios de postulación a los distintos recursos concursables, lo cual esta a cargo de proveedor externo en el caso del sistema de subvenciones, FIC y FRIL.

Laś postulaciones a través de dichos sistemas se realizan de tal forma que sea bajo las normas de seguridad establecidas:

- ✓ Protección de la confidencialidad y la integridad de la información.
- ✓ Otorgar confianza sobre la identidad de los postulantes a través de script de verificación de datos.

11. Anexos

Anexo "A" – Solicitud de Acceso Remoto por parte de Terceros

Las solicitudes de Acceso Remoto por parte de terceros deben contener necesariamente la siguiente información:

- **Datos del Solicitante:**

Nombres y Apellidos:	
Rut:	
Email:	
Teléfonos:	
Ubicación Física:	

- **Responsable del Servicio que avala la Solicitud:**

Nombre y Apellido:	
Email:	
Teléfono:	

- **Acceso Solicitado**

Cliente Software	_____	**Cliente Hardware**	_____	**LAN to LAN**	_____	
Justificación del Acceso:						

- **Frecuencia, Temporalidad y Tipo de Soporte:**

¿Acceso ligado a un contrato de soporte?	**Sí** _____	**No** _____
Tipo de Soporte:		
Vigencia del Contrato:		
Franja Horario de los Accesos		
Número Máximo de Conexiones Simultaneas:		

- **Servidores y Servicios para los que solicita Acceso (clientes software y hardware):**

Servidor	Dirección IP	Protocolo de Encapsulado	Puertos

Descripción del Servidor o subred a la que desea acceder

Ubicación de los Servidores (CPD, oficina Externa…)

- **Servidores y Servicios para los que Solicita Acceso (LAN to LAN)**

Sentido: Gobierno Regional de Los Ríos → exterior

Protocolo	Puerto	Protocolo	Puerto

Sentido: Exterior → Gobierno Regional de Los Ríos

Protocolo	Puerto	Protocolo	Puerto

Acuerdo de Confidencialidad

ACUERDO DE CONFIDENCIALIDAD

15 de mayo de 2017

a) Me comprometo a guardar estricta confidencialidad de la información del Gobierno Regional de Los Ríos a la cual tuve acceso con motivo del correcto desarrollo de mis funciones.

b) Guardaré secreto profesional sobre toda la información, documentos y asuntos a los que tuve acceso, estando obligado a no hacer público o transmitir cuantos datos conozca, incluso después de finalizar el plazo o la duración del acceso.

c) La información necesaria para el acceso (identificador de usuario, contraseñas, parámetros de configuración, direcciones IP internas, etc.) no podrá ser divulgada bajo ningún concepto a terceras personas, ajenas o no al Gobierno Regional de Los Ríos, así como tampoco podrá ser utilizada con posterioridad a la finalización de la autorización de acceso, o aun teniendo autorización, en equipamiento diferente al designado.

d) En caso de finalización de mi relación laboral con el Gobierno Regional de Los Ríos, me comprometo a realizar la devolución íntegra de toda la información a la cual tenga acceso con motivo del correcto desarrollo de mis funciones, así como también la devolución de todos los bienes que tuviese bajo mi responsabilidad.

e) El presente acuerdo tendrá vigencia durante y después del transcurso de la vigencia del convenio contractual.

Mediante el presente acepto las condiciones mencionadas en el listado anterior.

_____

Nombre, Firma y Timbre de Encargado de Seguridad de la Información Gobierno Regional de Los Ríos

_____

Nombre y Firma de Funcionario(a)

12. Registros de Control

Para asegurar la correcta implementación del Procedimiento de Control de Red a través del tiempo, se definen los siguientes controles, periodicidad y responsables. Estos son:

CONTROL	MEDIO DE VERIFICACIÓN	PERIODICIDAD	RESPONSABLE
Inspeccionar la correcta Implementación del Procedimiento de Control y Gestión de Red	▪ Informe de Monitoreo de Red Corporativa Edificio. ▪ Solicitud de Acceso Remoto por parte de Terceros ▪ Acuerdo de confidencialidad por parte de Terceros	Anual	Encargado(a) Seguridad de la Información

13. Mecanismos de Difusión

El Procedimiento de Control de Red será difundido de manera constante, a través de las plataformas tecnológicas de uso frecuente por los funcionarios(as) de la Institución, estas son:

CANAL DE COMUNICACIÓN	OBJETIVO	PERIODICIDAD	MEDIO DE VERIFICACIÓN
Intranet del Servicio	Notificar al personal del Servicio a través del correo electrónico institucional sobre la disponibilidad del Procedimiento de Control de Red, periódicamente y toda vez que esta se actualice y que el documento para consulta se encontrará en la intranet.	Anual	Print de pantalla de Intranet del Gobierno Regional de Los Ríos

Además, se realizarán actividades de difusión y sensibilización donde se dará a conocer el Procedimiento de Control y Gestión de Red. El detalle de estas actividades es:

CANAL DE COMUNICACIÓN	OBJETIVO	PERIODICIDAD	MEDIO DE VERIFICACIÓN
Jornada de Difusión/sensibilización (Presencial)	Que funcionarios y funcionarias de la Institución conozcan e internalicen el Procedimiento de Control.	Anual	Registro de participación de funcionarios y Funcionarias Gobierno Regional de Los Ríos.
Campaña Online "Mejoremos Nuestras prácticas en Seguridad de los Activos de la Información"	Entregar recomendaciones en detalles con técnicas de autocuidado en relación a los controles implementados sobre la Seguridad de los Activos de la Información del Gobierno Regional de Los Ríos.	Anual	Correo Electrónico difundiendo Campaña "Mejoremos Nuestras prácticas en Seguridad de los Activos de la Información"; Pantallazos Pagina Web de la Campaña.

Valdivia, octubre del 2019.