Procedimiento de

Gestión de Vulnerabilidades Técnicas

Unidad de Informática Gobierno Regional de los Ríos.

Nch 27001/2013 Control A.12.06.01

CONTROL DE CAMBIOS:

Versión	Fecha	Responsable	Acción
1.0	Agosto 2016	ACUM SALINAS LUIS PATRICIO	Elaborado
1.1	Septiembre-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 Departamento. 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 JEREZ
INTENDENTE
GOBIERNO REGIONAL DE LOS RÍOS

Tabla de contenido

1. OBJETIVO

El objetivo principal del presente procedimiento es diseñar e implementar una metodología de gestión y detección de vulnerabilidades técnicas que pudieran afectar a los sistemas, aplicaciones, software o equipos de comunicación en los que se procesa y almacena información principalmente sensible para la institución y para la continuidad de los procesos.

2. AMBITO DE APLICACIÓN

El presente procedimiento es de uso interno, especialmente aplicable a quienes ejercen sus labores en la unidad de informática del Gobierno Regional de Los Ríos y administran sistemas operacionales utilizados por la institución, estén estos implementados en servidores propios o de contratación externa.

3. MARCO REFERENCIAL

- ✓ NCh ISO 27002 /2013
- ✓ Guía Metodológica 2015 (SGSI)
- ✓ Política de Seguridad de la Información
- ✓ Manual de Procedimientos del Usuario

4. ROLES Y RESPONSABILIDADES

Responsable	Rol	Funciones
Jefe de Servicio	Liderar la implementación del presente Procedimiento de.	✓ Aprobar el documento. ✓ Autorizar los recursos necesarios para su implementación.
Comité de Seguridad de la Información	Aprobar y coordinar la implementación del procedimiento.	✓ Aprobar el procedimiento. ✓ Coordinar su correcta implementación y seguimiento. ✓ responsable de velar por el cumplimiento de este procedimiento al interior de la organización cuando corresponda.
Unidad de auditoría interna	Fiscalizar	✓ Responsable de fiscalizar el cumplimiento de este procedimiento al interior de la organización cuando corresponda.
Encargado de Seguridad de la Información	Gestionar e informar al comité acerca de la	✓ Encargado de la distribución de este documento y de asegurar su incorporación a la base documentaria del Servicio.

	implementación del procedimiento.	
Jefe División de Administración y Finanzas	Apoyar en la implementación del procedimiento.	✓ Proveer de condiciones, elementos, materiales y medidas de seguridad para que se pueda desarrollar correctamente la actividad.
Encargado Unidad de Informática	Liderar la implementación del procedimiento desde el área técnica.	✓ Coordinar que se ejecute correcta y periódicamente este procedimiento. ✓ Evaluar el conocimiento adquirido respecto al trabajo y designar al personal idóneo para la ejecución del mismo.

5. DEFINICIÓN DEL PROCEDIMIENTO

Los pasos a seguir para lograr una mejor gestión de vulnerabilidades técnicas consisten en lo siguiente:

5.1. MEDIDAS PREVENTIVAS

Será de responsabilidad de o los funcionarios del área informática adoptar las siguientes medidas preventivas:

1. Mantener registro actualizado de los equipos informáticos con los que cuenta la institución, lo anterior se debe realizar mediante un sistema de inventario o planilla Excel.
2. Mantener registro actualizado de los servidores y equipamiento de red.
3. Mantener registro actualizado de los programas, sistemas, aplicaciones y software instalados y funcionando en los distintos dispositivos informáticos, resguardando que se encuentren bajo condiciones de licenciamiento adecuado tal como lo indica la norma.
4. Restringir el acceso a terceros no autorizados a equipos y software sensibles, tal como se señala en el Procedimiento de Administración de Usuarios y Equipos Conectados a la Red del Gobierno Regional de Los Ríos, actualizado en septiembre de 2019.
5. Mantener de forma interna o por medio de proveedor externo un sistema de firewall o bloqueo de intentos de accesos a la red, que tenga la capacidad de monitorear e informar acerca de los intentos de conexión no autorizados.
6. Revisar, probar e instalar de forma periódica los parches o actualizaciones de seguridad y críticos que estén disponibles para reforzar la seguridad y estabilidad de los sistemas informáticos.
7. Mantener respaldo actualizado de los sistemas principalmente críticos y sensibles.

5.2. MEDIDAS CORRECTIVAS

Será de responsabilidad de o los funcionarios del área informática adoptar las siguientes medidas correctivas:

1. En caso de detectar vulnerabilidades técnicas desactivar todos los servicios de red.
2. Identificar el origen exacto de la vulnerabilidad.
3. Desconexión inmediata de la red del o los equipos en condición de vulnerabilidad.
4. Escáner en profundidad del comportamiento de la red para detectar o descartar ataques reales.
5. Resolver o minimizar al máximo las causas que originan la situación de vulnerabilidad.
6. Generar informe de las vulnerabilidades detectadas y las medidas correctivas realizadas.

7. Informar al comité de seguridad acerca de las detecciones de situación de vulnerabilidad, en el momento de ser detectadas y las medidas asociadas al evento.
8. Informar al comité de seguridad de todas las situaciones anómalas detectadas o informadas que pudieran afectar a los sistemas, red o equipos conectados.

6. REGISTROS DE OPERACIÓN

El presente documento ha sido revisado y aprobado por el comité de seguridad de la información del Gobierno Regional de Los Ríos, en concordancia con lo dispuesto en el sistema de gestión de seguridad de la información, por lo cual deberá ser revisado, al menos, una vez cada un año de acuerdo al grado de cumplimiento.

Los medios de verificación del cumplimiento del mismo serán los descritos en los puntos 5.1. MEDIDAS PREVENTIVAS Y 5.2. MEDIDAS CORRECTIVAS