Procedimiento de control de las vulnerabilidades técnicas

1 INDICE

2 OBJETIVO

Establecer el procedimiento necesario para realizar el seguimiento, control y atención de vulnerabilidades técnicas sobre los sistemas de información y equipos informáticos conectados a la red de datos del Gobierno Regional Metropolitano, con el propósito de mantener un nivel de aseguramiento adecuado de la plataforma y mitigar los riesgos asociados.

3 ALCANCE

Este procedimiento aplica a todos los equipamientos tecnológicos que pueden verse afectados a las vulnerabilidades técnicas en los sistemas de información y equipos en la red de datos del Gobierno Regional Metropolitano bajo administración propia o de terceros.

4 PREREQUISITO

Es importante tener un Inventario de Activos actualizados y completo. **Ver "Política de Clasificación de Activos"**

5 ROLES Y RESPONSABILIDADES

El Departamento de Informática será el encargado de evaluar y desarrollar el Procedimiento de control de las vulnerabilidades técnicas.

Jefe del Departamento de Informática: Será responsable de velar por la seguridad en el procedimiento siempre teniendo en cuenta las Políticas, Normas u otros documentos aprobados por el Servicio en materia de Seguridad de la Información.

Encargado de Seguridad: Rol asignado al encargado de realizar las actividades de Seguridad de la Información, este Rol es asignado por el jefe de Servicio mediante resolución.

Funcionario asignado por el Jefe del Departamento de Informática: Funcionario encargado del proceso completo en la detección y manejo de vulnerabilidades.

6 CONTROL NORMATIVO SSI

El siguiente procedimiento tiene por finalidad dar cumplimiento a los siguientes procedimientos de acuerdo a NCh-ISO27001.Of2013

Código del Control	Identificación del Control	Requisito de control
A.12.06.01	Gestión de las vulnerabilidades técnicas	Se debiera obtener oportunamente la información sobre las vulnerabilidades técnicas de los sistemas de información que se están utilizando, evaluar la exposición de la organización a estas vulnerabilidades, y se deben tomar las medidas apropiadas para abordar el riesgo asociado.

7 DEFINICIONES Y MODO DE OPERACION.

No	Actividad	Responsable	Registro
Inicio			
1	1.1 Solicitud de análisis de vulnerabilidades (se puede solicitar por correo llamada a la mesa de ayuda)	Funcionario asignado por el Jefe del Departamento de Informática o el Encargado de Seguridad de la Información	Herramienta de Gestión de Mesa de ayuda redmine.
2	2.1 Identificar los elementos a los cuales se les va a llevar a cabo el procedimiento de gestión de vulnerabilidades, a partir del inventario.	Funcionario asignado por el Jefe del Departamento de Informática o el Encargado de Seguridad de la Información	Informe de Vulnerabilidades
3	3.1 Configurar el alcance del análisis de vulnerabilidades en la herramienta correspondiente. 3.2.Ejecución de análisis de vulnerabilidades 3.3. Recolección de información del análisis de vulnerabilidades	Funcionario asignado por el Jefe del Departamento de Informática	Informe de Vulnerabilidades
4	4.1 Generar reporte de las vulnerabilidades existentes para cada elemento que sea parte del alcance, a	Funcionario asignado por el Jefe del Departamento de Informática	Informe de Vulnerabilidades

	través de la herramienta de rastreo de vulnerabilidades.		
	4.2 Generar Reporte de los nuevos elementos detectados por el análisis de vulnerabilidades y que no hacen parte del inventario disponible en la herramienta de gestión de activos de tecnología.	Funcionario asignado por el Jefe del Departamento de Informática	Reporte elementos detectados
5	5.1 Identificar y seleccionar las medidas de corrección que se deben aplicar para corregir cada vulnerabilidad identificada. 5.2 Documentar las vulnerabilidades que no puedan ser resueltas, ya sea porque no existen medidas de corrección o porque la aplicación de las medidas puede causar un impacto inaceptable en la operación de la plataforma. 5.3 Priorizar la aplicación de las medidas de corrección de acuerdo con la criticidad del sistema y el impacto potencial de la vulnerabilidad.	Funcionario asignado por el Jefe del Departamento de Informática	Registro de pruebas y corrección de vulnerabilidades
No	Actividad	Responsable	Registro
6	6.1 Elabora y documenta el Control de Cambios por cada sistema involucrado.	Funcionario asignado por el Jefe del Departamento de Informática	Formato Requerimiento de Cambio
FIN			

Nota: El plan del numeral 4.1 debe contener el listado de vulnerabilidades a corregir, el impacto potencial de las vulnerabilidades, el listado de acciones de corrección, el impacto potencial de la acción de corrección, la fecha y tiempo propuesto de aplicación y el responsable de ejecución de las actividades.

8 CRITERIOS OPERATIVOS

El procedimiento de Vulnerabilidades técnicas debe ejecutarse por lo menos una vez al año.

Para la detección de vulnerabilidades tecnicas se deberá tener en consideración los controles relacionados que se indican en la Política de Desarrollo de Sistemas siguiendo los procedimientos de respuesta indicados en la **Politica de Gestión de Incidentes de Seguridad.**

Para garantizar el buen funcionamiento en el procedimiento dirijase al **Protocolo Control y Tratamiento de la Seguridad de la Informacion** como a la **Política de la Seguridad Informática.**

9 DURACIÓN DEL CICLO DEL PROCEDIMIENTO

El ciclo de todo el procedimiento debe durar un máximo de 15 días.

Estos días pueden ser variables dependiendo de la complejidad de la solución que exista para la vulnerabilidad.

10 DEFINICIONES

Amenaza: Capacidades o métodos de ataque desarrollados para aprovechar una vulnerabilidad y potencialmente causar algún tipo de daño.

Cambio: Adición, modificación o eliminación de algo que podría afectar a los Servicios de TI. El Alcance debería incluir todos los Servicios de TI, Elementos de Configuración, Procesos, Documentación entre otros.

Gestión de Cambios de Tecnologías de la Información: Procedimiento responsable del control del Ciclo de Vida de los Cambios. Su objetivo primario es permitir la ejecución de los Cambios a realizar, con la mínima afectación sobre los Servicios de TI.

Herramienta de Gestión de Servicios: Son todos los sistemas, aplicaciones, controles, soluciones de cálculo, metodología, etc., que ayudan a la gestión de una empresa; para el caso de TI para el manejo y control de servicios es el software en donde se documentan los servicios de gestión tecnológica como Incidentes, Requerimientos, Problemas, Controles de Cambios, etc, todas estas correspondientes a Tecnologías de Información; algunas de las Herramientas que se encuentran hoy en día en el mercado son:

• Altiris de Symantec • IBM Service Management de IBM • CA Service Desk Manager de CA Technologies • Service Manager de Hewlett Packard • Aranda's Service Desk de Aranda Software • ZABBIX • DNA Netsupport

Plataforma Informática: Conjunto de software, hardware e infraestructura de comunicaciones y seguridad que proveen los diferentes servicios de información para la ejecución de los servicios.

Corrección: acciones aplicadas para cerrar o eliminar una vulnerabilidad. Las medidas de corrección pueden ser instalación de un parche de software, ajustes a la configuración o eliminación del software afectado.

Vulnerabilidad: Defectos en el desarrollo de software o mala configuración de los sistemas que representan una debilidad de seguridad y que puede ser explotada por una potencial fuente de amenaza, para ocasionar algún tipo de daño en los sistemas

11 REGISTRO DE OPERACION

El Departamento de Informática deberá emitir un informe que dé cuenta de:

A.12.06.01 Informe de evaluación de Vulnerabilidades técnicas detectadas

El informe deberá ser enviado al Encargado de Seguridad de manera semestral.

En caso de no haber movimiento en relación a algún control que se pide informar, deberá reportarse de igual manera señalando que no hubo movimiento por lo que no se pudo demostrar con algún medio de verificación durante el respectivo periodo.

Todo documento deberá venir formalizado por quienes sean responsables del proceso (Debe contener logo del Servicio, fecha de creación, nombre, cargo y firma del responsable)

12 DIFUSIÓN

El presente documento será difundido a través de correo electrónico a todo el personal del Servicio, así como también una copia de éste será publicada en la intranet Institucional.

13 REVISIÓN

La siguiente Norma será revisada, evaluada y/o actualizada según corresponda una vez al año por el Comité de Seguridad de la Información o cuando el mismo estime conveniente, en cuanto a su funcionamiento y correcta aplicación en la Institución.

15 APROBACIÓN

Elaborado por	Revisado por	Aprobado por
Carlos Hernández A. Analista Departamento de Informática	**José Ignacio Gutiérrez G.** Encargado de Seguridad SSI **Paulo Mendoza R.** Encargado Unidad de Soporte **Carolina Hidalgo M.** Jefa Departamento Planificación y Control Institucional	**Alejandro Segura B.** Presidente Comité de Seguridad

16 REGISTRO DE HISTORIAL DE VERSIONES O MODIFICACIONES

Versión	Autor	Página o Secciones	Fecha Modificación	Motivo
01	Carlos Hernández	todas	11-08.16	Creación Documento
02	Carlos Hernández	todas	10-07-17	Modificación de documento para cumplimiento a directrices de la red de expertos SSI. • Se incorpora control normativo SSI • Se incorpora registro de control
03	Mauricio Marin V.	07	2-08-2018	Se agrega en Registro de Control el siguiente párrafo: En caso de no haber movimiento en relación a algún control que se pide informar, deberá reportarse de igual manera señalando que no hubo movimiento por lo que no se pudo demostrar con algún medio de verificación durante el respectivo periodo. Se cambia título 7 por Definiciones y modo de operación Se cambia título 11 por registro de Operación