DIVISIÓN DE ADMINISTRACIÓN Y FINANZAS
DEPARTAMENTO DE INFORMÁTICA

RESOLUCION EXENTA Nº 3002

SANTIAGO, 29 NOV 2016

VISTOS:

Las facultades que me confieren el Decreto Supremo Nº 674/2014 del Ministerio del Interior y Seguridad Pública; el artículo 24 letra o) de la Ley Nº 19.175; el DFL N° 29 de 2004 del Ministerio de Hacienda, que fija el texto refundido, coordinado y sistematizado de la Ley N° 18.834, Estatuto Administrativo; la Ley N° 18.575 Orgánica Constitucional de Bases Generales de la Administración del Estado; lo dispuesto en la Ley N° 19.799 sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha firma; el Decreto N° 181/2002 que aprueba el Reglamento de la Ley N° 19.799; el Decreto Supremo N° 83/2005 del Ministerio Secretaría General de la Presidencia sobre seguridad y confidencialidad de los documentos electrónicos; la Resolución N° 1.600 de 2008 de la Contraloría General de la República; y

CONSIDERANDO:

1.- Que, se hace necesario contar con una normativa adecuada en materia de seguridad de activos de información, la cual vele por su integridad, confidencialidad y disponibilidad,

2.- Que, es afán de este Gobierno Regional dar fiel cumplimiento a la legislación vigente referente a seguridad de la información,

3.- Que, se debe tener claridad de las vulnerabilidades técnicas en los sistemas de información de manera oportuna para el control y mitigación de éstas de forma constante, y regular las medidas necesarias para abordar el riesgo asociado.

RESUELVO:

1.- **APRUÉBESE** el **PROCEDIMIENTO DE CONTROL DE LAS VULNERABILIDADES TÉCNICAS**, el cual se adjunta y es parte constitutiva de la presente Resolución.

2.- **PUBLÍQUESE** un ejemplar de la presente Resolución en la Intranet Institucional.

ANÓTESE, REGÍSTRESE Y DIFÚNDASE.

INTENDENCIA REGION METROPOLITANA
INTENDENTE

CLAUDIO ORREGO LARRAIN
INTENDENTE
REGION METROPOLITANA DE SANTIAGO

IFE/GEP/MRT/CHM/JGG

Distribución:
Administración Regional
División de Administración y Finanzas
División de Análisis y Control de Gestión
División de Planificación y Desarrollo
Departamento de Gestión Institucional
Departamento de Informática
Oficina de Partes.

15942431

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

Realizar la detección, corrección y seguimiento de 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

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 DESCRIPCIÓN DE ACTIVIDADES

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 través de la herramienta de rastreo de vulnerabilidades.	Funcionario asignado por el Jefe del Departamento de Informática	Informe 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.

7 CRITERIOS OPERATIVOS

El procedimiento de Vulnerabilidades técnicas debe ejecutarse por lo menos una vez cada 6 meses.

Para la detección de vulnerabilidades tecnicas se deberá tener en consideración los controles relacionados que se indican en el **Procedimiento de Actualizacion de Seguridad y Validacion de Data** y el **Procedimiento de prueba funcionales**. 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 **Norma de Seguridad Informatica.**

8 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.

9 PRODUCTO

Vulnerabilidad identificada, con corrección y Documentada.

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 ANEXOS

- Registro de pruebas y corrección de vulnerabilidades técnicas
- Informe Vulnerabilidades

Informe Vulnerabilidades

N°	Solicitante	Servidor, sistema	vulnerabilidades	impacto potencial	acciones de corrección	impacto potencial de la acción de corrección	Fecha y tiempo propuesto para corrección	Responsable

Registro de pruebas y corrección de vulnerabilidades técnicas

N°	Servidor, sistema	vulnerabilidad	acciones de corrección	Fecha	Tiempo usado	acciones de corrección	Se solucionó	Comentario	Responsable

12 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 de Gestión Institucional	**Mayuri Reyes Torres** Presidente Comité de Seguridad

13 Historial de revisiones

Versión	Autor	Cargo	Fecha	Cambio/Revisión