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.
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 técnicas 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 **Política de Gestión de Incidentes de Seguridad.**

Para garantizar el buen funcionamiento en el procedimiento diríjase al **Protocolo Control y Tratamiento de la Seguridad de la Información** 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 ANEXOS

11.1 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

11.2 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 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)

13 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.

14 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 FORMALIZACION EXTERNA

Mediante el acta fecha 23 de noviembre año 2021, se aprueba por parte del Comité de Seguridad de la Información, la Procedimiento de control de las vulnerabilidades técnicas

16 REGISTRO DE REVISION Y ACTUALIZACION HISTORICO

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 píde 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
04	Matias Benitez	Todas	08-07-2019	Se cambia pie de página.
05	Matias Benitez.	Todas	12-07-2019	Comité de la seguridad de la información revisa y aprueba procedimiento de control de las vulnerabilidades técnicas año 2019.
06	Carlos Hernández	8	17-11-2021	Se agrega capítulo 15 formalización externa
07	Carlos Hernández	Todas	23-11-2021	Comité SSI revisa y aprueba año 2021

17 FORMALIZACIÓN

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	**Mayuri Reyes T.** Presidente Comité de Seguridad

stg INTERNATIONAL SANTIAGO	**ACTA DE REUNION COMITÉ DE SEGURIDAD DE LA INFORMACION**	Página 1 de 3 Fecha 23/11/ 2021

ACTA DE REUNION: Comité de Seguridad de la Información

Objetivo	Situación SSI año 2021
Fecha y Hora	23-11-2021, 15:00
Lugar	Sala de Reunión 2° Piso

PUNTOS DE LA REUNION

1. Bienvenida
2. Actualización de Documentos
3. Vulnerabilidades año 2021
4. 67 vulnerabilidades detectadas en sitios y páginas webs
    a. Caída de Switch piso 5 - 13 de septiembre 2021
    b. Caída de Switch piso 1 - 27 de septiembre 2021
5. Envío Correo Phishing
6. Protectores de Pantalla
7. Capacitación SSI
8. Mejoras
    a. Switch
    b. GTD Ancho Banda
9. SGD, 0 Papel
10. Eliminación Activos
11. Necesidades Tecnológicas

Aprobación los siguientes documentos

1. **Instructivo correctivo y preventivo contra fallas de energía y otras fallas de servicio**
2. **Manual de gestión de archivos**
3. **Norma de acceso a la Red**
4. **Norma de Eliminación de Activos**
5. **Norma de la Seguridad de la información para la Gestión de Proyectos**
6. **Norma de Outsourcing**
7. **Norma de Trabajo Remoto**
8. **Norma de uso identificación y autentificación**
9. **Norma de uso de instalación legal de software**
10. **Norma de reutilización y devolución de activos**
11. **Plan de Continuidad**
12. **Plan de emergencia Institucional**
13. **Política clasificación de activos**
14. **Política de acceso físico**
15. **Política de correo electrónico e Internet**
16. **Política de Derechos de propiedad Intelectual**
17. **Política de desarrollos de sistemas**

18. Política de dispositivos móviles
19. Política de escritorios y pantallas limpias
20. Política de gestión de incidentes de seguridad
21. Política de gestión de la capacidad
22. Política Gestión de Personas
23. Política de la seguridad informática
24. Política de respaldo de la información
25. Política general de seguridad de la información
26. Política gestión de claves
27. Política manejo de activos
28. Política sobre el uso de controles criptográficos
29. Procedimiento de control de las vulnerabilidades técnicas
30. Procedimiento de Controles de Auditoria de Sistemas de Información
31. Programa de concientización sobre seguridad de la información
32. Protocolo y control de tratamiento de SSI

DESARROLLO DE LA PRESENTACIÓN

José Ignacio da la bienvenida y explica brevemente que es el SSI y las funciones del comité

Se da detalle al comité respecto a las vulnerabilidades CSIRT y las caídas de los switch

Claudio Muñoz y Mayuri Reyes, solicitan al comité la revisión de funcionamiento de cámaras de seguridad del Gore. Debido a problemas que existen actualmente

José Ignacio informa que esta demora se ha debido a que se necesita realizar una revisión inicial de todas las cámaras y su funcionamiento.

Se detallan las mejoras tecnológicas a realizar con carácter de importancia

- Cambios en los switch
- Importancia de dejar el sistema de cámaras en un circuito cerrado fuera de la red

Se recalca la importa de incluir SSI en la inducción a nuevos funcionarios

Se menciona a comité que se enviara cazabobos y que de ahí se realizara una capacitación a quienes caigan en él.

Se establece que el cambio de contraseñas debiera ser cada 6 meses de forma obligatoria empezando con un cambio masivo en marzo. Aplicándose tanto en AD como en sistemas.

Comité solicita que los mensajes de los protectores de pantalla sean un poco más "Rudos" refiriéndose a la gravedad de lo que podría ocasionar una vulneración importante de sistemas

Silvana Torres entrega información

- Acerca del expurgo de documentos
- 2022 se enviará soporte en papel a archivo nacional
- Se está digitalizando documentación antigua
- Menciona que para todo envío a archivo nacional o eliminación debe haber un testigo que vise la correcta digitalización de documentos, transformación digital 21808

José Ignacio retoma la palabra e indica al comité la importancia dentro de todo el proceso de 0 papel de contar con una cloud de respaldo para toda la gran cantidad de archivos que se está generando

Explica que se continuara siempre con el respaldo en cintas. Indica que se necesita realizar respaldo en cintas como parte de SSI

Se aprueban políticas y documentación SSI

Carolina Hidalgo solicita curso de ciberseguridad a comité y participantes

stgo GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO	**ACTA DE ASISTENTES COMITÉ DE SEGURIDAD DE LA INFORMACION**	Página 1 de 1 Fecha 23/11/ 2021

N°	NOMBRE	DEPARTAMENTO O UNIDAD	FIRMA
01	José Ignacio Gutiérrez	Departamento de Informática	
02	Mayuri Reyes T.	División Administración y Finanzas	
03	Héctor Valladares	Departamento Jurídico	
04	Carolina Hidalgo	Departamento Planificación y Control Institucional	
05	Silvana Torres	Departamento de Gestión Documental y Activos	
06	Claudio Muñoz	Departamento de Servicios Generales	
07	Paulo Serrano	Departamento de Gestión de Personas	
08	Luz Magaly Nuñez	Unidad de Transparencia	
09	Ariel Lagos	Prevencionista de Riesgo	
10	VIRGINIA SAAVEDRA	DAF	
11			
12			
13			