Procedimiento de Controles de Auditoría de Sistemas de Información

1 INDICE

2 OBJETIVO

El objetivo de este procedimiento es crear un marco referencial respecto de cómo debería ceñirse un control de auditoria para los sistemas de información de Gobierno Regional Metropolitano y dar recomendaciones a la Dirección para mejorar o lograr un adecuado control interno en ambientes de tecnología informática , poniendo atención a las vulnerabilidades técnicas de los sistemas de información y equipos informáticos , de acuerdo a métodos y procedimientos ya establecidos de manera de garantizar el buen funcionamiento de toda la infraestructura a título de enfrentar eficientemente las demandas del servicio, manteniendo así la confiabilidad de los activos de información

3 ALCANCE

Este procedimiento es aplicable a todo Sistema Informático de propiedad del Gobierno Regional Metropolitano, Software, Hardware, sean estos equipos de usuarios o servidores que contengan activos de la Información, bases de datos, procedimientos, etc., que son susceptibles de las vulnerabilidades técnicas en los sistemas de información. A los equipos en la red de datos del Gobierno Regional Metropolitano bajo administración del Departamento de Informática, con soporte o mantención propia o de terceros.

4 ROLES Y RESPONSABILIDADES

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

Auditoria Interna será responsable del cumplimiento de este procedimiento.

Los funcionarios deberán regirse de acuerdo a este procedimiento facilitando el acceso a cualquier proceso de auditoria respecto de los activos de información, y que como propietarios de la información deberán clasificarla y autorizarla de acuerdo a los controles establecidos.

5 CONTROL NORMATIVO SSI

El siguiente procedimiento tiene por finalidad dar cumplimiento a los siguientes controles de la Política NCh-ISO27001.Of2013

Código del Control	Identificación del Control	Requisito de control
A.12.07.01	Controles de auditoría de sistemas de información	Los requisitos y las actividades de auditoría que involucran verificaciones de los sistemas operacionales se deben planificar y acordar cuidadosamente para minimizar el riesgo de interrupciones en los procesos del negocio.

6 DEFINICION Y MODO DE OPERACION

El Gobierno Regional de la Región Metropolitana a través de su Departamento de Informática, establecerá las normas y procedimientos de Auditoria de los Sistemas de Información y proveerá software de auditoria de manera de monitorear constantemente la red y/o bien hacer un informe de una situación especial en un tiempo determinado. De no poder proveer el software podrá contratarse los servicios de una empresa externa especializada en el tema. Así mismo, velará porque los funcionarios hagan un uso responsable de los servicios y equipos proporcionados por el Servicio a fin de mantener la confidencialidad e integridad de los Sistemas de Información.

La auditoría de los sistemas de información se define como cualquier auditoría que abarca la revisión y evaluación de todos los aspectos (o de cualquier porción de ellos) de los sistemas automáticos de procesamiento de la información, para esto deberá seguir el siguiente procedimiento:

a) los requisitos de auditoría de acceso a los sistemas y datos deben ser acordados y coordinados con el Departamento de Informática.
b) los alcances de las pruebas de auditoría técnica deberían ser acordadas y controladas.
c) las pruebas de auditoría deben limitarse al acceso de sólo lectura al software y los datos.
d) Acceso distinto al de sólo lectura debe permitirse solamente para copias aisladas de los archivos del sistema, los cuales deben ser borrados una vez completada la auditoría, o darles una protección adecuada si es que hay una obligación de mantener dichos archivos bajo los requisitos de documentación de auditoría
e) los requisitos para el procesamiento especial o adicional deben ser identificados y acordados
f) pruebas de auditoría que pudieren afectar a la disponibilidad del sistema se deben ejecutar fuera de horas de oficina

g) todo el acceso debe ser monitoreado y registrado para producir un rastro de referencia
h) todo proceso de auditoria deberá tener una fecha de inicio y fecha de término establecida
i) durante el proceso de auditoria se deberán evaluar los planes de contingencia y respaldos además dar una opinión y evaluación de la Seguridad Informática.
j) revisar los sistemas operativos, programas utilitarios y sugerir modificaciones a las aplicaciones existentes.
k) La unidad de soporte simulará ataques a la red o equipamiento de manera de generar una base de posibles intrusiones

7 REGISTRO DE OPERACION

El Departamento de Informática deberá emitir un informe que dé cuenta de las solicitudes recibidas para:

- A.12.07.01 Informe de existencia de consideraciones y controles al realizar auditorías a los sistemas de información

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

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)

8 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.

9 REVISIÓN

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

10 FORMALIZACION EXTERNA

Mediante el acta fecha 23 de noviembre año 2021, se aprueba por parte del Comité de Seguridad de la Información, el Procedimiento de controles se auditoria de sistemas de información.

11 REGISTRO DE REVISION Y ACTUALIZACION HISTORICO

Versión	Autor	Página o Secciones	Fecha Modificación	Motivo
01	Mauricio Marín V.	todas	4-10-17	Creación Documento
02	Mauricio Marin V.	todas	13/06/2018	Comité de Seguridad hace revisión de documento para el año 2018,
03	Mauricio Marin	todas	2/11/2018	Revisión general del documento. Se cambia título 6 por Definición y Modo de Operación Se cambia título 7 por Registro de Operación
04	Matias Benitez.	Todas	12-07-2019	Comité de la seguridad de la información revisa y aprueba Procedimiento de controles se Auditoria de sistemas de información año 2019.
05	Carlos Hernández	6	17-11-2021	Se agrega capítulo 10 formalización externa
06	Carlos Hernández	Todas	23-11-2021	Comité SSI revisa y aprueba año 2021

12 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 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	
	Ariel Lagos	Prevencionista de Riesgo	
10	VIRGINIA SAAVEDRA	DAF	
11			
12			
13			