Política de Respaldo de la Información

1 INDICE

2 OBJETIVO

El objetivo del presente documento consiste en implantar una política de respaldo de manera de proteger toda información o activos de información en materia informática y de comunicaciones digitales en el Gobierno Regional Metropolitano contra todo tipo de fallas y que puedan facilitar la recuperación en el menor tiempo posible y sin pérdida de datos

3 ALCANCE

Esta política aplica para el Departamento de Informática, en lo que respecta al respaldo de los Activos de Información del Gobierno Regional Metropolitano contenidos en los Servidores, equipos de trabajo, que contengan datos, aplicaciones e información crítica para el Servicio así como también a todos los funcionarios (planta, contrata, reemplazos y suplencias) personal a honorarios y terceros (proveedores, compra de servicios, etc.), que presten servicios para el Gobierno Regional Metropolitano y que tengan activos de información importantes para el Servicio.

4 ROLES Y RESPONSABILIDADES

El Departamento de Informática será el encargado de aplicar esta política de Seguridad Informática.

Cada usuario tendrá disponible las normas de Seguridad Informática y será responsable de regirse de acuerdo a las Políticas y normas generales y específicas de la Seguridad de la Información, por la seguridad del equipo según indiquen las Políticas, Normas u otros documentos aprobados por el Servicio en materia de Seguridad de la Información, tal como se describen en el siguiente punto:

El usuario será responsable de todo respaldo de archivos correspondiente a sus funciones y labores diarias las que deberán ir a la carpeta creada por la Unidad de Soporte para este efecto.

El usuario no podrá poner en esta carpeta de respaldo información personal como: fotos, canciones, etc. u otro documento o archivo que no tenga que ver con las funciones propias para lo que fue contratado.

5 CONTROL NORMATIVO SSI

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

Código del Control	Identificación del Control	Requisito de control
A.12.03.01	Respaldo de información	Se deben hacer copias de respaldo y pruebas de la información, del software y de las imágenes del sistema con regularidad, de acuerdo con la política de respaldo acordada.

6 DEFINICIONES

La política de Respaldo de Información del GORE será el instrumento que guiará a los funcionarios en la importancia y sensibilidad de activos de la información y servicios críticos en su correcta utilización, así como la mantención de herramientas y alternativas de recuperación ante desastres tecnológicos, de tal forma que permiten al usuario continuar con su misión con el menor contratiempo posible

El implantar esta política requiere un alto compromiso de parte de todos los usuarios en la institución de modo de prever fallas y deficiencias, así como mantener la información de manera segura y que nuestro trabajo perdure en el tiempo.

6.1 Disposiciones Generales

El Departamento de Informática está conformado por 2 unidades: Soporte Informático y Desarrollo de Sistemas. La unidad de Soporte Informático es la encargada de brindar servicio directo de apoyo al usuario con el equipamiento, instalación, alteración, cambio de lugar, configuración, etc. La unidad de Desarrollo tecnológico, se encarga de proveer, administrar y desarrollar recursos tecnológicos para el servicio, con el propósito de facilitar el cumplimiento de la misión institucional a través de la mejora en sus procesos.

Por esto es que ha sido necesario emitir una política de Respaldo de la Información para la Red-GORE, que es un conjunto de recursos y facilidades y aplicaciones informáticas, de la infraestructura de telecomunicaciones con sus servicios asociados, provistos por el Departamento de Informática.
La siguiente Política aplicará en iguales condiciones para ambas Unidades.

La presente política tiene carácter de cumplimiento obligatorio para toda persona que utilice recursos tecnológicos de la red del Gobierno Regional Metropolitano.

6.2 Respaldos

6.2.1 Equipos usuarios

- Se creará una carpeta compartida para respaldar información en los escritorios de los usuarios
- Los usuarios deberán respaldar toda información pertinente al Servicio en las carpetas creadas para tal efecto en sus computadores.
- No podrán respaldar información personal
- El correo Institucional será respaldado todas las semanas de forma automática. Se permitirá el uso de correos externos para usos personales
- Esta carpeta estará conectada directamente a un servidor que hará las veces de repositorio. El traspaso de información se hará a través de un software que permite comparar y hacer una copia idéntica a lo solicitado por el usuario.
- La unidad de soporte reforzará esta procedimiento de forma periódica de manera concientizar a los usuarios de este procedimiento
- El Departamento de Informática es el responsable de proporcionar los servicios de respaldo a los recursos informáticos disponibles. El usuario de estos servicios deberá sujetarse a la Política de respaldo de información de la Red-GORE
- Tendrá acceso a los sistemas administrativos solo el personal del GORE que tenga la autorización del usuario responsable del sistema, aún si se trata de personal de apoyo administrativo o técnico.

6.2.2 Servidores

- El acceso lógico a equipo especializado de computación (servidores, base de datos, etc.) conectado a la red es administrado únicamente por la Unidad de Soporte Informático.
- La Unidad de Soporte Informático es la responsable de instalar y administrar el o los servidor(es).Es decir, sólo se permiten servidores autorizados por el Departamento de Informática.

- Serán los usuarios los responsables de subir la información a respaldar en los servidores, las veces que estimen conveniente

- Los servidores de bases de datos administrativos son de uso exclusivo para esta función, por lo que se prohíben los accesos de cualquiera, excepto para el personal del departamento de Informática. El uso de estos deberá ser autorizado por el Departamento de Informática.

- La Unidad de soporte hará los respaldos de estas carpetas diariamente de forma incremental en formato digital en el mismo servidor. La Unidad de soporte hará un respaldo full solo los días viernes, y se hará en medios de almacenamientos magnéticos en formato de cintas.

- En lo que respecta a la Unidad de Desarrollo, será esta unidad la que se encargará de respaldar todo código fuente y aplicaciones Estos respaldos se harán diariamente a través de un Software especializado que permitirá dejar un historial de todo cambio realizado.

- Los días viernes se hará un respaldo Full correspondiente a la unidad de desarrollo en medios de almacenamientos magnéticos en formato de cintas.

- Estas cintas una vez grabadas se mantendrán en el edificio del Gobierno Regional Metropolitano por el plazo máximo de una semana. Una vez cumplido este plazo serán retiradas por una empresa externa que garantiza su resguardo en un lugar externo.

- La información generada por los sistemas de respaldo (bases de datos, correos, archivos en general) del servicio será resguardada por el Departamento de Informática.

- El Departamento de Informática realizará un monitoreo constante sobre todos y cada uno de los servidores de forman parte de los repositorios considerados críticos, a fin de resguardar los activos de información considerando siempre el espacio disponible para esta función

7 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.

8 PERIODICIDAD DE EVALUACION Y REVISIÓN

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

9 FORMALIZACION EXTERNA

Mediante el acta fecha 23 de noviembre año 2021, se aprueba por parte del Comité de Seguridad de la Información, la Política de respaldo de la información.

10 REGISTRO DE REVISION Y ACTUALIZACION HISTORICO

Versión	Autor	Página o Secciones	Fecha Modificación	Motivo
01	Mauricio Marín	todas	03-10-17	Creación de Documento
02	Mauricio Marin V.	todas	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 6 por "Definiciones" Se cambia título 7 por Registro de Operaciones Se cambia título 9 por Periodicidad de evaluación y revisión
03	Matias Benitez	Todas	08-07-2019	Se cambia pie de página.
04	Matias Benitez.	Todas	12-07-2019	Comité SSI revisa y aprueba año 2019.
05	Carlos Hernández	7	17-11-2021	Se agrega capítulo 9 formalización externa
06	Carlos Hernández	Todas	23-11-2021	Comité SSI revisa y aprueba año 2021

11 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 PRESENTACION

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			