Política
Manejo de activos

1 INDICE

2 OBJETIVO

Desarrollar e implementar una política para el manejo de activos, de acuerdo al esquema de clasificación de información adoptado por la organización.

Definir los criterios y lineamientos esenciales, en cuanto a la generación, organización, acceso y almacenamiento de los activos de información y de los bienes asociados a su tratamiento, por tanto, se cumplirán los requisitos institucionales, legales o reglamentarios y las obligaciones contractuales en los ámbitos relacionados con su gestión en el Servicio.

Desarrollar e implementar los procedimientos para el manejo de activos, de acuerdo al esquema de clasificación de información adoptado por la organización.

3 ALCANCE

La presente política permitirá la correcta utilización de los activos provistos por el Gobierno Regional Metropolitano de Santiago, facilitando el manejo, procesamiento, almacenamiento y comunicación de la información conforme a su clasificación.

Esta política es aplicable a todos los funcionarios (planta, contrata, reemplazos y suplencias) personal a honorarios y terceros (proveedores, compra de servicios, etc.), que presten servicios en el Gobierno Regional Metropolitano.

4 ROLES Y RESPONSABILIDADES

La responsabilidad del activo de información es de su dueño o de quien este nomine como su responsable, no obstante, de aquello cada funcionario del servicio asumirá su parte de compromiso respecto a la información que utiliza, según los puntos qué se indican a continuación:

Propietario de la información: Deberá clasificar la información y autorizar la información considerando los controles adecuados.

Encargado de Transparencia Pasiva: Deberá asesorar en materias de clasificación de la información cuando fuera necesario.

Funcionario: Deberá cumplir con las normas establecidas en la presente política.

Los activos estarán identificados según el formato indicado en la **"Política Clasificación de Activos"** y se organizará en un Archivo de Gestión siguiendo los lineamientos entregados por el proceso indicado en el Cuadro de Clasificación del **"Manual de Gestión de Archivos".**

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.08.01.03	Uso aceptable de los activos	Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con la información y las instalaciones de procesamiento de información.
A.08.02.03	Manejo de activos	Se deben desarrollar e implementar los procedimientos para el manejo de activos, de acuerdo al esquema de clasificación de información adoptado por la organización.
A.18.01.03	Protección de los registros	Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso sin autorización, de acuerdo con los requisitos legislativos, regulatorios y contractuales

6 DEFINICIONES

El Servicio reconoce expresamente la importancia de la información y de los sistemas de información, así como de la necesidad de su protección, por constituir un activo estratégico y vital, hasta el punto de poder llegar a poner en peligro la continuidad del Servicio, o al menos suponer daños muy importantes, si se produjera una perdida irreversible de determinados datos.

Cada funcionario solo podrá realizar las tareas y acceder a los datos necesarios que se requieran para cumplir su cometido, es decir se considerará el principio del llamado "mínimo privilegio" para evitar accesos no autorizados.

Algunos de los riesgos en el manejo de los activos de información frente a los que se deberán establecer controles adecuados y razonables, tanto preventivos, como de detección y correctivos son: errores y omisiones, sabotajes, vandalismo, espionaje, transgresión de la privacidad y tráfico de datos, acciones de otros agentes externos no autorizados, y cualesquiera otros que puedan influir en que la información no sea exacta, completa, en definitiva integra, o no esté disponible dentro del tiempo fijado.

Para una mayor protección todos los archivos de tipo físico deberán ser almacenados en una sala con medidas de seguridad adecuadas y accesos controlados.

La información de carácter digital, deberá ser respaldada en servidores que cuenten con sistemas de respaldo

6.1 Restricciones de Acceso

La información deberá tener niveles de acceso según la clasificación de los activos indicada en el punto 6 de la **"Política Clasificación de Activos"**

6.2 Divulgación

En caso de que se solicite información se deberá identificar la categoría del mismo y seguir la siguiente tabla.

	En Tránsito	**Producto Final**
Información Secreta	Información altamente sensible, de uso exclusivamente interno. Su divulgación podría implicar un impacto no deseado para el Gobierno Regional Metropolitano	Información altamente sensible, de uso exclusivamente interno. Su divulgación podría implicar un impacto no deseado para el Gobierno Regional Metropolitano
Información Reservada	Su divulgación debe ser aprobada por el propietario	Transparencia pasiva[1]: independiente del ingreso de la solicitud (ya sea OIRS o web) son derivadas al Departamento correspondiente para su Gestión
Información Publica	Información que por su misma naturaleza puede ser divulgada	Transparencia activa[2]: esta información es divulgada a través de la web institucional.

[1] La transparencia pasiva se refiere al ejercicio del Derecho de Acceso a la Información, en virtud del cual toda persona tiene derecho a solicitar y recibir información que obre en poder de cualquier órgano de la Administración del Estado, en la forma y condiciones que establece la ley.

[2] De acuerdo al reglamento de la ley de Transparencia se entiende por transparencia activa: "La obligación que tienen los órganos de la Administración del Estado regulados por este reglamento de mantener a disposición permanente del público a través de sus sitios electrónicos y actualizados mensualmente los antecedentes que se definen en el artículo 51 de este reglamento"

6.3 Copiado e Impresión de información

En caso de que se requiera imprimir algún activo se deberá identificar la categoría del mismo y seguir la siguiente tabla.

	En Tránsito	**Producto Final**
Información Secreta	No está permitido copiar o imprimir información Secreta	Información altamente sensible, de uso exclusivamente interno. Su divulgación podría implicar un impacto no deseado para el Gobierno Regional Metropolitano
Información Reservada	No está permitido copiar o imprimir información Reservada	No está permitido copiar o imprimir información Reservada
Información Publica	Información que por su misma naturaleza puede ser copiada o impresa.	Información que por su misma naturaleza puede ser copiada o impresa.

6.4 Almacenamiento de información

Cuando no está en uso y especialmente en horario inhábil, toda la información **Reservada** deberá mantenerse almacenada, de modo de evitar que las personas no autorizadas tengan acceso a ella.

El almacenamiento de información **Reservada** no deberá realizarse en el disco duro u otro componente del computador personal sin un sistema de control de acceso adecuado (ver Norma de Uso para los Equipos Tecnológicos Portátiles y Norma de Seguridad Informática). La información **Reservada** y de USO INTERNO deberá ser grabada en el espacio que el Departamento de Informática defina para garantizar su seguridad y respaldo.

Cuando no esté en uso, la documentación escrita que contenga información **Reservada** deberá ser almacenada bajo llave.

El almacenamiento de los medios que contengan información debe ser acorde a las especificaciones del fabricante.

6.5 Registro de receptores de activos

Se debe registrar en la siguiente tabla los activos entregados a los receptores autorizados siguiendo la codificación de entrega respectiva para cada una.

CATEGORÍA DE INFORMACIÓN	CATEGORÍA DE INFORMACIÓN	DESCRIPCIÓN DEL CONTENIDO DE INFORMACIÓN	MEDIO DE SOPORTE	FORMATO	INFORMACIÓN PÚBLICA O DISPONIBLE	SOLICITADO POR	FIRMA	AUTORIZADO POR	FIRMA	FECHA	CODIGO DE ENTREGA

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 manejo de activos.

10 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	24-07-17	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 Marín V.	7	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
04	Matias Benitez	Todas	08-07-2019	Se cambia pie de página.
05	Matias Benitez.	Todas	12-07-2019	Comité SSI revisa y año 2019.
06	Carlos Hernández	7	17-11-2021	Se agrega capítulo 9 formalización externa
07	Carlos Hernández	Todas	23-11-2021	Comité SSI revisa y aprueba año 2021

11 FORMALIZACION

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			