Política de la Seguridad Informática

1 INDICE

2 OBJETIVO

El objetivo del presente documento consiste en implantar Políticas en materia informática y de comunicaciones digitales en el Gobierno Regional Metropolitano. Las actividades involucradas que compete a las tecnologías de la información y que son de uso diario por los funcionarios y lo referente a las políticas, normas y procedimientos han sido detenidamente planteadas, analizadas y revisadas a fin de no contravenir con las garantías básicas del individuo dado que no pretende intimidar las actividades de los funcionarios sino más bien muestra una buena forma de operar el sistema con seguridad, respetando en todo momento estatutos y reglamentos vigentes de la Institución. A su vez, se ciñe a la las leyes civiles y penales que rigen actualmente al país, y a los decretos y reglamentos gubernamentales que se aplican a esta materia.

3 ALCANCE

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 para el Gobierno Regional Metropolitano que usen equipamientos informáticos o que tengan directa o indirectamente relación con los Sistemas de Seguridad de la Información

4 ROLES Y RESPONSABILIDADES

El Departamento de Informática será el encargado de velar por el buen uso y apego a las Políticas de Seguridad Informática.

Las Jefaturas de Departamentos, deberán comprometerse con la Política de la Seguridad de la Información, y serán los responsables promover en sus subordinados el apego a esta política de manera irrestricta, debe ser periódicamente recordada.

Cada usuario tendrá disponible la Política de la Seguridad Informática y será responsable de regirse de acuerdo a ella, a las normas generales y específicas de la Seguridad de la Información, por la seguridad de los activos de información que pueda tener bajo su custodia y según indiquen las Políticas, Normas u otros documentos aprobados por el Servicio en materia de Seguridad de la Información. Todo esto con el solo objetivo de prevenir riesgos y evitar usos ilícitos, evitar las intrusiones de virus informáticos, para mantener la privacidad de sus propios datos como los de sus compañeros, para mantener la integridad de los activos de información, o para reducir el impacto sobre ellos.

5 CONTROL NORMATIVO SSI

La siguiente política 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.08.03.01	Gestión de los medios removibles	Se deben implementar los procedimientos para la gestión de los medios removibles, de acuerdo al esquema de clasificación adoptado por la organización.
A.08.03.03	Transferencia física de medios	Los medios que contengan información se deben proteger contra accesos no autorizados, uso inadecuado o corrupción durante el transporte.
A.09.02.05	Revisión de los derechos de acceso de usuario	Los propietarios de activos deben revisar los derechos de acceso de los usuarios de manera periódica.
A.11.02.04	Mantenimiento del equipamiento	El equipamiento debe recibir el mantenimiento correcto para asegurar su permanente disponibilidad e integridad.
A.12.04.01	Registro de evento	Se deben generar, mantener y revisar con regularidad los registros de eventos de las actividades del usuario, excepciones, faltas y eventos de seguridad de la información.
A.12.04.02	Protección de la información de registros	Las instalaciones de registro y la información de registro se deben proteger contra alteraciones y accesos no autorizados.
A.12.04.03	Registros del administrador y el operador	Se debieran registrar las actividades del operador y del administrador del sistema, los registros se deben proteger y revisar con regularidad.
A.12.04.04	Sincronización de relojes	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o dominio de seguridad deben estar sincronizados con una sola fuente horaria de referencia.

6 DEFINICIONES

La política de seguridad Informática del GORE será el instrumento para dirigir a los funcionarios acerca de la importancia y sensibilidad de la información y servicios críticos en su correcta utilización, así como la mantención de alternativas de recuperación ante desastres tecnológicos, de tal forma que permiten al usuario continuar con su misión con el menor contratiempo posible y:

- Aplicar normas de uso de las herramientas informáticas.
- Dirigir los procedimientos de utilización de los recursos informáticos.
- Restringir el uso de las tecnologías al uso laboral.
- Asegurar la disponibilidad de la información digital.

El implantar esta política requiere un alto compromiso de parte de todos los usuarios en el Gobierno Regional Metropolitano, de modo de prever fallas y deficiencias, así como mantener nuestra 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, modificaciones, cambio de lugar, configuración de software y periféricos, etc. La unidad de Desarrollo tecnológico, se encarga de proveer, administrar y desarrollar recursos tecnológicos como utilitarios y plataformas 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 políticas particulares para la Red-GORE, que es el nombre oficial de un conjunto de recursos y facilidades informáticas, de la infraestructura de telecomunicaciones con sus servicios asociados, provistos por el Departamento de Informática. De esta forma se realiza una clasificación de estas políticas según los ámbitos de la seguridad física y lógica de la información dentro de nuestra Institución.

Las presentes políticas tienen carácter de cumplimiento obligatorio para toda persona que utilice recursos tecnológicos de la red del Gobierno Regional Metropolitano.

6.2 Seguridad Física

6.2.1 Mantenimiento del equipamiento

- Todos los equipos de computación (equipos portátiles, estaciones de trabajo, servidores, y equipos accesorios), que estén o sean conectados a la Red-GORE, o aquel que en forma autónoma se tenga y que sea propiedad de la institución debe de sujetarse a la revisión y supervisión de instalación del Departamento de Informática.

- La protección física de los equipos corresponde a quienes en un principio se les asigna, y corresponde notificar los movimientos en caso de que existan, a los encargados correspondientes (Departamento de Informática, Unidad de Soporte Informático, Unidad de Patrimonio e Inventario). Todos y cada uno de los equipos son asignados a un responsable, por lo que es de su competencia hacer buen uso de los mismos.

- La Unidad de Soporte Informático, es la responsable de la realización del mantenimiento preventivo y correctivo de los equipos, además de la conservación de su instalación, la verificación de la seguridad física, y su acondicionamiento especifico a que tenga lugar. La unidad de soporte informático realizará una mantención preventiva de cada estación de trabajo una vez al año llevando un cronograma de acuerdo con cada usuario.

- Todo el equipo de computación (equipos portátiles, estaciones de trabajo, servidores y demás relacionados), y los de telecomunicaciones que sean propiedad del GORE debe estar actualizados tendiendo a conservar e incrementar la calidad del servicio que presta, mediante la mejora sustantiva de su desempeño.

- Dada la naturaleza insegura de los sistemas operativos y su conectividad en la red, el Departamento de Informática tiene la facultad de acceder sin previo aviso a cualquier equipo de computación que no esté bajo su supervisión y se encuentre conectado a la red.

- Los usuarios no podrán compartir carpetas, impresoras o cualquier dispositivo, sin la autorización del Departamento de Informática.

- La unidad de soporte realizará una mantención preventiva al equipamiento de la red anualmente. Está se efectuará previo aviso a los usuarios involucrados en el proceso.

6.3 Seguridad Lógica

- El acceso lógico a equipo especializado de computación (servidores, Switchs, Firewalls, base de datos, etc.) conectado a la red es administrado únicamente por la Unidad de Soporte Informático.

- Todo el equipo de computación que esté o sea conectado a la Red-GORE, o aquellas que en forma autónoma se tengan y que sean propiedad de la institución, deben de sujetarse a los procedimientos de acceso que emite el Departamento de Informática.

6.3.1 Revisión de los derechos de acceso de los usuarios

- 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.

- El manejo de información administrativa que se considere de uso restringido deberá tener acceso de usuario y password con el objetivo de garantizar su integridad. El control de acceso a cada sistema de información será determinado por la jefatura de departamento o unidad responsable de generar y procesar los daos involucrados.

- El Departamento de informática revisará cada 6 meses los derechos de accesos de los usuarios con accesos privilegiados de manera de contrastar las autorizaciones existentes ante eventuales movimientos o cambios de personal.

- La instalación y uso de los sistemas de información serán provistos únicamente por el Departamento de Informática.

- 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 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.

- Los accesos a las páginas web a través de los navegadores se sujetarán a las normas y restricciones de acceso por el servidor Proxy de la Red-Gore. Quedarán restringidos a modo

general los accesos a páginas de descargas de programas, con videos de cualquier tipo, Chat, música, sitios de contenido erótico, radios y canales de televisión.

- El Departamento de Informática tiene la facultad de llevar a cabo la revisión periódica de los accesos a nuestros servicios de información, y conservar información del tráfico emanado de cada equipo de Red-GORE.

- Los recursos disponibles a través de la Red-GORE serán de uso exclusivo para asuntos relacionados con las actividades sustantivas de la Institución donde corresponde solo al Departamento de Informática, mantener y actualizar la infraestructura de la Red-GORE.

6.3.2 Administración de medios extraíbles

El Departamento de Informática deberá seguir las siguientes pautas para la administración de medios extraíbles todas estas enfocada en mantener seguridad sobre activos que puedan ser manipulados fuera de un entorno seguro:

- Para todos aquellos activos extraíbles que ya no presten utilidad se deberá asegurar su irrecuperabilidad.

- De ser necesario se deberá requerir una autorización para los medios retirados de la organización y se deberá mantener un registro de tales retiros para poder mantener un seguimiento.

- Todos aquellos medios extraíbles que guarden información importante para el servicio deberán ser almacenados en un entorno seguro y protegido.

- Con el fin de mitigar el riesgo de que los medios se degraden mientras aún se necesitan los datos almacenados, los datos se deberían transferir a medios nuevos antes de que se vuelvan ilegibles;

- Cuando existan datos valiosos estos deberán ser almacenados obligatoriamente en cintas y enviados a bodega según indica la Política de Respaldo para reducir aún más el riesgo accidental de daños o pérdidas de datos.

- Se podrán utilizar en los equipos tecnológicos puertos USB u algún otro medio extraíble debido a que en este Servicio no se han determinado activos de carácter Secreto. Sin embargo, cada funcionario será responsable de la información que maneje en estos dispositivos.

6.3.3 Transferencia de medios físicos

El Departamento de Informática deberá seguir las siguientes para proteger los medios que contienen información que pueda ser transportada:

Se deberán utilizar servicios de transporte o courier confiables.

El medio de transporte que empaque deberá ser suficiente para proteger los contenidos de daños físicos que pudieran ocurrir durante el trayecto, por ejemplo, protección contra factores ambientales que puede reducir la efectividad de la restauración de los medios, como la exposición al calor, a la humedad y a los campos electromagnéticos.

Se deberán mantener registros, identificando el contenido de los medios, la protección aplicada, así como también un registro de las veces en que se transfirió a los custodios en tránsito y un recibo en el lugar del destino.

Consideración con respecto a transporte de archivos en papel:

Debido a que la información puede ser vulnerable al acceso no autorizado, al uso indebido o a la corrupción durante el transporte físico al enviar los medios a través del servicio postal o courier. En este control, los medios incluyen a los documentos en papel.

Cuando la información confidencial en los medios no está cifrada, se debería considerar una protección adicional de los medios.

6.3.4 De los Software de equipos y servidores

- Todos y cada uno de los equipos de la Red-Gore dispondrán de software de seguridad (antivirus, vacunas, privilegios de acceso, y otros que se apliquen) por tanto ningún usuario está autorizado a desinstalar el mismo de los equipos.

- La adquisición y actualización de software para los equipos se llevará a cabo de acuerdo a una calendarización propuesta por el Departamento de Informática. Cualquier programa requerido por algún usuario deberá ser solicitado por parte del departamento al que pertenece el funcionario al Departamento de Informática. Corresponde al Departamento de Informática autorizar cualquier adquisición y actualización del software.

- Cualquier software que requiera ser instalado para trabajar sobre la Red-GORE deberá ser evaluado por el Departamento de Informática y deberá contar con su respectiva licencia de uso y utilización

- Todo el software propiedad de la institución deberá ser usado exclusivamente para asuntos relacionados con las actividades de la Institución.

6.3.5 Registro y monitoreo de eventos

- El Departamento de Informática realizará un monitoreo constante sobre todos y cada uno de los servicios de red.

- El Departamento de Informática analizará semanalmente el tráfico de datos en la red por medio de la revisión de conexión Firewall institucional.

- El Departamento de Informática realizará una revisión anual de la configuración y estado general del equipo firewall.

- La unidad de soporte y la unidad de desarrollo deberán llevar registros de los movimientos que se realicen en los servidores (Anexo 10.1 Registro de movimientos), dejando detalle de:

  - Nombre del funcionario
  - nivel de autoridad o derechos de administración o privilegios
  - día y hora de inicio
  - día y hora de finalización
  - nombre del o los servidores manipulados
  - actividades en el sistema o procedimientos afectados
  - actualizaciones lógicas o físicas
  - Resultado, exitoso rechazado

6.3.6 Protección del registro de información

Como modo de protección ante posibles modificaciones por parte de los usuarios de los sistemas, se deben proteger todos los registros de operación de un sistema o equipo computacional evitando que puedan ser editados o modificados.
Para esto la unidad de soporte verificará permanentemente los perfiles de usuarios a fin de que cumplan lo estipulado en las políticas de seguridad restringiendo las credenciales.
En caso que la capacidad de almacenamiento supere el tamaño que pueda guardar en su registro un equipo, deberá dejarse una copia de ellos fuera del control del usuario para que sea usada en posibles procesos de auditoría

6.4 Registro de Administradores y Operadores

Para los administradores de quipos y para los operadores de sistemas, al igual que para los usuarios normales, se deberán proteger los sistemas de manera de evitar edición de los registros y así evitar modificaciones o alteraciones de los mismos.

Los registros deben estar protegidos, porque no pueden ser retirados o modificados por personas no autorizadas. Cuando se obtiene acceso a un sistema no autorizado, se podría eliminar toda la información generada por los registros, de manera de evitar todas las evidencias de las acciones que lleva a cabo. Por lo tanto, se tienen que establecer todas las reglas que facilitan la modificación de los registros solamente por ciertas personas y las medidas de control de acceso al sistema tienen que estar fortificada.

Con el fin de evitar mal uso de los sistemas, es que los privilegios de los administradores y los operadores tienen diferentes privilegios que los usuarios normales, lo que significa que pueden realizar más acciones en los sistemas informáticos que cualquier usuario normal. En algunos casos, la intrusión no se ha registrado por lo que si alguien quisiera tener acceso a un sistema no autorizado es muy probable que quisiera adquirir permisos de administrados y realizar todas las acciones con derechos de usuario que tiene el administrador. Para evitar esto se debe registrar toda la información sobre los usuarios, independientemente de los privilegios que tiene. Para esto se establecerá una GPO con el fin de garantizar que toda alteración a los registros quede señalada indicando cuando y quien realizó la modificación de los mismos.

6.4.1 Sincronización de relojes

Es importante saber que para poder trabajar en ambientes distribuidos, el orden en las secuencias de operaciones de procesos sea estricto y común para todos.

De aquí nace la necesidad de poder ejecutar procesos distribuidos con la seguridad que comenzarán todos al mismo tiempo.

Todos los sistemas se tienen que configurar con la misma fecha y hora, por lo que si se produce un incidente y queremos realizar una prueba de trazabilidad de lo que sucedido en los diferentes sistemas que se encuentran involucrados, puede ser difícil si cada uno tiene una configuración diferente. El escenario ideal es que todos los sistemas tengan el tiempo sincronizado y esto se puede conseguir de una forma automatizada con servidores de tiempo.

La sincronización de relojes en un sistema distribuido consiste en garantizar que los procesos se ejecuten en forma cronológica y a la misma vez respetar el orden de los eventos dentro del sistema.

Para lograr esto se creará una GPO que apuntará a un servidor específico en el que se actualizará la hora de acuerdo a las normas de ahorro de energía que establezca el Gobierno Central y será efectivo para distintos sistemas operativos que se usan en el Gobierno Regional Metropolitano.

7 ANEXOS

7.1 Registro de Movimientos

GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO

REGISTRO DE MOVIMIENTOS EN SERVIDORES

NOMBRE DEL FUNCIONARIO				
UNIDAD	SOPORTE		DESARROLLO	
NIVEL DE AUTORIDAD, DERECHOS O PRIVILEGIOS				
DIA Y HORA DE INICIO DE LOS TRABAJOS				
DIA Y HORA DE FINALIZACION DE LOS TRABAJOS				
NOMBRE DEL SERVIDOR MANIPULADO				
EN EL SISTEMA				
PROCEDIMIENTO AFECTADO				
ACTUALIZACION LOGICA	SI		NO	
ACTUALIZACION FISICA	SI		NO	
RESULTADO EXITOSO				
RESULTADO	APROBADO		RECHAZADO	

Nombre y firma
Especialista

Nombre y firma
Jefe Departamento de Informática

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 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.

10 FORMALIZACION EXTERNA

Mediante el acta fecha 12 de julio año 2019, se aprueba por parte del Comité de Seguridad de la Información, la Política de la seguridad informática.

11 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 Marín	todas	25-09-17	Modificación de Formato, se agrega índice, Revisión, Difusión.
04	Mauricio Marín V.	12	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.
05	Matias Benitez	Todas	08-07-2019	Se cambia pie de página.
06	Matias Benitez.	Todas	12-07-2019	Comité de la seguridad de la información revisa y aprueba Politica de la seguridad informatica año 2019.

12 FORMALIZACIÓN INTERNA

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	**Alejandro Segura B.** Presidente Comité de Seguridad