PROTOCOLO DE CONTROL Y TRATAMIENTO DE SEGURIDAD DE LA INFORMACION

1 INDICE

2 OBJETIVO

El presente documento tiene por finalidad definir y normar los métodos o procedimientos de acceso para el desarrollo de actividades con terceros, de modo de considerar y establecer mecanismos y reglas de protección a la información y al equipamiento tecnológico del Gobierno Regional Metropolitano. Dadas las actuales condiciones de avance en materia de tecnologías de información y comunicación, es que se deben definir los resguardos y garantías que permitan establecer acuerdos de confiabilidad en el desarrollo de actividades por terceros, en cualquiera de sus formas posibles y, ante la necesidad de otorgar permisos de acceso a información institucional, equipos de procesamiento de información o red interna de comunicación del Servicio se deben utilizar las definiciones del presente documento

3 ALCANCE

El presente documento se debe considerar para todo tipo de trabajo que involucre acceso a la información de la Institución, así como facilitar cualquier tipo de acceso a equipamiento de éste en cualquiera de sus formas. Se deben utilizar las normativas que aquí se definen, de modo de asegurar la protección e integridad de la información como de los equipos de procesamiento de información del Servicio.

4 ROLES Y RESPONSABILIDADES

Departamento de Informática

El departamento de Informática dará los permisos y accesos necesarios para personal externo, pertenecientes a proveedores que prestan servicios dentro de las dependencias del Gobierno Regional Metropolitano

A su vez el Departamento de Informática designará a un funcionario de la unidad de soporte para que acompañe al personal externo a cualquiera de las dependencias del Gobierno Regional Metropolitano, en especial a las de acceso restringido.

Departamento de Servicios Generales

EL departamento de Servicios generales deberá identificar, registrar y anunciar las visitas técnicas de proveedores, a fin de poder coordinar con el Departamento de Informática.

Los proveedores

Los proveedores deberán ceñirse a estos protocoles de manera de estar de acuerdo con los procedimientos que aquí se describen, de manera de reducir probables riesgos en equipos ajenos a su negocio.

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.15.01.01	Política de seguridad de la información para las relaciones con el proveedor	Se deben acordar y documentar, junto con el proveedor, los requisitos de seguridad de la información para mitigar los riesgos asociados al acceso del proveedor a los activos de la organización.
A.15.02.01	Supervisión y revisión de los servicios del proveedor	Las organizaciones deben supervisar, revisar y auditar la entrega del servicio.

6 DEFINICIONES Y MODO DE OPERACION

6.1 Acuerdos

Toda solicitud de acceso a información, equipos de procesamiento de información o red interna de datos por parte de personas externas al Servicio, debe ser solicitada a través del formulario Registro de Movimientos de Personal en Sala de Servidores (anexo 1) y canalizada formalmente al Jefe del Departamento de Informática del Gobierno Regional Metropolitano. En esta se deben especificar los siguientes puntos:

- Nombre del Funcionario
- Unidad
- Nombre del Proveedor
- Nombre del técnico
- Día y hora de comienzos de los trabajos
- Día y hora de finalización de los trabajos
- Nombre del servidor manipulado
- Detalle del Procedimiento
- Motivo del acceso.

En caso que el proveedor necesite estar por periodos más prolongados, entiéndase días corridos o semanas para algún trabajo específico, deberá solicitarlo formalmente o vía correo electrónico dando los antecedentes y razones de su solicitud a la contraparte interna del Gobierno Regional Metropolitano, quien deberá responder la solicitud argumentado su aceptación o negativa, La solicitud deberá contener a lo menos detalles como:

- Identificación de las áreas o unidades de procesamiento interna a las cuales el proveedor solicitará acceso. Deberá además entregar información o de orientación que originan el motivo de la solicitud.
- Definir si necesitará apoyo técnico desde la Unidad de Soporte del Departamento de Informática del Gobierno Regional Metropolitano
- Definición de intereses involucrados que puedan ser afectados por la solicitud.

De acuerdo a esto, el Encargado de Seguridad procederá a autorizar o rechazar la solicitud, fundamentando la decisión.

Lo anterior con el fin de acordar y documentar las solicitudes de acceso a la información a fin de mitigar los riesgos asociados al acceso de personal externo a los activos de la institución

Al aceptar una solicitud conforme al punto anterior, se debe establecer claramente el tipo de acceso requerido, el cual debe normarse de acuerdo a uno de los siguientes enfoques:

6.2 Acceso físico a medios de procesamiento de información

El acceso al Servicio o a alguna de sus dependencias estará representado en una o más personas las que deberán portar una credencial de visita solo para el piso y lugar correspondiente al desarrollo de sus funciones.
Se avaluará la posibilidad de otorgar una credencial permanente en caso que el acceso sea mayor a 1 mes. El Departamento de Informática en conjunto con el Encargado de Unidad responsable de la información realizará:

a) Acta de recepción de los bienes inventariarles involucrados para uso del tercero en el Gobierno Regional Metropolitano.

b) La creación de usuario-clave válido en concordancia con los requerimientos estipulados en la solicitud de acceso.

c) Evaluación de activos comprometidos, solo en caso que el acceso no

sea solo lectura. Se deberá identificar uno a uno los datos a los cuales el tercero tendrá acceso a carga o modificación donde finalmente se enunciarán todos los resultados (reportes, cálculos) a los que se podría ver afectada la integridad de la información.

d) Descripción de los servicios de información disponibles para el tercero.

e) Método de monitoreo o seguimiento de las actividades realizadas por el tercero. Donde dicho monitoreo debe tener una frecuencia semanal de envío al encargado de seguridad quien registrara las actividades.

f) Definición de un método especifico de protección de la integridad de la información. Esto como mínimo debe considerar el respaldo diario o la previa validación de información cargada por un funcionario responsable del Gobierno Regional Metropolitano, entre otros, los que deben ser definidos de acuerdo a la índole de la intervención del tercero.

Todo acceso otorgado bajo este tipo de requerimiento debe estar enmarcado dentro de la Política de Acceso Físico a Oficinas e Instalaciones del Gobierno Regional Metropolitano.

6.3 Acceso lógico desde la red Institucional del Gobierno Regional Metropolitano.

El Departamento de informática en conjunto con el Encargado de Unidad responsable de la información realizará:

a) La creación de usuario-clave válido en concordancia con los requerimientos estipulados en la solicitud de acceso.

b) Declaración del o los sistemas a los que se concederá el acceso.

c) Para cada uno de los sistemas involucrados de debe proporcionar:

- Evaluación de activos comprometidos sólo en caso que el acceso no sea solo lectura. Se deberá identificar uno a uno los datos a los cuales el tercero tendrá acceso a carga o modificación donde finalmente se enunciarán todos los resultantes (reportes, cálculos) a los que se podría ver afectada la integridad de la información.
- Descripción de los servicios de información disponibles para el tercero.
- Método de monitoreo o seguimiento de las actividades realizadas por el tercero. Donde dicho monitoreo debe tener una frecuencia semanal de envío al encargado de seguridad quien registrará las actividades.

- Definición de un método específico de protección de la integridad de la información. Esto como mínimo debe considerar el respaldo diario o la previa validación de información cargada por un funcionario responsable del Gobierno Regional Metropolitano, entre otros, los que deben ser definidos de acuerdo a la índole de la intervención del tercero.
- Fundamentar las razones en términos de beneficios y riesgos de los accesos otorgados.

Todo acceso otorgado bajo este tipo de requerimiento debe estar enmarcado dentro de la Política de Acceso Físico a Oficinas e Instalaciones del Gobierno Regional Metropolitano.

6.4 Acceso lógico a la red Institucional del Servicio

Solo estará permitido para esta modalidad el uso de Web-Services donde se deberá aplicar:
a) La creación de usuario-clave válido en concordancia con los requerimientos estipulados en la solicitud de acceso.

b) Evaluación de activos comprometidos, sólo en caso que el acceso no sea sólo lectura. Se deberá identificar uno a uno los datos de los cuales el tercero tendrá acceso a carga o modificación donde finalmente se enunciarán todos los resultantes (reportes, cálculos) a los que se podría ver afectada la integridad de la información.

c) Descripción de los servicios de información disponibles para el tercero.

d) Método de monitoreo o seguimiento de las actividades realizadas por el tercero. Donde dicho monitoreo debe tener una frecuencia semanal de envío al Encargado de Seguridad o quien éste defina, el cual registrará las actividades como mecanismo de control.

e) Definición de un método específico de protección de la integridad de los activos de información. Esto como mínimo debe considerar el respaldo diario o la previa validación de información cargada por un funcionario responsable del Gobierno Regional Metropolitano, entre otros, los que deben ser definidos de acuerdo a la índole de la intervención del tercero.

f) Fundamentar las razones en términos de beneficios y riesgos de los accesos otorgados.
Todo acceso otorgado bajo este tipo de requerimiento debe estar enmarcado dentro de la Política de Acceso Físico a Oficinas e Instalaciones del Gobierno Regional Metropolitano.

6.5 Acuerdo de Protección de activos

Se deberá establecer con el tercero un acuerdo formal de protección a la información el que será vinculado, de acuerdo a la índole del tercero, a través de un oficio si es con otro servicio público o del contrato si corresponde a un prestador de servicios, el que debe incluir las siguientes cláusulas de protección mínimas:

a) Se realizará un monitoreo o seguimiento de las actividades realizadas por el tercero, el que tendrá una evaluación periódica y permitirá evaluar si se cumplen las solicitudes de acceso autorizadas pudiendo detectar anomalías de acceso, carga errónea de información o cualquier actividad que pudiera afectar la información o equipamiento del Gobierno Regional Metropolitano lo que ocasionará la revocación inmediata de los permisos otorgados, desencadenando las acciones legales que se estimen pertinentes.

b) No se permitirá en ningún caso extraer información no especificada en la solicitud de acceso como tampoco realizar divulgación, venta o copia de ésta.

c) No se podrán realizar instalaciones o desinstalaciones de software de cualquier tipo sin previa autorización escrita por la jefatura del Departamento de Informática.

d) El tercero declara conocer la Política de Seguridad de la Información del Gobierno Regional Metropolitano.

e) Se deberá informar mensualmente al Encargado de Seguridad o quien éste defina y, si no aplica el período, al menos una vez, el detalle de actividades realizadas identificando usuario, fecha, información intervenida o alcanzada y resultados obtenidos.

El mantenimiento del equipamiento de procesamiento de información será única y exclusivamente mantenido por personal del Departamento de Informática del Gobierno Regional Metropolitano. Estará estrictamente prohibido conectar computadores portátiles o cualquier dispositivo de procesamiento de propiedad del tercero a la red de datos del Gobierno Regional Metropolitano, sin contar con una autorización por escrito emitida por el Departamento de Informática.

6.6 Supervisión y revisión

El Gobierno Regional Metropolitano deberá disponer de una contraparte técnica la cual estará encargada de monitorear y revisar los servicios del proveedor, garantizando de esta forma que los acuerdos se respeten y que los incidentes y problemas generados se gestionen correctamente.

La contraparte técnica del proveedor deberá tener las competencias suficientes, así como las habilidades y recursos técnicos para monitorear, revisar o auditar los requisitos técnicos en el control de la Seguridad de la Información.
SSI.

7 ANEXO 1

stg

REGISTRO DE MOVIMIENTO DE PERSONAL
EN SALA DE SERVIDORES

Nombre del Funcionario		
Unidad		
Nombre del Proveedor		
Nombre del tecnico		
Dia y hora de comienzo de los trabajos		
Dia y hora de finalizacion de los trabajos		
Nombre del Servidor manipulado		
Detalle del procedimiento		

Nombre y Firma del tecnico

Nombre y firma del funcionario

8 REGISTRO DE OPERACION

El Departamento de Informática deberá emitir un informe que dé cuenta de:

- A.15.01.01 Informe de solicitudes de acceso privilegiado de proveedores
- A.15.02.01 Informe de supervisión a accesos privilegiados

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)

9 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.

10 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.

11 FORMALIZACION EXTERNA

Mediante el acta fecha 23 de noviembre año 2021, se aprueba por parte del Comité de Seguridad de la Información, el Protocolo y control de tratamiento de SSI.

12 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	15-09-17	Modificación de Formato, se agrega índice, Revisión, Difusión.
04	Mauricio Marín V.	9	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 y Modo de Operación. Se cambia título 7 por Registro de Operación. Se agrega formulario de registro a sala de servidores
05	Matias Benitez	todas	08-07-2019	Se cambia pie de página.
06	Matias Benitez.	Todas	12-07-2019	Comité SSI revisa y aprueba año 2019
07	Carlos Hernández	10	17-11-2021	Se agrega capítulo 11 formalización externa
08	Carlos Hernández	Todas	23-11-2021	Comité SSI revisa y aprueba año 2021

13 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			