Norma de Acceso a la Red

1 INDICE

2 OBJETIVO

Establecer normas para garantizar el buen funcionamiento de las redes del Gobierno Regional Metropolitano y los servicios ofrecidos por el Departamento de Informática.

La aplicación de esta norma, buscar evitar el acceso no autorizado a la red digital del Gobierno Regional Metropolitano y está orientado a validar, verificar y proveer acceso lógico a la información, a las aplicaciones, bases de datos y servicios en general, logrando el control total en los accesos a la Red, los cuales exponen a la institución a pérdidas de activos de información, daño a los recursos disponibles.

3 ALCANCE

La Norma se aplica a todos los empleados, proveedores, contratistas, personal que esté vinculado con las firmas que presten servicios a Gobierno Regional Metropolitano de Santiago o que estén relacionados y que por sus funciones deban hacer uso de la Red digital del GORE o de su área local de conexión. Se incluyen, además, todas las dependencias que son parte de la institución o que tengan acceso a la red digital del Gobierno Regional Metropolitano.

4 ROLES Y RESPONSABILIDADES

El Departamento de Informática será el encargado de evaluar y conceder los permisos de acceso a la red del Servicio, así como la administración del sistema de acceso y el control de los roles de acceso a la misma

El Departamento de informática del Gobierno Regional Metropolitano de Santiago, es el responsable de la seguridad de los datos en la red y sus equipos, con el fin de ejecutar a cabalidad la tarea de mantener la infraestructura de la red.

El Departamento de Personal deberá informar las altas y las bajas de personal a modo de mantener actualizado el registro de usuarios

Todos los usuarios deberán regirse por todo lo establecido en esta norma, quedándoles estrictamente prohibido el uso de la red para fines personales. Deberán tomar todos los resguardos necesarios que el Departamento de Informática ha puesto su disposición.
No podrán conectar a la red otros equipos que no sean los del Servicio. Si necesita usar un equipo distinto a los provistos por el Servicio, será menester del Departamento de Informática su autorización previo chequeo del equipo y que este cumpla con las normas básicas de seguridad.

5 CONTROL NORMATIVO SSI

La siguiente norma 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.09.01.02	Accesos a las Redes y a los servicios de la red	Los usuarios sólo deben tener acceso directo a la red y a los servicios de la red para los cuales han sido autorizados.
A.13.01.01	Controles de red	Las redes se deben gestionar y controlar para proteger la información en los sistemas y aplicaciones.
A.13.01.02	Seguridad de los servicios de la red	Los mecanismos de seguridad, los niveles de servicio y los requisitos de la gestión de todos los servicios de red se deben identificar e incluir en los acuerdos de servicios de red, ya sea que estos servicios son prestados dentro de la organización o por terceros.
A.13.01.03	Separación en las redes	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en redes.

6 DEFINICION Y MODO DE OPERACION

6.1 Acceso a la Red

- Todo acceso a la Red se hará mediante la creación de una cuenta de usuario autorizada previamente por el Departamento de Gestión de personas. Esta cuenta de usuario será autenticada mediante una clave secreta que se validará en el Active Directory del Dominio del Gobierno Regional Metropolitano

- Toda la Red deberá estar físicamente protegidas en proporción a la criticidad o importancia de su función en el Gobierno Regional Metropolitano de Santiago.

- Los accesos a los distintos servidores o áreas serán permitidos de acuerdo a los privilegios otorgados a cada usuario de acuerdo lo establezca el Departamento de Informática del Gobierno Regional Metropolitano.

6.2 Mecanismos de seguridad física a áreas TI

- Todo acceso a las instalaciones de TI, solo se concederán al personal designado por el Departamento de Informática del Gobierno Regional Metropolitano de Santiago y contratistas, cuyas responsabilidades de trabajo requieran el acceso a dicha instalación.

- Las tarjetas de acceso magnéticas o claves de acceso no deben ser compartidas o cedidas a terceros.

- Las tarjetas de acceso magnético o claves de acceso que ya no sean necesarios o ya cumplieron su función, deberán ser devueltos al Departamento de Informática del Gobierno Regional Metropolitano de Santiago. Las tarjetas no deberán ser reasignadas a otra persona sin pasar por el proceso de re enrolamiento.

- La pérdida o robo de las tarjetas de acceso magnéticas o claves deberán ser reportados al Departamento de Informática del Gobierno Regional Metropolitano de Santiago.

- Los registros de acceso de las tarjetas de acceso magnéticas o claves deberán conservarse para mantener una revisión de los accesos y rutinas realizadas basados en la criticidad de los recursos que se protegen.

- El Departamento de informática del Gobierno Regional Metropolitano de Santiago, en colaboración con el área de personal, serán los encargados de recuperar y eliminar los accesos a los lugares restringidos de las personas que sean desvinculadas o que por cambios en el contrato cambien sus roles operativos.

- El Departamento de Informática, se encargará de revisar periódicamente los privilegios y derechos de acceso de las tarjetas de acceso magnético o claves para eliminar las de las personas que ya no requieran de estos privilegios.

- Cualquier uso de las instalaciones de TI deberá contar con la aprobación del Departamento de Informática del Gobierno Regional Metropolitano de Santiago.

- Todo dispositivo o equipo personal deberá contar con la autorización del Departamento de Informática para poder conectarse a la Red del Servicio previa revisión y escaneo del mismo a manera de evitar intrusiones de virus y propagación de este por la Red

6.3 Controles de Red

La administración de la red corresponderá al Departamento de Informática del Gobierno regional Metropolitano.

El personal autorizado debe tener libre acceso a las instalaciones críticas de TI las 24 horas del día.

El Departamento de Informática deberá velar por la protección contra interceptación, interferencia o daños en la red. La red deberá ser monitoreada con el fin de evitar accesos inadecuados o posibles ataques o intrusiones.

Los otros accesos a personal de servicios, oficiales de seguridad y otros actores, estarán restringidos y, según sea necesario, se solicitará a la jefatura correspondiente para gestionar con el Jefe del Departamento de Informática dichos privilegios. Cualquier otro tipo de personal, deberá ingresar acompañado a las instalaciones.

6.4 Seguridad de los servicios de redes

El Gobierno Regional Metropolitano, deberá disponer de soluciones de seguridad de redes administradas como firewalls y sistemas de detección de intrusos, con el fin de proteger la red Institucional.

El Departamento de Informática deberá monitorear de manera constante los servicios de red con el fin de asegurar un UpTime lo más cercano al 100%. Así mismo el Servicio debería garantizar que los proveedores de servicios de red implementen estas medidas.

Las funciones de seguridad de los servicios de red pueden ser:

- con aplicación de tecnología para la seguridad de los servicios de redes, como la autenticación, el cifrado y los controles de conexión de redes;
- parámetros técnicos necesarios para la conexión segura con los servicios de red de acuerdo con la seguridad y las reglas de conexión de redes;
- los procedimientos para el uso de servicios de redes para restringir el acceso a los servicios de red o aplicaciones, donde corresponda.

7 SEGREGACIÓN DE REDES

La red institucional, deberá ser segmentada en redes perimetrales con el fin de administrar la seguridad del Servicio.

De requerirlo, la red misma deberá ser segregada en diferentes niveles de acceso con el fin de evitar ataques tanto internos como externos.

La segregación deberá a lo menos contar con una LAN para los usuarios, una DMZ para Servidores y una red perimetral para los accesos WiFi.

Los accesos de confianza podrían generarse mediante grupos de accesos validados en Active Directory con privilegios según las funciones de cada usuario

8 REGISTRO DE OPERACION

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

- A.09.01.02 Informe de usuarios Autenticados a través de Active Directory para acceso a la Red.
- A.13.01.01 Informe de controles de red implementados en la institución.
- A.13.01.02 Informe de Seguridad de los servicios de red implementados en la institución.
- A.13.01.03 Informe de segregación de redes implementadas en la institución.

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)

9 REVISIÓN

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

10 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.

11 FORMALIZACION EXTERNA

Mediante el acta fecha 23 de noviembre año 2021, se aprueba por parte del Comité de Seguridad de la Información, la Norma de acceso a la red.

12 REGISTRO DE HISTORIAL DE VERSIONES O MODIFICACIONES

Versión	Autor	Página o Secciones	Fecha Modificación	Motivo
01	Mauricio Marín.	todas	29-09-17	Creación
02	Mauricio Marín.	8	1/08/2018	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 de "Aplicación" por "Definición y Modo de Operación" Se cambia periodicidad del informe de Semestral a anual. Se cambia título 8 de Registro de control por Registro de Operación.
03	Matias Benitez.	Todas	08-07-2019	Se cambia pie de página.
04	Matias Benitez.	Todas	12-07-2019	Comité de la seguridad de la información revisa y aprueba Norma de acceso a la red año 2019.
05	Carlos Hernández	8	23-11-2021	Se agrega capítulo 11 formalización externa
06	Carlos Hernández	Todas	23-11-2021	Comité de la seguridad de la información revisa y 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 **Matías Benítez P.** Analista Departamento de Informática **Carolina Hidalgo M.** Jefa Departamento Planificación y Control Institucional	**Mayuri Reyes T.** Presidente Comité de Seguridad

GOBIERNO REGIONAL METROPOLITANO DE 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

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			