Norma de Trabajo Remoto

1 INDICE

2 OBJETIVO

Ofrecer a los usuarios una guía sobre los requerimientos mínimos que deben ser cumplidos respecto al acceso remoto a la red institucional que provee el Gobierno Regional Metropolitano, como también las implicancias del mal uso. Es importante mencionar que el uso inapropiado de los recursos dispuestos para los usuarios, expone a la institución a riesgos innecesarios como los virus informáticos, interrupción de las redes y sus sistemas, como también problemas jurídicos tanto nacionales como internacionales.

3 ALCANCE

La siguiente norma cubre el uso apropiado de los accesos remotos, y aplica a todos los empleados, proveedores, contratistas, personal que esté vinculado con proveedores que presten servicios al Gobierno Regional Metropolitano o que estén relacionados. Se incluye, además, todas las dependencias que son parte de la institución. El Gobierno Regional Metropolitano sólo proveerá los métodos de acceso a la red, el usuario será responsable de contratar un servicio de Internet, coordinar su instalación de software necesario y todo lo asociado a ésta.

4 ROLES Y RESPONSABILIDADES

El Departamento de Informática será el encargado de evaluar y conceder los permisos de acceso remoto a la Red Informática Institucional.

Cada usuario con permisos de acceso remoto aprobado será responsable de velar por la seguridad del equipo que se conecte a la Red Institucional 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.

Todo usuario que se conecte remotamente a la Red Institucional sin el permiso correspondiente será bloqueado en su acceso y se informará al Encargado de Seguridad para su evaluación.

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.06.02.02	Trabajo Remoto.	Se debe implementar una norma, y medidas de apoyo a la seguridad para proteger la información a la que se accede, procesa o almacena en los lugares de trabajo remoto.

6 DEFINICION Y MODO DE OPERACIONES

6.1 Normas para uso de conexiones remotas

Para el Departamento de Informática:

1) Analizar y aprobar los métodos de conexión remota a la plataforma tecnológica.

2) Implantar los métodos y controles de seguridad para establecer conexiones remotas hacia la plataforma tecnológica.

3) Restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas.

4) Verificar la efectividad de los controles aplicados sobre las conexiones remotas a los recursos de la plataforma tecnológica de manera permanente.

5) El Departamento de Informática mantendrá un registro histórico de los usuarios a los que se les ha concedido acceso remoto mediante documento "registro usuario con acceso remoto".

Para los usuarios:

1) Deberá solicitar un acceso remoto mediante el formulario "solicitud de acceso remoto" disponible en la Intranet Institucional.

2) Los usuarios que realizan conexión remota deben contar con las aprobaciones requeridas para establecer dicha conexión a los dispositivos de la plataforma tecnológica y deben acatar las condiciones de uso establecidas para dichas conexiones.

3) Deben establecer conexiones remotas en computadores previamente identificados y, bajo ninguna circunstancia, en computadores público, de hoteles o cafés internet, entre otros.

4) Es de responsabilidad del funcionario, asegurarse que ninguna otra persona utilice su cuenta de acceso, entendiendo que es de uso exclusivo para quienes se les ha asignado dichos privilegios.

5) El acceso debe ser controlado utilizando una contraseña de autenticación fuerte, manteniéndola por períodos de expiración.

Los usuarios deberán comprender que los computadores conectados mediante un acceso remoto son una extensión a la red Institucional, y como tales están sujetos a las mismas normas y reglamentos que se aplican a los equipos computacionales del Gobierno Regional Metropolitano, es decir sus máquinas deben ser configuradas para cumplir con las instrucciones anteriormente descritas.

7 ANEXOS

7.1 Anexo1

GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO

SOLICITUD PARA ACCESO REMOTO A RED INSTITUCIONAL

DATOS SOLICITANTE

Nombre de Funcionario: RUN:

Departamento: Fecha de Solicitud:

Jefe Directo:

Mediante el presente la persona anteriormente individualizada, solicita por medio de su Jefatura directa al Departamento de Informática gestionar acceso para una conexión remota a la plataforma tecnológica.

Fechas de Conexión

/ / Inicio / / Termino

Identificación Computador

Nombre Equipo: _____ Dirección MAC: _____

Plataforma (Sistema Operativo): _____

_____ _____

FIRMA JEFATURA **FIRMA SOLICITANTE**

El acceso debe ser controlado por medio de contraseña de autenticación fuerte, manteniéndola por periodos de expiración. Los usuarios deberán comprender que los computadores conectados mediante un acceso remoto son una extensión de la red Institucional y se encuentran sujetos a normativas y reglamentos aplicables a los equipos computacionales del Gobierno Regional Metropolitano

7.2 Anexo2

GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO

Registro de usuarios con acceso remoto

ID	Rut	Nombre	Dependencia	Fecha	Período

8 REGISTRO DE OPERACION

El Departamento de Informática deberá emitir un informe que dé cuenta de las solicitudes recibidas para:

- A.06.02.02 Informe de Solicitud y registro de acceso remoto

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 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 norma 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, la Norma de trabajo remoto.

12 REGISTRO DE HISTORIAL DE VERSIONES O MODIFICACIONES

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 V.	todas	01-08-2018	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 a Definición y Modo de Operaciones Se quita el título 7 Se cambia título 8 a Registro de Operación Se cambia periodicidad del informe a anual
04	Matias Benitez	Todas	08-07-2019	Se cambia pie de página.
05	Matias Benitez.	Todas	12-07-2019	Comité SSI revisa y aprueba año 2019.
06	Carlos Hernandez	8	15-11-2021	Agrega capítulo 11 formalización externa Se actualiza índice
07	Carlos Hernandez	todas	23-11-2021	Comité SSI revisa y aprueba año 2021

13 FORMALIZACIÓN

Elaborado por	Revisado por	Aprobado por
Calos 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

stgo 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

stg 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			