Gobierno de Chile

GOBIERNO REGIONAL DE LOS LAGOS
Acción de Futuro

GOBIERNO REGIONAL DE LOS LAGOS
Acción de Futuro

SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

PROCEDIMIENTO "UBICACIÓN Y PROTECCION DE EQUIPAMIENTO"

CÓDIGO	**SSI-A.11.02.01**	**CLASIFICACIÓN INFORMACIÓN**		**Reservada**
			X	**Uso Interno**
				Pública
VERSIÓN	1.0	**FECHA DE LA VERSIÓN**	15-12-2017	
RESPONSABLE	Encargado (S) de Seguridad de la Información.			

Avda. Décima Región 480, 4° piso,
Edificio Intendencia Regional
Puerto Montt

Fono (65) 2283109 - 2283153 - 2280708
info@goreloslagos.cl
www.goreloslagos.gob.cl

Historial de modificaciones

Creación/Modificaciones del Documento

Versión	Fecha de modificación	Autor	Motivo	Páginas modificadas	Firma
1.0	19-12-2017	Oscar Oyarzo Pérez, Jefe Unidad de Informática	Creación de la primera versión del procedimiento	Todas	

Revisiones

Versión	Fecha	Autor	Observación	Páginas	Firma
1.0	19-12-2017	Oscar Oyarzo Pérez, Jefe Unidad de Informática	Sin observaciones	Todas	

Visto Bueno

Versión	Fecha	Encargado	Firma
1.0	19-12-2017	Fabiola Yáñez Rojas, Jefa Depto. Jurídico	

Distribuciones

Versión	Fecha	Encargado	Observaciones
1.0	Diciembre 2017	Carmen Mella Fagalde, Encargado (S) de Seguridad de la Información	Enviado por correo electrónico e instruida la publicación en intranet a la Unidad de Informática

Contenido

1. Objetivo

Asegurar que el equipamiento, relacionado a activos de información, se proteja y ubique de manera tal, que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y oportunidades de acceso no autorizado

2. Alcance o ámbito de aplicación interno.

El alcance del presente procedimiento es para todos los funcionarios del Gobierno Regional de Los Lagos, cualquiera sea su calidad contractual.

3. Roles y Responsabilidades.

3.1. Comité de Seguridad de la información:

- Definir los controles necesarios para la ubicación y protección del equipamiento.
- Identificar los equipos en áreas restringidas.

3.2. Coordinador del comité de seguridad de la Información:

- Responsable de validar y difundir el presente procedimiento.
- Apoyar al comité de seguridad de la información en la definición de medidas de protección necesarias.
- Velar porque se cumplan las medidas de protección definidas para los equipos.
- Controlar los sistemas de seguridad físicos (accesos físicos, áreas restringidas).

3.3. Dueños de activos físicos de información (jefes de departamentos y unidades):

- Los jefes de Departamentos o Unidades son los dueños de los activos físicos del área bajo su jurisdicción.
- Cumplir con los requerimientos del presente procedimiento.
- Generar y Mantener un inventario con el equipamiento, usuario del equipo del área bajo su jurisdicción.
- Informar al comité de seguridad de la información cualquier incidente que se vincule a la presente política.

3.4. Unidad de Informática:

- Gestionar (Identificar, Proteger y Respaldar) el equipamiento del Datacenter donde se encuentra ubicada la infraestructura de TI.

4. Definiciones.

Comité de seguridad de la información: Equipo de trabajo encargado de velar por la correcta aplicación de la política de seguridad de la información, aprobar y supervisar la aplicación de manuales y procedimientos de seguridad de la información, detectar y proponer soluciones a los incidentes de seguridad de la institución.

Activos de Información: Corresponde a todo aquello, material e inmaterial, que tiene algún valor para la institución y por lo tanto debe protegerse.

Datacenter: Espacio físico donde se almacenan los servidores y/o equipos de comunicaciones con los que opera el servicio, y en el cual los datos son almacenados, tratados y distribuidos al personal o procesos autorizados para consultarlos y/o modificarlos.

5. Procedimiento (Modo de Operación)

El procedimiento de ubicación y protección del equipamiento, hace referencia al tratamiento de los activos físicos/equipamiento (Datacenter, servidores, PC, Archivadores, equipos de comunicación etc.), que generan, almacenan e interactúan con medios de información sean estos tangibles (Papeles, Archivadores, dispositivos de almacenamiento, etc.) o intangibles (sistemas, programas, archivos digitales, Bases de Datos, etc.), generados y utilizados por la organización.

El Gobierno Regional de Los Lagos establece que los activos físicos/equipamiento, tendrán una ubicación conocida y un responsable, su adecuado uso y protección será responsabilidad tanto del dueño del activo como del funcionario a quien se le asigne.

5.1. Responsabilidades

- El dueño de los activos de información (jefes de departamentos o unidades), debe velar porque los activos físicos/equipamiento de propiedad de la institución se instalen dentro de inmuebles que le brinden una protección adecuada ante factores climáticos como humedad, calor, inundaciones, incendios, terremotos, etc.
- El dueño de los activos de información (jefes de departamentos o unidades), debe coordinar las tareas de concientización a todos los usuarios de activos de información del área bajo su jurisdicción en los procedimientos de seguridad de la información para la protección de los equipos, así como el de sus funciones en relación a la implementación de dicha protección.
- El dueño de los activos de información (jefes de departamentos o unidades), debe llevar y mantener un inventario de los activos de información físicos/equipamiento con que cuenta su departamento o unidad o área bajo su jurisdicción, este inventario deberá contener como mínimo características que permitan identificar el equipo, ubicación física del equipo, identificación por cargo y nombre del usuario de cada equipo, clave del equipo.
- El dueño de los activos de información (jefes de departamentos o unidades) debe asignar el equipamiento a un usuario responsable quien deberá velar por el resguardo y uso correcto del mismo, de manera de minimizar o evitar cualquier acceso no autorizado mediante la instalación de mecanismos de control adecuados (claves o controles que limiten el acceso, respaldos, etc.).
- Los usuarios responsables deberán evitar manipular comidas, bebidas y/o líquidos cerca de los equipos informáticos que puedan originar directa o indirectamente su mal funcionamiento
- Los usuarios responsables deberán establecer un entorno físico que no permita la visualización de contenido de la información sensible a distancia por personal

no autorizado, mantener claves que bloquen el contenido visual de los monitores o pantallas.

- Los usuario responsable deberán tener su equipo con clave, esta debe ser entregada al dueño de los activos de información (jefes de departamentos o unidades), quien llevara un registro de la ubicación y asignación del equipo.
- El usuario responsable al finalizar el uso del equipo asignado para sus labores se deberá asegurar que este quede apagados no basta con solo apagar la pantalla si es un PC.

Es recomendable instalar los activos de información físicos/equipamiento alejados de ventanas o fuentes generadoras de calor, lugares con poca ventilación, lugares sin iluminación, lejos de zonas de alto tráfico o acceso público.

Se deben utilizar sistemas físicos de seguridad como cajas fuertes, bóvedas o muebles con llave que dificulten el hurto, copia, modificación o destrucción de equipos, periféricos, documentos o medios de almacenamiento físico y digitales, a su vez estos sistemas mencionados constituirán un activos de información del Departamento o unidad y estarán bajo responsabilidad del dueño de los activos de información.

5.2. Reglas

Se deberá proteger los equipos, periféricos, equipos móviles físicamente contra la amenazas del medio ambiente, no deberá estar ubicados en lugares peligrosos o cerca de líquidos, Fuentes de calor o superficies inestables.

El dueño de los activos físicos (jefes de departamentos o unidades), deben saber la ubicación de los equipos bajo su área de jurisdicción, para ello deben llevar y mantener un inventario de los activos físicos con que cuenta su departamento o unidad o área bajo su jurisdicción, este inventario deberá contener como mínimo características que permitan identificar el equipo, ubicación física del equipo, identificación por cargo y nombre del usuario de cada equipo, clave del equipo.

No se debe manipular comidas, bebidas, líquidos y/o fumar cerca de los equipos informáticos que puedan originar directa o indirectamente su mal funcionamiento.

Se deberá proteger los equipos, periféricos, equipos móviles contra usos no autorizados mediante un bloqueo de seguridad sea físico o electrónico.

Se debe contar con sistemas de respaldo de energía UPS o grupos electrógenos que permitan la continuidad del servicio

Los equipos que sean fuente de generación de información física o digital (Impresoras, Scanner, etc.), no deberán quedar con información física al finalizar la jornada.

5.3. Incumplimiento, uso indebido y denuncias

a) Al detectar un uso indebido, se debe notificar inmediatamente al Coordinador de Seguridad de la Información y cuando corresponda, se deberán seguir los procedimientos locales de denuncia.

b) Si por cualquier motivo no se puede notificar al Coordinador de Seguridad de la Información, se puede presentar la denuncia de incumplimiento a cualquier miembro del Comité de Seguridad de la Información.

c) Las denuncias podrán ser de manera anónima. Esto se encuentra regulado en el Art. 90 B del DFL N°29 de 2004 del Ministerio de Hacienda, el que señala que las denuncias deben ser por escrito y firmadas por el denunciante. En ella podrá solicitarse que sean secretos los datos del denunciante.
d) No se permitirá ningún tipo de represalia contra ningún jefe, supervisor o empleado que, de buena fe, pida consejo al respecto o denuncie el incumplimiento de esta Política. Lo cual se encuentra regulado en el Art. 90 A del DFL N°29 de 2004 del Ministerio de Hacienda.
e) Si un jefe, supervisor o empleado presenta una denuncia falsa sobre un incumplimiento o un comportamiento cuestionable con la intención de perjudicar a otra persona, el denunciante será susceptible de una medida disciplinaria, conforme al Art. 62 N°9 del DFL 1.
f) El Coordinador de Seguridad de la Información debe ser informado inmediatamente en caso que se reciba cualquier comunicado (por teléfono, correo postal o correo electrónico) de parte de una autoridad de protección de datos u otro ente regulador.

5.4. Registros de Control del procedimiento.

- Inventario de activos de información físicos/equipamiento, con sus respectivos responsables.
- Imágenes de la ubicación y/o protección de activos de información (fotografías de los Datacenter).

6. Validez y gestión de documentos

Este documento es válido desde la fecha de su aprobación por parte del Encargado (S) de Seguridad de la Información.

El responsable de este documento es el Encargado de Seguridad de la Información que debe verificar, y si es necesario, actualizar el documento por lo menos una vez cada tres años o cuando el comité de seguridad de la información de defina.

Aprobado Por

Carmen Mella Fagalde **Encargada (S) de Seguridad de la Información**
20 de Diciembre de 2017