PS-NC-010

POLITICA DE SEGURIDAD FÍSICA Y AMBIENTAL

Sistema de Gestión de Seguridad de la Información – Nivel Central

Versión Oficial Actual v04 – Octubre del 2019

	Responsable	Fecha	Firma
Elaborado	Rodrigo Vidal / Encargado PMG SSI	Octubre 2019	
Revisado	José Villa / Área Seguridad de la Información (Representante Comité de Seguridad)	Octubre 2019	
Aprobado	Gabriel Reveco / Encargado Ciberseguridad (Presidente Comité de Seguridad de la Información)	Octubre 2019	

MINISTERIO DE SALUD COMITÉ SEGURIDAD DE LA INFORMACIÓN

MINISTERIO DE SALUD ENCARGADO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Toda versión impresa de este documento se considera como Copia No Controlada.

CONTENIDO

1 PROPOSITO 3
2 ALCANCE O AMBITO DE APLICACIÓN 3
3 MARCO NORMATIVO Y DOCUMENTOS RELACIONADOS 3
4 ROLES Y RESPONSABILIDADES 4
5 MATERIAS QUE ABORDA. 5
6 DIRECTRICES DE LA POLÍTICA 5
6.1 Definiciones particulares 5
6.2 Perímetros de seguridad física. 5
6.3 Controles de acceso físico. 6
6.4 Protección contra amenazas externas y del ambiente. 7
6.5 Trabajo en áreas críticas. 7
6.6 Áreas de acceso público, de entrega y de carga. 8
6.7 Ubicación y protección del equipamiento. 8
6.8 Mantenimiento del equipamiento tecnológico 9
6.9 Seguridad del cableado 9
6.10 Reutilización, retiro o eliminación segura de medios de almacenamiento 9
6.11 Sanciones respecto al uso inadecuado del equipamiento. 10
6.12 Suministro de energía y condiciones ambientales (elementos de soporte). 10
7 MECANISMO DE DIFUSIÓN. 11
8 PERÍODO DE REVISIÓN. 11
9 EXCEPCIONES AL CUMPLIMIENTO DE LA POLÍTICA 11
10 HISTORIAL Y CONTROL DE VERSIONES 11

1 PROPOSITO

Definir las directrices y requisitos para los perímetros de seguridad, controles de ingreso y protección física para resguarda las áreas donde se almacene o procese información sensible o existan medios de procesamiento de información. Asimismo, evitar la pérdida, los daños, el robo o el compromiso del equipamiento y la interrupción a las operaciones de la organización.

2 ALCANCE O AMBITO DE APLICACIÓN

Es aplicable a todos los funcionarios de planta, contrata, honorarios, consultores, practicantes y otros trabajadores, incluyendo las empresas que presten servicios en las dependencias y oficinas de la Subsecretarías de Salud Pública y Redes Asistenciales del MINSAL.

Aplica a todos los equipos entregados por la Subsecretaria de Salud Pública y Redes Asistenciales y que se encuentra en uso y fuera de las dependencias de la organización

En cuanto a las temáticas de protección abordadas, el ámbito de aplicación de esta política corresponde al (a los) Dominio(s) de Seguridad de la Información y Controles de Seguridad respectivos, detallados a continuación:

Alcance de Dominios y Controles de Seguridad de la Información (Nch-ISO 27001:2013)		
Nombre del Dominio	ID Control ISO 27001	Nombre del Control
Seguridad física y ambiental	A.11.01.01	Perímetro de seguridad física
	A.11.01.02	Controles de acceso físico
	A.11.01.04	Protección contra amenazas externas y del ambiente
	A.11.01.05	Trabajo en áreas seguras
	A.11.01.06	Áreas de entrega y carga
	A.11.02.01	Ubicación y protección del equipamiento
	A.11.02.02	Elementos de soporte
	A.11.02.03	Seguridad en el cableado
	A.11.02.04	Mantenimiento del equipamiento
	A.11.02.07	Seguridad en la reutilización o descarte de equipos
	A.11.02.08	Equipo del usuario desatendido
	A.11.02.09	Política de escritorio y pantalla limpios (como referencia externa)

3 MARCO NORMATIVO Y DOCUMENTOS RELACIONADOS

- Marco Normativo

- NCh-ISO27001:2009: Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información – Requisitos.
- El Marco Jurídico referido a los Sistemas de Seguridad de la Información (SSI), publicado en el portal del CSIRT del Ministerio del Interior.
  - Decretos Supremos y Normas Internacionales de Seguridad de la Información y Ciberseguridad:
  - Leyes relacionadas
- Decreto Supremo 47, del Ministerio de Vivienda y Urbanismo, Ordenanza general de la ley General de Urbanismo y construcciones".
- Decreto 594, del Ministerio de Salud "Reglamento sobre condiciones sanitarias y ambientales básicas en los lugares de trabajo".

- **Documentos Relacionados**
  - Política de pantallas y escritorios limpios.
  - Política equipamiento fuera de las instalaciones de la organización.
  - Procedimiento de gestión de derechos de acceso y devolución de activos.
  - Documentos de la Unidad de Higiene y Seguridad, publicados en sitio intranet http://intranet.minsal.cl/index.php/paginas/ver/38/
    - Reglamento Interno Higiene y Seguridad MINSAL
    - Procedimiento Guardias
    - Planes de Emergencia

4 ROLES Y RESPONSABILIDADES

- **Departamento de Administración y Servicios.**
  - Generar y difundir las directrices para la seguridad de los perímetros físicos del Minsal.
  - Implementar cuando sea requerido los controles de acceso físico a áreas críticas.

- **Departamento TIC.**
  - Gestionar y Controlar el acceso a la sala de procesamiento de datos.
- **Unidad de Higiene y Seguridad.**
  - Implementar y controlar las medidas de seguridad (aplicables en cada caso), definidas en esta política.

- **Autoridades y Jefaturas de División.**
  - Definir las áreas críticas de su dependencia.
  - Gestionar y controlar los accesos a áreas críticas de su dependencia
  - Designar y solicitar equipo a funcionario.
- **Jefa Depto. Administración y Desarrollo Institucional:**
  - Entrega de equipo.

- **Usuario:**

- Hacer uso responsable del equipo, informar del extravío/perdida; dejar constancia en Carabineros y pagar cuando corresponda.
- Obtener permiso oficial de su jefatura para salida de cualquier activo sensible.

5 MATERIAS QUE ABORDA.

- Perímetro de seguridad física
- Controles de acceso físico
- Protección contra amenazas externas y del ambiente
- Trabajo en áreas seguras
- Áreas de entrega y carga
- Ubicación y protección del equipamiento
- Elementos de soporte
- Seguridad en el cableado
- Mantenimiento del equipamiento
- Seguridad en la reutilización o descarte de equipos
- Equipo del usuario desatendido

6 DIRECTRICES DE LA POLÍTICA

6.1 Definiciones particulares

- Equipamiento:
  - Documentos, objetos o dispositivos que realizan o apoyan la realización de una función (BlackBerry; teléfono móvil; teléfono portátil; impresora; televisor; radio; grupo electrógeno; computador; modem, computador portátil, documentos u otros).

- Equipamiento crítico:
  - Aquel que debe estar siempre disponible, íntegro y que la información que contiene no debe sea divulgada.

6.2 Perímetros de seguridad física.

La protección física se debe realizar mediante la creación de diversas barreras o medidas de control físicas alrededor de las dependencias del Minsal y de las instalaciones de procesamiento de información.

Los perímetros de seguridad deben estar claramente definidos, la ubicación y la resistencia de cada uno de los perímetros dependerá de los requisitos de seguridad de los activos dentro del perímetro.

El perímetro de los edificios o lugares que contengan instalaciones de procesamiento de información, debe tener solidez física (por ejemplo, no tendrá zonas que se puedan derribar fácilmente); los muros externos deben ser sólidos y todas las puertas exteriores deben estar protegidas contra accesos no autorizados, mediante mecanismos de control, por ejemplo: vallas, alarmas, cerraduras, etc..; puertas y ventanas deben ser bloqueadas cuando se encuentren descuidadas y se debe contar con protección externa para las ventanas ubicadas en niveles bajos.

Debe existir un área de recepción atendida por personal u otros medios de control de acceso físico al área o edificio; dicho acceso físico debe ser restringido sólo al personal autorizado.

Donde existan puertas contra incendio, éstas deben tener alarma, ser supervisadas y probadas conjuntamente con las paredes para establecer el nivel requerido de resistencia de acuerdo a las normas regionales, nacionales e internacionales apropiadas; deberían funcionar de acuerdo con las disposiciones locales de protección contra el fuego de modo de garantizar la seguridad.

En las salas de cómputo o comunicaciones deben existir sistemas de detección de intrusos acorde a estándares internacionales y deben cubrir todos los lugares que permitan el acceso, debiendo estar adecuadamente protegidas contra accesos no autorizados, mediante mecanismos de control de acceso, provisto de alarmas.
Las áreas sin personal donde se almacene o procese información sensible, deben estar siempre equipadas con sistemas de seguridad.

Las áreas de procesamiento de información gestionadas por la organización deben estar físicamente separadas de aquellas gestionadas por terceras partes.

6.3 Controles de acceso físico.[1]

Las visitas autorizadas a ingresar al perímetro de seguridad con información sensible deben quedar registradas en recepción, detallando nombre, empresa, motivo de ingreso, fecha y hora de ingreso y egreso. Durante su permanencia debe estar siempre acompañado por personal debidamente autorizado, a menos que su acceso se haya aprobado previamente.

El acceso a las áreas donde se procesa o almacena información sensible debe ser controlado y restringido sólo a personas autorizadas (algunos medios de restricción de acceso físico son: portero electrónico, medios magnéticos con uso de clave, huella digital o tarjeta electrónica, guardias de seguridad, acceso restringido por llave, etc.).

El acceso a áreas seguras o sensibles de personal de terceras partes debe ser autorizado, supervisado y sólo cuando este acceso sea requerido.

[1] Procedimiento de Guardias

Las jefaturas directas, ante la situación de un cambio de cargo de un funcionario, deben revisar sus permisos de acceso físico asignados y verificar que éstos sigan siendo válidos de acuerdo a su nueva función.

Cuando un funcionario termina su relación laboral con el Minsal, es responsabilidad de las Jefaturas Directas informar formalmente al Departamento TIC de estas situaciones, para proceder a revocar los accesos de acuerdo a lo establecido en el Procedimiento de gestión de derechos de acceso y devolución de activos.

6.4 Protección contra amenazas externas y del ambiente[2].

En áreas donde exista una gran cantidad de productos combustibles o donde se almacenen, trasvasijen o procesen sustancias inflamables o de fácil combustión, deberá establecerse una estricta prohibición de fumar y encender fuegos, debiendo existir procedimientos específicos de seguridad para la realización de labores de soldadura, corte de metales o similares (estos lugares deben estar debidamente señalados). Estas áreas deben encontrarse a una distancia prudencial de las áreas definidas como seguras.

Todo lugar de trabajo en que exista algún riesgo de incendio, ya sea por la estructura del edificio o por la naturaleza del trabajo que se realiza, debe contar con extintores de incendio, del tipo adecuado a los materiales combustibles o inflamables que en él existan o se manipulen.

El número total de extintores dependerá de la superficie a proteger de acuerdo a lo señalado en el artículo 46 del Decreto Supremo N° 594.

Se deben almacenar los equipos redundantes y la información de resguardo en un sitio seguro y distante del lugar del Data Center, para evitar daños ocasionados ante eventuales contingencias en el sitio principal.

En el caso del Data Center, se debe impedir el ingreso de equipos fotográficos, de video, audio o cualquier equipo que pueda registrar información, a menos que este ingreso sea debidamente autorizado.

6.5 Trabajo en áreas críticas.

Las áreas críticas del Minsal corresponden a aquellas donde se encuentren ubicados los activos definidos como críticos.

Cualquier área que sea definida como crítica, debe ser protegida bajo las directrices definidas en esta política, contar con acceso restringido y controlado, que sólo permita el acceso a personal debidamente autorizado.

---

[2] Reglamento Interno de Higiene y Seguridad

El responsable de cada dependencia es quién define las áreas críticas (si aplica), en las dependencias que tenga a cargo. Cada vez que se definida un área de trabajo como crítica, el responsable de la dependencia debe informar al Encargado de Seguridad de la Información.

El responsable de cada dependencia debe mantener un registro actualizado con los funcionarios autorizados a ingresar de forma permanente a las áreas críticas.

El acceso de personal no habitual o personas externas, debe ser autorizado por la Jefatura respectiva o quien ésta faculte para ello. En este caso, el acceso debe quedar registrado, detallando nombre, empresa, motivo del ingreso, fecha y hora del ingreso y egreso. En estas áreas se debe evitar la ejecución de trabajos por parte de terceros, sin la debida supervisión.

Para todos los efectos, Minsal define como área crítica la sala de procesamiento de datos del Nivel Central, donde se almacenan los equipos de procesamiento de datos.

6.6 Áreas de acceso público, de entrega y de carga.

El acceso a la entrega y carga desde fuera del edificio debe ser restringido a personal debidamente identificado y autorizado.

Donde sea aplicable, las puertas externas deben ser aseguradas cuando se abran las puertas internas.

Cuando sea aplicable, el material que ingrese debe ser inspeccionado para evitar posibles amenazas antes de que sea ingresado a su lugar de utilización.

Donde sea aplicable los envíos entrantes y salientes deben segregarse físicamente.

6.7 Ubicación y protección del equipamiento.

El equipamiento debe ser ubicado y protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas, peligros ambientales, robo o hurto y oportunidades de acceso no autorizado.
Los lugares de trabajo deben localizarse preferentemente en ubicaciones que no queden expuestas al acceso de personas externas. De esta forma se protege tanto el equipamiento tecnológico como los documentos que pudiera estar utilizando el funcionario.

Los equipos que queden cerca de zonas de atención o tránsito de público, deben situarse de forma que las pantallas no puedan ser visualizadas por personas externas.

Se debe considerar las directrices de la Política de pantallas y escritorios limpios, evitando de esta forma los riesgos de acceso no autorizado, pérdida o daño en la información de MINSAL.

Los activos de información que requieren protección especial se deben aislar de accesos no autorizados.

No se deben ingerir alimentos o bebidas cerca de los equipos o dispositivos de procesamiento de información, así como colocar o manipular líquidos en su cercanía.

Los usuarios deben estar informados y concientizados de su responsabilidad en asegurarse que los equipos no supervisados y bajo su cargo, cuenten con la protección adecuada y se respetan los procedimientos establecidos al respecto.

6.8 Mantenimiento del equipamiento tecnológico

El equipamiento tecnológico central del CPD y los equipos de comunicaciones de la red MINSAL, deben mantenerse adecuadamente según la criticidad de los procesos que soportan, con el objeto de garantizar su disponibilidad e integridad, para solventar la continuidad operacional comprometida.

En los procesos de instalación de equipos, se deberá tener especial cuidado de no bloquear los sistemas de seguridad del recinto. Al término de la jornada, los equipos no instalados deberán ser dejados ordenados de manera que no entorpezcan la operación y las vías de evacuación.

Se debe establecer un programa de aprobación, control y mantenimiento preventivo que contemple un adecuado servicio de soporte técnico periódico para todos los equipos y dispositivos.

6.9 Seguridad del cableado

Los cables eléctricos y de telecomunicaciones que transportan datos o apoyan a los servicios de información se deben proteger contra la intercepción, interferencia o posibles daños.

MINSAL establecerá estándares mínimos a cumplir según funcionalidad y criticidad de las instalaciones. Normalmente se integran puntos de Voz y Datos, lo que se precisa en el estándar.

Las instalaciones de cableado estructurado para puntos de computación como telefónicos deben ser realizados por empresas que certifiquen el trabajo en base a la normativa técnica pertinente. Se debe mantener vigente los planos y el estado de las certificaciones por parte del encargado de Informática de la Organización.

6.10 Reutilización, retiro o eliminación segura de medios de almacenamiento

Se deberían verificar todos los equipos que contengan medios de almacenamiento para garantizar que cualquier tipo de datos sensibles y software con licencia se hayan

extraído o se hayan sobrescrito de manera segura antes de su retiro, eliminación o reutilización.

Se deben eliminar los medios de forma segura cuando no se necesiten más, usando procedimientos formales, acorde a la sensibilidad de la información y dejando registros de auditoría de tal acción.

Cada dueño de activo debe establecer el nivel de protección en cada caso.

6.11 Sanciones respecto al uso inadecuado del equipamiento.

Cuando los equipos de responsabilidad de un usuario sufran deterioro o daño por mal uso o uso irresponsable, el usuario se someterá a las medidas administrativas estipuladas por el estatuto administrativo.

6.12 Suministro de energía y condiciones ambientales (elementos de soporte).

El equipamiento debe estar protegido contra posibles fallas en el suministro de energía u otras anomalías eléctricas, en lo posible evitar puntos únicos de falla, mediante el uso de suministro de energía no interrumpible (UPS) y en lo posible, equipo generador.

Cada instalación que contenga equipos TI debe contar a lo menos con un sistema de extinción de incendios por ejemplo extintores que cumplan las especificaciones para incendios en equipos eléctricos, con su correspondiente identificación que indique la vigencia y el tipo de carga que contienen, así como también los implementos necesarios para su uso adecuado.

Estos equipos deben ser inspeccionados y probados en forma periódica, para asegurar su correcto funcionamiento y autonomía, siendo objeto de un programa de mantenimiento preventivo, el que debe considerar también, los tableros de energía eléctrica.

Las salas de procesamiento, deben tener el equipamiento necesario para mantener las condiciones de humedad y temperatura que los equipos contenidos en ella, requieren para su correcto funcionamiento. Debe proveerse un mecanismo automático de control, que permita generar una alarma audible ante falla de este equipamiento.

Las instalaciones eléctricas y de gas de los lugares de trabajo deberán ser construidas, instaladas, protegidas y mantenidas orientándose técnicamente según lo que establecen las normas vigentes establecidas por la autoridad competente.

Se deben ubicar los tableros de electricidad y de datos en lugares seguros y claramente identificados.

Se deben situar las llaves de corte de suministro de emergencia cerca de alguna de las salidas o de los tableros de alarmas.
Se debe inspeccionar en forma periódica el cableado, así como las cajas de conexión y los paneles de electricidad de distribución.

Se debe contar con UPS (unidades de suministro continuo de energía), estabilizadores y/o grupos electrógenos fijos y/o móviles para los recursos informáticos donde se procesa, comunica y conserva información considerada restringida y/o confidencial y/o crítica que afecte el patrimonio de la Organización.

7 MECANISMO DE DIFUSIÓN.

La comunicación de la presente política se efectuará de manera que el contenido de la documentación sea accesible y comprensible para todos los usuarios, a lo menos se deberá hacer difusión mediante los siguientes canales:

- Publicación en la intranet de Minsal http://isalud.minsal.cl/
- Correo informativo.

8 PERÍODO DE REVISIÓN.

La revisión del contenido de esta Política se efectuará a lo menos cada dos años por el Comité de Seguridad de la Información, o atendiendo necesidades de cambios para garantizar su idoneidad, adecuación y efectividad.

9 EXCEPCIONES AL CUMPLIMIENTO DE LA POLÍTICA

Frente a casos de especiales, el Comité de Seguridad de la Información evaluará y podrá establecer condiciones puntuales de excepción en el cumplimiento de las presentes directrices, siempre que no infrinja la legislación vigente. Toda excepción debe ser documentada y generar un proceso de revisión de la política, que determine si se deben agregar directrices en lo particular.

10 HISTORIAL Y CONTROL DE VERSIONES

Versión	Fecha	Pág. o Sección modificada	Motivo del cambio
0	Octubre 2012	Creación del documento	Creación del documento
1	Octubre 2013	Todas	Documento pasa de procedimiento a Política. Se amplía el alcance para la Subsecretaría de Redes Asistenciales.
2	Agosto 2014	2. Alcance 6. Política	Actualización y ampliación de la política, se incluyen controles de la norma NCh-ISO 27001.Of2009: 9.1.5 El trabajo en las áreas aseguradas.

			9.1.6 Áreas de acceso público, de entrega y de carga.
3	Octubre 2017	Todas	Se actualiza la referencia normativa de la versión 2013 de la norma 27001. Se actualizan las referencias normativas del documento. Se modifica el formato de la política (código, forma). Se ajustan los contenidos a los nuevos requisitos de la norma.
4	Octubre 2019	Todas	Se actualizan las referencias normativas del documento. En el punto 6.1.2 se incluyen directrices para la seguridad de las instalaciones eléctricas ty comunicaciones TI En el punto 6.8 se incluyen directrices sobre el mantenimiento del equipamiento. En el punto 6.9 se incluyen directrices sobre la instalación del cableado.