PS-NC-012

POLÍTICA SEGURIDAD EN EL USO DE INTERNET

Sistema de Gestión de Seguridad de la Información – Nivel Central

Versión Oficial Actual v02 – Julio 2020

Responsable		Fecha	Firma
Elaborado	Rodrigo Vidal / Unidad Seguridad TIC	Julio 2020	
Revisado	José Villa / Área Seguridad de la Información (Representante Comité de Seguridad)	Julio 2020	
Aprobado	Gabriel Reveco / Encargado Ciberseguridad (Presidente Comité de Seguridad de la Información)	Julio 2020	

Contenido

1 PROPOSITO

Definir e implementar restricciones de acceso a la navegación en Internet a usuarios, evitando con esto acceso a sitios web que sean riesgosos para el normal funcionamiento de las estaciones de trabajo y la red de datos de Minsal y sus Áreas dependientes.

2 ALCANCE O AMBITO DE APLICACIÓN

Todos los recursos computacionales que tengan acceso Internet, de Minsal y sus Áreas dependientes donde sea implementada esta política.

Esta política se aplica a toda la información electrónica contenida en los servidores centrales, estaciones de trabajo y equipos comunicacionales, que contengan datos, configuraciones, aplicativos y servicios críticos para el MINSAL.

Es aplicable a todos los funcionarios (planta, contrata, reemplazos y suplencia), personal a honorarios y terceros (proveedores, compra de servicios, etc.), que presten servicios para la Subsecretaría de Salud Pública y la Subsecretaría de Redes Asistenciales.

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
Administración de activos	A.08.01.03	Uso aceptable de los activos
	A.08.02.03	Manejo de activos

3 MARCO NORMATIVO Y DOCUMENTOS RELACIONADOS

- Marco Normativo
  - NCh-ISO27001:2013: 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

- **Documentos Relacionados**
  - Documento del Sistema de Gestión de Seguridad de la Información, disponibles en isalud.minsal.cl.

4 ROLES Y RESPONSABILIDADES

- **Encargado de Seguridad de la Información / Encargado de Ciberseguridad**
  - Revisar las categorías de navegación y las excepciones a las mismas.
  - Auditar la integridad de las categorías de permiso de navegación
  - Controlar la navegación de Internet.
  - Informar al Comité de Seguridad las situaciones anómalas acontecidas.
  - Enviar avisos por violación a las normas, políticas, procedimientos, estándares.

- **Departamento Tecnologías de la Información y Comunicaciones**
  - Implementar los filtros y reglas definidas en la presente política.

- **Usuarios**
  - Debe cumplir con lo establecido en esta política.

5 MATERIAS QUE ABORDA.

- Uso de Internet
- Uso aceptable de los activos
- Manejo de activos

6 DIRECTRICES DE LA POLÍTICA

6.1 Directrices Generales

Los permisos para el uso de Internet estarán limitados por la necesidad de acceso que requiera el desarrollo de la función de cada usuario.

El servicio de Internet se encuentra disponible para todos los usuarios que prestan servicios a la Institución, su uso es según el perfil asignado.

La asignación de perfiles es realizada por el Departamento Tecnologías de la Información y Comunicaciones a través de las IPs asignadas a los equipos.

6.2 Uso aceptable de Internet

Los usuarios de MINSAL deben utilizar como primera opción para conectarse a Internet los medios dispuestos por la Institución. De existir problemas con la conexión principal, los usuarios pueden acceder a través de otros canales de proveedores de servicios de Internet externos. Cuando se use la conexión alternativa, esta debe ser resguardada con medidas de seguridad tales como firewall entre la institución y la salida a Internet, equipos de escritorio actualizados en cuanto a antivirus, firewall del equipo, antimalware y parches de seguridad.

Se permitirá el uso ocasional o eventual de este servicio en tanto no interfiera con las funciones de los usuarios y no cause conflictos con la actividad del MINSAL.

Se permitirá el acceso a redes sociales, siempre y cuando la función del usuario lo requiera.

Las soluciones inalámbricas deben contar con portales cautivos1 para que las "visitas"2 que necesiten conexión a Internet solo puedan usar de manera controlada este medio, además de asegurar que la red de trabajo de la Institución se mantenga aislada de los mismos.

No se deben almacenar contraseñas en los navegadores.

6.3 Restricciones en el uso de Internet

No está permitido descargar desde Internet, material que infrinja el Ordenamiento Jurídico Nacional y/o las disposiciones contenidas en el Reglamento Interno, en el Código de ética o en la normativa establecida por la Institución.

El uso de las redes sociales como streaming de información, chats, foros, blogs y sitios de entretenimiento solo serán permitidos con la debida autorización formal de su Jefatura, Jefe TIC y Encargado de Seguridad de la Información.

El ingreso a páginas web con contenido pornográfico no está permitido.

La conexión de internet proporcionada por la red Minsal, no puede usarse para propósitos comerciales o de índole político.

El usuario no debe Transgredir la propiedad intelectual, secreto comercial, patentes, regulaciones u otra propiedad intelectual, incluyendo, pero sin limitarse a la instalación o distribución de software, que no se encuentre apropiadamente licenciado para el uso de la institución.

El usuario no puede Interferir o denegar cualquier servicio informático, utilizando programas, scripts, comandos o cualquier otro método, siendo realizados de forma interna o externa a la Institución.

El usuario que no tenga permiso no puede acceder a sitios de "hacking" o sitios reconocidos como inseguros, los cuales puedan poner en riesgo la integridad y confidencialidad de la información del Minsal.

Los usuarios no podrán publicar ningún tipo de información perteneciente al Minsal en sitios personales u otros, sin la autorización correspondiente del propietario de dicha información.

---

[1] Se entiende por "portal cautivo" a un ambiente limitado en cuanto a opciones de navegación y uso de aplicaciones, su uso está disponible para las visitas.
[2] Aquellas personas ajenas a la institución.

El usuario debe abstenerse de:

- Causar algún daño grave e inminente en la calidad o estabilidad del servicio informático o de las redes.

- Transgredir los derechos de cualquier persona o compañía protegida por “copyright”, secreto comercial, patentes, regulaciones u otra propiedad intelectual, incluyendo, pero sin limitarse a la instalación o distribución de software, que no se encuentre apropiadamente licenciado para el uso de la institución.

- Exportar software, información técnica, tecnología, software de encriptación u otro que implique violación a la legislación internacional y nacional sobre control de exportaciones ilegales.

- Utilización de activos computacionales para actividades circunscritas como ilícitas.

- Introducir programas maliciosos a la red o servidores (ej. Troyanos, virus, malware, otros).

- Realizar ofertas fraudulentas de productos o servicios utilizando activos institucionales.

- Efectuar infracciones de seguridad, interrupciones de servicios, que incluyen, pero no limitan, al acceso de información, conexión a servidores o cuentas sin una autorización expresa.

- En relación a interrupción de servicios, incluye, pero no se limita a, inspección de tráfico, inundación por ping, falsificación de paquetes de red, denegación de servicios y falsificación de información de ruteo para fines maliciosos.

- Realizar cualquier tipo de escaneo o monitoreo de redes o seguridad a menos que exista una notificación de la unidad de seguridad o sea parte de la actividad de su de trabajo.

- Eludir la autentificación de usuario o la seguridad de cualquier dispositivo, red o cuenta.

- Interferir o denegar cualquier servicio informático, utilizando programas, scripts, comandos o cualquier otro método, siendo realizados de forma interna o externa a la institución.

- Proveer información de cualquier tipo pertenecientes a la institución a partes externas, sin la debida formalización de la autorización.

- Se prohíbe todo lo que se considere como contenido con naturaleza ilegal (relacionados con hechos delictivos, pudiendo ser terrorismo, piratería, documentos electrónicos con infracción al derecho de autor, pornografía infantil, estafas y otros)

6.4 Monitoreo

Toda información entrante o saliente a Internet será monitoreada y registrada, por lo que podría ser revisada y auditada sin previo aviso, si las autoridades lo consideran necesario.

6.5 Filtro de contenido

A fin de establecer un adecuado acceso a sitios Web, se establecerán grupos de acceso de acuerdo con perfiles de los usuarios, estos grupos corresponderán a diferentes tipos de categorías de acuerdo a una definición estándar de la industria. A modo de ejemplo y con el propósito de establecer una definición formal al respecto utilizaremos, referencialmente, la definición de filtros WSA (Web Security Appliance)[3] que estarán permitidas en nuestros servicios de navegación:

6.6 Tipos de Filtros.

Para todos los usuarios conectados la red Ministerial con acceso a Internet se establecen tres niveles de acceso:

1. Acceso Completo (Filtro Ético)
2. Acceso General
3. Acceso Restringido

La definición de los usuarios por cada uno de los filtros definidos deberá ser asignada por el Encargado de Seguridad de la Información, sin embargo, el Filtro Ético será la mínima asignación posible, esto significa que nadie en la organización podrá tener acceso a las páginas definidas en este filtro.

[3] Esta definición está basada en las categorías establecidas por CISCO, solamente a modo de ejemplificar el procedimiento, pero se puede utilizar las categorías que estén disponibles en las plataformas institucionales propias

6.6.1 Filtro de Acceso Completo

Los usuarios que por su perfil hayan sido clasificados en el grupo de acceso Completo sólo tendrán las restricciones de navegación que corresponden al filtro Ético de la Red de Conectividad del Estado no tendrán otras restricciones, las restricciones del Filtro Ético y Completo serán las que se muestran a continuación:

Filtro de Contenido			
Grupo	**Grupo**	**Acceso Completo**	
Caetgoría WSA	**Descripción del Bloqueo**	**Block**	**Monit.**
Adult	Contenido para Adultos	X	
Child Abuse Content	Contenido de Abuso Infantil	X	
Dating	Sitio de Citas	X	
Extreme	Contenido Extremo	X	
Filter Avoidance	Sitios que utilizan protocolo Proxy para salarse medidas de seguri	X	
Freeware and Shareware	Sitios de descarga ilegales de software	X	
Gambling	Sitios de casinos y apuestas en línea	X	
Games	Sitios de juegos en línea	X	
Hacking	Contenido de Hacking	X	
Illegal Activities	Contenido de Actividades Ilegales	X	
Illegal Downloads	Contenido de Descargas Ilegales	X	
Illegal Drugs	Contenido de Drogas Ilegales	X	
Parked Domains	Sitios que venden dominios web con problemas	X	
Pornography	Contenido de Pornografía	X	
Weapons	Sitios relacionados con armas	X	

6.6.2 Filtro de Acceso General

Los usuarios que por su perfil hayan sido clasificados en el grupo de acceso General tendrán las restricciones del filtro Ético más algunos sitios adiciones que se detallan a continuación:

Filtro de Contenido			
Grupo Categoría WSA	**Grupo Descripción del Bloqueo**	**Acceso General**	
		Block	**Monit.**
Adult	Contenido para Adultos	X	
Child Abuse Content	Contenido de Abuso Infantil	X	
Dating	Sitio de Citas	X	
Extreme	Contenido Extremo	X	
Filter Avoidance	Sitios que utilizan protocolo Proxy para salarse medidas de seguri	X	
Freeware and Shareware	Sitios de descarga ilegales de software	X	
Gambling	Sitios de casinos y apuestas en línea	X	
Games	Sitios de juegos en línea	X	
Hacking	Contenido de Hacking	X	
Illegal Activities	Contenido de Actividades Ilegales	X	
Illegal Downloads	Contenido de Descargas Ilegales	X	
Illegal Drugs	Contenido de Drogas Ilegales	X	
Parked Domains	Sitios que venden dominios web con problemas	X	
Pornography	Contenido de Pornografía	X	
Weapons	Sitios relacionados con armas	X	
Advertisements	Anuncios Comerciales	X	
Alcohol	Sitios de elaboración y distribución de bebidas alcoholicas	X	
Astrology	Sitios de Astrología (Horóscopo Tarot, otros)	X	
Dynamic and Residential	Acceso a Redes domesticas de Casa Residenciales	X	
Entertainment	Sitios de Entrenimiento (Peliculas, videos, musicales, sitios de fans	X	
Internet Telephony	Sitios utilizados para servicios de telefonía por internet	X	
Lingerie and Swimsuits	Sitios utilizados para compra de lencería y trajes de baño	X	
Non-sexual Nudity	Sitios de desnudos de cuerpos humanos NO con carácter sexual	X	
Peer File Transfer	Sitios para transferencia de archivos	X	
SaaS and B2B	Sitios de servicio de reuniones y ventas en línea	X	
Safe for Kids	Sitios de educacion y animación en linea para niños	X	
Sex Education	Sitios relacionados con educacion sexual, embarazos	X	
Software Updates	Sitios relacionados con parches informáticos	X	
Web Hosting	Sitios web con entrega de información de nuestro sitios Web	X	
Uncategorized	Sitios que no esten categorizados dentro de estos 78 grupos	X	

6.6.3 Filtro de Acceso Restringido

Los usuarios que por su perfil hayan sido clasificados en el grupo de acceso Restringido tendrán las restricciones del filtro Ético más algunos sitios adiciones que se detallan a continuación:

Filtro de Contenido			
Grupo Categoría WSA	**Grupo Descripción del Bloqueo**	**Acceso Restringido**	
		Block	**Monit.**
Adult	Contenido para Adultos	X	
Child Abuse Content	Contenido de Abuso Infantil	X	
Dating	Sitio de Citas	X	
Extreme	Contenido Extremo	X	
Filter Avoidance	Sitios que utilizan protocolo Proxy para salarse medidas de seguri	X	
Freeware and Shareware	Sitios de descarga ilegales de software	X	
Gambling	Sitios de casinos y apuestas en línea	X	
Games	Sitios de juegos en línea	X	
Hacking	Contenido de Hacking	X	
Illegal Activities	Contenido de Actividades Ilegales	X	
Illegal Downloads	Contenido de Descargas Ilegales	X	
Illegal Drugs	Contenido de Drogas Ilegales	X	
Parked Domains	Sitios que venden dominios web con problemas	X	
Pornography	Contenido de Pornografía	X	
Weapons	Sitios relacionados con armas	X	
Advertisements	Anuncios Comerciales	X	
Alcohol	Sitios de elaboración y distribución de bebidas alcoholicas	X	
Astrology	Sitios de Astrología (Horóscopo Tarot, otros)	X	
Dynamic and Residential	Acceso a Redes domesticas de Casa Residenciales	X	
Entertainment	Sitios de Entrenimiento (Peliculas, videos, musicales, sitios de fans	X	
Internet Telephony	Sitios utilizados para servicios de telefonía por internet	X	
Lingerie and Swimsuits	Sitios utilizados para compra de lencería y trajes de baño	X	
Non-sexual Nudity	Sitios de desnudos de cuerpos humanos NO con carácter sexual	X	
Peer File Transfer	Sitios para transferencia de archivos	X	
SaaS and B2B	Sitios de servicio de reuniones y ventas en línea	X	
Safe for Kids	Sitios de educacion y animación en linea para niños	X	
Sex Education	Sitios relacionados con educacion sexual, embarazos	X	
Software Updates	Sitios relacionados con parches informáticos	X	
Web Hosting	Sitios web con entrega de información de nuestro sitios Web	X	
Uncategorized	Sitios que no esten categorizados dentro de estos 78 grupos	X	
Chat and Instant Messaging	Sitios que permitan servicios Chat's y mensajería instantanea	X	
Online Communities	Sitios que entregan información de grupos de interes y sociedades	X	
Online Storage and Backup	Sitios que permitan almacenar contenido de informacion en la nub	X	
Social Networking	Sitios que prestan servicios de redes sociales en línea	X	
Streaming Audio	Sitios quepermitenn transmision de audio en vivo (radios)	X	
Streaming Video	Sitios que permitenn transmision de video en vivo (TV y Youtube)	X	

6.6.4 Acceso a sitios web sin restricciones

Las siguientes categorías de sitios Web no estarán sujetas a restricciones.

Filtro de Contenido							
Grupo Categoría WSA	Grupo Descripción del Bloqueo	Acceso Restringido		Acceso General		Acceso Completo	
		Block	Monit.	Block	Monit.	Block	Monit.
Real Estate	Sitios de busqueda de arriendos, ventas, remates de propiedades		X		X		X
Sports and Recreation	Sitios de deportes, reglas, normas y estadísticas		X		X		X
Digital Postcards	Sitios que permitan enviar servicos de tarjetas y saludos digitales		X		X		X
Arts	Sitios que entregan contenido de arte, museos, galerias, etc		X		X		X
Auctions	Sitios de subastas en línea		X		X		X
Business and Industry	Sitios de Marketing, Comercio, Negocios etc.		X		X		X
Cheating and Plagiarism	Sitios de trabajos escrito plagio de documentos		X		X		X
Computer Security	Sitios de ofrecimiento de servicios de seguridad tecnológica		X		X		X
Computers and Internet	Sitios con información tecnica (Software y Hardware)		X		X		X
Dining and Drinking	Sitios con información de restaurantes y bares		X		X		X
Education	Sitios con información de Educacion		X		X		X
Fashion	Sitios con infromación de confeccion y moda		X		X		X
File Transfer Services	Sitios con información para transmision de datos		X		X		X
Finance	Sitios con información Financiera		X		X		X
Government and Law	Sitios con información legal		X		X		X
Hate Speech	Sitios con discursos mal intencionados		X		X		X
Health and Nutrition	Sitios con infoirmacion de nutrición y Salud		X		X		X
Humor	Sitios de Humor		X		X		X
Infrastructure and Content Deliv. Net.	Sitios con información de Infraesteructura y Redes tecnologia		X		X		X
Job Search	Sitios con información de Trabajos		X		X		X
Lotteries	Sitios de juegos de azar		X		X		X
Mobile Phones	Sitios con onformación de compañias de telefonía celular		X		X		X
Nature	Sitios con información de naturaleza		X		X		X
News	Sitios con información de noticias		X		X		X
Non-governmental Organizations	Sitios con información de organizaciones no gubernamentales		X		X		X
Online Trading	Sitios con información de venta en linea (ebay)		X		X		X
Organizational Email	Sitios con información de organizaciones no gubernamentales		X		X		X
Personal Sites	Sitios con informaciones personales		X		X		X
Photo Search and Images	Sitios con información y busqueda de Fotografia e imágenes		X		X		X
Politics	Sitios con información de carácter político		X		X		X
Professional Networking	Sitios con conformación de Profesionales de Redes		X		X		X
Reference	Sitios con inmformación de referencias		X		X		X
Religion	Sitios con información religiosa		X		X		X
Science and Technology	Sitios con información de Siencia y Tecnología		X		X		X
Search Engines and Portals	Sitios con infroamción de motores de busqueda y portales web		X		X		X
Shopping	Sitios con información de compras		X		X		X
Social Science	Sitios con información de Ciencia sociales		X		X		X
Society and Culture	Sitios con información de sociedades y cultura		X		X		X
Tobacco	Sitios con información de Tabaco		X		X		X
Transportation	Sitios con información de transporte		X		X		X
Travel	Sitios con información de Viejes		X		X		X
Web Page Translation	Sitios con información de traducción		X		X		X
Web-based Email	Sitios con informacion de correos basados en la web		X		X		X

6.6.5 Incidentes de Seguridad.

Los usuarios del Ministerio que identifiquen o perciban o sospechen de algún problema de seguridad se deben contactar inmediatamente Encargado de Seguridad de Sistemas de Información de la Institución.

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
01	Agosto 2013	Todas	Creación del documento
02	Julio 2020	Todas	Actualización del documento