Gobierno de Chile

MINISTERIO DE SALUD
DIVISIÓN JURÍDICA
JMS/AMB/SRO/MAS/GGR/AMSCH/NAA

APRUEBA POLITÍCA USO DE INTERNET PARA AMBAS SUBSECRETARÍAS.

EXENTA Nº 497 /

SANTIAGO, - 8 AGO. 2013

VISTOS: Lo dispuesto en la ley N° 19.880 que establece Bases de los Procedimientos Administrativos; en el decreto con fuerza de ley N°1, de 2014, del Ministerio de Salud, que fija el texto refundido, coordinador y sistematizado del decreto ley N° 2763, de 1979 y las leyes N° 18.933 y N°18.469; en el decreto supremo N° 136, de 2004, del Ministerio de Salud, que aprueba Reglamento Organico del Ministerio de Salud y el derecho de acceso a la información; en la ley N° 19.799 sobre documentos electrónicos, forma electrónica y servicios de certificación de dicha firma; en el decreto supremo N° 83, de 2004, del Ministerio Secretaria General de la Presidencia, que aprueba Norma Técnica para Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos; en la ley N° 19.233 sobre delitos informáticos; en la Norma Chilena NCh-ISO 27001.Of2009 Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Requisitos; en el Memorándum A18 N° 285, de 14 de agosto de 2012, del Jefe de Departamento Gestión Sectorial de TIC; en la resolución N° 1.600, de 2008, de la Contraloría General de la República; y

CONSIDERANDO:

1° Que, las nuevas tecnologías de la información y de las comunicaciones (TIC) al ser incorporadas progresivamente a los procesos institucionales y al quehacer personal de los funcionarios al ejercer sus labores en el Ministerio de Salud, presentan una serie de beneficios, ventajas y oportunidades de diversa índole, pero conlleva también ciertos riesgos, que pueden afectar a los activos de información institucional.

2° Que, por consiguiente, gestionar la seguridad de la información es un imperativo que se debe cumplir en el marco de la normativa gubernamental existente, y que consiste básicamente en la realización de todas aquellas actividades y tareas que sean necesarias para establecer los niveles de seguridad que la propia institución determine, basándose para ello en metodologías y técnicas estándares en estas materias, con el firme propósito de lograr introducir un ciclo de mejoramiento continuo y sostenible en el tiempo, que permita lograr niveles de integridad, confidencialidad y disponibilidad, con todos sus activos de información relevantes para la institución, como un principio clave en la gestión de procesos.

3° Que, debido a la implementación del sistema de seguridad de la información en conjunto por la Subsecretaría de Redes Asistenciales y la Susbsecretaría de Salud Pública, se ha creado la Política Uso de Internet, según los requisitos de la Norma ISO 27002 y lo dispuesto por la red de expertos.

4° Que, en mérito y conforme a lo anterior, dicto la siguiente:

RESOLUCIÓN:

1° APRUÉBASE la Política Uso de Internet para las Subsecretarías de Salud Pública y de Redes Asistenciales, cuyo texto es el siguiente:

POLÍTICA USO DE INTERNET
2013

NOTA DE CONFIDENCIALIDAD DE ACUERDO A CLASIFICACIÓN

Este documento es de propiedad exclusiva del Ministerio de Salud y su uso debe estar ceñido a lo dispuesto en la clasificación del mismo, quedando prohibida la divulgación y/o reproducción total o parcial del contenido de éste sin la debida autorización por parte del Comité de Seguridad de la Información Sectorial. Su uso y distribución sólo está autorizado al interior del MINSAL y por parte del personal debidamente habilitado.

Aprobó	**Revisó**
Encargado de Seguridad de la Información Redes	Comité de Seguridad de la Información
Encargado de Seguridad de la Información Pública	

I. DECLARACION INSTITUCIONAL.

A través de esta Política MINSAL establece las normas para regular el uso y navegación de Internet. Esta Política se ampara en la Política TI de Salud Pública.
Se define Internet como un servicio provisto para los usuarios, aplicaciones y desde la integración con otros sectores expresamente autorizados por MINSAL, que lo requieran como apoyo a sus funciones/funcionamiento. Se les permite el uso siempre cuando cumplan con las directrices sobre el uso adecuado de este recurso de información, indicadas en esta política.
Se entiende por:

- Uso aceptable de internet: Uso para el cometido de las funciones o aplicaciones siempre y cuando no viole o incumpla alguna normativa o restricción de esta política.

Los usuarios/sistemas que violen las disposiciones establecidas en este documento están sujetos a acciones disciplinarias contractuales según lo define el estatuto administrativo o acciones civiles o contrato según corresponda.

Todos los usuarios[1] (según la definición "de otros sectores" implica honorarios y personal contratado como compra de servicio o subcontratado) están obligados a acusar recibo y comprensión de las normas contenidas en el presente documento.

Las disposiciones contenidas en esta Política tienen por objeto maximizar el uso de los recursos del MINISTERIO, protegiendo el ancho de banda con que se cuenta, y la integridad de la información de la Institución.

El uso de todos los recursos de Internet podrá ser auditado.

Estarán disponibles servicios de internet con atributos restringidos.

II. OBJETIVO.

- Sensibilizar y formar al personal sobre las amenazas que pueden presentarse a través de internet.
- Fomentar el uso correcto y eficaz de los recursos del MINSAL.
- Regular la conexión de las aplicaciones y sitios externos.

III. ALCANCE.

Esta política se aplica a todo los usuarios con acceso a Internet y servicios relacionados.

IV. RESPONSABILIDADES.

Encargado de Seguridad de la Información.

- 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.

Funcionarios de MINSAL.

- Todo funcionario de MINSAL tiene la obligación de informar a sus Jefaturas Directas de cualquier actividad que contravenga lo aquí estipulado o que simplemente le resulta sospechosa.
- Ser responsable del acceso permitido para el uso de internet.

Los administradores de las aplicaciones:

- Responsables de hacer modificaciones a la aplicación.

V. DEFINICIONES.

a. Internet: Servicio provisto para los usuarios, aplicaciones y desde la integración con otros sectores expresamente autorizados por MINSAL, que lo requieran como apoyo a sus funciones/funcionamiento.

VI. DESARROLLO DEL TEMA.

El uso correcto de Internet se define desde dos ámbitos:

a. Desde el Usuario.

i. Gestión de perfiles

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 Gestor TI a través de las IPs asignadas a los equipos.

---

[1]Se incluye dentro de los usuarios a los administradores, jefes de proyecto o de otros sectores.

ii. Uso 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 cautivos[2] para que las "visitas"[3] 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.

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

Cuando un usuario tenga una duda respecto a lo que constituye un uso aceptable de Internet debe consultar al Encargado de Seguridad de la Información o al Gestor TI correspondiente.

No se deben almacenar contraseñas en los navegadores.

iii. Restricciones al uso 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 TI y Encargado de Seguridad de la Información.

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

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 MINISTERIO.

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

---

[2] 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.
[3] Aquellas personas ajenas a la institución.

El acceso a las siguientes categorías no está permitido:

Potencialmente Cuestionables
• Abuso de drogas ilícitas y alcohol • Hacking • Ilegal o no Éticos • Discriminación • Violencia Explicita • Grupos extremistas • Proxy Anónimos- Navegación de incognitos • Plagio • Abuso de menores
Sitios y Contenidos de Adultos
• Ocultismo • Aborto • Otro material adulto • Juegos • Nudismo y sitios subidos de tono • Pornografía • Citas • Tabaco • Venta de Armas • Deporte de caza y juegos de guerra
Consumo de ancho de banda
• Sitios de descarga de programas • Sitios de almacenamiento de archivos y de compartición • Sitios de descarga y uso de streaming • Uso de software P2P • Radio y televisión por Internet • Telefonía por Internet
Riesgos de Seguridad
• Sitios maliciosos • Phishing

• Spam URLs
Personal
• Propaganda • Negocios y corretaje • Juegos

Cualquier excepción deberá ser estudiada por el Encargado de Seguridad y el Comité de Seguridad de la Información.

El uso de todos los recursos de Internet podrá ser auditado.

b. Desde las aplicaciones propias y de terceros.

Los referentes TI de las distintas organizaciones pertenecientes al sector público de la salud deben identificar las aplicaciones tanto internas como externas que necesitan ser accedidas, a fin de asegurar su acceso.

Datos a informar:

Aplicaciones Internas
IP Interna
Puertos a Utilizar
IP Pública Asignada
IP Pública que accederá (si corresponde)
URL
Objetivo de la Aplicación
Jefe TI que autoriza
Contacto Técnico, email, Teléfono

Aplicaciones Externas
Rangos Internos que deben acceder
Puertos a Utilizar
IP Pública Destino
URL
Objetivo de la Aplicación
Jefe TI que autoriza
Contacto Técnico, email, Teléfono

Todas aquellas aplicaciones/sistemas o equipos que funcionan internamente pero que son soportadas por terceros que necesitan acceso desde Internet, se les asignarán accesos vía VPN.

Para el flujo de información generado desde las aplicaciones internas y/o externas, se debe utilizar el protocolo SSL[4] , cuando estas aplicaciones ocupen y/o utilicen datos confidenciales según la Ley de protección de datos personales N° 19.628.

VII. CONTROL DE VERSIONES.

VERSION	FECHA DE	MOTIVO DEL CAMBIO

[4] **SSL** son las siglas en inglés de ***Secure Socket Layer*** (en español **capa de conexión segura**). Es un protocolo criptográfico (un conjunto de reglas a seguir relacionadas a seguridad, aplicando criptografía) empleado para realizar conexiones seguras entre un cliente (como lo es un navegador de Internet) y un servidor (como lo son las computadoras con páginas web).

	APROBACION	
0	Julio 2013	Creación de la Política de Uso de Internet.

ANÓTESE Y COMUNÍQUESE.-

DR. JORGE DÍAZ ANAÍZ
SUBSECRETARIO DE SALUD PÚBLICA

DR. LUIS CASTILLO FUENZALIDA
SUBSECRETARIO DE REDES ASISTENCIALES

Distribución:
Gabinete Subsecretaría de Redes Asistenciales.
Gabinete Subsecretaría de Salud Pública.
Departamento de Control de Gestión Ministerial
Departamento de Gestión de la Información
Departamento de Tecnologías de la Información SSP
Departamento de Tecnologías de la Información SRA
Gabinete del Ministro
División Jurídica
Oficina de Partes