PS-NC-012

POLÍTICA PROTECCIÓN DE MENSAJES ELECTRÓNICOS

Sistema de Gestión de Seguridad de la Información – Nivel Central

Versión Oficial Actual v02 – Junio 2020

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

Contenido

1 PROPOSITO

El propósito de esta Política es definir las normas para el uso correcto y protección del servicio de correo electrónico del Ministerio de Salud (Minsal), y regular el uso, la confidencialidad e integridad y el almacenamiento de los correos electrónicos.

2 ALCANCE O AMBITO DE APLICACIÓN

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, a quienes se les otorgue una casilla de correo electrónico.

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
Seguridad de las operaciones	A.12.02.01	Controles contra código malicioso
Seguridad de las comunicaciones	A.13.02.01	Políticas y procedimientos de transferencia de información
	A.13.02.03	Mensajería electrónica

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.**
  - Definir los controles de seguridad para la protección de los correos electrónicos.

- Recibir alertas de seguridad.
- Activar el procedimiento de gestión de incidentes de seguridad de la información.

- **Departamento de Gestión Sectorial TIC.**
  - Velar por la disponibilidad permanente del servicio de correo electrónico.
  - Planificar y ejecutar los cambios en el hardware y software asociado al servicio de correo electrónico.
  - Administrar el servicio de correo electrónico.
  - Habilitar mecanismos tecnológicos de manera de prevenir el uso de técnicas de ataque a sistemas de correo electrónico.
  - Generar las condiciones que permitan el tráfico y manejo seguro de la información que es enviada o recibida a través de correo electrónico.

- **Departamento TIC (Soporte).**
  - Registrar y asignar las solicitudes asociadas al servicio de correo electrónico.
  - Ejecutar las solicitudes relacionadas al servicio de correo electrónico.

- **Funcionarios.**
  - Cumplir con las normas definidas en esta política.

5 MATERIAS QUE ABORDA.

- Uso aceptable de los activos
- Manejo de activos
- Controles contra código malicioso
- Políticas y procedimientos de transferencia de información
- Mensajería electrónica

6 DIRECTRICES DE LA POLÍTICA

6.1 Acceso al correo electrónico

Las cuentas de correo electrónico asignadas a los funcionarios son propiedad del Minsal y son suministradas únicamente con el propósito de enviar y recibir comunicaciones de los miembros del Ministerio, proveedores y terceros relacionados a los fines institucionales.

Las cuentas de correo electrónico son asignadas de manera personal e intransferible, quedando prohibido su uso por terceros. Cada funcionario será el único responsable de las acciones que se realicen con su cuenta[1].

[1] La asignación de cuentas de correo electrónico se realiza de acuerdo con lo descrito en el Procedimiento gestión de derechos de acceso y devolución de activos.

Como consecuencia de lo anterior, cada funcionario tiene la obligación de mantener la confidencialidad de su contraseña de correo, según lo establecido en la **Política de Seguridad sobre identificación y autenticación de usuarios**[2].

Solamente cuando exista una razón de interés institucional que afecte las operaciones, el Minsal tendrá la facultad para verificar que se está dando el uso adecuado a estos medios, por lo que podrá acceder a la información contenida en los mismos para realizar investigaciones por sospecha y abuso.

6.2 Uso del correo electrónico

El uso aceptable del correo se basará fundamentalmente en la comunicación entre funcionarios, proveedores y terceros para fines institucionales.

La plataforma de correo autorizada es la proporcionada por el Minsal, quedando estrictamente prohibida la utilización de otro sistema de correo para fines institucionales.

El uso de recursos de Ministerio de Salud para envío o recepción de correos electrónicos personales es aceptada, pero los correos que no estén relacionados con el trabajo deben guardarse separadamente de los relacionados con su labor.

La solicitud de creación de cuentas genéricas y listas de distribución es responsabilidad del Jefe de la Unidad o Departamento que requiera dicha funcionalidad. Éstas deberán ser asignadas a una persona, la cual será responsable de la cuenta y aparecerá como tal. Las listas de distribución sólo podrán contener correos institucionales.

6.3 Uso prohibido

Se prohíbe el uso del correo electrónico para:

- Fines ajenos a los de la institución, como, por ejemplo; transmitir archivos de música, videos, imágenes, presentaciones, mensajes masivos (SPAM), que no estén relacionados con las actividades del Minsal.

- Crear o distribuir mensajes que puedan ser ofensivos o difamatorios, acerca de la raza, género, características físicas o sicológicas, destreza, edad, orientación sexual, creencias o prácticas religiosas, creencias políticas o nación de origen.

- Difundir mensajes con contenidos tales como política, campañas electorales, religión, entretenimiento, utilidad pública, opinión de terceros, distribución de software ilegal, software no licenciado o pornografía.

[2] Documento disponible en isalud.minsal.cl seguridad de la información.

- Enviar y recibir mensajes con archivos adjuntos que excedan el tamaño máximo autorizado.

- Utilizar cuentas de correo electrónico de otros usuarios.

- Difundir de forma masiva las direcciones de correo del ministerio, ya sea para facilitar su uso con fines comerciales, publicitarios u otros no asociados al trabajo.

- Suscribirse a sitios Web a nombre propio, de la institución o de terceras personas, con la casilla de correo del Minsal, con fines distintos a los requeridos para las tareas propias del servicio.

- Enviar correos electrónicos con archivos que no hayan sido revisados mediante antivirus. Será responsabilidad del usuario emisor del mensaje la revisión mediante antivirus. Las áreas receptoras de mensajes infectados con virus deberán abstenerse de abrirlos y deberán informar a Soporte TIC sobre su existencia.

- Se prohíbe difundir por correo electrónico, dentro o fuera del Ministerio, información clasificada como confidencial. En este caso todo correo electrónico deberá tener en el campo asunto la palabra CONFIDENCIAL, y, de ser posible, se deberá utilizar técnicas de encriptación.

- En caso de recibir un correo electrónico desde algún usuario no identificado, o con sospecha de algún tipo de amenaza de seguridad, se deberá informar a Soporte TIC sobre dichos eventos.

6.4 Confidencialidad e integridad de los correos electrónicos

Con el objetivo de mantener la confidencialidad e integridad de los correos electrónicos, todos los funcionarios tienen la obligación de mantener confidenciales sus claves de acceso y utilizar claves robustas, de acuerdo con lo establecido en la **Política de Seguridad en la Identificación y Autenticación de Usuarios**.

Será responsabilidad del funcionario usuario de una cuenta de correo electrónico modificar su clave de acceso si considera que podría haber sido vulnerada.

Será responsabilidad del remitente toda la información transmitida por correo electrónico.

Se podrá acceder al contenido de los correos electrónicos de los usuarios del servicio de correo del Ministerio de Salud o de los documentos adjuntos, en los siguientes casos:

a) En cualquier clase de litigio, previa orden judicial, que requiera comprobar el uso del correo electrónico, en aquellos casos en los que haya indicios de que el funcionario ha hecho un mal uso. El acceso debe hacerse en presencia del funcionario o, si la este quiere, de un representante.

b) Para llevar a cabo tareas de mantenimiento o vinculadas a la seguridad del sistema. En tales casos, se informará al funcionario de las tareas que deben llevarse a cabo y se le ofrecerá la posibilidad de estar presente.

6.5 Archivo y almacenamiento

El servicio de correo electrónico debe ser utilizado exclusivamente como un medio de transmisión de información y no de almacenamiento o gestión de información. En consecuencia, cada funcionario es responsable de almacenar la información relevante en carpetas de trabajo personales creadas directamente en su equipo. Es decisión del funcionario la forma de organizar su correo y su archivo en carpetas personales.

Cada funcionario es responsable del uso racional del correo electrónico en cuanto a: capacidad asignada, límites de tamaño de correo y cantidad de destinatarios.

corresponde a cada usuario velar por que la gestión de la información contenida en su correo electrónico sea adecuada. Para ello debe revisar periódicamente la bandeja de entrada y, si procede, la de salida, como mínimo una vez al día. En este sentido, se recomienda eliminar los mensajes que no deban conservarse y archivar el resto en la carpeta o subcarpeta apropiada, especialmente los que pueden tener un contenido personal.

Los mensajes que formen parte de un procedimiento, u otros que deban conservarse, tienen que estar debidamente archivados en el expediente correspondiente, puesto que es previsible que se borren al cabo de un tiempo o se llegue a un tope de capacidad.

Los correos electrónicos con fines privados deben ser borrados o movidos cada día por si es necesario hacer un traspaso o eliminación de la cuenta por motivos profesionales.

6.6 Formato de correo electrónico

Toda dirección de correo electrónico debe identificar al usuario que se asigna haciendo referencia, a lo menos, a su nombre y apellido. Por ejemplo: nombre.apellido@minsal.cl.

Todo correo electrónico enviado desde una cuenta del Minsal debe incluir, en su pie de página, una advertencia en cuento a su uso y autorizaciones, quedando bajo responsabilidad del receptor el cuidado y resguardo de la información. El formato para utilizar es el siguiente:

“Este mensaje y sus adjuntos pueden contener información confidencial y es para uso exclusivo de la persona o entidad de destino. Si no es usted el destinatario indicado, queda notificado que la lectura, utilización, divulgación, reenvió o copia sin autorización no está autorizado por el firmante y se encuentra estrictamente prohibido en virtud de la legislación

vigente. Si ha recibido este mensaje por error, le rogamos que nos lo comunique inmediatamente por esta misma vía y proceda de inmediato a su destrucción".

6.7 Correos sospechosos

Se debe sospechar de correos cuando:

- El cuerpo del mensaje presente cambios de aspecto (logotipos, pie de firma, etc.) con respecto a los mensajes recibidos anteriormente por ese mismo remitente;
- El mensaje contiene una «llamada a la acción» que nos urge, invita o solicita hacer algo no habitual;
- Se soliciten credenciales de acceso a una web o aplicación (cuenta bancaria, ERP, etc.)

Ante cualquier duda en uno de estos puntos, no se debe abrir el correo e información de inmediato al área de soporte TIC.

6.8 Identificación del remitente

No se deben abrir correos sin identificar el remitente. Si el remitente no es un contacto conocido se debe prestar especial atención ya que puede tratarse de un nuevo cliente o de un correo malicioso. Si el remitente es un contacto conocido, pero por otros motivos (cuerpo del mensaje, archivos adjuntos, enlaces, etc.) se sospecha que se ha podido suplantar su identidad, debes contactar con éste por otro medio para confirmar su identidad, en caso de un incidente informar al área de soporte TIC.

6.9 Análisis de archivos adjuntos

Al recibir un mensaje con un adjunto, se debe analizar cuidadosamente antes de abrirlo. Aunque el remitente sea conocido puede haber sido suplantado y no percibirnos. La descarga de adjuntos maliciosos podría infectar los equipos con algún tipo de malware (programa maligno). Se debe tener activado y actualizado el antivirus para identificar los archivos maliciosos. Para identificar los correos maliciosos se debe prestar atención a los siguientes puntos:

- Tiene un nombre que nos incita a descargarlo, por ser habitual o porque tiene un contenido atractivo;
- El icono no corresponde con el tipo de archivo (su extensión), se suelen ocultar ficheros ejecutables bajo iconos de aplicaciones como Word, PDF, Excel, etc.;
- Tiene una extensión familiar, pero en realidad está seguida de muchos espacios para que no veamos la extensión real (ejecutable) en nuestro explorador de ficheros, por ejemplo: listadoanual.pdf .exe;
- Solicita habilitar opciones deshabilitadas por defecto como el uso de macros;
- No se reconoce la extensión del adjunto y puede que se trate de un archivo ejecutable (hay muchas extensiones con las que no se está familiarizado); es o encubre un archivo JavaScript (archivos con extensión .js).

6.10 Inspección de enlaces

Al recibir un mensaje con un enlace, antes de hacer clic se debe:

- Revisar la URL, situar el puntero del ratón, sobre el texto del enlace, para visualizar la dirección antes de hacer clic en él;
- Identificar enlaces sospechosos que se parecen a enlaces legítimos revisando que:
  - ✓ Pueden tener letras o caracteres de más o de menos y pasarnos desapercibidas;
  - ✓ Podrían estar utilizando homógrafos, es decir caracteres que se parecen entres sí en determinadas tipografías (1 y l, O y 0), por ejemplo www.m1nsal.cl, www.mlnsal.cl.

6.11 Uso de correo en redes públicas

No utilizar el correo electrónico desde conexiones públicas (por ejemplo, wifi de una cafetería, el ordenador de un hotel, wifi de un hotel, etc.), en estos casos nuestro tráfico de datos puede ser interceptado por cualquier usuario de esta red. Como alternativa, es preferible utilizar redes de telefonía móvil como el 3G o 4G, desde el celular, o una conexión por VPN.

6.12 Cifrado y firma digital

El correo electrónico debe contar con cifrado y firma digital para proteger la información confidencial y asegurar la autenticidad del remitente.

6.13 Ausencia del funcionario o funcionaria

En caso de ausencia programada superior a 3 días, el titular de la cuenta de correo deberá activar el mensaje de ausencia de oficina para facilitar otra dirección de contacto que garantice la continuidad de la actividad.

6.14 Cese de la relación contractual

La Institución puede cancelar la prestación del servicio de correo, ya sea por el término de la relación contractual con el funcionario o cuando el usuario esté haciendo un mal uso de dicho servicio.

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	Julio 2014	Todas	Creación del documento
02	Junio 2020	✓ Correos sospechosos ✓ Identificación del remitente ✓ Análisis de archivos adjuntos ✓ Inspección de enlaces ✓ Uso de correo en redes públicas Cifrado y firma digital	Actualización del documento Se incluyen nuevas cláusulas de seguridad