



RESOLUCION EXENTA N° 7916

PUNTA ARENAS, 09 AGO. 2018

VISTOS: Los antecedentes respectivos: 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 2005, del Ministerio de Salud, que fija el texto refundido, coordinador y sistematizado del Decreto Ley N°2763, de 1979 y de las leyes N°18.933 y N°18.469; en el Decreto Supremo N°136, de 2004, del Ministerio de Salud, que aprueba Reglamento Orgánico del Ministerio de Salud; 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 Secretaría 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 27002 Of.2013; y 10 manifestado en la Resolución Exenta N° 1161 del 04.10.2016 que Aprueba el Sistema de Seguridad de la Información; Resolución Exenta N°4322/26.04.2018 Estructura Orgánica del Servicio de Salud Magallanes; Resolución Exenta N°6440/25.06.2018 que modifica la Resolución Exenta N°4322/26.04.2018; Resolución Exenta N°2888/20.07.2011 de la DSSM, que encomienda como Subdirectora Médica del Servicio de Salud Magallanes a Dra. Maria Cristina Diaz Muñoz; Decreto Exento N°83/12.04.2018 Ministerio de Salud, pone término y establece orden de subrogancia al cargo de Director del Servicio de Salud Magallanes; Decreto Exento N°97/31.05.2018 que modifica Decreto N°83 que establece orden de subrogancia al Cargo de Director del Servicio de Salud Magallanes y en uso de las facultades dicto lo siguiente:

CONSIDERANDO:

La necesidad de contar con adecuadas políticas de seguridad de la información, destinadas a proteger los recursos de información y la tecnología utilizada para su procesamiento. Todo, con el firme propósito de lograr introducir un ciclo de mejoramiento continuo y sostenible en el tiempo que permita alcanzar niveles de integridad, confidencialidad y disponibilidad, con todos los activos de información relevantes para la institución, como un principio clave en la gestión de procesos,

Memorándum N°15/07.07.2018 de Gestor Regional TI de la Dirección del Servicio de Salud Magallanes, que solicita validar Políticas de Seguridad y Procedimientos,

RESOLUCION

1.- APRUÉBASE a contar del 11 de Julio de 2018 y hasta nueva revisión la **POLÍTICA DE SEGURIDAD EN EL USO DE ESTACIÓN DE TRABAJO** del Departamento Control de Gestión y Tecnología de Información y Comunicaciones.

2.- Entiéndase como parte integrante de la presente resolución dicho documento, que a continuación se indica:

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DSSM



POLÍTICA DE SEGURIDAD EN EL USO DE ESTACIÓN DE TRABAJO

Preparado por:	Equipo TIC SS Magallanes				
Revisado por	Pablo Alexis Cona Romero				
Revisado por					
Aprobado por:	Pablo Alexis Cona Romero	Fecha de Aprobación:	10-07-18		
		Fecha de Publicación:	Julio 2018		
		Vigente desde:	11-07-18		
		Vigente Hasta:	Nueva Revisión		
Control de versiones					
Versión	Fecha de Vigencia	Aprobado por	Fecha publicación	Firma	Comentario
1.0	10-07-18	Pablo Alexis Cona Romero	11-07-18		

(*) La presente versión substituye completamente a todas las precedentes, de manera que éste sea el único documento válido de entre todos los de la serie.

NOTA DE CONFIDENCIALIDAD DE ACUERDO A CLASIFICACIÓN: Este documento es propiedad exclusiva de la Dirección del Servicio de Salud Magallanes, queda prohibido cualquier reproducción, distribución o comunicación pública total o parcial, salvo autorización expresa del Comité de Seguridad de la Información. Antes de utilizar alguna copia de este documento, verifique que el número de versión sea igual al que se encuentra publicado en intranet.

Cualquier pregunta o comentario sobre esta Política de Seguridad de Información dirigirla al Departamento TIC.

POLÍTICA DE SEGURIDAD EN EL USO DE ESTACIÓN DE TRABAJO

DECLARACIÓN

Los dispositivos tecnológicos de propiedad de Servicio de Salud de Magallanes, incluyendo las estaciones de trabajo y computadores portátiles, son asignados a los colaboradores para apoyar la realización de su trabajo dentro de la institución debiendo ser utilizados solamente para esos fines.

ÁMBITO

- Se define como Estaciones de trabajo y otros equipos personales el conjunto de elementos tecnológicos de hardware y software que lo componen.
- A nivel de Hardware incluyen: pantalla, teclado, mouse, unidad central (CPU), unidad de CD/ DVD interna/externa, impresoras, scanners, teléfonos fijos y móviles, tablets, medios de almacenamiento externo, lectores biométricos, tarjetas de red inalámbricas, fax y cables.
- A nivel de Software incluyen: Los programas de aplicación, sistemas de información o aplicaciones, software de escritorio, software de administración, sistemas operativos y rutinas de comunicación o de uso general.

ROLES Y RESPONSABILIDADES

- Departamento de Tecnologías de Información y Comunicación (TIC's)
 - ✓ Incorporar, deshabilitar y/o modificar cualquier dispositivo de hardware o software, incluido el intercambio de componentes de un computador personal con otro.
 - ✓ Disponer de medios seguros para que el usuario almacene sus datos sensibles.
 - ✓ Autorizar el traslado o reasignación de equipos de computación o comunicaciones.
 - ✓ Velar por la recuperación y respaldo de la información de todos los equipos o computadores personales que están en condiciones de desecho o reutilización.
- Representante del Comité de Seguridad de la Información
 - ✓ Controlar y revisar el cumplimiento de la política y los procedimientos asociados a ella.
 - ✓ Autorizar dispositivos no pertenecientes al estándar institucional, siempre que esté plenamente justificado por el/la Subdirector/ra responsable de su uso

REGLAS DE LA POLÍTICA

1. Marco de Utilización

- 1.1. Es responsabilidad del Departamento de Tecnologías de Información disponer de medios seguros para que el usuario almacene sus datos sensibles.
- 1.2. Es considerado como falta grave el traslado fuera de las instalaciones de la Dirección del Servicio de Salud, de todo tipo de componentes computacionales, programas, software u otros elementos definidos sólo para su uso interno sin la correspondiente guía de traslado o despacho emitida por la Unidad de Inventario del Departamento de Finanzas y en excepciones autorizada por el Comité de Seguridad de la Información.
- 1.3. Todo medio de almacenamiento removible, debe ser revisado por posible presencia de virus y validarse la autenticidad de su información, por medios tecnológicos o manuales.
- 1.4. Toda estación de trabajo conectada a la red de MINSAL deberá usar la configuración de definida por el Comité de Seguridad de la Información.
- 1.5. Toda estación de trabajo conectada a la red de MINSAL deberá configurarse de acuerdo al "estándar"2, correspondiente a las funciones del usuario al cual está asignada.
- 1.6. Se habilitará una zona de red aislada a la red interna que permita el trabajo de personas que se desempeñen temporalmente en la institución

2. Alteraciones a la Configuración

- 2.3. La correcta utilización de estos dispositivos es de responsabilidad del colaborador, debiendo éste, informar a través de los canales formales cualquier falla o deterioro de los dispositivos, así como la indebida instalación de programas computacionales no autorizados por Comité de Seguridad de la Información.
- 2.4. La incorporación, deshabilitación o modificación de cualquier dispositivo de hardware o software, incluido el intercambio de componentes de un computador personal con otro debe efectuarse sólo por el soporte definido para dichas acciones, previa autorización y justificación por el superior calificado del usuario respectivo.
- 2.5. Está prohibido deshabilitar los mecanismos de control de acceso, el software antivirus o cualquier otro componente de seguridad de un computador

- 2.3. Está prohibido deshabilitar los mecanismos de control de acceso, el software antivirus o cualquier otro componente de seguridad de un computador
- 2.4. Todo cambio correctivo debe ser solicitado al Departamento de Tecnologías de Información.
- 2.5. Cualquier otro requerimiento de cambio de configuración debe ser previamente autorizado y justificado por el superior respectivo y efectuado por el Departamento de Tecnologías de Información.

3. Uso de Disco Duro

- 3.1. Los archivos almacenados en el disco local de las estaciones de trabajo y su respaldo es responsabilidad directa del usuario, exceptuando lo establecido en la "Política de respaldo de datos". El usuario es además responsable de administrar periódicamente sus archivos, haciendo uso de las herramientas que la institución les disponga para esto.

4. Traslado de equipos

- 4.1. Todo traslado o reasignación de equipos de computación o comunicaciones debe ser autorizado por el Comité de Seguridad de la Información, o a quien defina.
- 4.2. Los equipos ingresados en forma temporal deben cumplir la política para el control de acceso físico de personas y equipos.

5. Reutilización de Equipos

- 5.1. El Departamento de Tecnologías de Información es responsable de velar por el buen uso de la información de todos los equipos o computadores personales que están en condiciones de desecho o reutilización.

ANÓTESE, COMUNIQUESE Y ARCHÍVESE.



MARIA CRISTINA DIAZ MUÑOZ
DIRECTORA (S) SERVICIO SALUD MAGALLANES

MCDM/OPVV/ncr

Nº 3476

DISTRIBUCION:

DEPTO. SUBD. RECURSOS HUMANOS

DEPTO. CONTROL DE GESTIÓN Y TECNOLOGIA DE INFORMACION Y COMUNICACIONES

OFICINA DE PARTES

COPIA