RESOLUCION EXENTA Nº 7909

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 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 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:

C O N S I D E R A N D O :

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,

R E S O L U C I O N

1.- APRUÉBASE a contar del 11 de Julio de 2018 y hasta nueva revisión la **POLÍTICA DE SEGURIDAD FÍSICA Y AMBIENTAL** 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 FÍSICA Y AMBIENTAL

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.

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

POLÍTICA DE SEGURIDAD FÍSICA

DECLARACIÓN

Como parte de las políticas de seguridad de la información, se debe velar por el resguardo físico de los equipos e instalaciones sensibles relacionados con su tratamiento, a fin de velar por la integridad y disponibilidad de la información contenida.

ÁMBITO

- Controles de seguridad física para las instalaciones, sitios primarios y de contingencia, el sistema eléctrico y las condiciones ambientales de Sala de servidores, la prevención de incendios.

ROLES Y RESPONSABILIDADES

- Departamento de Tecnologías de Información

➢ Capacitar al responsable y al personal autorizado para el ingreso a la Sala de servidores.
➢ Designar personal responsable de los tableros de distribución eléctrica.
➢ Designar formalmente un responsable y personal autorizado para el ingreso al Data Center.

REGLAS DE LA POLÍTICA

1. Reglas Generales de Acceso

1.1. MINSAL deberá entregar a todo el personal una tarjeta de identificación según los estándares definidos.

1.2. El personal de MINSAL y externos que trabajan habitualmente en dependencias de MINSAL, deben portar siempre su identificación en lugar visible.

1.3. El acceso de personal interno o externo a una dependencia restringida, debe quedar registrado, detallando nombre, empresa, motivo del ingreso, fecha y hora del ingreso y egreso. Durante su permanencia debe estar siempre acompañado por personal debidamente autorizado.

1.4. Cuando un funcionario termina su relación laboral con MINSAL, sus permisos de acceso a dependencias deben ser revocados y su tarjeta de identificación debe ser retenida, conforme lo establece la Política de Seguridad de RRHH.

2. Sala de Servidores

2.1. La sala de servidores, requiere de operadores, de vigilancia permanente, 7x24, y de todos los sistemas de soporte críticos duplicados.

2.2. La sala de servidores debe estar ubicado en un área con baja probabilidad de sufrir desastres naturales o desastres producidos por el hombre. Estar alejado de baños, cocinas, kitchenettes y muros exteriores. Estar protegida del fuego, agua y vandalismo, y tener acceso fácil para salir o llegar en caso de una emergencia.

2.3. Impresoras, consolas y servidores deben tener su propia área dentro de la sala de servidores.

2.4. Almacenar los medios de respaldo en un lugar protegido y alejado de los sistemas que se respaldan.

2.5. Contar con estaciones de emergencia en las proximidades de la sala de servidores.

2.6. Dichas estaciones deben incluir un conjunto de elementos básicos de seguridad definido como estándar por MINSAL.

2.7. Todos los funcionarios deben ser entrenados en el correcto uso de extintores de incendios y en la ubicación de las vías de escape y de las zonas de seguridad física.

2.8. Se prohíbe fumar, comer o beber en la sala de servidores. Pudiendo existir otro lugar expresamente definido para ello.

2.9. La responsabilidad de la seguridad física de la sala de servidores recae en el Departamento de Tecnologías de Información.

2.10. El Gestor de Red deberá designar formalmente un responsable de la sala de servidores.

4. Suministro Eléctrico.

4.1. Disponer de un adecuado suministro de energía de respaldo, necesario y suficiente para mantener los sistemas críticos a través de UPS y grupos electrógenos.

4.2. Identificar en forma adecuada las tomas de energía conectadas a UPS para evitar conectar otro tipo de elementos.

4.3. Los tableros de distribución eléctrica deben mantenerse protegidos, no deben estar expuestos al público en general, donde puedan ser dañados o manipulados.

4.4. A la entrada de la sala, contar con un botón de pánico que, en caso de emergencia, corte la energía en la Sala de Servidores. Éste debe estar protegido de una activación casual.

4.5. Definir la frecuencia de revisiones del suministro eléctrico, que incluya la verificación de conexión a tierra.

4.6. Los tableros de distribución eléctrica deberán estar siempre disponibles para el personal que el Departamento de Tecnologías de Información designe. Esto es, que tengan un fácil acceso a dichos instrumentos sin que nada bloquee su manipulación (biombos, tabiques, muebles, módulos, etc.)

4.7. Todos los tableros de distribución eléctrica deben estar debidamente rotulados según los estándares definidos.

5. Humedad, Ventilación y Aire Acondicionado (HVAC).

5.1. Las condiciones ambientales de la sala deben cumplir con los requerimientos mínimos de temperatura y humedad de los equipos que alberga.

5.2. Los conductos usados para HVAC deben ser incombustibles.

5.3. Se deben conectar los sistemas de HVAC a los sistemas de alarma, de manera de cortar el suministro en caso de incendio.

5.4. En caso de usar piso falso como mecanismo de ventilación, no permitir el movimiento de palmetas con perforación sin la adecuada autorización.

5.5. Todos los equipos de control de condiciones ambientales deben estar protegidos contra la manipulación indebida.

5.6. Los equipos de HVAC deben poseer una plataforma de respaldo adecuada, que permita la operación de los dispositivos críticos.

6. Prevención por Daño de Fuego y Agua

6.1. Frente a una emergencia, la prioridad de salvamento serán siempre las personas, sin embargo, es conveniente y necesario que el personal sea instruido y entrenado en métodos de control de pérdidas para rescatar elementos de alto valor institucional.

6.2. Categorizar los activos a proteger, considerando: las Instalaciones, los equipos de soporte, los componentes periféricos y los suministros.

6.3. La sala de servidores debe ser equipado con alarmas de detección de fuego, agua e intrusos.

6.4. Todo acceso al área restringida debe contar con algún mecanismo de alarma que esté monitoreando.

6.5. Inspeccionar los sistemas de prevención y detección de incendios por autoridades idóneas.

6.6. Evitar el uso en paredes, pisos y cielos de materiales combustibles. Las puertas y vidrios deben ser en lo posible blindadas y capaces de detener el fuego.

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE.

SERVICIO DE SALUD MAGALLANES * XII REGIÓN * DIRECTOR

MARIA CRISTINA DIAZ MUÑOZ
DIRECTORA (S) SERVICIO SALUD MAGALLANES

MCDM/OPVV/ncr
N° 3418
DISTRIBUCION:
DEPTO. SUBD. RECURSOS HUMANOS
DEPTO. CONTROL DE GESTIÓN Y TECNOLOGIA DE INFORMACION Y COMUNICACIONES
OFICINA DE PARTES

COPIA