POLITICA GENERAL DE SEGURIDAD FÍSICA

DIRECCION DEL SERVICIO DE SALUD

VIÑA DEL MAR - QUILLOTA

NOTA DE CONFIDENCIALIDAD

LA INFORMACIÓN CONTENIDA EN EL PRESENTE DOCUMENTO, ES DE PROPIEDAD Y USO EXCLUSIVO DEL SERVICIO DE SALUD VIÑA DEL MAR – QUILLOTA, PARA LOS FINES QUE DETERMINE, Y SOLO LOS FUNCIONARIOS DE ESTA INSTITUCIÓN EXPRESAMENTE AUTORIZADOS PODRÁN CONOCER Y UTILIZAR SU CONTENIDO DE ACUERDO A SU FINALIDAD.

Firmas de los responsables.

ELABORADO POR	REVISADO POR	APROBADO POR
Representante del Comité de Seguridad	Encargado de Seguridad	Directora(a) del Servicio

SERVICIO DE SALUD
DIRECCIÓN
VIÑA DEL MAR - QUILLOTA

INDICE

CONTROL DE VERSIONES

REVISIONES DEL DOCUMENTO DE POLITICA				
Nº Revisión	**Fecha Aprobación**	**Motivo de la revisión**	**Páginas Modificadas**	**Autor**
0(Cero)		Elaboración inicial	Todas	RCA
1				
2				
3				

1.- DECLARACIÓN INSTITUCIONAL

Esta política general define los criterios y lineamientos esenciales para el Servicio de Salud Viña del Mar – Quillota, en cuanto a establecer normas para garantizar el buen funcionamiento del Datacenter/Sala de Comunicaciones y servicios ofrecidos por el Subdepartamento de TI.

La aplicación de esta política, busca evitar el acceso no autorizado ofreciendo además, controles para la auditorias más eficientes, logrando el control total en los acceso en el Servicio de Salud Viña del Mar – Quillota, los cuales exponen a la institución a pérdidas de información, daño a los recursos disponibles, como también problemas jurídicos tanto nacionales como internacionales.

2.- OBJETIVOS DE LA SEGURIDAD FÍSICA

Esta política tiene como finalidad establecer las reglas para garantizar, controlar, monitorear y remover el acceso físico a los recursos informáticos del Servicio de Salud Viña del Mar - Quillota. Todo esto tendiente a evitar accesos no autorizados, daños o interferencias en el funcionamiento de la organización. Las medidas de protección deben ser consistentes con el nivel de clasificación de los activos y el valor de la información procesada y almacenada en las instalaciones.

3.- ÁMBITO DE APLICACIÓN DE LA POLÍTICA DE SEGURIDAD FÍSICA

El alcance de la política de seguridad física a todos los accesos restringidos que contenga el Servicio de Salud Viña de Mar – Quillota, aplicando a todos los empleados, proveedores, contratitas, personal que esté prestando servicios al Servicio de Salud Viña del Mar – Quillota o que estén relacionados. Se incluye además, todas las dependencias que son parte de la institución.

4.- ROLES Y RESPONSABILIDADES

Director/a del Servicio de Salud Viña del Mar-Quillota

- Sancionar las propuestas realizadas por el comité de seguridad, respecto a las políticas de seguridad física,
- Aprobar los recursos necesarios para implementación adecuada de las acciones comprometidas en la política de seguridad física.

Comité de Seguridad

- Este comité tiene a su cargo la elaboración inicial de las políticas de seguridad física del Servicio de Salud, el control de la implementación y su correcta aplicación.
- Coordinar la respuesta a incidentes de seguridad física.
- Establecer puntos de enlace con otros organismos externos que permitan estar actualizado en las tendencias de seguridad física, así como para la realización de auditorías externas.
- Supervisar la implementación de la presente política.
- Proponer estrategias y soluciones específicas para la implementación de los controles necesarios para implantar la presente política.
- Monitorear los incidentes de seguridad y proponer estrategias para dar solución a las situaciones de riesgo detectadas en esta política.
- Monitorear el avance general en la implementación de la presente política.
- Divulgar la política de seguridad al interior de la institución.
- Implementar las medidas de seguridad definidas en la presente política.
- Mantener esta política de seguridad física, con el fin de asegurar su vigencia y nivel de eficacia.

Subdepartamento de TI

- Capacitar al responsable y/o personal autorizado para el ingreso a los Datacenter/Sala de Comunicaciones.
- Designar personal responsable de los tableros de distribución eléctrica.
- Designar formalmente un responsable y personal autorizado para el ingreso al Datacenter/Sala de Comunicaciones.

5.- MARCO GENERAL PARA LAS POLÍTICAS DE SEGURIDAD FÍSICA

5.1.- Acceso a las instalaciones

- Todos los sistemas de seguridad física deben cumplir con todas las regulaciones aplicables como tal, pero no están limitadas solo a las normas de construcción y prevención de incendios. Las instalaciones de TI, deberán estar físicamente protegidas en proporción a la criticidad o importancia de su función en el Servicio de Salud Viña del Mar -Quillota.
- Todo acceso físico a las personas será restringido, debiéndose gestionar y documentar el ingreso, el que solo se concederá al personal designado por el Subdepartamento de TI del Servicio de Salud Viña del Mar – Quillota y contratistas, cuyas responsabilidades de trabajo requieran el acceso a dicha instalación.
- El proceso para la obtención de las credenciales, tarjetas de acceso a las instalaciones de TI deberán incluir la aprobación del Jefe del el Subdepartamento de TI del Servicio de Salud Viña del Mar – Quillota.
- Las credenciales y/o tarjetas de acceso no deben ser compartidas o cedidas, además las tarjetas que ya no sean necesarias o ya cumplieron su función, deberán ser

devueltos a l el Subdepartamento de TI del Servicio de Salud Viña del Mar – Quillota. Las tarjetas no deberán ser reasignadas a otra persona, deberán ser destruidas.

- La pérdida o robo de las tarjetas de acceso deberán ser reportadas al Subdepartamento de TI del Servicio de Salud Viña del Mar – Quillota, quien las destruirá.
- Los registros de accesos de las tarjetas de acceso deberán conservarse para mantener una revisión de los accesos y rutinas realizadas basadas en la criticidad de los recursos que se protegen, ante eventuales delitos.
- El Subdepartamento de TI del Servicio de Salud Viña del Mar – Quillota, en colaboración con el área de personal, serán los encargados de recuperar y eliminar los accesos a los lugares restringidos de las personas que sean desvinculadas o que por cambios en el contrato, cambien sus roles operativos.
- Los visitantes deberán ser escoltados en el acceso a las zonas controladas por las instalaciones TI del Servicio de Salud Viña del Mar – Quillota.
- El Sub departamento de TI, se encargará de revisar periódicamente los privilegios y derechos de accesos de las tarjetas de acceso para eliminar las de las personas que ya no requieran de éstos privilegios.
- Las señaléticas para el acceso a las salas y localidades restringidas deberán ser simples, sin embargo, deberá informar de forma simple la importancia de la ubicación y el acceso restringido a las instalaciones.
- El personal autorizado debe tener las (24) horas de libre acceso a las instalaciones críticas de TI.
- El acceso al Datacenter/Sala de Comunicaciones y rack de redes TI estarán restringidos sólo a los administradores de redes y Jefe de Informática.
- El Subdepartamento de TI del Servicio de Salud Viña del Mar – Quillota es el responsable de la seguridad de los datos en la red y sus equipos, con el fin de mantener la integridad y completitud de los datos.

5.2.- Datacenter/Sala Comunicaciones

- El recinto donde se encuentra el Datacenter/Sala de Comunicaciones, requiere de operadores, de vigilancia permanente 7x24, y de todos los sistemas de soporte críticos duplicados.
- El Datacenter/Sala de Comunicaciones debe estar ubicado en un área con baja complejidad de sufrir desastres naturales o desastres producidos por el hombre. Estar alejado de baños, cocinas, y muros exteriores. Estar protegida del fuego, agua y vandalismo y tener acceso fácil para salir o llegar en caso de una emergencia.
- Impresoras, consolas y servidores deben tener su propia área dentro del Datacenter/Sala de Comunicaciones.
- Almacenar los medios de respaldo en un lugar protegido y alejado de los sistemas que se respaldan.
- Todos los funcionarios del Sub departamento de TI deben ser entrenados obligatoriamente en el uso de extintores de incendios y en la ubicación de las vías de escape y de las zonas de seguridad físicas.
- Se prohíbe fumar, comer o beber en el Datacenter/Sala de Comunicaciones. Pudiendo existir otro lugar expresamente definido para ello.

- El Subdepartamento de TI deberá designar formalmente un responsable en el Datacenter/Sala de Comunicaciones.

5.3.- Seguridad ambiental

- Todos los servidores o equipos de comunicación deberán contar con estabilizadores de tensión y/o UPS y deberán estar instalados de acuerdo a las instrucciones del proveedor, esto para mantener el servicio operativo en caso de corte de la energía eléctrica.
- El ambiente del Datacenter/Sala de Comunicaciones deberá estar siempre limpio y ordenado, adecuadamente ambientado con aire acondicionado, con control de temperatura y humedad, regulado desde la misma Sala, a fin de mantener estable la temperatura de los servidores. No se almacenará material combustible innecesario dentro o cerca del Datacenter/Sala de Comunicaciones, tales como papeles, cajas, etc.
- La Sala de Servidores deberá contar con extintores portátiles de fuego ubicado en posiciones estratégicas y conocidos por todos los funcionarios del Subdepartamento de TI. Los mismos tendrán una etiqueta de inspección con la indicación de la clase de incendios a los que extinguen y además deberán ser revisados de acuerdo a los estándares establecidos para cada tipo.

5.4.- Suministro eléctrico

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

- Identificar en forma adecuada, las tomas de energía conectadas a UPS para evitar conectar otro tipo de elementos.
- Los tableros de distribución eléctrica deben mantenerse protegidos, no deben estar expuestos al público en general, donde puedan ser dañados o manipulados, además deberán estar siempre disponible para el personal del Subdepartamento de TI que se designe. Esto es, que tengan un fácil acceso a dichos instrumentos sin que nada bloquee, su manipulación (biombos, tabiques, muebles, módulos, etc.)
- A la entrada de la sala, contar con un botón de pánico para el caso de incendio, o siniestros naturales que, en caso de emergencia, corte la energía en el Datacenter/Sala de Comunicaciones y en los equipos de comunicaciones. Este debe estar protegido de una activación casual.
- Definir la frecuencia de revisiones de la capacidad eléctrica del recinto, que incluya la verificación de conexión a tierra.
- Todos los tableros de distribución eléctrica deben estar debidamente rotulados según los estándares definidos.

5.5.- Humedad, Ventilación y Aire Acondicionado (HVAC)

- Las condiciones ambientales de la sala debe cumplir con los requerimientos mínimos de temperatura y humedad de los equipos que alberga.
- Los conductos usados para HVAC deben ser incombustibles.

- En caso de usar piso falso como mecanismo de ventilación, no permitir el movimiento de palmetas con perforación sin la adecuada autorización.
- Todos los equipos de control de condiciones ambientales deben estar protegidos contra la manipulación indebida.
- Los equipos de HVAC deben poseer una plataforma de respaldo adecuada, que permita la operación de los dispositivos críticos.

5.6.- Prevención por Daño de fuego y agua

- Categorizar los activos a proteger, considerando: las instalaciones, los equipos de soporte, los componentes periféricos y los suministros.
- Frente a una emergencia, la prioridad de salvamento serán las personas, sin embargo es conveniente y necesarios que el personal sea instruido y entrenado en métodos de control de pérdidas para rescatar elementos de alto nivel institucional.
- El Datacenter/Sala de Comunicaciones debe ser equipado con alarmas de detección de fuego y personas no autorizadas.
- Inspeccionar los sistemas de prevención y detección de incendios por autoridades idóneas, calendarizando inspecciones preventivas.
- Evitar el uso en paredes, pisos y cielos de materiales combustibles. Las puertas deben ser en lo posible blindadas y capaces de detener el fuego.
- Instalar alarmar audibles y visibles dentro y fuera de la sala. Conectar los sistemas de alarma de la sala al centro de seguridad, donde los guardias puedan tomar acciones inmediatas en caso de emergencia.

5.7.- Como parte del rol de Guardias y Vigilante se considera:

- Conocer la ubicación y disposición de los espacios físicos de los, Datacenter/Sala de Comunicaciones, así como la importancia de prevenir accesos no autorizados de las mismas.
- Reconocer elementos computacionales, disco portables o removibles y cintas de respaldo computadores portátiles y periféricos de fácil transporte.
- Conocer y aplicar las políticas de seguridad de la información relacionadas con el control de acceso y seguridad física.
- Conocer y aplicar los procedimientos de obtención de autorización válida para accesos a áreas restringidas en casos de excepción o situaciones de emergencia.

6.- APLICACIÓN DE LAS POLITICAS DE SEGURIDAD FISICA

La infracción a las obligaciones establecidas en esta norma, podrá constituir una violación al principio de probidad administrativa, y será sancionada en conformidad a lo dispuesto en la Ley N° 18.834, sobre Estatuto Administrativo. Lo anterior es sin perjuicio de la responsabilidad civil o penal que corresponda.

El Subdepartamento de TI no se hará responsable por incidentes producidos por el no cumplimiento de estas políticas de seguridad.

7.- MONITOREO

El Subdepartamento de TI del Servicio de Salud Viña del Mar – Quillota verificará la aplicación de estas políticas de seguridad física.

8.- GLOSARIO DE TERMINOS

- Datacentrer/Sala de Comunicaciones: Centro de procesamiento de datos
- RRFF: Recursos Físicos
- RRHH: Recursos Humanos
- Rack: Soporte metálico destinado a alojar equipamiento electrónico, informático y de comunicaciones.
- TI: Tecnologías de Información