HOSPITAL CARLOS VAN BUREN
SUBDIRECCIÓN ADMINISTRATIVA
CR GESTIÓN DE LA INFORMACIÓN
CRB/SOG/jbv
INT: N°007/2024

RESOLUCIÓN EXENTA N°:
6263 27.12.2024

VISTOS:

NORMAS LEGALES Y REGLAMENTARIAS: D.F.L. N° 29 del 2004, que fija texto refundido, coordinado y sistematizado de la Ley N° 18.834 sobre Estatuto Administrativo; el D.F.L. Nº 1/2005, que fija texto refundido, coordinado y sistematizado del D.L. Nº 2763/79; su Reglamento aprobado por D.S. Nº 140/2004 del Ministerio de Salud; la Resolución Nº 06/19 de la Contraloría General de la República y en uso de las facultades delegadas por D.S. N° 38/05 Reglamento orgánico de los establecimientos de Salud de Menor Complejidad y de los Establecimientos de Autogestión en Red, que delega facultades a los Directores de Hospitales Autogestionados; la Resolución Exenta N° 110612/2879/2024, de fecha 22.07.2024, del Servicio de Salud Valparaíso San Antonio y la Resolución Exenta N° 4867 de fecha 07.10.2022.

CONSIDERANDO:

PRIMERO: Que, dentro del contexto de la normativa ISO/IEC 27001 y con la clara comprensión de la imperante necesidad de establecer una gobernanza sólida para la seguridad de la información, se subraya la importancia formalizar la Política General de Seguridad de la Información y Ciberseguridad para el Hospital Carlos Van Buren.

SEGUNDO: Que, dicha política sienta un marco normativo que regula el uso de los recursos informáticos de la Institución, así como el uso y las medidas de seguridad para el tratamiento de los datos sensibles de los pacientes.

RESUELVO:

1 º **ESTABLÉZCASE** la Política General de Seguridad de la Información del Hospital Carlos Van Buren.

2º **COMUNÍQUESE**, la presente resolución a todos los funcionarios del Hospital Carlos Van Buren, considerando al menos los siguientes canales:

- Página web https://hospitalcarlosvanburen.cl/
- Intranet http://10.6.96.210/menu/login.php
- Correo informativo desde el Departamento de Comunicaciones de la Institución

3º **PUBLÍQUESE**, La presente Resolución para su adecuado conocimiento y difusión, en la página web del Hospital Carlos Van Buren, el texto de la presente resolución.

ANÓTESE, COMUNÍQUESE Y CÚMPLASE,

SIMON ROJAS DOLL
Firmado digitalmente por SIMON ROJAS DOLL
Fecha: 2024.12.27 11:12:30 -03'00'

SIMÓN ROJAS DOLL
DIRECTOR (S)
HOSPITAL CARLOS VAN BUREN

DISTRIBUCIÓN:
CR de Gestión de la Información
Subdirección de Gestión y Desarrollo de las Personas
Unidad de Comunicaciones
Oficina de Partes

Política General de Seguridad de la Información

Hospital Carlos Van Buren

Octubre 2024

Tabla de contenidos

1. Propósito

Esta Política General de Gestión de Seguridad de la Información, tiene como propósito establecer los lineamientos para la gestión de la Seguridad de la Información, en el Hospital Carlos Van Buren, la cual se encuentra alineada con las políticas emanadas desde el Nivel Central del Ministerio de Salud.

2. Alcance o ámbito de aplicación

Esta política 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 el Hospital.

La presente política se aplica sobre todo tipo de información, considerando todo medio de soporte y presentación, como son la voz y medios digitales, ya sean magnético, óptico, electrónico o fotográfico.

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:

Nombre del Dominio	ID Control ISO 27001	Nombre del Control
Políticas de seguridad de la información	A.05.01.01	Políticas para la seguridad de la información
	A.05.01.02	Revisión de las políticas de seguridad de la información
Organización de la seguridad de la información	A.06.01.01	Roles y responsabilidades de la seguridad de la información
Cumplimiento	A.18.02.01	Revisión independiente de la seguridad de la información

3. Marco normativo

- Documentos del Sistema de Gestión de Seguridad de la Información (SGSI) de MINSAL, disponibles en isalud.minsal.cl.
- Política Nacional de Ciberseguridad (PNCS)
- 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. o Leyes relacionadas.
- Políticas de Seguridad de la Información de Minsal, disponibles en isalud.minsal.cl.

4. Roles y responsabilidades

Encargados Seguridad de la Información del HCVB

- Liderar las iniciativas en materias de seguridad de la información, plantearlas al comité de seguridad de la información, y mantener informado al jefe de servicio, de los acuerdos establecidos en estos escenarios.
- Velar por la ciberseguridad, y actuar frente a infracciones a la privacidad y amenazas, sus tendencias y escenarios estratégicos que pudieren afectar al Hospital.
- Alinear los esfuerzos de las distintas áreas de la Institución, respecto a la protección de los sistemas tecnológicos y a la información contenida en ellos, según los criterios de Ciberseguridad.
- Gestionar internamente el tratamiento de los incidentes que estén vinculados a los activos de información de la institución, identificados y/o reportados tanto por el Ministerio del Interior como por instancias internas del Hospital, efectuando la reportabilidad y el seguimiento adecuado de dichos eventos.
- Apoyar el proceso de sensibilización en materias de ciberseguridad al interior de la institución. Organizando actividades de concientización y capacitación en seguridad para educar a los funcionarios sobre buenas prácticas y comportamientos seguros.
- Organizar y presidir el comité de seguridad de la información, que tendrá a su cargo la actualización de políticas y procedimientos, de Ciberseguridad y Seguridad de la Información de la institución, el control de su implementación, y velar por su correcta aplicación.
- Coordinar las acciones necesarias para resguardar y asegurar la continuidad del negocio frente a incidentes de Ciberseguridad.
- Resguardar que se informe adecuadamente a todas las personas naturales y jurídicas que puedan tener acceso a los activos de información de la institución, acerca de las Políticas de Ciberseguridad y Seguridad de la Información vigentes, y en particular sobre las obligaciones que le correspondan en relación a la gestión de incidentes.
- Comunicar los incidentes de ciberseguridad de los que tenga conocimiento en ejercicio de sus funciones, al Ministerio del Interior y Seguridad Pública, mediante su notificación al Centro de Respuesta ante Incidentes de Seguridad Informática (“CSIRT”), en el sitio web: https://csirt.gob.cl, en representación del jefe del servicio, en su calidad de autoridad máxima de la institución.
- Establecer puntos de enlace con encargados de seguridad de la información y ciberseguridad, de otros organismos públicos y especialistas externos, que le permitan estar al tanto de las tendencias, normas y métodos en estas materias.
- Definir políticas y procedimientos de seguridad de la información y ciberseguridad, así como un plan de acción para mitigar riesgos y proteger los sistemas y datos de la organización.
- Apoyar en la identificación, evaluación y gestión de los riesgos de seguridad de la información del Hospital, realizando evaluaciones periódicas de vulnerabilidades y amenazas. Implementando controles y medidas para minimizar la exposición a riesgos potenciales y proteger los activos críticos.
- Encargado de implementar y mantener los controles de seguridad adecuados para proteger la infraestructura, los sistemas y los datos. Esto puede incluir firewalls, sistemas de detección de intrusos, sistemas de prevención de pérdida de datos y otros mecanismos de seguridad.
- Evaluar la seguridad de proveedores y terceros con acceso a información sensible de la organización para asegurarse de que cumplan con los estándares de seguridad requeridos.

Comité de ciberseguridad

- Proponer a la dirección de la institución, las políticas, procedimientos e instrucciones de seguridad de la información y su actualización.
- Supervisar la implementación de la estructura documental del Sistema de Seguridad de la Información aplicable a la institución.
- Proponer a la dirección de la institución, estrategias o soluciones específicas para implementar o controlar los componentes de la estructura documental del Sistema de Seguridad de la Información.
- Arbitrar conflictos en materia de seguridad de la información y los riesgos asociados, y proponer soluciones sobre ello.
- Revisar y monitorear los incidentes de seguridad de la información a fin de establecer acciones preventivas y correctivas.
- Revisar los elementos del Sistema de Seguridad de la Información y proponer mejoras a través del Encargado de Seguridad de la Información.
- Difundir los componentes de la estructura documental del Sistema de Seguridad de la Información a través de la Intranet y los medios de comunicación establecidos dentro de la institución.
- Monitorear cambios significativos que pudieran variar los riesgos presentes en la Institución
- Establecer acciones y proponer iniciativas para mejorar la seguridad de la información.
- Supervisar la realización de auditorías de Seguridad de la Información, internas o externas.

Usuarios finales

- Se debe entender como usuarios finales a todos quienes tienen la responsabilidad de acatar las políticas y normativas definidas, independiente que además tengan otro rol nominado en este ámbito.
- Debe considerar a todos los funcionarios (planta, contrata, reemplazos y suplencia), personal a honorarios, terceros (proveedores, compra de servicios, tratamiento por encargo, servicios externalizados, etc.)
- Los requerimientos de seguridad hacia terceros y personal a honorarios, deben estar considerados en los TDR: Términos de referencia del acuerdo base del servicio contratado.

5. Materias que aborda

- Políticas para la seguridad de la información.
- Revisión de las políticas de seguridad de la información.
- Roles y responsabilidades de la seguridad de la información.
- Revisión independiente de la seguridad de la información.

6. Directrices de la política

6.1 Declaración Institucional

El Hospital Carlos Van Buren (HCVB) se compromete a gestionar la seguridad de la información como un proceso continuo en el tiempo, que se debe cumplir en el marco de la normativa gubernamental existente, por medio de todas aquellas actividades y tareas que sean necesarias para establecer los niveles de seguridad que la propia institución determine.

Para estos efectos, el HCVB se basará 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 adecuados de integridad, confidencialidad y disponibilidad, de todos sus activos de información relevantes para la institución, como un principio clave en la gestión de sus procesos.

Para la gestión de la Seguridad de la Información al Interior del HCVB se ha decidido contar con un programa de implantación del tipo "Sistema de Gestión de Seguridad de la Información" (SGSI), basado en los requisitos de la Norma NCh-lS027001: 2013, y las prácticas para los controles de seguridad de la Norma NCh-lS027002:2022, con el objetivo de preservar los activos de información institucional con respecto a:

- **Su Integridad**: la información no puede ser alterada ni eliminada por cambios no autorizados o accidentales. Este principio fundamental de seguridad busca garantizar la precisión, suficiencia y validez de la información, métodos de procesamiento y todas las transacciones de acuerdo con los valores y expectativas del negocio, así como evitar fraudes o irregularidades de cualquier índole que haga que la información sea alterada.

- **Su Confidencialidad**: la información confidencial, privada y sensible sólo debe ser conocida por el personal que la requiera para el desarrollo de sus funciones. Este principio fundamental de seguridad busca garantizar que toda la información de los ciudadanos, funcionarios y proveedores, y sus medios de procesamiento o conservación, estén protegidos del uso no autorizado o divulgación accidental, sabotaje, espionaje industrial, violación de la privacidad y otras acciones que pudieran poner en riesgo dicha información. Este principio deberá aplicarse en concordancia con lo previsto en la ley 20.285 de acceso a la información pública.

- **Su Disponibilidad**: La información debe estar disponible para el personal, usuarios y entidades reguladoras de manera oportuna y acorde a sus niveles de autorización. Este principio fundamental de seguridad busca garantizar que los usuarios autorizados tengan acceso a la información cuando ésta es requerida por el proceso institucional. Para ello se debe procurar que la información y la capacidad de procesamiento sean resguardados y puedan ser recuperados en forma rápida y completa ante cualquier hecho contingente que interrumpa la operatividad o dañe las instalaciones, medios de almacenamiento o equipamiento de procesamiento.

Tratándose de la información sujeta a las normas de transparencia, la disponibilidad impone que se encuentren en el portal de transparencia activa y que permita responder oportunamente los requerimientos efectuados por los ciudadanos en virtud de su derecho de acceso a la información pública.

Según lo expuesto anteriormente, las Autoridades del Hospital se comprometen a:

- Apoyar los objetivos y principios de la seguridad de la información, y a proveer los recursos necesarios para la gestión de actividades en seguridad.
- Promover un plan de acción de mejora continua con el fin de asegurar una adecuada gestión de la seguridad de la información, según lo dispuesto en la NCh-ISO 27001:2013 y otras normativas vigentes que, conforme a lo dispuesto en el número 7 de esta política general, estarán disponibles permanentemente en el sitio intranet del HCVB.
- Implementar las obligaciones que emanan del Derecho de Acceso a la Información pública, con el debido respeto a la protección de los datos sensibles e información confidencial, de acuerdo a la ley.

6.2 Objetivos de la Gestión de Seguridad de la Información en el Hospital

6.2.1 Objetivo General

Lograr niveles adecuados de integridad, confidencialidad y disponibilidad para todos los activos de información institucionales relevantes, asegurando la continuidad operacional de los procesos.

6.2.2 Objetivos Específicos

- Identificar y catastrar todos los activos de información relevantes que están presentes directa o indirectamente en cada proceso institucional, abarcando tanto los procesos críticos institucionales, como los de soporte.
- Realizar actividades necesarias de análisis de riesgo, según normativas, técnicas y estándares disponibles y aplicables, para diseñar e implantar medidas y controles que permitan mitigar los riesgos que sean identificados, sin perder de vista el enfoque de la gestión por procesos institucionales.
- Proteger la información, sus medios de procesamiento, conservación y transmisión del uso no autorizado o revelaciones accidentales, errores, fraudes, sabotaje, violación de la privacidad y otras acciones que pudieran perjudicarla o ponerla en riesgo.
- Mantener y hacer uso de la estructura y el marco de estándares, políticas y procedimientos en materia de seguridad de la información.
- Minimizar la posibilidad de ocurrencia de hechos contingentes que pudieran interrumpir la operación del negocio y reducir el impacto de los daños a las instalaciones, medios de almacenamiento, equipos de procesamiento y de comunicación.
- Hacer uso de planes de continuidad operacional ante hechos contingentes que interrumpan la operación del servicio.
- Sensibilizar y capacitar a los funcionarios del HCVB acerca de su responsabilidad para mantener la seguridad de la información y su adecuado uso, estableciendo una cultura organizacional que incorpore el tema de seguridad de la información como un aspecto relevante en los procesos de negocio del Hospital.

6.3 Gestión de la Política y otros documentos del sistema de Gestión de Seguridad de la información

La estructura documental de ese sistema está compuesta por una Política General de Seguridad de la Información, políticas específicas de seguridad de la información, procedimientos de operación, instructivos y registros.

La referida estructura documental aplicable al hospital Carlos Van Buren, se desprende de las políticas y procedimientos emanados desde el Nivel Central del Ministerio de Salud. Esta documentación debe asegurar:

- Integren el modelo de seguridad con las metodologías y políticas existentes para el Hospital.
- Que se cumplan las normas legales y reglamentarias referidas a seguridad, tanto para la información, como para los medios que la contienen.
- Que la información cumpla con los niveles de autorización y responsabilidad correspondientes para su utilización, divulgación, administración, seguimiento y custodia.
- Que la información, sus medios de procesamiento, conservación y transmisión estén protegidos del uso no autorizado o revelaciones accidentales, errores, fraudes, sabotajes, espionaje, violación de la privacidad y otras acciones que pudieran perjudicarla.
- Que los medios de procesamiento, conservación y comunicación de la información cuenten con medidas de protección física que eviten el acceso y/o utilización indebida por personal no autorizado.
- Que los derechos de propiedad sobre la información y sistemas estén establecidos.
- Que las comunicaciones internas y externas cuenten con mecanismos que protejan la integridad, disponibilidad y confidencialidad en la transmisión de información.
- Que se delimiten los ámbitos físicos de acción de las políticas de seguridad, dependiendo de los distintos niveles de riesgo que presentan los medios de procesamiento, conservación y comunicación.
- Que el acceso a los servicios del Hospital, ya sea por medios internos o externos, se realice de acuerdo con las atribuciones de las personas o entidades que las utilicen.
- Que las actividades y uso de recursos críticos, relacionados con productos y servicios, sean monitoreados y su información sea conocida en forma oportuna por los niveles correspondientes.

Las versiones vigentes de la normativa del SGSI y los documentos de apoyo, serán publicados en el sitio intranet de HCVB, desde donde tendrá amplio acceso a los funcionarios.

6.4 Identificación de riesgos

A lo menos cada dos años el Comité de Seguridad de la Información, debe gestionar la actualización de los riesgos de seguridad de la información del hospital, que debe ser construido a partir del análisis de las amenazas y vulnerabilidades a los que se encuentran expuestos los activos de la información relevantes. La metodología de análisis y gestión de riesgos debe estar enfocada en los procesos de provisión institucional, sus actividades, actores y activos, siendo referente:

- CAIGG, apartado Líneas de Acción / Gestión de Riesgos, en el sitio web https://www.auditoriainternadegobierno.gob.cl/
- Norma NCh-ISO 31000:2012 — Principios y directrices para la Gestión de Riesgos.

- Marco COSO ERM — www.coso.org.
- DIPRES, Guía Metodológica Sistema de Seguridad de la Información.

En el caso de los riesgos residuales, deben ser relevados por el Comité de Seguridad de la Información, al Comité de Riesgos de la Institución para su análisis.

6.5 Revisión y medición

A lo menos una vez al año, el Comité de Seguridad de la Información del HCVB debe evaluar el estado del SGSI e informar al equipo Directivo los resultados, considerando cambios que surjan en el transcurso de este período que podrían afectar el enfoque de la organización a la gestión de la seguridad de la información, incluyendo cambios al ambiente de la organización, circunstancias del negocio, disponibilidad de recursos, condiciones contractuales, reguladoras, y legales, o cambios al ambiente técnico. Para ello debe considerar los siguientes aspectos:

- Retroalimentación de las partes interesadas.
- Resultados de las revisiones efectuadas por terceras partes.
- Estado de acciones preventivas y correctivas.
- Cambios en los procesos institucionales, nueva legislación, tecnología etc.
- Alertas ante amenazas y vulnerabilidades.
- Información relacionada a incidentes de seguridad.
- Recomendaciones provistas por autoridades relevantes.
- Medición de los indicadores del Sistema.

Revisión independiente de la seguridad de la información: a lo menos cada dos años se deberá revisar la Política General de Seguridad de la Información, y el estado del SGSI mediante auditorías internas o externas.

6.6 Cumplimiento

Todos los usuarios del Hospital Carlos Van Buren ya sean funcionarios de planta, contrata, honorarios, asesores, consultores, practicantes, y otros trabajadores, deberán dar complimiento, en lo que les corresponda, a esta Política General de Seguridad de la Información, las políticas específicas y los procedimientos relacionados que se aprueben al efecto.

Para el caso de terceros y por el solo hecho de participar en algún proceso de compras del Hospital, el oferente deberá dar cumplimiento a las Políticas y Procedimientos vigentes de seguridad de la información del Ministerio de Salud, publicadas en link https://www.minsal.cl/seguridad_de_la_informacion/ y sus correspondientes modificaciones, las cuales se presumen conocidas por el contratista o adjudicatario, para todos los efectos legales. Será de responsabilidad del Contratista darlas a conocer y resguardar su cumplimiento por sus empleados y colaboradores internos o externos.

6.7 Sanciones

El incumplimiento de las obligaciones emanadas de esta Política, de las Políticas específicas del Sistema, Procedimientos u otros documentos que se deriven de éstos, serán sancionadas en los términos de las leyes vigentes y aplicables bajo el Estatuto Administrativo para los funcionarios del hospital. Cuando el incumplimiento se trate de personas que no tengan responsabilidad administrativa o empresas que se encuentren dentro del alcance de esta política, se procederá al término anticipado del contrato, por incumplimiento de obligaciones, sin perjuicio de las responsabilidades civiles y penales que se deriven de tales infracciones.

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 del HCVB http://10.6.96.210/menu/login.php
- Correo informativo.

8. Excepciones al cumplimiento de la política

Frente a casos 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.