5935 05.12.2024

RESOLUCION EXENTA 1C N°

ACTUALIZA POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DEL SERVICIO DE SALUD ÑUBLE.

VISTOS: estos antecedentes: DFL N° 1/2005 texto refundido y actualizado del Decreto Ley N° 2.763/79, que crea los Servicios de Salud; el D.S. N° 140/04, Reglamento Orgánico de los Servicios de Salud; el Decreto Exento N°12/2024, del Ministerio de Salud, sobre subrogancia de la Directora del Servicio de Salud Ñuble; la Resolución N° 6/2019, de la Contraloría General de la República sobre exención del trámite de toma de razón y; 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; la Ley N° 21.459, que Establece Normas Sobre Delitos Informáticos, Deroga La Ley N° 19.223 Y Modifica Otros Cuerpos Legales con el Objeto de adecuarlos al Convenio de Budapest; la Norma ISO 27001, sobre Gestión de Seguridad de la Información; la Resolución Exenta 1C N° 2253 de 18.04.2024 de la Directora del SSÑ, que modifica la Conformación y funciones del Comité de Seguridad de la Información en el Servicio de Salud Ñuble y deja sin efecto la Resolución Exenta 1C N° 6840 de 20.12.2018; la Resolución Exenta 1C N° 159 de 14.01.2019 del Director del Servicio de Salud Ñuble, la cual Aprueba la Política General de Seguridad de la Información del Servicio de Salud Ñuble; y

CONSIDERANDO:

1.- Que la seguridad de la información es un tema de relevancia para este Servicio de Salud, considerando el gran volumen de información sensible con la que se trabaja, lo cual hace prioritario mantener y mejorar continuamente la gestión de seguridad de la información, basada en preservar los principios de confidencialidad, integridad y disponibilidad de la misma;

2.- Es por expresado en el punto anterior, que existe la necesidad de actualizar la actual Política General de Seguridad de la Información en el Servicio de Salud Ñuble, con el objeto de poder contar con un marco normativo acorde a los avances tecnológicos y así desarrollar controles acordes a dicha realidad;

3.- Que el Comité de Seguridad de la Información, en sesión de fecha 4 de diciembre de 2024, habiendo quorum suficiente, aprobó por unanimidad de sus asistentes la nueva Política de Seguridad de la Información en el Servicio de Salud Ñuble, por lo cual:

RESUELVO

1°.- ACTUALICESE la Política de Seguridad de la Información en el Servicio de Salud Ñuble, documento que consta de 22 páginas, en los términos y condiciones en él expresados, la cual se adjunta y forma parte integrante de la presente resolución.

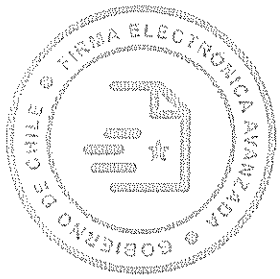
2° DEJESE constancia que la nueva Política de Seguridad de la Información fue aprobada por unanimidad de los integrantes del Comité de Seguridad de la Información con fecha

MOCP PDGJ CAAG PARC(S)

04.12.2024, tal como consta en Acta de Reunión, la cual también se adjunta y que forma parte de la presente resolución.

3°.- PÓNESE TERMINO, a contar de esta fecha, a la Resolución Exenta 1C N° 159 de 14.01.2019 del Director del Servicio de Salud Ñuble, la cual Aprueba la Política General de Seguridad de la Información del Servicio de Salud Ñuble.

ANÓTESE Y COMUNÍQUESE



Firmado por:
Alex Rodrigo Paredes Poblete
Directora Servicio Salud Ñuble (s)
Fecha: 05-12-2024 14:48 CLT
Servicio de Salud Ñuble

Distribución:

- 1/1B/1C/2/3/4/5/6
- Integrantes del Comité de Seguridad de la infromación del SSÑ

MOCP PDGJ CAAG PARC(S)

Política General de Seguridad de la Información del Servicio de Salud Ñuble

Elaborado y Revisado	Aprobado
Sección de Seguridad de la Información	Comité de Seguridad de la Información

CONTENIDO

1 PROPÓSITO

El propósito de esta Política General de Seguridad de la Información y Ciberseguridad es establecer un marco de referencia y directrices que ayuden a proteger la información y los activos de información del Servicio de Salud Ñuble de manera integral y efectiva. Esta política tiene como objetivo principal salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información, así como mitigar los riesgos relacionados con la ciberseguridad.

2 CONTEXTO

El Servicio de Salud Ñuble es una institución pública dependiente del Ministerio de Salud, cuya misión es “Somos un servicio de salud que busca promover el autocuidado y el acceso oportuno a las prestaciones de salud de las Personas de Ñuble, a través del fortalecimiento del Modelo de Atención Integral, la coordinación de la red asistencial y la participación ciudadana, gestionando el uso eficiente de los recursos, para entregar servicios con equidad, calidad y pertinencia cultural; contando con el compromiso de sus trabajadores y trabajadoras”.

La Institución, como principal giro, es entregar prestaciones de Salud a la ciudadanía y por lo tanto la información registrada y administrada contiene un nivel de detalle y de privacidad muy alto, y es así que los procesos asociados a esta situación son Atención de Urgencia, Atención Ambulatoria, Atención Hospitalaria, Atención de Especialidad, Pabellón, Laboratorio, Imagenología, Anatomía Patológica y Procedimientos Terapéuticos, además de los procesos para la administración de recursos tales como Contabilidad, Abastecimiento, Recursos Humanos entre otros. Para todos ellos hay Infraestructura de Tecnologías de Información que deben ser resguardada y sobre las cuales se debe velar por su Seguridad, tales como la infraestructura de telecomunicaciones, los servidores de Bases de datos, los servidores de aplicaciones, entre otros.

3 ALCANCE O ÁMBITO DE APLICACIÓN

El alcance de la Política General de Seguridad de la Información y Ciberseguridad abarca de manera integral y transversal todas las operaciones, sistemas, recursos y procesos relacionados con la gestión de la información y la ciberseguridad en el Servicio de Salud Ñuble.

Aplicable a todos los funcionarios/as en su calidad de planta, contrata, reemplazos y suplencia, personal a honorarios y terceros (proveedores, compra de servicios, otros), que presten servicios en la Dirección del Servicio de Salud o establecimientos de la Red Asistencial.

Esta política abarca los siguientes controles definidos en la norma NCh-ISO 27001.Of2013:

- A.05.01.01 Políticas para la seguridad de la información.
- A.05.01.02 Revisión de las políticas de seguridad de la información
- A.06.01.01 Roles y responsabilidades en seguridad de la información.
- A.18.02.01 Cumplimiento.

4 MARCO NORMATIVO Y DOCUMENTOS RELACIONADOS

- 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.
  - Leyes relacionadas.
- El Marco normativo para las funciones en el sector Salud, como:
  - Ley 19.628 Sobre la protección de la vida privada, Ministerio Secretaria General de la Presidencia.
  - Ley 20.285 Sobre acceso a la información pública, Ministerio Secretaría General de la Presidencia.
  - D.F.L. Número 29 que fija texto refundido, coordinado y sistematizados de la Ley Nº 18.834, sobre estatuto Administrativo.
  - Ley 19.653 Ministerio Secretaría General de la Presidencia, Sobre Probidad Administrativa aplicable a los Órganos de la Administración del Estado.
  - Decreto 41/2012 que aprueba reglamento sobre fichas clínicas que regula el contenido, almacenamiento, administración, protección y eliminación de fichas clínicas de manera de resguardar el correcto empleo, disponibilidad y confidencialidad de las mismas.
- Normas del Sistema de Gestión de Seguridad de la Información:
  - NCh-ISO 27001:2013 Análisis de Requisitos e Implementación.
  - NCh-ISO 27002:2013 Código de prácticas para los controles de seguridad de la información.
- Políticas de Seguridad de la Información del Servicio de Salud Ñuble.
- Documentos del Sistema de Gestión de Seguridad de la Información (SGSI)
- Ley Marco de Ciberseguridad N°21.663

5 ROLES Y RESPONSABILIDADES

Comité de Seguridad de la Información

- 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 y 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.

Encargado de Seguridad de la Información y Ciberseguridad

- 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 Servicio de Salud Ñuble.
- 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 Ministerio y la Red de Salud, 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 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 Servicio de Salud Ñuble, 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 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.

Encargado de los Activos de Información

- Responsable de su identificación, así como gestionar el riesgo y niveles de seguridad asociados.
- El desempeño de estas funciones no podrá ser externalizado bajo ninguna forma.

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 otros roles nominados 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.
- Las principales responsabilidades de los usuarios sobre el uso de la información institucional son:
    - Utilizar la información sólo para el propósito para el que recibió autorización de uso.
    - Conocer las políticas y procedimientos de seguridad de la información que se han institucionalizado.
    - Cumplir con los controles establecidos en las políticas y procedimientos definidos en el sistema de seguridad de la información del Servicio de Salud Ñuble.
    - Tomar las medidas adecuadas para evitar que la información se divulgue o use sin autorización.
    - Comunicar las debilidades detectadas, los eventos e incidentes relativos a la seguridad de la información.
    - Responder por el uso de cualquier recurso de procesamiento de la información y cualquier uso desarrollado bajo su responsabilidad.

6 MATERIAS QUE ABORDA

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

7 PRINCIPIOS BÁSICOS

Declaración Institucional

El Servicio de Salud de Ñuble se compromete a gestionar de manera continua la seguridad de la información y ciberseguridad, en conformidad con la normativa gubernamental vigente. Para lograr este propósito, llevará a cabo las acciones necesarias para establecer niveles aceptables de seguridad determinados internamente, basándose en metodologías y técnicas estándares. El objetivo es instaurar un ciclo de mejora constante y sostenible que asegure la integridad, confidencialidad y disponibilidad de los activos de información esenciales para la institución, como un pilar fundamental en la gestión de sus procesos.

El Servicio de Salud de Ñuble se compromete a impulsar un plan de mejora continua, fundamentado principalmente en la normativa NCh-ISO 27001:2013, con el propósito fundamental de asegurar una gestión idónea de la seguridad de la información y ciberseguridad. Este enfoque busca optimizar, profesionalizar y reforzar la protección de todos los activos de información pertenecientes a la institución. No obstante, podrá recurrir a estándares reconocidos a nivel nacional o internacional, que se adecuen a sus necesidades, con el propósito de monitorear con mayor efectividad la evolución de su nivel de madurez.

Con miras a cumplir esta misión, se ha decidido establecer, implementar, administrar y continuar perfeccionando un Sistema de Gestión de Seguridad de la Información (SGSI). Dicho sistema se cimentará en directrices claras que se ajusten a las demandas institucionales y a los requisitos regulatorios pertinentes. La implementación exitosa de estas medidas permitirá asegurar la confiabilidad y robustez de las prácticas relacionadas con la seguridad de la información y la ciberseguridad en el Servicio de Salud de Ñuble

A raíz de lo expuesto previamente, la dirección del Servicio de Salud de Ñuble establece los siguientes principios que sustentarán la seguridad institucional:

i. Incentivar la percepción de la Información como un recurso esencial en el ámbito de la salud, reconociendo su valor estratégico y su papel fundamental en la toma de decisiones.
ii. Proteger la privacidad y confidencialidad de toda información sensible o personal, independientemente de su formato o medio de almacenamiento, a fin de respetar los derechos individuales y la integridad de los datos.
iii. Preservar la integridad de los datos, reconociendo que su exactitud y actualización pueden ser vitales.

iv. Garantizar el acceso a la información crítica únicamente para usuarios autorizados y en momentos pertinentes, asegurando así la disponibilidad y el uso adecuado de los recursos.
v. Implementar un modelo de gestión de riesgos para la seguridad de la información, con el fin de identificar y mitigar riesgos relevantes mediante controles apropiados.
vi. Cumplir con el marco normativo establecido para la seguridad de la información en el sector salud e institucional, a través de la gestión de controles definidos.
vii. Realizar respaldos seguros que permitan la protección de la información gestionada por el sector salud y definir responsabilidades y frecuencia de pruebas de restauración para sistemas críticos.
viii. Establecer mecanismos para identificar, analizar, notificar, responder y aprender de debilidades, eventos e incidentes de seguridad de la información, para su mitigación y prevención.
ix. Desarrollar programas educativos para el personal del sector salud, con el propósito de mejorar su comprensión y competencias en el ámbito de seguridad de la información y ciberseguridad
x. Apoyar la construcción de una plataforma de intercambio recíproco de experiencias y aprendizaje en todos los aspectos de la seguridad de la información del sector Salud.
xi. Procurar que las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los funcionarios, proveedores o terceros.

8 OBJETIVOS DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD EN EL SERVICIO DE SALUD ÑUBLE

Objetivo General

Establecer un marco integral de seguridad de la información y ciberseguridad que garantice la protección, confidencialidad, integridad y disponibilidad de los activos de información del Servicio de Salud de Ñuble**,** así como la mitigación de riesgos cibernéticos, con el propósito de salvaguardar los intereses públicos, asegurar el cumplimiento de las obligaciones legales y normativas, y fortalecer la confianza de los ciudadanos y partes interesadas en la gestión de datos y servicios electrónicos ofrecidos por la institución.

Objetivos Específicos

- Identificar y registrar los activos de información relevantes, tanto directos como indirectos, presentes en los procesos institucionales. Esto abarca tanto los procesos críticos institucionales como los de soporte.

- Implementar un modelo de gestión de riesgos para la seguridad de la información y ciberseguridad, que permitan una comprensión precisa de las amenazas potenciales, con el fin de identificar y mitigar riesgos relevantes mediante controles apropiados.
- Garantizar la protección integral de la información en términos de su procesamiento, conservación y transmisión. Esto implica prevenir cualquier acceso no autorizado, revelaciones accidentales, errores, fraudes, sabotajes, violaciones de privacidad y otras acciones que puedan ponerla en peligro.
- Establecer protocolos claros para la gestión de incidentes de seguridad de la información y ciberseguridad, con el fin de detectar, notificar, responder y recuperarse de manera eficiente ante cualquier evento no deseado
- Utilizar y mantener de manera efectiva la estructura y el conjunto de estándares, políticas y procedimientos en materia de seguridad de la información y ciberseguridad.
- Minimizar la probabilidad de eventos contingentes que puedan interrumpir la operación normal del negocio y reducir el impacto de posibles daños a las instalaciones, medios de almacenamiento, equipos de procesamiento y comunicación.
- Sensibilizar y capacitar a los funcionarios del Servicio de Salud de Ñuble acerca de su responsabilidad en el mantenimiento de la seguridad de la información y su uso adecuado. Esto incluye la creación de una cultura organizacional que integre la seguridad de la información y ciberseguridad como un aspecto fundamental en los procesos y servicios del Servicio de Salud de Ñuble.

9 LINEAMIENTOS ESPECIFICOS

Responsabilidad y organización

El Servicio de Salud Ñuble dispondrá de una unidad que asuma la función de definición, impulso y control de la seguridad de la información y ciberseguridad en la institución, que participe en la toma de decisiones y estrategias relacionadas con su ámbito de acción.

Del mismo modo deberá asegurar el reporte adecuado, y a los niveles oportunos, de los riesgos relacionados con seguridad de la información y ciberseguridad, así como de los mecanismos de mitigación y control de estos que sean necesarios.

Esta unidad contará con suficientes capacidades y recursos, materiales y humanos, para la consecución de sus objetivos, y dependerá funcionalmente del Departamento de Informática, participará de alguna de sus comisiones especializadas o de cualquier otro órgano o miembro de la alta dirección, siempre que se mantenga la debida independencia respecto de los responsables de sistemas de redes y de información.

El máximo responsable de esta unidad será el Encargado de Seguridad de la Información y Ciberseguridad. Esta figura será una persona con el conocimiento, experiencia y competencias adecuadas para desarrollar la función y contará con la suficiente capacidad de decisión e influencia en la organización.

Existirá un Comité de Seguridad de la Información y Ciberseguridad, constituido formalmente, en el que estarán representado, además del Encargado de Seguridad de la Información y Ciberseguridad, un número adecuado de áreas del Servicio de Salud Ñuble para adoptar cualquier resolución, con relevancia en materia de seguridad de la información, que pueda afectar sustancialmente a la actividad de la organización.

Gestión de Seguridad de la Información y Ciberseguridad de forma transversal

La Gestión de Seguridad de la Información y Ciberseguridad se deberá implementar de manera transversal en todo el Servicio de Salud Ñuble**,** y no limitarse exclusivamente a la responsabilidad del Departamento de Informática. Esta gestión debe abordar procesos interdepartamentales y contar con la participación de los responsables de dichos procesos.

Seguridad Informática de los Recursos Humanos

Se debe establecer la necesidad de informar y educar a todos los empleados y terceros relacionados con el Servicio de Salud Ñuble, sobre lo que se espera de ellos en estas materias.

Gestión de Activos

Se debe de realizar gestión y protección efectiva de los activos, considerando su clasificación según su nivel de importancia, representa una prioridad primordial para el Servicio de Salud Ñuble. Estos activos abarcan no solo el hardware y el software, sino también los dispositivos de comunicación, elementos de apoyo, información y datos en todas sus formas y formatos.

La clasificación de los activos se realiza considerando aspectos clave como la confidencialidad, integridad y disponibilidad de los datos, así como las funciones que dichos activos respaldan y la normativa vigente aplicable.

Autenticación, autorización y control de Acceso

Es esencial garantizar que el acceso de los usuarios esté debidamente autorizado y prevenir el acceso no autorizado a los sistemas de información. Para lograr esto, se deben de establecer procedimientos formales de control en la asignación de derechos de acceso a los sistemas de información, abarcando todas las etapas del ciclo de vida del acceso del usuario, desde su registro inicial hasta su desvinculación.

La asignación de derechos de acceso debe ser abordada con especial atención para evitar la asignación de privilegios que permitan a los usuarios eludir los controles del sistema. Para reforzar estas medidas, se implementará una política de escritorio y pantalla limpios. Esto servirá para reducir tanto el riesgo de acceso no autorizado como el peligro de robo o daño a documentos y otros medios de almacenamiento de información.

El enfoque integral de autenticación, autorización y control de acceso es crucial para asegurar la confidencialidad, integridad y disponibilidad de los activos de información, así como para prevenir posibles vulnerabilidades y salvaguardar la seguridad de los sistemas de información en su totalidad.

Seguridad física y ambiental

Se deben identificar los riesgos vinculados al acceso físico a las instalaciones y a la infraestructura tecnológica de la institución, tanto por parte de los funcionarios como de terceros. El objetivo primordial es prevenir cualquier tipo de acceso no autorizado, así como evitar daños e interferencias en las instalaciones y en la información resguardada en ellas.

Seguridad operativa

Se debe establecer la implementación de mecanismos de gestión y monitoreo destinados a salvaguardar la infraestructura de tecnologías de información ante posibles amenazas, tanto físicas como tecnológicas. El propósito principal es optimizar la operación de las plataformas tecnológicas, garantizando un procesamiento preciso y seguro de la información.

Adquisición, desarrollo y mantenimiento de los sistemas

La adquisición, desarrollo y mantenimiento de sistemas de información abarca sistemas operativos, infraestructura, aplicaciones empresariales, servicios y aplicaciones desarrolladas internamente por la institución. Por lo que será esencial la identificación y el acuerdo de todos los requisitos de seguridad antes de la fase de desarrollo y/o implementación de los sistemas. Estos requisitos deben ser debidamente justificados, acordados y documentados como parte integral de los procedimientos para sistemas de información.
En el caso de desarrollos de software internos o aquellos contratados a terceros, es crucial asegurar que la seguridad sea un componente integral de los sistemas de información desarrollados. Esto implica la inclusión de los requisitos de seguridad desde la etapa de especificación del software y a lo largo de todo el ciclo de vida del proyecto de desarrollo de software. La ciberseguridad se integra en cada etapa para garantizar la protección adecuada de la información y la continuidad operativa, respaldando así la confidencialidad, integridad y disponibilidad de los activos de información y los sistemas involucrados.

Interoperatividad

Se deberán definir estándares y protocolos de comunicación compartidos para asegurar que diferentes sistemas y tecnologías puedan interactuar de manera segura y eficiente. Establecer el cifrado y autenticación en las comunicaciones entre sistemas y dispositivos para prevenir accesos no autorizados y asegurar la confidencialidad de los datos transmitidos. Definir procedimientos seguros para el intercambio de datos, con mecanismos de validación de integridad para prevenir alteraciones no autorizadas. Así como la definición de planes de contingencia y procedimientos de recuperación ante fallos que consideren la interoperabilidad, de modo que cualquier interrupción no comprometa la seguridad global. La incorporación de estos elementos asegurará una protección cohesiva y robusta de los sistemas y datos, permitiendo una colaboración segura y eficiente entre diferentes sistemas y plataformas del Servicio de Salud Ñuble.

Ciberseguridad

Se debe establecer un conjunto integral de prácticas y políticas destinadas a proteger los sistemas, redes y datos contra amenazas cibernéticas. Esto debe incluir la implementación de medidas de autenticación sólidas, el uso de encriptación para proteger la confidencialidad de la información, la actualización constante de software y sistemas para mitigar vulnerabilidades, la capacitación periódica del personal en concienciación sobre seguridad, la monitorización constante de actividad sospechosa y la elaboración de planes de respuesta ante posibles incidentes, todo ello con el objetivo de mantener la integridad, disponibilidad y privacidad de los activos digitales de manera efectiva y continua.

Gestión de Incidentes

Es esencial garantizar la comunicación oportuna de debilidades, problemas y eventos de seguridad relacionados con los sistemas de información, permitiendo la adopción inmediata de medidas correctivas. Para lograrlo, se debe establecer un procedimiento formal para informar sobre cualquier evento de seguridad de la información, así como para gestionar la respuesta ante incidentes. Además, se implementar un proceso de escalado que indique las acciones a tomar al recibir un informe de evento de seguridad de la información. Estos procedimientos serán ampliamente difundidos para que todos los miembros del equipo estén al tanto.

La gestión efectiva de incidentes en seguridad de la información y ciberseguridad asegura una respuesta ágil y coordinada ante cualquier eventualidad, garantizando la minimización de impactos y la continuidad operativa.

Aspectos de la continuidad del negocio

Se requiere adoptar medidas preventivas y de mitigación para evitar y reducir al mínimo los impactos de los incidentes de seguridad de la información que puedan afectar la integridad de las redes, equipos y sistemas esenciales para la prestación de servicios. El objetivo principal es asegurar la continuidad operativa y facilitar la recuperación efectiva de la plataforma tecnológica y sus servicios.

En todos los escenarios, será imprescindible desarrollar, implementar, poner en práctica y evaluar un plan de respuesta integral que brinde una cobertura adecuada a las redes, equipos y sistemas. Este plan se alineará con estándares internacionales o nacionales de amplio reconocimiento y se centrará en garantizar, desde la perspectiva de los clientes, la preservación de la integridad, disponibilidad y confidencialidad de la información.

La planificación de la continuidad del negocio en el ámbito de la seguridad de la información se erige como un pilar fundamental para proteger la estabilidad de las operaciones y salvaguardar los activos críticos, brindando así la tranquilidad de una respuesta efectiva ante situaciones adversas.

Cumplimiento

Anualmente, se llevará a cabo la generación de procedimientos de auditoría con el propósito fundamental de prevenir cualquier tipo de incumplimiento de leyes, estatutos, regulaciones u obligaciones contractuales, así como de los requisitos de seguridad de la información y ciberseguridad que puedan afectar el diseño, operación, uso y gestión de los sistemas de información del Servicio de Salud Ñuble. Estos procedimientos establecerán plazos periódicos para garantizar la ejecución de un control riguroso sobre la normativa vigente en esta materia. Asimismo, se realizará el seguimiento y se atenderán de manera efectiva las recomendaciones pertinentes para asegurar la conformidad con las regulaciones en constante evolución.

10 GESTIÓN DE LA POLITICA Y OTROS DOCUMENTOS DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

La documentación aplicable al Servicio de Salud Ñuble deben asegurar:

- La integración del modelo de seguridad de la información, con las metodologías y políticas existentes para el Servicio de Salud Ñuble.
- Que se cumplan las normas legales y reglamentarias referidas a seguridad de la información y ciberseguridad, 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 se encuentren 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 Servicio de Salud Ñuble 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.

11 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, 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:

- Norma NCh-ISO 31000:2018 sobre directrices para la gestión de riesgos.
- Norma NCh-ISO/IEC 27005:2020 sobre las tecnologías de información, y la gestión del riesgo de seguridad de la información.
- Política General de Seguridad de la Información del Servicio de Salud Ñuble.

12 TERMINOLOGÍA

En este apartado se introducen los términos utilizados en la gestión de riesgos, su comprensión facilitará el resto de la lectura de la presente política.

- Activo: Todo elemento lógico o físico, componente de hardware, equipamiento o sistema relacionado con la información, que permita su generación, almacenamiento, soporte, envío o intercambio, sea a otros órganos de la Administración del Estado o con personas naturales o jurídicas.
- Activo de Información: Datos o información cuyo tratamiento es esencial para el funcionamiento y desarrollo del Servicio de Salud Ñuble que lo utiliza, genera, almacena, envía o intercambia, y que deben ser protegidos en su confidencialidad, integridad, disponibilidad u otros factores de importancia.
- Ciberseguridad y Seguridad de la Información: Conjunto de acciones, políticas, medidas preventivas y reactivas destinadas a la prevención, mitigación, manejo, respuesta y estudio de las amenazas y riesgos de incidentes de seguridad, a la reducción de sus efectos y el daño causado; antes, durante y después de su ocurrencia; respecto de los activos y activos de información y la continuidad de servicios, con el fin de proteger, preservar y restablecer la confidencialidad, integridad y disponibilidad de aquellos y de las plataformas electrónicas del Servicio de Salud Ñuble, aumentando su resiliencia en el tiempo.
- Gestión de Riesgo: Proceso estructurado y proactivo por el cual se identifican, evalúan, controlan y tratan los riesgos derivados de una o más amenazas determinadas.
- Incidente de Seguridad: Todo evento de seguridad o una serie de ellos, de carácter indeseado o inesperado, que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los sistemas informáticos, los activos y activos de información, datos almacenados, transmitidos o procesados, o los servicios correspondientes ofrecidos por dichos sistemas y que puedan afectar al normal funcionamiento de los mismos.
- Confidencialidad: propiedad de la información que se mantiene inaccesible y no se revela a individuos, entidades o procesos no autorizados.
- Disponibilidad: propiedad de la información de asegurar protección frente a interrupciones en el acceso.
- Integridad: Atributo de los activos y activos de información relativo a la exactitud, autenticidad y completitud de los mismos.
- Plataforma electrónica (en adelante también "plataforma"): Software o conjunto de software, datos e infraestructura tecnológica que sustenta procesos o procedimientos.
- Riesgo: Efecto de la incertidumbre sobre los activos de información y los objetivos de una entidad, habitualmente expresado en relación a las consecuencias de un evento o incidente de seguridad y su probabilidad de ocurrencia.

- Servidor: Equipo virtual o físico dedicado a entregar servicios de red, servicios de bases de datos, sitios web, sistemas informáticos, carpetas compartidas y, en general, brindar los recursos necesarios para responder las peticiones de usuarios.
- Sistema Informático: Conjunto de componentes lógicos y físicos que, interactuando entre sí, permiten que su totalidad o una parte de ellos, realicen la función para la cual fueron diseñados.
- Usuarios(as): Personas naturales o sus apoderados(as), y los(as) representantes de las personas jurídicas o entidades y agrupaciones sin personalidad jurídica que actúan como interesados(as) en un procedimiento administrativo, así como los(as) funcionarios(as) que acceden a las plataformas electrónicas que soportan procedimientos administrativos o procesos relacionados con estos.

13 REVISIÓN Y MEDICIÓN

A lo menos una vez al año, el Comité de Seguridad de la Información del Servicio de Salud Ñuble debe evaluar el estado del SGSI e informar al nivel directivo de 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.

14 CUMPLIMIENTO DE LA PRESENTE POLITICA

Todos los usuarios del Servicio de Salud Ñuble 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 servicio, el oferente deberá dar cumplimiento a las políticas y procedimientos vigentes de seguridad de la información del Servicio de Salud Ñuble, las cuales se presumen conocidas por el contratista o adjudicatario, para todos los efectos legales.

15 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

- **Leyes o Decretos**
  - Ley 19.650, que perfecciona las normas del área de la salud.
  - Ley N° 19.966, que Establece un Régimen de Garantías Explícitas en Salud. La Ley N°19.966 fue promulgada el 25 de agosto de 2004 y publicada el 03 de septiembre de 2004.
  - Ley Nº 19.628, de 1999, Ministerio Secretaría General de la Presidencia, sobre protección de la vida privada.
  - Ley Nº 20.285, de 2008, Ministerio Secretaría General de la Presidencia, sobre acceso a la información pública.
  - Ley N° 20.584, de 2012, Ministerio de Salud, Subsecretaría de Salud Pública, regula derechos y deberes que tienen las personas en relación con acciones vinculadas a su atención en salud.
  - Ley N° 20.120, de 2006, Ministerio de Salud, Subsecretaría de Salud Pública, sobre la investigación científica en el ser humano, su genoma, y prohíbe la clonación humana.
  - Ley N° 20.724, de 2014, Ministerio de Salud, modifica el código sanitario en materia de regulación de farmacias y medicamentos.
  - D.F.L. Nº29, de 2005, Ministerio de Hacienda, que fija texto refundido, coordinado y sistematizado de la Ley N° 18.834, sobre estatuto Administrativo.
    Decreto con Fuerza de Ley Nº 1/19653, Ministerio Secretaría General de la Presidencia, que fija texto refundido, coordinado y sistematizado de la ley Nº 18.575, orgánica constitucional de Bases Generales de la Administración del Estado.
  - Decreto N°273 que establece obligación de reportar incidentes de ciberseguridad.
  - Ley Nº 21.180 sobre Transformación Digital del Estado, Decreto N°7 sobre Norma técnica de seguridad de la información y ciberseguridad.
  - Ley N° 21.663 Ley Marco de Ciberseguridad

16 INDICADORES

Área	Criterio
Cobertura de la norma ISO 27001	Al medir la cobertura de la norma es posible hacer seguimiento del avance de la implementación de los controles que mitigan los riesgos de seguridad.
Niveles de madurez	Si bien se avanza en la implementación de controles, es necesario que estos sean efectivos, motivo por el que es necesario medir su madurez.
Gestión de incidentes	Dado el nivel de exposición al riesgo que existe hoy en el sector, es necesario contar con procesos robustos de gestión de incidentes, para dar respuesta a los riesgos que pudieran concretarse, mientras se alcanza un nivel de madurez y cobertura suficiente.
Análisis de vulnerabilidades técnicas	Además de dar respuesta a los problemas que pudieran surgir, es necesario realizar análisis que permitan identificar las vulnerabilidades técnicas, y ejecutar acciones preventivas para disminuir el nivel de riesgo y número de incidentes.
Capacitación	Capacitar a los funcionarios en seguridad de la información no solo protege a la organización de amenazas cibernéticas, sino que también contribuye a crear una cultura de seguridad consciente y proactiva en toda la institución.

A continuación, se presentan los distintos indicadores por área:

Cobertura de la norma ISO 27001

- Número de Controles Implementados: Mide cuántos de los controles de seguridad especificados en ISO 27001 han sido implementados en la organización.
- Nivel de Documentación de Políticas y Procedimientos: Mide cuántas de las políticas y procedimientos de seguridad requeridos por ISO 27001 han sido documentados.

Niveles de madurez

- Medición del Nivel de madurez (de acuerdo con el modelo de madurez del PMI) en los procesos operativos y de gestión de seguridad de la información, según el marco de Seguridad ISO 27001.

Gestión de incidentes

- Tasa de Incidentes de Seguridad: Registra la cantidad de incidentes de seguridad reportados en un período determinado. Esto puede incluir intentos de intrusión, phishing, malware, etc.
- Tiempo de Resolución de Incidentes: Mide el tiempo que lleva resolver y cerrar un incidente de seguridad después de haber sido detectado.

Análisis de vulnerabilidades técnicas

- Vulnerabilidades Críticas por Aplicación: Calcula la cantidad de vulnerabilidades de seguridad críticas (de alto riesgo) identificadas en cada aplicación.
- Tiempo Promedio de Resolución de Vulnerabilidades: Mide el tiempo que lleva resolver las vulnerabilidades de seguridad identificadas, desde su descubrimiento hasta su resolución completa.

Capacitación

- Capacitación en Seguridad: Calcula el porcentaje de funcionarios que han recibido capacitación en seguridad de la información según lo definido en ISO 27001.

17 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 sitio web de Servicio de Salud Ñuble
- Publicación en la intranet del Servicio de Salud Ñuble.

18 REGISTROS

Se mantendrá una planilla que permita disponer de la información actualizada de la situación de la documentación y para conocer la evolución histórica.

19 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.

20 CONTROL DE VERSIONES

VERSION/ REVISION	FECHA	MODIFICACIONES
1.0	01/01/2017	Elaboración de las Política General de Seguridad
2.0	08/07/2024	Revisión de la Política General de Seguridad

21 REFERENCIAS

NCh-ISO27001:2013: Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información – Requisitos.