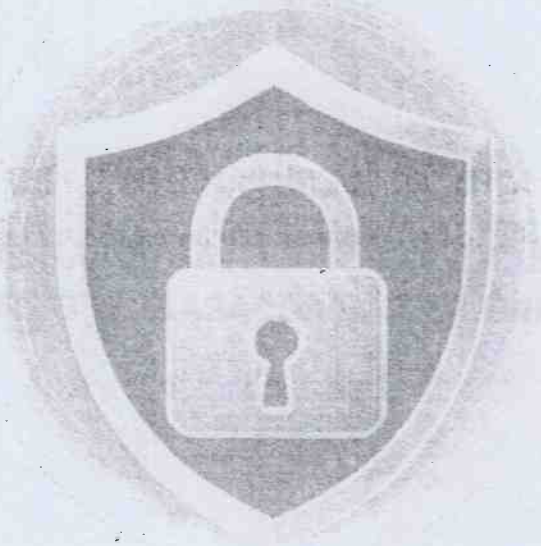
INSTRUCTIVO DE SEGURIDAD DE LA INFORMACION Y CIBERSEGURIDAD PARA EL SECTOR SALUD

ITS-NC- 007
Versión Oficial v 2.0 – Abril 2025

	Responsable	Fecha	Firma
Elaborado	**Pablo Fabres F. – José Villa C.** Unidad de Seguridad de la Información y Ciberseguridad	Marzo 2025	
Revisado	**José Villa C.** Encargado de Seguridad de la Información y Ciberseguridad	Abril 2025	
Aprobado	**Jorge Herrera R.** Jefe Departamento de Tecnologías de Información y Comunicaciones	Abril 2025	



CIBERSEGURIDAD
MINSAL

VISADO

Resumen

La acelerada transformación digital del Estado y la creciente adopción de tecnologías avanzadas en el Sector Salud han traído consigo importantes beneficios en términos de eficiencia y acceso. Sin embargo, también han aumentado de manera alarmante la exposición a riesgos y la ocurrencia Incidentes de ciberseguridad, afectando la continuidad operativa de sistemas y la exposición de datos. Dada la importancia de los sistemas de salud y la alta sensibilidad de la información relacionada, es fundamental garantizar una protección prioritaria e ineludible de activos críticos para nuestro sector.

Como antecedente, el Instructivo de Ciberseguridad que fue aprobado mediante la Resolución Exenta N° 785 el 03 de noviembre de 2021 marcó un hito para el sector en esta materia. Sin embargo, con la evolución de la tecnología y las modificaciones legales y reglamentarias surgen nuevos desafíos, que demandan su actualización.

Entre los desafíos técnicos, se pueden mencionar: la expansión de la telemedicina, la Interoperabilidad de los sistemas, el uso creciente de dispositivos médicos conectados a Internet (IoT), la dependencia de proveedores a través de la cadena de suministros, el aumento de los servicios en la nube a través de estrategias híbridas o multicloud, la incorporación de la Inteligencia Artificial en procesos clínicos, la a estandarización e interoperabilidad segura de datos entre los sistemas de salud, la urgencia de fortalecer una arquitectura de seguridad sólida que esté alineada con la Arquitectura de Referencia del Minsal, dada la creciente sofisticación de las amenazas.

A ello se suma los avances de la Ley sobre Transformación Digital del Estado que conlleva la digitalización de los trámites y procedimientos administrativos, lo que involucra desafíos adicionales, en materia de interoperabilidad, en la puesta a disposición de servicios a usuarios finales y gestión de riesgos informáticos que conlleva.

En el ámbito normativo, destacan la entrada en vigor de la Ley N° 21.663, ley Marco de Ciberseguridad y sus reglamentos y demás normas complementarias, que mandatan el establecimiento de normas, instrucciones y directrices de ciberseguridad que sean aplicables a las instituciones que se encuentren bajo el ámbito de cada una de las respectivas competencias institucionales y 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.

En este contexto se pone a disposición de la Red, el nuevo Instructivo de Seguridad de la Información y Ciberseguridad para el Sector Salud, el cual tiene carácter de obligatorio para las instituciones del ecosistema del Ministerio de Salud (Minsal).

Este documento tiene como objetivo principal es, establecer lineamientos, directrices y controles de seguridad que deben ser adoptados por estas instituciones, promoviendo una gobernanza de ciberseguridad coordinada en todo el sector, fomentando la adopción de prácticas modernas, sobre los nuevos desafíos y la protección de los derechos de las personas

en el entorno digital, lo cual es fundamental para proteger los sistemas críticos, mantener la integridad de la información y garantizar la continuidad operativa en el Sector Salud, todo lo anterior en línea con estándares internacionales de seguridad.

El cumplimiento de los lineamientos previstos en este instructivo permitirá dar cumplimiento a la legislación nacional vigente y fortalecer la resiliencia del Sector Salud frente a las amenazas cibernéticas.

INDICE

1. INTRODUCCION

El Sector Salud, al manejar información altamente sensible y se operan sistemas críticos para la atención de la población. Salud se encuentra entre los sectores más vulnerables ante estas amenazas. Ataques dirigidos, brechas de datos, interrupciones de servicios y vulnerabilidades explotadas a través de terceros representan riesgos reales que pueden afectar gravemente la confidencialidad, disponibilidad e integridad de la información sanitaria. Casos emblemáticos a nivel internacional, como el ataque a SolarWinds, y experiencias recientes en organismos públicos nacionales han evidenciado la necesidad urgente de reforzar los mecanismos de protección y gobernanza de la información.

En este contexto, en cumplimiento de lo establecido en la Ley Marco de Ciberseguridad N° 21.663, y en concordancia con la Política Nacional de Ciberseguridad y los estándares de seguridad emitidos por la Agencia Nacional de Ciberseguridad (ANCI), el presente Instructivo de Seguridad de la Información y Ciberseguridad para el Sector Salud tiene carácter obligatorio y establece los lineamientos, directrices y controles que deben ser adoptados e implementados por todas las entidades que integran el ecosistema del Ministerio de Salud (Minsal)[1].

Esto incluye, de manera explícita a las Secretarías Regionales Ministeriales (Seremis), los Servicios de Salud, los Hospitales de Alta y Mediana Complejidad, los Establecimientos de Atención Primaria y demás organismos públicos o autónomos del sector que se encuentren bajo su dependencia o relación administrativa.

La adopción de estas directrices surge del mandato legal de la Ley Marco, que establece la necesidad de crear normas, instrucciones y directrices de ciberseguridad que sean aplicables a los órganos de la Administración del Estado, dentro del ámbito de sus competencias. Esto asegura una gestión que sea coordinada, eficaz y alineada con los estándares internacionales. Cumplir con estas directrices es fundamental para proteger los sistemas críticos, mantener la integridad de la información y asegurar la continuidad operativa en el Sector de Salud.

2. PROPÓSITO

El presente Instructivo de Seguridad de la Información y Ciberseguridad para el Sector Salud establece los lineamientos, directrices y controles de seguridad que deben ser adoptados por las instituciones que integran el ecosistema del Ministerio de Salud (Minsal), Seremis, Servicios de Salud, Hospitales, Establecimientos de Atención Primaria y demás Organismos Autónomos del sector.

Este instructivo considera lo previsto en la Ley N° 21.663, que establece un marco de ciberseguridad para fortalecer la protección de la información crítica, asegurar la continuidad operativa y mejorar la resiliencia de los sistemas de información.

[1] Ley 21.663 Artículo 26.

También incluye las disposiciones de la Ley N° 21.180 sobre la Transformación Digital del Estado, lo que garantiza la seguridad en la digitalización de los procesos administrativos y la interoperabilidad segura entre diferentes instituciones.

Además, se alinea con las mejores prácticas de estándares internacionales de seguridad, como ISO/IEC 27001:2022 e ISO/IEC 27002:2022 para la gestión de la seguridad de la información; NIST SP 800-53 y el NIST Cybersecurity Framework (CSF) para la gestión de riesgos y controles de ciberseguridad; CIS Controls v8 para implementar medidas de protección efectivas; y HIPAA (Health Insurance Portability and Accountability Act) para asegurar la seguridad, privacidad y confidencialidad de la información de salud en entornos digitales, entre otros.

El propósito principal de este instructivo es reforzar la seguridad y la privacidad de la información en los sistemas tecnológicos y servicios del sector salud, mediante lineamientos que permitan minimizar los riesgos de afectación a la confidencialidad, integridad, disponibilidad y trazabilidad de los datos, en estricto cumplimiento de la Ley N° 19.628 sobre Protección de la Vida Privada, así como su actualización a través de la Ley N° 21.719 sobre Protección de Datos Personales, la ley N° 20.584 y sus modificaciones, introducidas por la Ley N° 21.541 sobre Telemedicina y la Ley N° 21.668 sobre Interoperabilidad de Fichas Clínicas y las normas reglamentarias que desarrollan estas leyes.

Este instructivo es obligatorio y establece las pautas, directrices y controles técnicos y administrativos que todas las Instituciones del Sector Salud deben seguir e implementar. También se alinea con la normativa actual del Minsal, especialmente con la Política General de Seguridad de la Información y Ciberseguridad, que fue aprobada por la Resolución Exenta N° 1465/2023. Esta política ofrece un marco de referencia y directrices que buscan proteger de manera integral y efectiva la información y los sistemas tecnológicos de las instituciones, cumpliendo con los estándares internacionales y las exigencias legales nacionales.

3. ALCANCE Y APLICABILIDAD

3.1. Alcance

Este instructivo es aplicable a todas las Instituciones del Sector Salud, esto incluye:

- Ministerio de Salud.
- Subsecretarías de Salud Pública y Redes Asistenciales.
- Secretarías Regionales Ministeriales (SEREMI)
- Servicios de Salud y sus respectivos establecimientos hospitalarios.
- Centros de Atención Primaria de Salud (APS).
- Organismos Autónomos de Salud.
- Entidades externas que operen o administren sistemas de información en salud.

3.2. Aplicabilidad

El cumplimiento de este instructivo es esencial para todas las instituciones del sector salud que manejen, procesen o almacenen información sensible, así como para los proveedores de servicios tecnológicos que colaboren con este sector. A estos efectos, todos los procesos de compra que se realicen por instituciones del sector, deberán contener la obligación del proveedor de ceñirse a los lineamientos previstos en este instrumento.

Las pautas establecidas deben aplicarse en:

- Infraestructura tecnológica: redes, servidores, plataformas en la nube y dispositivos conectados.
- Sistemas de información: software de gestión clínica, registros clínicos electrónico (RCE), sistemas de telemedicina, bases de datos, entre otros.
- Gestión de accesos: autenticación, control de privilegios y monitoreo de actividad en los sistemas.
- Protección de datos sensibles: cifrado, seudonimización, anonimización y resguardo de la información de pacientes y profesionales.
- Gestión de incidentes de ciberseguridad: detección, respuesta y mitigación de riesgos conforme a marcos normativos y estándares internacionales.

4. ELEMENTOS CLAVES PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

4.1. Gobernanza

La gobernanza en ciberseguridad se refiere al conjunto de decisiones, directrices y controles que la alta dirección implementa para garantizar que se cumplan los objetivos estratégicos de la institución. Esto no solo apoya la misión organizacional, sino que también ayuda a gestionar los riesgos que podrían poner en peligro su consecución.

En este contexto, la Ley N° 21.663 sobre Ciberseguridad, publicada en abril de 2024, establece que las instituciones públicas deben implementar ***una estructura de gobernanza que asegure una gestión eficaz para proteger sus sistemas críticos de información.***

Por su parte el NIST Cybersecurity Framework 2.0 (CSF 2.0), destaca que la función de gobierno permite que la alta dirección comprenda y gestione los riesgos de ciberseguridad en relación con la estrategia organizacional, enfocándose en cómo estas amenazas pueden afectar los objetivos institucionales.

Adicionalmente, 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 exige contar con un marco de gobernanza de la seguridad de la información que permita a la institución detectar, obtener evidencias y denunciar oportunamente los incidentes de seguridad de la información que sean producto de acciones que pudieran revestir caracteres de delito.

En este contexto y con el objetivo de fortalecer la cultura de seguridad en nuestra institución, es fundamental implementar medidas concretas que aseguren una gobernanza efectiva en cuanto a la Seguridad de la Información y la Ciberseguridad en todos las Instituciones del sector relacionados con el MINSAL.

Esto implica que las instituciones del sector salud deben:

- **Designar a un responsable de ciberseguridad**, encargado de coordinar la gestión de riesgos y el cumplimiento normativo.
- **Implementar políticas y procedimientos de seguridad**, alineados con estándares nacionales e internacionales.
- **Conformar Comités de Seguridad de la Información**, Ciberseguridad y Protección de Datos Personales, que supervisen la ejecución de estrategias de seguridad y la respuesta ante incidentes.
- **Establecer roles y responsabilidades claras**, garantizando una adecuada asignación de funciones dentro de la organización.
- **Implementar una estrategia de monitoreo continuo y mejora de capacidades de ciberseguridad**, incluyendo auditorías, capacitaciones y simulacros de respuesta a incidentes.

4.2. Compromiso del Nivel Directivo

El compromiso de la alta dirección es fundamental para el éxito de cualquier estrategia de ciberseguridad. Este compromiso se manifiesta en la creación e implementación de políticas institucionales, que son declaraciones claras de intenciones y directrices estratégicas en el ámbito de la seguridad de la información.

Un ejemplo a nivel nacional es la Política Nacional de Ciberseguridad, que ha contado con el respaldo de tres presidentes de la república, quienes han actuado como patrocinadores de alto nivel, impulsando reformas y medidas clave para mejorar la seguridad digital del país. Este tipo de compromiso debería ser replicado en cada organización, tanto del sector público como del privado.

Por su parte, la Ley N° 21.663 establece que las "***Autoridades y directivos de las instituciones tienen un rol fundamental en la gobernanza de la ciberseguridad**, debiendo asumir un compromiso activo y vinculante en la gestión de riesgos y protección de la infraestructura crítica*", compromiso que implica:

- **Incorporar la ciberseguridad en la estrategia institucional**, garantizando su alineación con los objetivos organizacionales.
- **Asignar recursos suficientes y adecuados**, incluyendo talento humano, tecnologías y programas de capacitación.
- **Fomentar una cultura organizacional de seguridad**, mediante campañas de concienciación, liderazgo visible y formación continua.
- **Supervisar y evaluar regularmente** el cumplimiento de las políticas y la eficacia de los controles de seguridad.

- **Adoptar un enfoque integral frente a incidentes**, priorizando la prevención, detección oportuna y mitigación de impactos.

El compromiso de la dirección no solo refuerza la capacidad de la institución para enfrentar amenazas, sino que también legitima y promueve la implementación de una gobernanza sólida en ciberseguridad.

4.3. Estrategia de Seguridad y un Plan Director de Seguridad

La importancia de usar las tecnologías de la información y comunicación (TIC) de manera responsable no puede subestimarse. Con el aumento de los riesgos y amenazas, como los ciberataques que hemos visto en los últimos años, es crucial que estos escenarios sean controlados y monitoreados de manera profesional, siguiendo normas y mejores prácticas, ya que los procesos de negocio y los servicios de las organizaciones dependen en gran medida de las TIC.

Para resguardar los activos de información y garantizar la continuidad de servicio se debe implementar un conjunto de acciones que gestionen la seguridad de la información y la ciberseguridad en el sector salud, de manera proactiva, para crear un entorno sólido que prevenga cualquier afectación a los servicios informáticos.

En cumplimiento de estos imperativos, la estrategia de seguridad de la información y la ciberseguridad de Minsal queda establecida en su Plan Director [2], el que, en línea con los intereses estratégicos de la organización, con un enfoque basado en riesgos y siguiendo los estándares de la industria en esta materia, aborda una serie de iniciativas en apoyo al resguardo de la información, de los activos digitales y procesos tecnológicos que son cruciales para las operaciones del Minsal, para crear condiciones de base que otorguen confianza digital en la organización.

Adicionalmente, para llevar a cabo una implementación efectiva de la seguridad de la información y la ciberseguridad en las Instituciones del Sector Salud, se requiere del compromiso individual de la alta dirección de quienes la conforman en su totalidad.

Para ello, es importante que deban tener en cuenta las siguientes consideraciones clave:

Sponsor directivo: Se debe designar un representante de la alta dirección de la institución, con atribuciones suficientes para garantizar el alineamiento de los objetivos de la política de seguridad de la información con el cumplimiento de objetivos estratégicos organizacionales, el carácter vinculante de los lineamientos que se establezcan y la correcta atribución y comunicación de los roles y responsabilidades relacionados con la seguridad de la información.

[2] Plan de Seguridad de la Información y Ciberseguridad para el Sector de Salud (años 2024-2025), aprobada mediante Resolución Exenta N°969/2024 o el vigente.

Garantizar recursos adecuados: La alta dirección de la institución debe asegurar que se asignen los recursos necesarios para respaldar la seguridad de la información y ciberseguridad, considerando recursos financieros, tecnológicos y humanos.

Compromiso de instituciones del sector: Es esencial obtener la participación y el compromiso activo de las instituciones del sector, su colaboración no solo contribuirá a la eficacia del sistema de gestión de la seguridad de la información y ciberseguridad a nivel sectorial y nacional, sino que también se espera que respalden con otros roles de gestión relevantes, según corresponda a sus áreas de responsabilidad.

Es crucial que **cada institución del sector salud desarrolle y mantenga su propio Plan Director de Ciberseguridad**, adaptado a su realidad operativa, contexto de riesgos, infraestructura tecnológica y nivel de madurez en seguridad de la información. Este plan estratégico no solo ayuda a alinear los objetivos de protección con la misión de la institución, sino que también facilita la planificación, ejecución y seguimiento de iniciativas de seguridad de manera sistemática, priorizando acciones según el impacto potencial en los Servicios de Salud. Tener un plan director institucional refuerza la capacidad de respuesta ante incidentes, mejora la gestión del riesgo tecnológico y asegura la continuidad operativa de los sistemas clínicos y administrativos, contribuyendo así a crear un entorno digital confiable y resiliente en beneficio de los pacientes y la comunidad.

5. DIRECTRICES PARA LA IMPLEMENTACIÓN SGSI PARA LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

En el contexto de fortalecer la ciberseguridad en el sector salud, se debe implementar un Sistema de Gestión de Seguridad de la Información (SGSI) que se base en principios de gobernanza, gestión de riesgos, cumplimiento normativo y mejora continua como el núcleo del modelo de protección institucional.

Este sistema, que se alinea con estándares internacionales como ISO/IEC 27001:2022 y la Ley Marco de Ciberseguridad N°21.663, permite establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de manera sistemática y continua.

La implementación efectiva de este modelo estructurado de gobernanza de la seguridad de la cimentará las bases que permitan asegurar la protección de la confidencialidad, integridad y disponibilidad de los activos críticos de información.

Este modelo debe tener en cuenta los siguientes componentes fundamentales:

5.1. Gobernabilidad de la seguridad de la información y ciberseguridad

La gobernabilidad se encarga de establecer la estructura organizativa, así como los roles y responsabilidades, y los mecanismos de supervisión que son esenciales para dirigir y controlar la gestión de la seguridad de la información. Es fundamental definir un modelo de gobernanza institucional que incluya:

- Designación formal de responsables (Encargado de Seguridad de la Información y Ciberseguridad (CISO), Comité de Seguridad de la Información con los responsables locales en cada Institución o Establecimiento del sector salud).
- Integración de la seguridad en los niveles estratégicos, tácticos y operativos.
- Políticas, lineamientos e instructivos formales aprobados por la autoridad institucional.
- Mecanismos de rendición de cuentas y reporte hacia la alta dirección.
- Coordinación transversal entre áreas clínicas, administrativas, TI y jurídicas.

5.2. Roles y Responsabilidades

Bajo el Modelo de Implementación para la Seguridad de la Información y Ciberseguridad, que está alineado con un SGSI y adaptado al contexto del sector salud, es fundamental que los roles y responsabilidades estén bien definidos. Esto garantiza una ejecución efectiva, una rendición de cuentas clara y la sostenibilidad a largo plazo. A continuación, se presentan los roles principales y las responsabilidades que les corresponden:

Alta Dirección Institucional / Dirección del Establecimiento de Salud

- Aprobar formalmente la política de seguridad de la información.
- Proveer los recursos necesarios (humanos, tecnológicos, financieros) para la implementación del SGSI.
- Asumir la responsabilidad final del tratamiento de riesgos institucionales.
- Participar en la revisión de informes de impacto y presentación de riesgos críticos.
- Aprobar planes de tratamiento y priorización de iniciativas.

Encargado de Seguridad de la Información y Ciberseguridad (CISO)

- Liderar la implementación, mantenimiento y mejora del SGSI a nivel institucional.
- Coordinar el Comité de Seguridad de la Información.
- Supervisar la elaboración del análisis de riesgos, plan de tratamiento y seguimiento de controles.
- Asegurar el cumplimiento normativo y la implementación de controles alineados a marcos como ISO/IEC 27001, NIST y legislación nacional.
- Gestionar incidentes de seguridad y liderar la respuesta ante ciberataques.
- Promover la cultura de seguridad mediante capacitaciones y campañas de concientización.

Comité de Seguridad de la Información

- Instancia transversal con representación de áreas clínicas, administrativas, legales y de TI.
- Analizar riesgos institucionales desde múltiples perspectivas.
- Evaluar los planes de tratamiento propuestos y sugerir prioridades.
- Apoyar la integración de la seguridad en procesos estratégicos, operativos y clínicos.
- Monitorear el cumplimiento de políticas y procedimientos internos.

Responsables Locales de Seguridad (en cada unidad o establecimiento)

- Implementar y mantener controles de seguridad en su área de responsabilidad.
- Coordinar con el CISO el levantamiento de activos, análisis de riesgos y respuesta a incidentes.
- Sensibilizar al personal sobre las políticas y buenas prácticas de seguridad.
- Participar en auditorías internas o revisiones de cumplimiento.

Encargado de Tecnología / Jefe de Informática

- Implementar controles técnicos (firewalls, cifrado, autenticación, etc.) conforme a los lineamientos del SGSI.
- Garantizar la alta disponibilidad, respaldo y continuidad operativa de los sistemas.
- Colaborar en el levantamiento de activos tecnológicos e integración de medidas de seguridad en nuevos proyectos.
- Aplicar pruebas de seguridad sobre APIs, plataformas y redes críticas.

Usuarios Finales / Funcionarios de Salud

- Cumplir con las políticas, lineamientos y procedimientos institucionales de seguridad.
- Participar en capacitaciones obligatorias.
- Reportar oportunamente incidentes o eventos sospechosos.
- Proteger sus credenciales de acceso y manejar la información con responsabilidad.

Auditor Interno / Control Interno

- Evaluar periódicamente el nivel de cumplimiento del SGSI.
- Verificar la eficacia de los controles implementados.
- Emitir informes con hallazgos y recomendaciones a la alta dirección.
- Apoyar la preparación de evidencias para fiscalizaciones externas.

5.3. Identificación de los activos de información y su orden de criticidad.

El SGSI requiere que se elabore un Inventario de Activos de Información. La gestión de la seguridad debe comenzar identificando, clasificando y valorando los activos de información que respaldan los procesos institucionales. Esto incluye:

- Elaboración de un **Inventario de Activos de Información**, tanto digitales como físicos.
- Clasificación por criticidad (alta, media, baja) considerando el impacto en la confidencialidad, integridad, disponibilidad y trazabilidad.
- Inclusión de activos tecnológicos (sistemas HIS, servidores, dispositivos IoT, bases de datos) y activos informacionales (datos clínicos, administrativos, legales).
- Asignación de responsables por activo (custodios).
- Relación entre activos y procesos institucionales, para facilitar el análisis de riesgos.

5.4. Gestión de Riesgos.

La gestión de riesgos es un proceso metódico que se encarga de identificar, analizar, evaluar y abordar los riesgos que podrían poner en peligro la seguridad de la información dentro de una organización. Esto implica entender las amenazas y vulnerabilidades que podrían surgir, evaluar la probabilidad de que se materialicen y el impacto que podrían tener, y luego tomar decisiones bien fundamentadas sobre cómo gestionar esos riesgos.

En este sentido, la gestión de riesgos es crucial para las instituciones del sector salud por varias razones:

- **Protección de la Información del Paciente:** Se encarga de mantener la confidencialidad, integridad y disponibilidad de los datos de los pacientes, cumpliendo con las obligaciones legales y éticas necesarias.
- **Continuidad del Negocio:** Ayuda a identificar y mitigar los riesgos que podrían interrumpir los servicios esenciales, asegurando que las operaciones sigan funcionando sin contratiempos.
- **Cumplimiento Legal:** Facilita el cumplimiento de la Ley 21.663 sobre el Marco de Ciberseguridad y otras normativas relevantes, evitando así sanciones y responsabilidades legales.
- **Toma de Decisiones Informada:** Proporciona una base sólida para tomar decisiones sobre inversiones en seguridad y para asignar recursos de manera eficiente.
- **Mejora de la Resiliencia:** Refuerza la capacidad de la organización para enfrentar y recuperarse de incidentes de seguridad, minimizando daños y pérdidas.
- **Generación de Confianza:** Muestra a los pacientes, al personal y a otros interesados que la organización se toma en serio la seguridad de la información, lo que genera confianza en sus servicios.

5.4.1. Metodologías de Gestión de Riesgos en el Sector Salud

La gestión de riesgos en el sector salud es fundamental para proteger la información, asegurar la continuidad de los servicios clínicos y salvaguardar los datos personales sensibles de los pacientes. Para lograrlo, las instituciones de salud deben implementar metodologías de gestión de riesgos que estén alineadas con estándares internacionales como ISO 31000 (Gestión de Riesgos), ISO/IEC 27005 (Gestión de Riesgos en Seguridad de la Información), el Marco de Gestión de Riesgos del NIST (NIST Risk Management Framework - NIST RMF) y MAGERIT[3]. También pueden seguir las directrices establecidas por el Minsal a través de su

[3] MAGERIT: Metodología de análisis y gestión de riesgos de seguridad de los sistemas de información, desarrollada por el Consejo Superior de Administración Electrónica (CSAE) del Gobierno de España.

Política de Gestión de Riesgos de Seguridad de la Información[4], complementándolas con lo que indica la Ley N° 21.663 de Ciberseguridad de Chile.

Estas metodologías permiten identificar, analizar, evaluar y tratar de manera sistemática los riesgos que pueden afectar la confidencialidad, integridad, disponibilidad y trazabilidad de la información crítica, lo que contribuye a fortalecer la ciber resiliencia en las organizaciones de salud.

5.4.1.1. Flujo de Gestión de Riesgos

Este flujo describe de manera clara y ordenada las etapas clave para identificar, analizar, evaluar, tratar y monitorear los riesgos que pueden afectar la seguridad de la información en las instituciones de salud.
El objetivo de su implementación es reforzar la protección de los activos críticos de información, asegurar la continuidad de los servicios de atención sanitaria y garantizar el cumplimiento de la Ley N° 21.663 sobre Ciberseguridad, así como otros marcos normativos y estándares internacionales que sean relevantes.
Establecimiento del Contexto: Definir los objetivos, alcance, criterios de riesgo y la metodología a utilizar.

- Se debe establecer claramente el propósito y los límites del proceso de gestión de riesgos.
- Se deben definir los criterios para evaluar los riesgos, considerando el impacto potencial (en la atención al paciente, finanzas, reputación, etc.) y la probabilidad de ocurrencia.
- Se debe seleccionar una metodología de gestión de riesgos (ej., ISO 27005, NIST SP 800-30) y documentarla.

Identificación de Riesgos: En base al inventario de los activos de información identificar las amenazas, las vulnerabilidades que les afectad y se desarrollan escenarios de riesgo.

- En base al inventario de los activos de información (datos de pacientes, sistemas, dispositivos, etc.) y clasificarlos según su criticidad.
- Se deben identificar las amenazas relevantes para el sector salud (ej., ransomware, robo de datos) y las vulnerabilidades que podrían ser explotadas.
- Se deben desarrollar escenarios de riesgo que describan cómo las amenazas podrían afectar a los activos.

Análisis de Riesgos: Evaluar el impacto y la probabilidad de los riesgos, y se determina el nivel de riesgo.

- Se debe evaluar el daño potencial que cada riesgo podría causar a la organización y la probabilidad de que ocurra.
- Se debe combinar la evaluación del impacto y la probabilidad para determinar el nivel de riesgo (ej., alto, medio, bajo).

DEPARTAMENTO TIC VISADO

[4] https://www.minsal.cl/seguridad_de_la_informacion/

Evaluación de Riesgos: Comparar los niveles de riesgo con los criterios de aceptación y se priorizan los riesgos.

- Se debe determinar si los niveles de riesgo son aceptables o si requieren tratamiento.
- Se deben priorizar los riesgos para su tratamiento, enfocándose en los de mayor impacto y probabilidad.

Tratamiento de Riesgos: Se debe elaborar e implementar un Plan de Tratamiento de los riesgos que detalle las acciones, responsables, plazos y recursos

- Desarrollar un Plan de Tratamiento que detalle las acciones, responsables, plazos y recursos.
- Seleccionar e implementar controles para mitigar o reducir los riesgos a un nivel aceptable, como implementar controles de seguridad, transferir el riesgo a un seguro, evitar la actividad riesgosa.
- Identificar los riesgos respecto de los que procede transferir (por ejemplo, contratando un seguro) o aceptar los riesgos.

Monitoreo y Revisión: Se debe revisar el proceso de gestión de riesgos y medir la efectividad de los controles en relación con los objetivos de tratamiento de los riesgos.

- Se debe realizar un seguimiento continuo de los riesgos y la implementación de los controles.
- Se debe revisar periódicamente el proceso de gestión de riesgos para asegurar su eficacia y realizar mejoras.

Un ejemplo de Matriz de Riesgos de Seguridad de la Información en el Sector Salud en Anexo punto N° 21.4.

5.4.2. Plan de Tratamiento

Como resultado del análisis de riesgos, es fundamental crear un Plan de Tratamiento formal que defina de manera clara las acciones que se llevarán a cabo para reducir los riesgos a niveles aceptables. Este plan debe incluir:

- Actividades concretas y responsables designados para su ejecución.
- Justificación técnica y normativa de cada medida adoptada (por ejemplo, controles técnicos, procedimientos, cambios de configuración).
- Calendario de implementación con fechas claras para cada acción, y recursos asignados para su cumplimiento.
- Criterios de validación o cierre de cada actividad.

El Plan de Tratamiento necesita la aprobación de la autoridad correspondiente y debe ser monitoreado periódicamente por el Comité de Seguridad de la Información.

5.4.3. Informe de Impacto y Presentación Directiva

Para garantizar una gestión efectiva del riesgo, es fundamental elaborar un Informe de Impacto que reúna los hallazgos más importantes del análisis de riesgos, identificando de manera clara:

- Riesgos que afectan la continuidad de operación clínica y administrativa.
- Vulnerabilidades de mayor impacto en sistemas críticos (HIS, bases de datos, redes internas, etc.).
- Potenciales consecuencias a la ciudadanía, legales, operativas y reputacionales.

Este informe debe ser presentado a la dirección del establecimiento de salud o institución a través de una Presentación Directiva. Esto facilitará la comprensión de los riesgos, promoverá decisiones informadas y fortalecerá la rendición de cuentas en lo que respecta a la seguridad de la información.

La retroalimentación recibida en esta presentación debe ser parte del proceso de mejora del SGSI. Esto ayudará a fortalecer la conexión entre la seguridad de la información y los objetivos de la institución.

5.4.4. Mejora continua.

El modelo debe incorporar un enfoque de mejora continua (ciclo PDCA: Planificar – Hacer – Verificar – Actuar), tal como lo establece la ISO 27001:

- Revisión periódica de políticas y controles.
- Evaluaciones de madurez y auditorías regulares.
- Actualización de análisis de riesgos.
- Reforzamiento de capacidades institucionales a través de formación y sensibilización.
- Retroalimentación a partir de incidentes, brechas o hallazgos detectados.

5.5. Política General, Específicas y Procedimientos

De acuerdo con la estructura de gobernanza en ciberseguridad que se ha establecido, cada institución del Sector Salud tiene la responsabilidad de elaborar, formalizar, implementar y mantener una Política General de Seguridad de la Información y Ciberseguridad. Esta política servirá como el marco rector de alto nivel, definiendo las directrices estratégicas y los principios fundamentales para la protección integral y efectiva de todos los activos de información institucionales, asegurando la confidencialidad, integridad y disponibilidad de sus sistemas y datos.

La Política General es una declaración formal del compromiso de la Dirección con la seguridad de la información y la ciberseguridad, estableciendo una postura proactiva para garantizar la continuidad operativa, el desarrollo seguro de servicios digitales y la mejora continua en la atención a los usuarios. Este documento estratégico debe ser redactado de manera clara,

utilizando un lenguaje accesible para todos los niveles de la organización, y debe estar completamente alineado con las leyes, decretos y estándares nacionales e internacionales vigentes.

Una vez aprobada y ampliamente difundida esta Política General entre todo el personal, la institución deberá avanzar en el desarrollo e implementación de dos niveles de instrumentos normativos complementarios que permitan llevar a la práctica las directrices estratégicas.

5.5.1. Políticas Específicas

Estas políticas abordarán áreas críticas y específicas de la seguridad de la información, proporcionando lineamientos detallados para la gestión de:

- Accesos físicos y lógicos a los activos de información.
- Relaciones con terceros y la gestión de la seguridad en la cadena de suministro.
- Continuidad operativa, incluyendo los procesos de respaldo, recuperación ante desastres y continuidad del negocio.
- Clasificación, etiquetado y manejo seguro de la información según su nivel de sensibilidad.
- Seguridad de los activos de hardware y software.
- Comunicaciones seguras y protección contra malware.
- Gestión de incidentes de seguridad.
- Cumplimiento normativo específico (ej. protección de datos personales, seguridad de la información de salud).
- Uso aceptable de los recursos informáticos.
- Seguridad en el desarrollo de software. Estas políticas específicas permitirán un tratamiento más granular de los diversos escenarios operativos y los riesgos particulares asociados a cada ámbito.

5.5.2. Procedimientos e Instructivos Operacionales

Es crucial que las instituciones del Sector Salud establezcan y mantengan un conjunto normativo interno sólido, que se actualice periódicamente y que sea de cumplimiento obligatorio para todo el personal.

Los procedimientos e instructivos operacionales describirán de manera clara y detallada las etapas de cada proceso, los roles y responsabilidades asignadas en cada fase, los flujos de trabajo, además de los mecanismos técnicos y administrativos necesarios para implementar de manera efectiva los controles de seguridad establecidos en la Política General y en las Políticas Específicas.

Su elaboración debe alinearse estrictamente con las mejores prácticas y estándares reconocidos tanto a nivel nacional como internacional, como ISO/IEC 27001, las directrices del NIST, los Controles CIS y las normativas nacionales relevantes (Ley N° 21.663 sobre Ciberseguridad y Ley N° 19.628 sobre Protección de la Vida Privada).

Para asegurar que estos instrumentos normativos estén bien estructurados y sean coherentes, se ofrece un modelo con los componentes mínimos requeridos en el Anexo, punto 21.5.

Su utilización se considera una buena práctica recomendada.

Este marco normativo necesita estar respaldado por una estructura de gobernanza en ciberseguridad que sea efectiva, así como por un Comité de Seguridad de la Información y Ciberseguridad que tenga la autoridad y la responsabilidad de asegurar su cumplimiento. La correcta implementación y el estricto seguimiento de estos instrumentos van a fortalecer de manera significativa la resiliencia de la organización frente a las amenazas cibernéticas, permitiendo anticipar y mitigar proactivamente los riesgos, además de contribuir directamente a la mejora continua de los servicios y a la consolidación de la confianza de la ciudadanía.

En el marco de la gestión de la seguridad de la información, se recomienda contar, al menos, con procedimientos documentados para los siguientes procesos críticos:

- Procedimiento de gestión de ficha clínica electrónica y en papel.
- Procedimiento de gestión de agendas y programación de atenciones.
- Procedimiento de gestión y control de inventarios de activos tecnológicos y clínicos.
- Procedimiento de gestión de respaldos y recuperación ante desastres.
- Procedimiento de control de accesos físicos y lógicos.
- Procedimiento de tratamiento de incidentes de seguridad de la información.
- Procedimiento de alta, modificación y baja de usuarios.
- Procedimiento de entrega de información a terceros (por ejemplo, por solicitudes judiciales, auditorías, etc.).

En aquellos casos en que no sea posible documentar todos los procedimientos operativos, se recomienda priorizar según los siguientes criterios:

- Procesos que involucren el tratamiento de datos personales o sensibles de salud.
- Procesos que afecten la continuidad operativa del establecimiento.
- Procesos que incluyan el uso de sistemas informáticos críticos (HIS, RIS, PACS, sistemas de laboratorio, etc.).
- Procesos donde intervengan múltiples unidades y/o actores externos.
- Procesos que hayan sido objeto de incidentes, hallazgos de auditoría o vulnerabilidades anteriores.

6. DIRECTRICES PARA UNA ARQUITECTURA DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Con el fin de reforzar la ciberseguridad en el sector salud, se requiere que cada institución de este ámbito adopte e implemente de manera proactiva un **Modelo de Seguridad por Capas o Defensa en Profundidad (DiD)**, que garantice una defensa en profundidad, integrando

diversos controles técnicos, físicos y administrativos en todos los niveles de la infraestructura tecnológica.

Esta estrategia, que es tanto integral como estructurada, implica la aplicación de diversos controles de seguridad, administrativos, físicos y técnicos, que resultan fundamentales para proteger de manera efectiva activos críticos como información sensible, sistemas operativos e infraestructura tecnológica. La flexibilidad del modelo permite una implementación efectiva y adaptada a las necesidades específicas de cada institución en el sector.

Este modelo se basa en el principio de seguridad y privacidad por defecto y desde el diseño, tal como se establece en la Ley 21.663 sobre el Marco de Ciberseguridad, la ley N° 19.628, de protección de la vida privada y la ley N° 20.584 de Derechos y Deberes de los Pacientes.

Como resultado de lo anterior, todos los sistemas informáticos, aplicaciones y tecnologías de la información deben ser concebidos, implementados y gestionados con la seguridad y la privacidad de los datos como pilares fundamentales desde el principio. Al integrar la seguridad y la privacidad en cada fase del ciclo de vida de los sistemas, se garantiza una protección más sólida y proactiva, lo que complementa la estrategia de defensa en profundidad que caracteriza al Modelo de Seguridad por Capas.

Esta estrategia es crucial en el sector de la salud, donde es fundamental garantizar en todo momento la confidencialidad, integridad y disponibilidad de los datos clínicos y operacionales. Implementar múltiples niveles de defensa de manera adecuada ayuda a fortalecer la resiliencia digital frente a amenazas tanto internas como externas, además de facilitar el cumplimiento de las normativas nacionales e internacionales relacionadas con la ciberseguridad y la protección de datos personales.

6.1. Capas de Seguridad en Entornos de Salud

A continuación, se presentan los controles prioritarios para reforzar la ciberseguridad en el sector salud de manera escalonada:

6.1.1. Capa de Seguridad Física

Implemente controles de acceso físico sólidos para limitar el acceso a las instalaciones, centros de datos, salas de servidores críticos y otras áreas sensibles, permitiéndolo solo al personal que esté debidamente autorizado.

Esto debe incluir, al menos:

- Sistemas de control de acceso biométrico y tarjetas inteligentes: Utilizar el uso de lectores biométricos (huella, iris) y tarjetas RFID personalizadas para permitir acceso solo a personal autorizado.
- Videovigilancia perimetral y en zonas críticas (CCTV) con grabación y monitoreo, integrado con sistemas de analítica de video y alertas.
- Zonificación física y separación de áreas: Establecer zonas de seguridad diferenciadas con niveles de acceso específicos. Implementación de barreras físicas, jaulas de racks y

salas blancas para infraestructura TI. Implementar sistemas de detección de intrusos (IDS) físicos para alertar sobre accesos no autorizados

- Sensores ambientales: Controlar las condiciones ambientales (temperatura, humedad) y la alimentación eléctrica (SAI/UPS, generadores de respaldo) para garantizar la disponibilidad. Detectores de humo, humedad, temperatura y fallos eléctricos conectados a sistemas de gestión de instalaciones (BMS).

6.1.2. Capa de Seguridad de Red

Implemente mecanismos sólidos para controlar el tráfico de red, con el fin de evitar accesos no autorizados a los sistemas y datos de la institución. Además, segmente la red de manera lógica y/o física para limitar la propagación de incidentes de seguridad en caso de que se presenten. Esto debe incluir:

- Firewalls de última generación (NGFW): Implemente y configure firewalls de última generación entre la red institucional y las redes externas, utilizando inspección profunda de paquetes (DPI), filtrado por aplicación y geo-bloqueo. Configure listas blancas y negras de direcciones IP y puertos para permitir el tráfico necesario y bloquear fuentes de amenazas conocidas. Active mecanismos de protección contra amenazas avanzadas, como el análisis de tráfico cifrado (inspección SSL/TLS), prevención de intrusiones (IPS) y sandboxing para detectar malware desconocido.
- IDS/IPS: Implemente sistemas IDS/IPS para monitorear el tráfico de red en busca de actividades sospechosas o maliciosas, bloqueando o alertando sobre posibles intrusiones.
- Listas de Control de Acceso (ACLs): Utilice ACLs en enrutadores y switches para controlar el tráfico a nivel de dirección IP y puerto, restringiendo las comunicaciones entre segmentos de red según sea necesario.
- Segmentación de Red: Implemente la segmentación de la red utilizando VLANs, subredes o arquitecturas de Zero Trust para aislar sistemas críticos y limitar el movimiento lateral de posibles atacantes. Use microsegmentación para aislar sistemas críticos, redes clínicas, administrativas, IoT y visitantes.
- VPNs seguras: Utilice cifrado IPsec o SSL, autenticación robusta y túneles cifrados por usuario o dispositivo para asegurar las comunicaciones a través de redes no confiables.
- Políticas de Filtrado de Contenido: Implemente políticas de filtrado de contenido web y de correo electrónico para prevenir el acceso a sitios maliciosos y la descarga de archivos peligrosos.
- Monitoreo del Tráfico de Red: Establezca un sistema de monitoreo continuo del tráfico de red para detectar anomalías, patrones sospechosos y posibles incidentes de seguridad en tiempo real.

6.1.3. Capa de Seguridad del Perímetro

Implemente una capa de seguridad perimetral que controle y proteja de manera rigurosa todos los puntos de entrada a la red institucional, ya sea desde Internet o cualquier otra red externa. Esta capa de seguridad debe incluir:

- Firewalls de Aplicación Web (WAF): Implemente WAF para proteger nuestras aplicaciones web de amenazas como inyecciones SQL y cross-site scripting (XSS).
- Protección contra DDoS (Distributed Denial of Service): Utilice sistemas dedicados o servicios en la nube que ayuden a mitigar ataques de denegación de servicio distribuidos.
- Filtrado de Contenido Web: Implemente soluciones de filtrado de contenido web para bloquear el acceso a sitios maliciosos conocidos, categorías de contenido inapropiadas o cualquier sitio que pueda poner en riesgo la seguridad de la institución.
- Gestión de Amenazas Unificada (UTM): Considere la implementación de soluciones UTM que integren diversas funciones de seguridad perimetral (como firewall, IPS, antivirus de gateway, filtrado web, etc.) para una gestión centralizada y una protección más efectiva.
- Políticas de Acceso Remoto Seguro: Defina e implemente políticas estrictas para el acceso remoto a la red institucional (por ejemplo, a través de VPNs con autenticación fuerte y cifrado), controlando quién puede acceder y desde dónde.
- Monitoreo y Alertas: Establece un sistema de monitoreo y alertas. Intégrelos con un SIEM.

6.1.4. Capa de Aplicación:

Desarrolle y configure todas las aplicaciones institucionales de manera segura, implementando medidas proactivas para prevenir vulnerabilidades y proteger los datos que procesan. Esto implica adoptar las siguientes prácticas obligatorias:

- Ciclo de Vida de Desarrollo de Software Seguro (SSDLC): Se debe implementar un SSDLC que incluya medidas de seguridad a nivel de aplicaciones, como autenticación, autorización y pruebas de seguridad, para salvaguardar la integridad y confidencialidad de los datos. Adoptar estándares de desarrollo seguro reconocidos, como los que propone OWASP o NIST, y aplicar marcos de trabajo como el SSDLC es una excelente práctica.
- Validación de Entradas: Implemente mecanismos sólidos para validar todas las entradas de usuario y así prevenir ataques de inyección, como SQL Injection, XSS (Cross-Site Scripting) y CSRF (Cross-Site Request Forgery). Al realizar consultas a bases de datos, es recomendable utilizar procedimientos almacenados y consultas preparadas para evitar inyecciones SQL. Además, es importante emplear librerías y frameworks de terceros que sean confiables y que integren mecanismos de seguridad robustos.
- Codificación Segura: Adopte prácticas que sigan guías y estándares reconocidos, como el OWASP Top Ten, para evitar vulnerabilidades comunes en el software.
- Control de Acceso a la Aplicación: Implemente mecanismos de autenticación y autorización sólidos, basados en roles, ayudará a gestionar quién puede acceder a las funcionalidades y datos dentro de la aplicación.
- Gestión Segura de Sesiones: Asegúrese de que las sesiones de usuario se manejen de manera segura, generando identificadores de sesión robustos, protegiendo contra el secuestro de sesiones y asegurando la invalidación adecuada al cerrar la sesión.

- Realizar pruebas de penetración (pentesting) específicas para las aplicaciones y realización de análisis de seguridad estáticos (SAST) y dinámicos (DAST).
- Manejo Seguro de Errores y Excepciones: Configure las aplicaciones para manejar errores y excepciones de forma segura, evitando la divulgación de información sensible o detalles internos del sistema.
- Utilizar cifrado para datos sensibles dentro de la aplicación. Implemente cifrado para proteger los datos sensibles dentro de la aplicación. También es importante implementar registros de auditoría detallados que registren la actividad de la aplicación (logs).
- Protección de Datos Sensibles: Implemente medidas de seguridad para los datos sensibles que maneja la aplicación. Esto incluye cifrado tanto en tránsito como en reposo, así como la anonimización o seudonimización cuando sea necesario, y el enmascaramiento de datos en entornos que no son de producción.
- Gestión segura de APIs: Las APIs, tanto internas como externas, deben ser desarrolladas siguiendo principios de seguridad desde el diseño, implementando autenticación robusta (como OAuth 2.0), autorización granular, cifrado TLS 1.2 o superior y protecciones contra las vulnerabilidades más comunes que se encuentran en el OWASP API Top 10. Además, es esencial incluir la validación de entradas, limitar las tasas de consumo, mantener una trazabilidad completa de los accesos y contar con documentación actualizada.
- Para la exposición de los servicios API REST: Utilice mecanismos de autenticación para su uso privado, ya sea mediante tokens (como JWT u otros), certificados, llaves criptográficas, o cualquier otro método de autenticación cuya efectividad se haya comprobado por métodos fiables entre puntos.

6.1.5. Capa de Seguridad de los Datos

Implemente medidas de seguridad sólidas para salvaguardar la información, tanto cuando está almacenada en los sistemas como cuando se está utilizando, protegiéndola de accesos no autorizados, modificaciones inapropiadas o eliminaciones accidentales o maliciosas. Esto significa seguir las siguientes directrices obligatorias:

- Autenticación Fuerte: Utilice mecanismos de autenticación robustos (incluyendo la Autenticación Multifactor - MFA cuando sea posible) para verificar la identidad de los usuarios antes de permitir el acceso a los datos.
- Cifrado de Datos en Reposo: Cifre la información sensible almacenada en bases de datos, servidores, dispositivos de almacenamiento y cualquier otro medio utilizando algoritmos de cifrado fuertes y estándares reconocidos por la industria como AES-256. Además de implementar una gestión de claves criptográficas segura.
- Cifrado de Datos en Tránsito: Asegure la protección de la información sensible durante su transmisión a través de redes internas y externas mediante el uso de protocolos de cifrado seguros TLS 1.2 o superior para datos en tránsito.
- Firmas Digitales: Utilice firmas digitales basadas en criptografía de clave pública, en atención a que esta tecnología permite verificar la autenticidad e integridad de los datos y documentos, asegurando el no repudio. Tenga en cuenta que, tratándose de instrumentos públicos, éstos deben ser firmados con Firma Electrónica Avanzada.

- Prevención de Pérdida de Datos (DLP): Implemente herramientas y políticas de DLP para monitorear y controlar el movimiento de información sensible, previniendo su fuga o extracción no autorizada.
- Anonimización y Seudonimización: Cuando sea apropiado y legalmente permitido, aplique técnicas de anonimización o seudonimización a los datos sensibles para reducir el riesgo de identificación directa.
- Políticas de Retención y Eliminación Segura de Datos: Defina e implemente políticas claras para la retención de datos según los requisitos legales y del negocio, y establezca procedimientos seguros para la eliminación de datos que ya no sean necesarios, evitando su recuperación no autorizada.
- Auditoría de Acceso a Datos: Implemente un sistema de auditoría que registre los accesos, las modificaciones y las eliminaciones de datos sensibles, permitiendo el seguimiento y la detección de actividades sospechosas. Clasificación y etiquetado de la información: Uso de etiquetas automatizadas y manuales para categorizar y aplicar políticas.
- Autenticación: Verificar la identidad de los usuarios antes de otorgar acceso a sistemas y datos. Utilizando mecanismos robustos como autenticación multifactor (MFA), uso de contraseñas complejas y políticas de rotación, e idealmente, autenticación basada en certificados o biometría. Técnicamente, se deben implementar protocolos seguros como OAuth 2.0 y SAML 2.0 para la autenticación y federación de identidades.
- Autorización: Definir qué recursos y datos pueden acceder los usuarios autorizados, mediante la implementación de listas de control de acceso (ACLs, RBAC y ABAC) aplicadas consistentemente en la capa de aplicación y la infraestructura.
- DLP (Data Loss Prevention): Prevención de fuga de datos vía correo, USB, impresión o nube.
- Sistemas de respaldo automatizados: Realizar copias de seguridad (backups) periódicas y seguras de los datos, con almacenamiento local y en la nube, pruebas regulares de recuperación (DRP - Plan de Recuperación ante Desastres / BIA - Análisis de Impacto al Negocio).

6.1.6. Capa de Seguridad de Dispositivos y Endpoints

Implemente medidas de seguridad integrales para proteger todos los dispositivos de los usuarios finales, como estaciones de trabajo, portátiles, dispositivos móviles y tablets, que acceden a los recursos de la Institución. Esta protección debe incluir los siguientes aspectos obligatorios:

- Implementación de Antimalware Avanzado: Instale y mantenga actualizado software antimalware robusto en todos los endpoints, con capacidades de detección en tiempo real, análisis heurístico y protección contra amenazas emergentes (virus, spyware, ransomware, etc.). Se recomienda el uso de tecnologías de protección avanzada (NGAV), que incorporen detección basada en comportamiento y análisis heurístico para anticipar nuevas variantes de malware.
- EDR (Endpoint Detection and Response) / XDR (Extended Detection and Response): Se deberá implementar una solución de EDR, que permita el monitoreo continuo de la actividad en los endpoints, la detección temprana de amenazas y una respuesta

DEPARTAMENTO TIC VISADO

automatizada ante incidentes. Para entornos más complejos, se sugiere la adopción de plataformas XDR, que correlacionen eventos entre múltiples vectores como red, correo electrónico y nube. Estas soluciones deben integrarse con el sistema de gestión de eventos e información de seguridad (SIEM) institucional.

- Firewall Personal: Active y configure correctamente firewalls personales en todos los dispositivos para controlar el tráfico de red entrante y saliente a nivel del endpoint.
- Gestión Centralizada de Dispositivos Móviles (MDM/UEM): Implemente una solución de Gestión de Dispositivos Móviles (MDM) o Gestión Unificada de Endpoints (UEM) para aplicar políticas de seguridad, gestionar la configuración, realizar inventario, controlar el acceso a aplicaciones y datos, y habilitar el borrado remoto en caso de pérdida o robo de dispositivos móviles.
- Control de Acceso al Dispositivo: Exija el uso de mecanismos de autenticación fuertes (contraseñas complejas, PINs, biometría) para acceder a los dispositivos y configure el bloqueo automático por inactividad.
- Cifrado de Disco Completo: Implemente el cifrado de disco completo en los portátiles y otros dispositivos que puedan contener información sensible y puedan ser extraviados o robados.
- Gestión de Parches y Actualizaciones: Establezca un proceso centralizado y automatizado para la aplicación oportuna de parches de seguridad del sistema operativo, las aplicaciones y el firmware de los dispositivos.
- Control de Aplicaciones: Implemente políticas para controlar la instalación y ejecución de aplicaciones en los dispositivos, permitiendo solo software autorizado y bloqueando aplicaciones potencialmente riesgosas.
- Prevención de Pérdida de Datos (DLP) en el Endpoint: Considere la implementación de soluciones DLP en los endpoints para monitorear y controlar la transferencia de información sensible, previniendo su fuga accidental o intencional.
- Control de dispositivos extraíbles: Es obligatorio establecer políticas de control sobre el uso de dispositivos extraíbles, como unidades USB. Estas políticas deben restringir el uso de medios no autorizados, registrar los eventos de conexión y exigir cifrado en los dispositivos permitidos. Además, los puertos USB deben ser deshabilitados por defecto, salvo cuando exista una justificación funcional documentada.
- Para los dispositivos móviles institucionales o personales autorizados (BYOD), se debe implementar una solución de gestión centralizada como MDM (Mobile Device Management) o UEM (Unified Endpoint Management). Estas plataformas deben permitir aplicar políticas de seguridad como el cifrado de datos, la autenticación reforzada, la instalación controlada de aplicaciones y el borrado remoto en caso de pérdida o robo.
- Políticas de Uso Seguro de Dispositivos: Defina y comunique claramente las políticas de uso seguro de los dispositivos, incluyendo las restricciones sobre la instalación de software no autorizado, la conexión a redes no seguras y el almacenamiento de información sensible en dispositivos personales no gestionados.

6.1.7. Capa de Seguridad Operacional y de Monitoreo

Implemente un conjunto de acciones y herramientas que permitan detectar, responder y contener amenazas de seguridad de manera oportuna. Esta capa de seguridad operativa y de monitoreo debe incluir los siguientes elementos esenciales:

- Implementación de un Centro de Operaciones de Seguridad (SOC) o Funciones Equivalentes: Establezca un equipo o funciones dedicadas para el monitoreo continuo de la seguridad, el análisis de alertas y la gestión de incidentes.
- Sistemas de Gestión de Eventos e Información de Seguridad (SIEM): Implemente un SIEM para la recopilación, correlación y análisis de logs de seguridad de diversas fuentes (firewalls, IDS/IPS, servidores, endpoints, aplicaciones, etc.) con el fin de detectar actividades sospechosas y posibles incidentes en tiempo real.
- Monitoreo Continuo de la Infraestructura: Establezca un monitoreo constante de la salud, el rendimiento y la seguridad de la infraestructura tecnológica, incluyendo la red, los servidores, las aplicaciones y las bases de datos.
- Alertas y Notificaciones en Tiempo Real: Configure sistemas de alerta para notificar de manera inmediata al personal de seguridad sobre eventos sospechosos o incidentes detectados.
- Procesos de Gestión de Incidentes Definidos: Desarrolle e implemente procedimientos claros y documentados para la identificación, análisis, contención, erradicación, recuperación y lecciones aprendidas de los incidentes de seguridad.
- Equipos de Respuesta a Incidentes (IRT): Designe y capacite equipos de respuesta a incidentes con roles y responsabilidades definidos para actuar con rapidez y eficacia ante las amenazas.
- Inteligencia de Amenazas (Threat Intelligence): Integre fuentes de inteligencia de amenazas en los procesos de monitoreo y análisis para comprender mejor el panorama de amenazas y anticipar posibles ataques.
- Análisis Forense: Desarrolle capacidades de análisis forense para investigar incidentes de seguridad, identificar sus causas raíz, determinar el alcance del daño y recopilar evidencia para acciones futuras.
- Ejercicios y Simulacros de Respuesta a Incidentes: Realice simulacros periódicos de respuesta a incidentes para probar la efectividad de los procedimientos y la preparación del personal.
- Comunicación de Incidentes: Establezca protocolos claros para la comunicación de incidentes de seguridad a las partes interesadas relevantes, incluyendo la alta dirección y, según la normativa, la Agencia Nacional de Ciberseguridad (ANCI).
- Inteligencia de amenazas TI / CTI (Threat Intelligence / Cyber Threat Intelligence): Información contextualizada para anticiparse a campañas y vectores emergentes.
- Pruebas de seguridad: Evaluaciones periódicas de vulnerabilidades, realizar pruebas de penetración (pentesting), análisis de vulnerabilidades automatizados, revisiones de seguridad del código fuente (SAST/DAST), auditorías y simulacros de incidentes.

6.1.8. Capa de Seguridad en la Nube

Para las instituciones del sector salud que utilicen o que están pensando en usar servicios en la nube (como IaaS, PaaS o SaaS), es fundamental incorporar una Capa de Seguridad en la Nube dentro de su Modelo de Defensa en Profundidad. Esta capa se centra en los controles y servicios específicos que son necesarios para salvaguardar los activos, aplicaciones y datos que se encuentran en estos entornos, teniendo en cuenta el modelo de responsabilidad compartida con el proveedor de la nube.

En este contexto, las instituciones del sector salud tendrán que implementar controles de seguridad sólidos y específicos para reducir los riesgos que conlleva el uso de servicios en la nube. Esto es crucial para garantizar la confidencialidad, integridad y disponibilidad de la información en este ámbito.

- Gestión de Identidades y Accesos en la Nube (IAM): Para asegurar un acceso seguro y controlado a los recursos de la nube, configure y gestione de manera centralizada las identidades de usuarios, la agrupación en roles y los permisos de acceso utilizando los servicios de IAM provistos por su proveedor de nube, tales como AWS IAM, Azure Active Directory o Google Cloud IAM. Es fundamental aplicar rigurosamente el principio de mínimo privilegio, asignando a cada usuario o servicio únicamente los permisos estrictamente necesarios para llevar a cabo sus funciones específicas. Adicionalmente, implemente la Autenticación Multifactor (MFA) de forma obligatoria para todas las cuentas que tengan acceso a recursos sensibles o con privilegios elevados en su entorno de nube, añadiendo una capa adicional de seguridad.
- Gestión de la Postura de Seguridad en la Nube (CSPM): Despliegue e integre herramientas y servicios de Gestión de la Postura de Seguridad en la Nube (CSPM) para establecer un monitoreo continuo de la configuración de todos sus recursos en la nube. Configure estas soluciones para que identifiquen y generen alertas automáticas ante configuraciones inseguras, vulnerabilidades conocidas y cualquier desviación de las mejores prácticas de seguridad y los estándares de cumplimiento normativo aplicables al sector salud en Chile. Es crucial establecer flujos de trabajo claros y asignar responsabilidades para la revisión y la ejecución oportuna de acciones de remediación para cualquier alerta generada por el sistema CSPM, manteniendo así una postura de seguridad sólida.
- Seguridad de la Red en la Nube: Defina, configure y gestione sus Redes Privadas Virtuales (VPC/VNet), subredes lógicas y firewalls virtuales (Grupos de Seguridad, Listas de Control de Acceso) utilizando las funcionalidades que ofrece su proveedor de servicios en la nube para establecer un perímetro de red seguro en el entorno cloud. Implemente una segmentación lógica robusta de sus cargas de trabajo en la nube mediante la creación de subredes aisladas y aplique reglas de firewall estrictas para controlar el flujo de tráfico permitido entre estos recursos, basándose en el principio de necesidad. Para la conectividad híbrida con su infraestructura local, en caso de ser requerida, establezca conexiones seguras y cifradas utilizando Redes Privadas Virtuales (VPN) o conexiones directas (Direct Connect u otras soluciones equivalentes) para proteger la comunicación.
- Protección de Datos en la Nube: Implemente el cifrado robusto de los datos sensibles en reposo utilizando los servicios de cifrado que proporciona su proveedor de nube, como

AWS KMS, Azure Key Vault o Google Cloud KMS, asegurándose de gestionar las claves de cifrado de forma segura y conforme a las mejores prácticas. Asimismo, asegúrese de que todos los datos que se transmiten hacia y desde su entorno de nube estén protegidos mediante protocolos de cifrado fuertes, como TLS/SSL versión 1.2 o superior, para garantizar la confidencialidad durante la transferencia. Es fundamental definir e implementar políticas de retención y eliminación de datos que cumplan estrictamente con las regulaciones y leyes de protección de datos del sector salud en Chile, incluyendo la Ley N° 19.628 y otras normativas aplicables. Considere también la implementación de servicios de Prevención de Pérdida de Datos (DLP), ya sean nativos de la nube o de terceros, para monitorear y prevenir la fuga de información sensible fuera de su entorno controlado en la nube, fortaleciendo la protección de la información crítica.

- Monitorización y Registro en la Nube: Active y configure de manera exhaustiva los servicios de registro (logging) y monitorización que ofrece su proveedor de nube, como AWS CloudWatch, Azure Monitor o Google Cloud Logging, para obtener visibilidad sobre la actividad en su entorno. Establezca mecanismos para el análisis continuo de estos registros con el fin de detectar actividades inusuales o potencialmente maliciosas, identificar posibles incidentes de seguridad en etapas tempranas y facilitar el análisis forense detallado en caso de incidentes confirmados. Para una gestión de seguridad centralizada, integre los registros de seguridad de la nube con su Sistema de Gestión de Eventos e Información de Seguridad (SIEM) centralizado, si su institución dispone de uno, permitiendo una correlación y análisis más eficientes de los eventos de seguridad.
- Seguridad de Cargas de Trabajo en la Nube (Instancias, Contenedores, Funciones): Implemente medidas de seguridad específicas y adaptadas al tipo de carga de trabajo que se ejecute en la nube para proteger cada componente de su infraestructura cloud. Para instancias virtuales, aplique el endurecimiento de los sistemas operativos mediante la eliminación de servicios innecesarios y la configuración de parámetros de seguridad robustos, y utilice software de seguridad de endpoints (EDR/XDR) optimizado para entornos de nube para la detección y respuesta a amenazas. En el caso de contenedores, asegure el ciclo de vida de las imágenes mediante el escaneo de vulnerabilidades, configure políticas de seguridad a nivel de orquestación (como Kubernetes) y gestione los clústeres de forma segura. Para arquitecturas basadas en Funciones como Servicio (FaaS), siga las mejores prácticas de desarrollo seguro (SDLC seguro) y aplique una gestión de permisos granular para las funciones, adhiriéndose estrictamente al principio de mínimo privilegio para limitar el impacto potencial de cualquier vulnerabilidad.
- Cumplimiento y Gobernanza en la Nube: Implemente políticas y controles específicos diseñados para asegurar el cumplimiento de las normativas del sector salud en Chile, como la Ley N° 21.663 y la Ley N° 19.628, así como otras regulaciones internacionales relevantes que puedan aplicar a su institución (por ejemplo, HIPAA si maneja datos de pacientes internacionales). Realice auditorías periódicas de la configuración de su entorno de nube, tanto internas como externas, para verificar el cumplimiento continuo de estas políticas y regulaciones, generando informes de cumplimiento detallados para la documentación y la toma de decisiones. Utilice las herramientas de cumplimiento y gobernanza que ofrece su proveedor de nube para automatizar la monitorización del cumplimiento y facilitar la generación de informes, optimizando así el proceso de aseguramiento del cumplimiento normativo.

- Consideraciones Adicionales:
  - Modelo de Responsabilidad Compartida: Es fundamental que comprenda cuáles son las responsabilidades de seguridad de su institución y cuáles son las del proveedor de la nube.
  - Selección del Proveedor: Asegúrese de elegir proveedores de nube que cumplan con los estándares de seguridad y las regulaciones específicas del sector salud.
  - Evaluación Continua: Realice evaluaciones de seguridad de manera regular en su entorno de nube para poder identificar y mitigar nuevas amenazas y vulnerabilidades.

6.1.9. Tabla de cumplimiento por capas (ejemplo)

Capa de Seguridad	Objetivo Principal	Controles Claves	Referencias de Cumplimiento
Seguridad Física	Restringir acceso físico a instalaciones y áreas críticas.	Control biométrico y tarjetas inteligentes; CCTV y analítica de video; Zonificación y barreras físicas; Sensores ambientales, SAI/UPS	ISO 27001 A.11; NIST SP 800-53 PE; HIPAA §164.310; Ley 21.663 Art. 5; Ley 19.628 (disponibilidad)
Seguridad de Red	Prevenir accesos no autorizados y segmentar la red.	NGFW, filtrado de paquetes; IDS/IPS; VLANs y microsegmentación; VPN seguras	ISO 27001 A.13; NIST SP 800-53 SC; HIPAA §164.312(e); Ley 21.663 Art. 7; Ley 19.628 (confidencialidad)
Seguridad del Perímetro	Proteger los puntos de entrada a la red institucional.	WAF; Protección DDoS; Proxy inversos; Gateway remoto seguro	ISO 27001 A.13; NIST SP 800-53 SC-5; HIPAA §164.312(b); Ley 21.663 Art. 7; OWASP Top 10
Seguridad en la Aplicación	Desarrollar y mantener aplicaciones seguras.	SSDLC, OWASP/NIST; SAST/DAST, pentesting; Gestión segura de APIs (OAuth2, TLS 1.2+); Controles en frontend (XSS, CSRF, validación, HTTPS)	ISO 27001 A.14; NIST SP 800-218 (SSDF); HIPAA §164.312(c); Ley 21.663 Art. 8; Ley 19.628 Art. 4
Seguridad de los Datos	Proteger la información en reposo y en tránsito.	Cifrado AES-256, TLS 1.2+; Firmas digitales; Clasificación de datos; MFA, OAuth2, SAML; DLP, backups seguros	ISO 27001 A.8, A.10, A.18; NIST SP 800-57/111/88; HIPAA §164.312(a-c); Ley 21.663 Art. 3-4; Ley 19.628 Art. 7-8
Seguridad de Endpoints	Proteger dispositivos que acceden a la red y datos.	Antivirus/Antimalware; EDR/XDR; Gestión de parches; Control de USB; MDM/UEM	ISO 27001 A.12, A.13; NIST SP 800-171; HIPAA §164.310(d); Ley 21.663 Art. 9

Capa de Seguridad	Objetivo Principal	Controles Claves	Referencias de Cumplimiento
Seguridad Operacional y Monitoreo	Detectar y responder a amenazas en tiempo real.	Monitoreo continuo, SIEM; SOC 24/7; CTI (Cyber Threat Intelligence); Pentesting, auditorías, DRP	ISO 27001 A.16, A.12.4, A.17; NIST SP 800-137; HIPAA §164.308(a)(6); Ley 21.663 Art. 10-11
Seguridad en Nube	Asegurar la protección de los recursos y servicios desplegados en entornos cloud.	Gestión de identidades y accesos (IAM); Configuración segura de servicios (CSPM); Cifrado en tránsito y reposo; SLA con proveedores; Monitoreo de uso y amenazas en la nube	ISO 27001 A.5.19, A.5.23, A.5.30; NIST SP 800-144; NIST SP 800-53 AC, SC, AU; CIS Controls v8; Ley 21.663 Art. 6, 9; Ley 19.628 Art. 8

6.1.10. Amenazas Cibernéticas en el Sector Salud:

La transformación digital en el sector salud ha aumentado la exposición de las instituciones a amenazas cibernéticas que ponen en riesgo la confidencialidad, integridad, disponibilidad y privacidad de la información. Estas amenazas impactan tanto en los sistemas clínicos como en los dispositivos médicos, afectando directamente la calidad de la atención y la seguridad de los pacientes, quienes deben tener en cuenta las instituciones del sector.

A continuación, se describen los principales tipos de amenazas cibernéticas que enfrenta el sector salud junto con sus impactos potenciales y los controles claves para su mitigación:

Tipo de Ataque	Descripción	Impactos Potenciales	Controles Clave para su Mitigación
Ransomware	Malware que cifra los datos y exige un rescate económico para su liberación.	- Interrupción de servicios clínicos críticos (HIS, PACS, LIS). - Pérdida de acceso a datos esenciales para la atención médica. - Costos financieros por rescate, recuperación y multas regulatorias. - Daño reputacional significativo.	- Copias de seguridad cifradas y segregadas (ISO 27001 A.12.3). - EDR/XDR con capacidad de contención automática. - Segmentación de red y control de tráfico lateral (NIST SP 800-207). - Plan de respuesta ante incidentes (ISO 27035). - Parches y actualizaciones periódicas.
Ataques a la Cadena de Suministro	Explotación de vulnerabilidades en proveedores de software, hardware o servicios para comprometer los	- Introducción de malware en sistemas de misión crítica. - Compromiso de datos sensibles. - Impacto indirecto en la	- Evaluación y monitoreo continuo de proveedores (ISO 27001 A.15). - Requisitos de seguridad en contratos (Ley 21.663, CIS v8 IG1 Control 15.1).

DEPARTAMENTO TIC VISADO

Tipo de Ataque	Descripción	Impactos Potenciales	Controles Clave para su Mitigación
	sistemas internos de las instituciones de salud.	confiabilidad de la atención médica.	- Gestión de riesgos de terceros (NIST SP 800-161). - Control de acceso mínimo necesario. - Aislamiento de entornos críticos.
Robo de Datos de Pacientes	Acceso no autorizado y filtración de información médica sensible, incluyendo historiales clínicos, datos personales y resultados de laboratorio.	- Multas severas por incumplimiento de normativas de privacidad. - Litigios legales. - Pérdida de confianza de los pacientes y del público.	- Cifrado en reposo y en tránsito (ISO 27001 A.10). - Gestión de identidad y acceso (IAM) robusta. - DLP (prevención de fuga de datos). - Auditoría y monitoreo continuo (SIEM). - Concientización y capacitación en privacidad.
Ataques a Dispositivos Médicos	Manipulación o interrupción del funcionamiento de dispositivos médicos conectados, como bombas de infusión, marcapasos o monitores de pacientes.	- Riesgo directo para la seguridad y la vida de los pacientes. - Interrupciones en procedimientos médicos críticos. - Potencial de litigaciones legales graves.	- Gestión de inventario de activos médicos (ISO 27001 A.8). - Segmentación de red para dispositivos IoMT. - Control de firmware y actualizaciones seguras. - Evaluaciones de seguridad periódicas. - Supervisión continua del comportamiento de los dispositivos.
Ingeniería Social (Phishing y Spear Phishing)	Técnicas de engaño dirigidas a personal administrativo y clínico para obtener credenciales o instalar malware.	- Acceso no autorizado a sistemas clínicos. - Instalación de ransomware o spyware. - Compromiso de redes internas y bases de datos sensibles.	- Programas de concientización y simulacros de phishing. - Autenticación multifactor (MFA). - Filtros de correo y sandboxing. - Política de mínimo privilegio. - Monitoreo de accesos inusuales.
Ataques de Denegación de Servicio (DDoS)	Saturación de los sistemas de información a través de tráfico malicioso, impidiendo su disponibilidad.	- Caída de plataformas de telemedicina, servicios de urgencias o sistemas administrativos. - Afectación directa a la continuidad de la atención médica. - Pérdida de ingresos y deterioro de la imagen institucional.	- Servicios de mitigación DDoS (WAF y CDN con capacidad de absorción). - Alta disponibilidad y redundancia (ISO 27001 A.17). - Plan de continuidad operativa y DRP. - Monitorización de tráfico en tiempo real.

7. PROTECCION DE LOS ACTIVOS CRITICOS

Los activos críticos en las instituciones del sector salud son esos elementos clave que aseguran que la organización funcione de manera segura y eficiente. Si estos activos se ven comprometidos o destruidos, las repercusiones pueden ser graves: la calidad de los servicios de salud puede verse afectada, la seguridad de los pacientes puede estar en riesgo y la continuidad de las operaciones puede verse amenazada. Entre estos activos se incluyen, pero no se limitan a, la información sensible de los pacientes, los sistemas de gestión hospitalaria, los dispositivos médicos conectados, la infraestructura de redes y los sistemas de comunicación.

Proteger y salvaguardar los activos críticos debe ser una prioridad en el ámbito de la seguridad de la información y la ciberseguridad en las instituciones del sector salud. Para lograrlo, es esencial se implementen controles preventivos, detectivos y correctivos adecuados, asegurando que estos activos sean identificados, monitoreados y protegidos en todo momento.

7.1. Identificación de Activos Críticos

El primer paso para proteger los activos críticos es identificarlos de manera precisa. Esta identificación debe hacerse en colaboración con los responsables de las diferentes áreas de la institución, para así entender el valor y la importancia de cada activo en relación con los servicios que se ofrecen.

Los activos críticos incluyen, pero no se limitan a:

- Datos sensibles: Información personal de pacientes, historiales médicos, diagnósticos, tratamientos, etc.
- Sistemas y plataformas: Sistemas de gestión hospitalaria, sistemas de registros médicos electrónicos (EMR), plataformas de administración de citas, etc.
- Infraestructura tecnológica: Servidores, bases de datos, redes, dispositivos de almacenamiento, sistemas de respaldo, etc.
- Dispositivos médicos conectados: Equipos médicos que dependen de sistemas tecnológicos para su funcionamiento (p. ej., respiradores, monitores cardíacos, dispositivos de imágenes, etc.).

7.2. Clasificación de Activos y Niveles de Criticidad

Todos los activos del sector salud deben clasificarse según su **nivel de criticidad** para la operación institucional, considerando su confidencialidad, integridad, disponibilidad y cumplimiento regulatorio. Se recomienda el siguiente esquema:

Nivel de Criticidad	Descripción	Ejemplos
Crítico (C1)	Interrumpir su operación institucional; afecta gravemente la continuidad operacional o expone datos personales sensibles.	Historia Clínica Electrónica, Core HIS, Sistema de Imagenología (RIS/PACS), ERP institucional, plataformas de telemedicina, Sistemas informáticos que manejan información sensible.
Alto (C2)	Su fallo tiene impacto relevante en procesos operativos o de soporte.	Sistemas de agenda, laboratorio (LIS), gestión documental, correo institucional, Portales ciudadanos.
Medio (C3)	Su indisponibilidad es tolerable por tiempos definidos sin afectar la seguridad o integridad del paciente o la Institución.	Portales informativos, intranet, sistemas de apoyo no críticos.
Bajo (C4)	No afecta procesos misionales y su uso es complementario.	Sistemas de capacitación, encuestas internas, aplicativos no sensibles.

7.3. Controles para la Protección de los Activos Críticos

La protección y defensa de los activos críticos es fundamental en la estrategia de seguridad de la información en el sector salud. Identificar correctamente, evaluar riesgos, implementar controles de seguridad y establecer una buena gobernanza son pasos clave para mantener estos activos a salvo de amenazas cibernéticas y otros peligros, garantizando así la continuidad operativa y la protección de la información sensible de los pacientes.

Para proteger los activos críticos, es esencial implementar un conjunto de controles de seguridad que aborden tanto las amenazas como las vulnerabilidades que se hayan identificado. Estos controles deben incorporar las medidas, que se describen a continuación:

7.3.1. Control de Acceso

- Autenticación Multifactor (MFA): Implemente la Autenticación Multifactor (MFA) de forma obligatoria para acceder a todos los sistemas y activos críticos, requiriendo al menos dos métodos de verificación distintos, como su contraseña más un código de su teléfono (TOTP o notificación push) o su huella digital. Asegúrese de integrar esta funcionalidad con el sistema centralizado de gestión de identidades (IAM) para facilitar su administración y seguimiento.
- Autorización Basada en Roles y Atributos (RBAC): Defina e implemente un sistema de autorización que asigne permisos de acceso a los activos críticos basándose en los roles laborales o atributos específicos de los usuarios. Otorgue únicamente el nivel de acceso mínimo necesario para que cada usuario realice sus tareas, utilizando un sistema centralizado de gestión de roles y permisos y aplicando listas de control de acceso (ACLs) detalladas a nivel de sistemas, aplicaciones y bases de datos.
- Gestión de Cuentas y Credenciales: Establezca políticas robustas para la administración de cuentas de usuario, incluyendo la creación, modificación, suspensión y eliminación.

Obligue al uso de contraseñas complejas que cumplan con criterios de seguridad y cámbielas periódicamente. Utilice herramientas de gestión de contraseñas empresariales para un almacenamiento seguro y configure el bloqueo automático de cuentas tras varios intentos fallidos de inicio de sesión, además de monitorear la creación de cuentas con privilegios elevados.

- Control de Acceso a la Red: Aísle los activos críticos del resto de la red mediante la segmentación, utilizando VLANs y microsegmentación. Controle estrictamente el tráfico de red hacia y desde estos activos configurando firewalls internos con reglas específicas que permitan solo las comunicaciones necesarias, basándose en listas blancas de direcciones IP y puertos autorizados.
- Seguridad en Dispositivos Médicos: Implemente medidas de seguridad específicas para proteger los dispositivos médicos conectados a la red. Asegure la autenticación y el control de acceso propios de estos dispositivos y segméntelos lógicamente en la red mediante VLANs dedicadas o reglas de firewall restrictivas que limiten su comunicación a los sistemas esenciales para su operación y gestión.
- Gestión de Vulnerabilidades: Implemente un proceso continuo para identificar, clasificar y corregir las vulnerabilidades en todos los sistemas y aplicaciones. Utilice herramientas automatizadas de escaneo, evalúe y priorice las vulnerabilidades según su riesgo, y aplique parches y actualizaciones de seguridad de manera proactiva para mantener los sistemas protegidos.

7.3.2. Protección de Datos

- Cifrado de Datos: Implemente el cifrado robusto de toda la información sensible, tanto cuando se transmita (en tránsito) como cuando esté almacenada (en reposo), utilizando algoritmos como AES-256 o superior. Asegure una gestión segura de las claves de cifrado, preferentemente mediante Módulos de Seguridad de Hardware (HSM). Utilice protocolos de comunicación seguros como TLS 1.2 o superior para todo el tráfico web y la transferencia de datos, acompañados de conjuntos de cifrados seguros, y configure y administre correctamente los certificados digitales para garantizar la integridad y confiabilidad de las comunicaciones.
- Prevención de Pérdida de Datos (DLP): Implemente herramientas de software DLP y defina políticas claras para prevenir la fuga de información sensible desde los activos críticos. Configure el software DLP para monitorear y controlar la transferencia de archivos, el correo electrónico y otros canales de comunicación, estableciendo reglas basadas en la clasificación de la información para evitar su divulgación no autorizada.
- Integridad de los Datos: Implemente mecanismos para asegurar que los datos críticos no sean modificados por personal o procesos no autorizados. Utilice sumas de verificación (checksums), hashes criptográficos y firmas digitales para detectar alteraciones, e implemente un sistema de control de versiones para rastrear y gestionar los cambios. Mantenga registros de auditoría detallados de todas las modificaciones realizadas a los datos para su revisión y análisis.
- Monitoreo Continuo: Establezca sistemas de monitoreo en tiempo real que supervisen la actividad de los sistemas y la red en busca de comportamientos sospechosos,

intentos de acceso no autorizado o fallas en los sistemas críticos. Configure alertas para identificar y responder rápidamente a posibles incidentes de seguridad.

- Análisis de Logs: Implemente un sistema centralizado de gestión de logs (SIEM) para recopilar y analizar todos los registros de actividad relevantes para los activos críticos. Configure el SIEM para correlacionar eventos, detectar patrones anómalos y generar alertas tempranas de posibles incidentes de seguridad, facilitando la investigación y respuesta.
- Pruebas de Penetración: Realice pruebas de penetración de forma periódica en los sistemas de información y la infraestructura que soportan los activos críticos. Estas pruebas deben simular ataques reales para identificar posibles vulnerabilidades que podrían ser explotadas, permitiendo tomar medidas correctivas antes de que ocurran incidentes.

7.3.3. Seguridad de la Infraestructura:

- Fortalecimiento de Sistemas Operativos y Aplicaciones: Configure de forma segura los sistemas operativos y las aplicaciones que dan soporte a los Activos Críticos, aplicando las mejores prácticas de "hardening". Desactive todos los servicios y funcionalidades que no sean esenciales. Asegure la configuración correcta de los permisos de archivos y directorios, e implemente políticas de seguridad locales para restringir acciones no autorizadas.
- Gestión de Parches y Vulnerabilidades: Establezca un proceso robusto para la gestión de parches y vulnerabilidades en los Activos Críticos. Identifique, evalúe y aplique las actualizaciones de seguridad necesarias para los sistemas operativos, aplicaciones y firmware de manera oportuna. Utilice herramientas automatizadas para la gestión de parches y realice escaneos de vulnerabilidades de forma periódica para detectar y corregir posibles debilidades.
- Protección Antimalware Avanzada: Implemente soluciones antimalware de última generación en todos los equipos (endpoints y servidores) que interactúan con los Activos Críticos. Elija software que ofrezca detección basada en el comportamiento, análisis en entornos aislados (sandboxing) y análisis de amenazas en tiempo real para una protección más efectiva contra software malicioso avanzado.
- Registros y Monitoreo de Seguridad (Logging y SIEM): Active el registro detallado de la actividad en los sistemas y aplicaciones que soportan los Activos Críticos. Centralice estos registros en un sistema SIEM (Security Information and Event Management) para su análisis y correlación. Configure el SIEM para detectar comportamientos anómalos, generar alertas automáticas ante posibles incidentes de seguridad y facilitar la investigación forense en caso de ser necesario.

7.3.4. Resiliencia y Recuperación:

- Respaldos Regulares (Backups): Implemente un sistema de respaldos automáticos y periódicos para todos los datos críticos, almacenándolos de forma segura en ubicaciones separadas geográficamente, idealmente utilizando servicios seguros en la

nube o sitios de recuperación ante desastres. Asegúrese de cumplir con la regla 3-2-1 de respaldos, manteniendo al menos tres copias en dos medios diferentes, con una copia fuera del sitio principal, aislada y protegida contra accesos no autorizados. Automatice pruebas de restauración periódicas para verificar la integridad y funcionalidad de los respaldos como parte de los planes de continuidad operativa y recuperación ante incidentes.

- Planes de Recuperación ante Desastres (DRP): Desarrolle, implemente y mantenga un Plan de Recuperación ante Desastres (DRP) para asegurar la continuidad operativa de los activos críticos frente a interrupciones. Identifique y clasifique los activos esenciales, defina los objetivos de recuperación (RTO y RPO), implemente sitios de respaldo (frío, tibio o caliente) según la criticidad, y realice simulacros periódicos para validar la efectividad del plan. Mantenga el DRP actualizado ante cambios tecnológicos o de riesgo.
- Plan de Respuesta ante Incidentes: Establezca y documente un Plan de Respuesta ante Incidentes de Ciberseguridad que incluya procedimientos claros y técnicos para la identificación, contención, erradicación y recuperación de los activos críticos en caso de verse comprometidos. Defina roles y responsabilidades técnicas dentro del plan y asegúrese de que el equipo esté capacitado para ejecutar los procedimientos necesarios.

7.3.5. Seguridad en la Nube:

- Configuración Segura de Servicios Cloud: Configure los servicios en la nube que alojan los Activos Críticos siguiendo las directrices de seguridad recomendadas por el proveedor. Implemente políticas de Gestión de Identidades y Accesos (IAM) específicas para el entorno cloud, defina y configure reglas de firewall y grupos de seguridad para controlar el tráfico de red, y asegúrese de utilizar las opciones de cifrado que ofrece el proveedor de la nube para proteger los datos en reposo y en tránsito.
- Monitorización de la Seguridad en la Nube: Utilice las herramientas de monitorización y seguridad nativas del proveedor de la nube para supervisar la actividad y detectar posibles amenazas dirigidas a los Activos Críticos. Configure alertas para eventos de seguridad relevantes, como intentos de acceso no autorizados o configuraciones sospechosas, e integre los registros de actividad de la nube con su sistema SIEM (Security Information and Event Management) para una visión centralizada de la seguridad.

7.4. Matriz de controles por Nivel de Criticidad de Activos

Se detalla a continuación, una propuesta de controles que deben ser implementados de acuerdo con la criticidad de los activos:

Control/Requisito	Tipo	C1 (Crítico)	C2 (Alto)	C3 (Medio)	C4 (Bajo)
Autenticación Multifactor (MFA)	Acceso	Obligatorio	Obligatorio	Recomendado	Opcional
Autorización Basada en Roles y Atributos (RBAC)	Acceso	Obligatorio	Obligatorio	Recomendado	Opcional
Gestión de Cuentas y Credenciales	Acceso	Obligatorio	Obligatorio	Recomendado	Opcional
Control de Acceso a la Red (Segmentación)	Red	Obligatorio	Obligatorio	Recomendado	Opcional
Seguridad en Dispositivos Médicos (Autenticación y Segmentación)	Dispositivos	Obligatorio	Recomendado	Opcional	Opcional
Gestión de Parches y Escaneo periódico de vulnerabilidades	General	Obligatorio	Obligatorio	Recomendado	Opcional
Cifrado en tránsito y reposo (TLS 1.2+/AES-256)	Datos	Obligatorio	Obligatorio	Recomendado	Opcional
Prevención de Pérdida de Datos (DLP)	Datos	Obligatorio	Recomendado	Opcional	Opcional
Integridad de los Datos (Checksums, hashes criptográficos Firmas, Auditoría)	Datos	Obligatorio	Recomendado	Opcional	Opcional
Monitoreo Continuo	Seguridad	Obligatorio	Recomendado	Opcional	Opcional
Análisis de Logs (SIEM)	Seguridad	Obligatorio	Recomendado	Opcional	Opcional
Pruebas de Penetración Periódicas	Seguridad	Obligatorio	Recomendado	Opcional	Opcional
Fortalecimiento de Sistemas Operativos y Aplicaciones (Hardening)	Sistemas	Obligatorio	Recomendado	Opcional	Opcional
Gestión de Parches y Vulnerabilidades	Sistemas	Obligatorio	Obligatorio	Recomendado	Opcional
Protección Antimalware Avanzada	Endpoints/Servidores	Obligatorio	Obligatorio	Recomendado	Opcional

Control/Requisito	Tipo	C1 (Crítico)	C2 (Alto)	C3 (Medio)	C4 (Bajo)
Registros y Monitoreo de Seguridad (Logging y SIEM)	Seguridad	Obligatorio	Recomendado	Opcional	Opcional
Copias de respaldo con prueba de restauración	Respaldo	Obligatorio	Obligatorio	Recomendado	Opcional
Planes de Recuperación ante Desastres (DRP)	Respaldo	Obligatorio	Recomendado	Opcional	Opcional
Plan de Respuesta ante Incidentes	Seguridad	Obligatorio	Obligatorio	Recomendado	Opcional
Configuración Segura de Servicios Cloud (Features de Seguridad)	Nube	Obligatorio	Recomendado	Opcional	Opcional
Monitorización de la Seguridad en la Nube	Nube	Obligatorio	Recomendado	Opcional	Opcional
Revisión anual de contratos y cláusulas de seguridad	Contratos	Obligatorio	Obligatorio	Recomendado	Opcional
Evaluación de código seguro (OWASP, SAST/DAST)	Seguridad	Obligatorio	Recomendado	Recomendado	Opcional

8. PROTECCION DE INFORMACION

La protección de la información es fundamental en la gestión de la seguridad y ciberseguridad en el sector salud. Dado la sensibilidad de los datos clínicos, personales y administrativos que se manejan en las instituciones de salud, es vital implementar controles y medidas que garanticen su resguardo frente a accesos no autorizados, pérdida, alteración o divulgación indebida. Esta protección debe estar presente a lo largo de todo el ciclo de vida de la información, desde su creación hasta su destrucción segura.

Para cumplir con esta responsabilidad, las instituciones deben seguir las siguientes directrices:

8.1. Clasificación de la Información

- Toda información institucional debe ser clasificada conforme a su nivel de sensibilidad, confidencialidad e impacto en caso de compromiso.
- La clasificación mínima debe incluir las siguientes categorías: Pública, Uso Interno, Confidencial y Información Sensible de Salud.

- Esta clasificación debe estar documentada, difundida y aplicada de manera transversal en todos los procesos tecnológicos y operativos.

8.2. Control de Acceso a la Información

- Se debe aplicar el principio de privilegio mínimo, asegurando que cada usuario acceda únicamente a la información necesaria para el desempeño de sus funciones.
  - Es obligatorio implementar mecanismos de autenticación fuerte (por ejemplo, autenticación multifactor) en sistemas que gestionen información crítica o sensible.
  - Todos los accesos deben ser registrados, monitoreados y auditados de forma continua.

8.3. Protección en Tránsito y en Reposo

- La información debe ser cifrada cuando se almacene (en reposo) y durante su transmisión (en tránsito) mediante el uso de algoritmos criptográficos robustos aprobados por estándares internacionales como NIST o ISO/IEC.
- Se deberán implementar mecanismos criptográficos robustos para proteger el acceso y almacenamiento de credenciales de usuario, bases de datos del sistema y la transmisión de información sensible.
- Está prohibido el uso de canales inseguros para el envío de información sensible, incluyendo correos electrónicos sin cifrado o dispositivos de almacenamiento portátiles sin protección.
- Seguridad en la Transmisión de Datos: Todos los sitios y sistemas web deben cifrar las comunicaciones entre cliente y servidor utilizando HTTPS con certificados emitidos por entidades acreditadas en el país.
- Se debe emplear TLS 1.2 o superior como estándar mínimo para garantizar la seguridad en la transmisión de datos, acompañados de conjuntos de cifrados seguros.
- Cifrado en Reposo: Toda información almacenada debe estar protegida mediante AES-256 o RSA-4096, u otros algoritmos aprobados en la política de uso de criptografía.
- Se deben utilizar sistemas de gestión segura de claves criptográficas para su generación, almacenamiento y rotación periódica.
- Protección de Contraseñas: El almacenamiento de contraseñas debe realizarse con algoritmos diseñados para resistir ataques de fuerza bruta, como bcrypt, PBKDF2 y Argon2.
- Monitoreo y Prevención de Vulneraciones: Se deben aplicar controles técnicos y administrativos para la detección temprana de intentos de vulneración del sistema de cifrado.
- Los sistemas deben estar configurados para seleccionar siempre la opción de cifrado más segura disponible.

8.4. Almacenamiento y Resguardo

- La información debe ser almacenada únicamente en infraestructuras autorizadas por el Ministerio de Salud o por el organismo correspondiente, que cumplan con estándares de seguridad y con ubicación geográfica bajo jurisdicción nacional, salvo autorización expresa.
- Los sistemas de respaldo deben garantizar la recuperación segura e íntegra de la información en caso de incidentes o fallas.

8.5. Eliminación y Destrucción Segura

La eliminación y destrucción de información en las instituciones del sector salud debe realizarse bajo estrictos estándares de seguridad, con el fin de evitar la recuperación no autorizada de datos sensibles o críticos.

Este proceso debe ser trazable, auditable y alineado con la normativa vigente, incluyendo la Ley N° 21.719 sobre Protección de Datos Personales y la Ley N° 21.663 sobre Ciberseguridad. Adicionalmente, en este proceso debe tenerse en cuenta lo previsto en la ley N° 20.584 sobre derechos y deberes del paciente, en el decreto N° 41, Reglamento de ficha clínica y su normativa complementaria.

Las siguientes directrices deberán ser cumplidas por todas las instituciones y proveedores que gestionen datos en el marco del Ministerio de Salud:

- La información clínica que conste en la ficha clínica y los documentos correspondientes a resultados de exámenes, recetas médicas, licencias médicas y demás documentos que la normativa señala que integran la ficha clínica no podrán ser objeto de borrado sin la autorización expresa y por escrito de la dirección médica del establecimiento.
- La eliminación de información deberá efectuarse mediante métodos seguros de borrado lógico (como sobre escritura múltiple con herramientas certificadas) y, cuando aplique, destrucción física de los soportes (por ejemplo, trituración, desmagnetización o incineración), de acuerdo con los estándares internacionalmente aceptados (NIST SP 800-88 Rev. 1, ISO/IEC 27040, entre otros).
- Toda eliminación de información crítica o sensible debe ser registrada mediante actas o bitácoras, especificando el tipo de datos, el método utilizado, los responsables del proceso y la fecha de ejecución. Estos registros deben conservarse conforme a la política de retención documental del organismo.
- Toda modificación, cancelación o destrucción de datos deberá realizarse únicamente bajo instrucción explícita del mandante o autoridad responsable de la información. Dichas instrucciones deberán ser documentadas y vinculadas al acta del proceso.
- En los casos en que la información sea gestionada por un tercero (procesador de datos), este será responsable de ejecutar el proceso de eliminación conforme a los lineamientos contractuales y regulatorios, dejando constancia formal de cada una de las etapas y resultados del procedimiento.

- Todo dispositivo digital o soporte magnético que vaya a ser descartado debe someterse previamente a procesos de formateo o sanitización segura, evitando cualquier posibilidad de recuperación de datos. Está prohibido reutilizar equipos con datos sensibles sin aplicar procedimientos de limpieza certificados.
- En proyectos de digitalización, queda estrictamente prohibido que los proveedores eliminen, destruyan o desechen los documentos originales sin contar con una autorización formal del mandante, la cual debe estar debidamente documentada.

8.6. Protección en Entornos de Nube

Cuando se utilicen servicios en la nube o se externalicen procesos que involucren el tratamiento de información, las Instituciones del Sector Salud deben exigir al proveedor garantizar niveles de seguridad equivalentes o superiores a los establecidos por la normativa nacional vigente y las directrices ministeriales.

Para ello, los contratos deben incluir obligatoriamente cláusulas explícitas que aseguren la confidencialidad, integridad y disponibilidad de la información, así como el cumplimiento riguroso de la Ley N° 21.719 sobre Protección de Datos Personales, la Ley N° 21.663 Marco de Ciberseguridad, y otros cuerpos regulatorios aplicables.

Estas cláusulas deberán estar alineadas con las directrices definidas por el MINSAL en el Instructivo sobre Cláusulas de Protección de Datos y Seguridad, en su versión actualizada y vigente.

Además, es necesario implementar controles técnicos sólidos para proteger tanto la capa de software como los servicios que se despliegan en la nube, asegurando que estén a salvo de vulnerabilidades y accesos no autorizados:

Encriptación de Datos: Para proteger datos confidenciales y sensibles, se deben aplicar técnicas de cifrado robustas que impidan accesos no autorizados.

- Toda la información almacenada en entornos de nube debe cifrarse utilizando estándares avanzados como AES-256.
- Los datos en tránsito deben protegerse mediante protocolos seguros, tales como TLS 1.3.
- Las claves criptográficas deben ser generadas, administradas y almacenadas en sistemas seguros, preferentemente en Módulos de Seguridad de Hardware (HSM).
- Se debe implementar autenticación multifactor (MFA) para el acceso a claves y sistemas donde se almacenen datos cifrados.

Seudonimización: Cuando se trate de datos personales sensibles, se recomienda aplicar técnicas de seudonimización, conservando en servidores locales los códigos que permitan su reidentificación. Esto busca evitar riesgos asociados a normativas de desencriptación forzosa en otras jurisdicciones, garantizando el cumplimiento de la Ley 19.628 y los artículos 19 Nº1 y Nº4 de la Constitución Política.

- Se recomienda el uso de técnicas como tokenización y enmascaramiento, que sustituyen los datos reales por valores irreversibles fuera del sistema autorizado.
- Las claves de seudonimización deben gestionarse de forma segura y almacenarse en sistemas separados.

Elasticidad: Se debe planificar anticipadamente la capacidad requerida en servicios cloud, permitiendo la asignación dinámica de recursos según las necesidades.

- Los servicios contratados deben ser elásticos, capaces de escalar automáticamente.
- Los contratos deben contemplar márgenes de crecimiento sin necesidad de nuevas licitaciones.

Garantía de Disponibilidad: Los sistemas deben estar diseñados para operar en esquemas de alta disponibilidad (HA), con recursos distribuidos en múltiples regiones o zonas.

- Deben establecerse mecanismos de restauración rápida ante incidentes críticos, como ciberataques o desastres, mediante planes BCP/DRP alineados con estándares internacionales.

Geolocalización y Protección de Datos Sensibles: El tratamiento de datos de geolocalización debe limitarse a lo estrictamente necesario.

- Si estos datos se procesan fuera de Chile, el proveedor debe garantizar estándares de protección equivalentes a los nacionales.
- Se deben aplicar medidas como cifrado en tránsito y en reposo, y controles de acceso restringido.
- Los titulares deben poder ejercer sus derechos de acceso, y cuando corresponda, rectificación o cancelación, sin afectar la función del organismo.
- El MINSAL deberá mantener trazabilidad mediante registros de tratamiento y accesos, y realizar auditorías periódicas que aseguren la aplicación efectiva de estas medidas.

Automatización de Respaldos y Pruebas de Restauración: Los sistemas críticos deben contar con respaldos automatizados en la nube, con pruebas regulares de restauración que aseguren su disponibilidad y funcionalidad en caso de contingencias.

Distribución de Copias: Las copias deben almacenarse en múltiples regiones, incluyendo al menos una en infraestructura ubicada en Chile.

- Se deberá evitar la replicación automática fuera del país, o bien, controlarla estrictamente.
- Se recomienda un enfoque híbrido: copia primaria en infraestructura propia (local o privada) y secundaria en nube pública, garantizando redundancia y control.

Monitoreo y Registro de Eventos: El proveedor debe habilitar registros detallados (logs) en todas las capas del sistema.

- Se deben usar herramientas de gestión de parches, configurar alertas de vulnerabilidades críticas y permitir respuestas automáticas.
- Se debe auditar:
  - Autenticaciones y accesos (exitosos/fallidos).
  - Eventos de red sospechosos.
  - Modificaciones en configuraciones y permisos.
  - Accesos y manipulaciones de datos sensibles, cumpliendo el principio de minimización.

Protección contra Amenazas

Se debe implementar una arquitectura de seguridad en capas con mecanismos de detección, prevención y respuesta ante amenazas avanzadas, incluyendo:

Web Application Firewall (WAF):

- Configure un WAF delante de las aplicaciones web expuestas en la nube para inspeccionar el tráfico HTTP/HTTPS y bloquear ataques a nivel de aplicación.
- Implemente reglas de protección contra vulnerabilidades comunes como Cross-Site Scripting (XSS), Inyección SQL (SQLi) y File Inclusion Remota (RFI), basándose en firmas de ataque conocidas y comportamiento anómalo. Personalice las reglas según las necesidades específicas de las aplicaciones. Integrar el WAF con sistemas de registro y alerta para monitorizar y responder a posibles incidentes.

Protección contra ataques de Denegación de Servicio Distribuido (DDoS)

- La infraestructura debe estar protegida contra intentos de saturar servicios mediante múltiples peticiones simultáneas.
- Un ataque DDoS puede dejar fuera de línea portales de atención, sistemas de agendamiento y otras aplicaciones críticas.
- Se deben emplear servicios de mitigación que identifiquen patrones anómalos de tráfico y redirijan ataques antes de que lleguen a los sistemas internos.
- Esta protección debe estar habilitada tanto a nivel de red como de aplicación.

Inteligencia de Amenazas e Indicadores de Compromiso (IoCs)

- La solución debe integrar fuentes de inteligencia de amenazas (Threat Intelligence) para anticiparse a ataques conocidos y emergentes.
- Los IoCs (Indicadores de Compromiso) son evidencias técnicas (IPs, hashes de archivos, dominios maliciosos, etc.) que permiten detectar intrusiones en curso o pasadas.
- Estas capacidades deben:
  - Estar integradas con los sistemas de monitoreo y análisis de seguridad (como SIEM o XDR).
  - Permitir respuestas automatizadas ante detecciones críticas.
  - Aportar a una mejora continua del sistema defensivo y a una postura de seguridad proactiva.

Políticas de IAM Basadas en Mínimos Privilegios y Roles:

- Defina e implemente políticas de Gestión de Identidades y Accesos (IAM) que otorguen a usuarios, grupos y servicios cloud únicamente los permisos mínimos necesarios para realizar sus funciones. Utilizar roles para agrupar permisos basados en responsabilidades laborales.
- Cree roles con permisos específicos para cada función. Asignar usuarios y servicios a estos roles en lugar de otorgar permisos directos. Revisar y auditar periódicamente las políticas de IAM para asegurar el cumplimiento del principio de mínimo privilegio. Utilizar herramientas de gestión de IAM proporcionadas por el proveedor de la nube.

Zero Trust Network Access (ZTNA):

- Implemente un modelo de acceso Zero Trust para los servicios cloud, donde cada solicitud de acceso se verifica rigurosamente basándose en la identidad del usuario, el contexto de la solicitud (ubicación, hora, dispositivo) y el cumplimiento de las políticas de seguridad del dispositivo.
- Configure una solución ZTNA que valide la identidad del usuario mediante mecanismos fuertes (MFA), evalúe el estado de seguridad del dispositivo antes de otorgar acceso y aplique políticas de acceso granular basadas en el contexto. Utilizar microsegmentación para limitar el radio de explosión en caso de compromiso.

Autenticación Multifactor (MFA):

- Habilite y exija Autenticación Multifactor (MFA) para todos los accesos a la consola de administración de la nube, a los servicios cloud y a los recursos sensibles.
- Configure MFA utilizando al menos dos factores de autenticación diferentes, como una contraseña y un código generado por una aplicación móvil (TOTP), un token de hardware, o datos biométricos. Asegurar la correcta implementación y el cumplimiento de las políticas de MFA.

Secure Access Service Edge (SASE):

- Evalué e implemente una solución SASE para integrar funciones de seguridad en la nube con capacidades de red definidas por software (SD-WAN), centralizando la gestión y el control del acceso a los servicios cloud desde el borde de la red.
- Configure la SD-WAN para optimizar la conectividad y el rendimiento. Implementar los componentes de seguridad SASE como Firewall como Servicio (FWaaS), Puerta de Enlace Web Segura (SWG), Agente de Seguridad de Acceso a la Nube (CASB) y Zero Trust Network Access (ZTNA), según los requisitos de acceso y seguridad.

9. RESPUESTA ANTE INCIDENTES DE SEGURIDAD DE LA INFORMACION Y CIBERSEGURIDAD, CONTINUIDAD OPERACIONAL

Es crucial responder de manera efectiva a los incidentes que afectan la seguridad de la información y la ciberseguridad en el sector salud. Esto no solo protege los datos sensibles, sino que también asegura la seguridad de los pacientes y garantiza que los servicios de salud

funcionen sin contratiempos. La respuesta a estos incidentes debe ser planificada, eficiente y seguir las mejores prácticas de seguridad.

Además, los planes de continuidad operativa deben garantizar que las funciones esenciales sigan funcionando, incluso si se presenta un incidente. Este apartado tiene como objetivo establecer los procedimientos necesarios para gestionar los incidentes de seguridad de la información y asegurar la continuidad operativa en las instituciones del sector salud.

9.1. Incidentes de seguridad de la Información y Ciberseguridad

De acuerdo con la Ley N° 21.663, su Reglamento de Reporte de Incidentes (Decreto N° 295/2024) y los estándares internacionales de ciberseguridad, todas las instituciones, tanto públicas como privadas, incluyendo las del Sector Salud, están obligadas a desarrollar, implementar y mantener un Plan de Respuesta ante Incidentes (IRP). Este plan es crucial para gestionar de manera efectiva y oportuna cualquier evento que ponga en riesgo la seguridad de la información y la ciberseguridad, y debe facilitar la coordinación con la Agencia Nacional de Ciberseguridad.

El IRP debe estar en línea con la normativa vigente, revisarse de forma regular y contar con procedimientos claros para la notificación y el reporte de incidentes, especialmente aquellos que involucren datos sensibles o que puedan afectar la continuidad operativa. Es fundamental que el plan se mantenga actualizado y sea accesible para el personal pertinente.

La respuesta ante incidentes debe ser un proceso bien planificado, documentado y ejecutado rápidamente para reducir al mínimo los riesgos sobre la disponibilidad, integridad y confidencialidad de la información.

9.1.1. Plan de Respuesta ante Incidentes (IRP) [5]

El Plan de Respuesta ante Incidentes (IRP) es un documento esencial que define los pasos organizativos y técnicos a seguir para detectar, analizar, contener, eliminar y recuperarse de incidentes relacionados con la ciberseguridad o la seguridad de la información que puedan afectar a los sistemas, datos o servicios de una institución. Su objetivo principal es reducir al mínimo el impacto de estos incidentes, restablecer la normalidad en las operaciones de manera efectiva y aprender de la experiencia para reforzar las defensas en el futuro.

Para garantizar una gestión efectiva de los incidentes de seguridad de la información y ciberseguridad, las Instituciones del Sector Salud deben crear, implementar y mantener un Plan de Respuesta ante Incidentes (IRP) que contemple y desarrolle de manera detallada las siguientes etapas fundamentales:

- **Preparación**:
  - Debe definir los roles y responsabilidades dentro del equipo encargado de responder a incidentes, asegurando que cada miembro sepa exactamente qué hacer si ocurre un problema.

[5] CISA - cybersecurity incident & vulnerability response playbooks.

- Desarrolle y lleve a cabo simulacros de incidentes cibernéticos es clave para que el personal esté bien preparado.
- Asegúrese de que todos los sistemas y datos críticos estén respaldados correctamente y que los procedimientos de restauración estén listos para usarse.

- **Detección y Notificación**:
  - Establezca mecanismos de monitoreo continuo, como un SIEM (Sistema de Gestión de Información y Eventos de Seguridad), es esencial para detectar incidentes en tiempo real.
  - Implemente procedimientos claros para que los colaboradores puedan reportar incidentes de seguridad de inmediato, incluyendo contactos de emergencia.
- **Evaluación y Contención**:
  - Evalué la naturaleza y el alcance del incidente, lo que incluye identificar los activos afectados y la magnitud de la brecha de seguridad.
  - Implemente medidas para contener el incidente y evitar que se propague, como desconectar sistemas comprometidos o revocar accesos.
- **Erradicación**:
  - Elimine las amenazas y vulnerabilidades relacionadas con el incidente, asegurándose de que los sistemas afectados sean limpiados y que se apliquen parches o soluciones de seguridad para prevenir futuros problemas.
- **Recuperación**:
  - Restaure los sistemas y servicios afectados es crucial, asegurando que se sigan los procedimientos de recuperación previamente establecidos.
  - Verifique los sistemas restaurados estén libres de amenazas y funcionando de manera segura.
- **Revisión Post-Incidente**:
  - Realizar un análisis post-incidente para identificar las lecciones aprendidas, actualizar los procedimientos y mejorar los controles de seguridad.
  - Redactar un informe detallado que incluya las causas identificades, las acciones tomadas, el impacto del incidente y las recomendaciones para evitar incidentes futuros.

9.1.2. Comunicación en Caso de Incidente

Es crucial que exista una **estrategia de comunicación clara** durante un incidente de seguridad. Esta debe cubrir tanto las comunicaciones internas como externas, y debe incluir:

- Notificación inmediata a los responsables y a los equipos clave dentro de la institución (IT, seguridad, gerencia).
- Comunicación con autoridades competentes, si el incidente involucra una violación de datos sensibles o si hay obligación de reportarlo bajo la ley.
- Manejo de la comunicación con el público y los pacientes, especialmente si el incidente afecta los servicios que reciben.

9.1.3. Reporte de Incidentes de Ciberseguridad: Procedimiento y Plazos

Obligatoriedad del Reporte: De acuerdo con el Artículo 3° del Decreto N° 295/2024, que aprueba el reglamento de reporte de incidentes de ciberseguridad, todos los organismos del Sector Salud que presten servicios esenciales están obligados a reportar aquellos incidentes que se consideren de impacto significativo, según los criterios definidos en dicho decreto

El reporte es crucial para la documentación exhaustiva del incidente y para la comunicación oficial con las autoridades competentes, en particular con la Agencia Nacional de Ciberseguridad (ANCI).

Plataforma Oficial de Reporte (ANCI): A estos efectos, la Agencia ha dispuesto en siguiente portal de notificación de incidentes: https://portal.anci.gob.cl/.

Las instituciones del Sector Salud deberán utilizar este sitio web para notificar sus incidentes significativos.

Canales de Comunicación Alternativos (Contingencia): En caso de contingencia o problemas con la plataforma principal, la ANCI mantiene operativos los siguientes canales alternativos para el reporte y la comunicación:

- **Teléfono:** 1510
- **Correo Electrónico:** ayuda@anci.gob.cl

Es fundamental que las instituciones del Sector Salud conozcan y utilicen los canales designados y sigan los procedimientos establecidos para el reporte oportuno y adecuado de los incidentes de ciberseguridad, cumpliendo así con las obligaciones legales y contribuyendo a la seguridad del sector a nivel nacional.

Requisitos para el Reporte: Para realizar el reporte a través de la plataforma, el responsable delegado por la dirección de la notificación dentro de la institución del Sector Salud (CISO) deberá **registrarse utilizando su Clave Única**. Posteriormente, deberá completar la información solicitada en cada uno de los tres pasos del proceso de reporte.

Contenido del Reporte y Taxonomía: El contenido específico que debe incluirse en cada etapa del reporte está regulado por el Decreto N° 295/2024. Adicionalmente, para proporcionar una guía técnica y facilitar la clasificación de los incidentes, la ANCI ha aprobado y publicado una Taxonomía de Incidentes de Ciberseguridad a través del DS 7/2025.

Etapas y procedimiento de Reporte en la Plataforma ANCI: El proceso de reporte se realiza en tres etapas secuenciales dentro de la plataforma:

Alerta Temprana:

- Oportunidad: dentro de las **3 horas** posteriores a la detección del incidente.
- Contenido: Información preliminar disponible sobre la naturaleza, el alcance y el posible impacto del incidente.

- Contenido:
  - Descripción del incidente, incluyendo el tipo de amenaza detectada (ej., malware, acceso no autorizado, denegación de servicio).
  - Identificación de los sistemas, aplicaciones o datos afectados.
  - Gravedad estimada del incidente.
  - Acciones iniciales que se han tomado para contener el incidente.
  - Impacto potencial en la institución y en los servicios prestados.

Segunda Notificación:

- **Oportunidad:** dentro de los **72 hrs** siguientes a la confirmación del incidente.
- **Destinatario:** ANCI y autoridades competentes.
- **Contenido:** Reporte detallado del incidente, que incluya:
  - Información adicional sobre la evolución del incidente.
  - Detalles sobre las medidas adoptadas para la contención y erradicación del incidente.
  - Descripción de la restauración de los sistemas afectados y la reanudación de la operación normal.
  - Evaluación del impacto real en la confidencialidad, integridad y disponibilidad de los datos.
  - Informe de cualquier brecha de seguridad o violación de datos personales.

Informe Final:

- **Oportunidad**: Dentro del **plazo máximo de 15 días corridos** contados desde el envío de la alerta temprana.
- **Condición**: Al concluir la gestión del incidente. Una vez que el incidente ha sido completamente contenido, erradicado y los sistemas restaurados.
- **Destinatario**: Este informe debe entregarse a las autoridades competentes, así como al Comité de Seguridad de la Información de la institución.
- **Contenido**: El informe debe incluir el registro detallado de la información levantada respecto del incidente.
  - Un resumen completo del incidente desde su detección hasta su resolución.
  - El detalle las causas del incidente, las acciones de respuesta implementadas.
  - Evaluación del impacto total del incidente y las lecciones aprendidas
  - Medidas preventivas adoptadas para evitar futuras para mitigar riesgos futuros.
  - Cualquier recomendación para mejorar los controles de seguridad
  - Protocolos de respuesta ante incidentes.

Coordinación Central: Las instituciones del sector salud pueden, además, establecer coordinaciones estratégicas con el Ministerio de Salud, a través de su CISO o de la Unidad de Seguridad de la Información y Ciberseguridad, del Departamento de Tecnologías de Información y Comunicaciones. Estas coordinaciones permiten articular acciones conjuntas en ámbitos como la gestión de proveedores de red, la aplicación de recomendaciones iniciales para el fortalecimiento de la postura de ciberseguridad institucional. Asimismo, estas instancias pueden facilitar el apoyo técnico y operativo necesario para el restablecimiento

oportuno de los servicios afectados, en coordinación con el CSIRT Nacional, asegurando una respuesta eficaz ante incidentes de ciberseguridad de alto impacto.

Adicionalmente, se mantendrán operativos los siguientes canales Ministeriales disponibles para comunicarse en caso de contingencia:

- Al teléfono 800 123 573
- Al correo electrónico mds@minsal.cl
- Al correo electrónico seguridadtic@minsal.cl

- **Informe de Lecciones Aprendidas**:
  - Este informe debe ser realizado por el equipo de respuesta tras la resolución del incidente, y debe incluir un análisis detallado de las lecciones aprendidas, con el objetivo de mejorar la estrategia de ciberseguridad de la institución.
  - Este informe debe ser distribuido internamente a todas las partes interesadas y, si es necesario, se debe presentar a las autoridades competentes.

9.1.4. Confidencialidad y Protección de la Información

Según lo establecido en la Ley N° 21.663, las instituciones tienen la responsabilidad de asegurarse de que la información relacionada con incidentes de ciberseguridad se comparta únicamente con las autoridades competentes y otras partes que estén debidamente autorizadas.

Por lo tanto, toda la información que se encuentra en las alertas, reportes e informes sobre incidentes, debe ser tratada con la máxima confidencialidad. Esto es crucial para prevenir la divulgación no autorizada de datos sensibles y para proteger la seguridad de los sistemas y la información involucrada.

9.2. Continuidad operacional

El objetivo de la continuidad operativa es garantizar que las funciones críticas de la institución continúen sin interrupciones, incluso durante un incidente de seguridad. Esto es fundamental para asegurar que los servicios de salud no se vean comprometidos y que los pacientes no sufran consecuencias negativas debido a la caída de los sistemas o la pérdida de información.

9.2.1. Plan de Continuidad Operacional (BCP) y Plan de Recuperación ante Desastres (DRP)

Cada institución debe desarrollar un Plan de Continuidad de Negocio (BCP, por sus siglas en inglés) específico para el sector salud, integrado con un Plan de Recuperación ante Desastres (DRP), que contemple los siguientes elementos:

- **Análisis de Impacto en el Negocio (BIA):**

- Identificar las funciones críticas que deben mantenerse operativas en todo momento, como el acceso a los historiales médicos de los pacientes, la administración de tratamientos y la operación de dispositivos médicos.
- Determinar el tiempo máximo tolerable de inactividad (RTO - Recovery Time Objective) y el punto de recuperación de los datos (RPO - Recovery Point Objective) para cada servicio crítico.

- **Estrategias de Respaldo y Recuperación:**
  - Asegurar que se implementen respaldos regulares y se mantengan en ubicaciones seguras (preferiblemente en la nube o en centros de datos redundantes).
  - Tener un plan de recuperación ante desastres que incluyan la restauración de sistemas críticos.
  - Desarrollar un plan detallado de recuperación ante desastres (DRP) que abarque la restauración de sistemas críticos, la recuperación de datos al punto definido por el RPO y la reanudación de servicios dentro del RTO establecido.
- **Planes de Emergencia:**
  - Desarrollar planes específicos para situaciones de emergencia, como desastres naturales, fallos en la infraestructura, o ciberataques que puedan afectar la operación de la institución.
  - Establecer procedimientos claros para la evacuación de datos y la reubicación temporal de servicios en centros alternativos si es necesario.

9.2.2. Monitoreo de la Continuidad Operacional

El monitoreo continuo es clave para asegurar la efectividad del plan de continuidad operacional. Las instituciones deben implementar sistemas que permitan:

- Monitorear la salud de los sistemas críticos en tiempo real, con alertas automáticas si algún sistema falla o se ve comprometido.
- Verificar periódicamente que los respaldos se estén realizando de acuerdo con el cronograma y que los procedimientos de recuperación sean efectivos.
- Realizar simulacros regulares para poner a prueba la respuesta ante incidentes y la efectividad de los planes de recuperación de manera constante.

10. CIBERSEGURIDAD EN DISPOSITIVOS MEDICOS IoT

Los dispositivos médicos que cuentan con conectividad a redes (IoT) son una parte esencial de la infraestructura tecnológica en el Sector Salud. Se integran directamente en procesos clínicos clave y en el cuidado de los pacientes. Debido a su naturaleza interconectada y a la sensibilidad de los datos de salud que manejan, es crucial que estos dispositivos cumplan con estrictos estándares de seguridad de la información y ciberseguridad.
En el ámbito del Sector Salud, los dispositivos IoT abarcan una amplia variedad de equipos y sistemas, que incluyen, pero no se limitan a:

DEPARTAMENTO TIC VISADO

- Equipos médicos conectados para el monitoreo continuo de signos vitales, administración precisa de fluidos y medicamentos (bombas de infusión), soporte ventilatorio (ventiladores) y regulación cardíaca (marcapasos).
- Dispositivos portátiles diseñados para la realización de diagnósticos en diversos entornos.
- Dispositivos implantables y conectados como marcapasos y desfibriladores, que requieren una gestión segura de sus comunicaciones.
- Equipos de imagenología con capacidades de telemetría para la transmisión y análisis remoto de imágenes diagnósticas.
- Sensores corporales portátiles o vestibles (wearables) utilizados para el seguimiento de parámetros fisiológicos.
- Sistemas integrales para el monitoreo remoto de pacientes en sus hogares o en centros de atención extendida.
- Dispositivos inteligentes implementados en entornos críticos como quirófanos, unidades de cuidados intensivos y ambulancias, que pueden controlar funciones vitales o asistir en procedimientos complejos.
- Equipos de diagnóstico avanzados con funcionalidades de conectividad y generación automática de reportes.
- Sensores y dispositivos vestibles para el seguimiento remoto de la condición de pacientes crónicos o en rehabilitación.
- Infraestructura inteligente dentro de los establecimientos de salud, como cámaras de seguridad conectadas, refrigeradores biomédicos con monitoreo de temperatura, y estaciones clínicas inteligentes para el acceso a información del paciente.
- Estos dispositivos IoT tienen la capacidad de recolectar y transmitir información de salud altamente sensible, lo que los sitúa bajo la rigurosa supervisión de normativas de seguridad y privacidad tanto a nivel internacional como nacional.

Es fundamental considerar:

La gestión de los dispositivos IoT en el sector de la salud necesita un enfoque integral que considere tanto la ciberseguridad como el cumplimiento de normativas vigentes. Esto significa que se deben implementar medidas técnicas y organizativas, como llevar un inventario detallado de los dispositivos, segmentar la red para mantenerlos aislados de otros sistemas, asegurar la autenticación de dispositivos y usuarios, aplicar actualizaciones de seguridad de manera regular, monitorear continuamente su actividad, cifrar los datos que transmiten y almacenan, mantener un registro de eventos relevantes para la seguridad, y desarrollar planes de respuesta específicos para incidentes relacionados con estos dispositivos.

La conexión de estos dispositivos a través de redes locales o Internet con otros sistemas clínicos, como HIS, RIS y PACS, trae consigo mejoras notables en la eficiencia y la calidad de la atención médica. Sin embargo, esta conectividad también plantea nuevos y complejos riesgos en cuanto a la seguridad de la información y la ciberseguridad, los cuales deben ser gestionados de manera proactiva.

La gestión efectiva de los riesgos relacionados con el IoT en el ámbito de la salud implica implementar medidas de protección específicas, tal como se indica en las guías y regulaciones actuales emitidas por el Ministerio de Salud, de acuerdo con:

10.1. Instrucciones de Seguridad para Dispositivos Médicos IoT:

Al momento de adquirir, implementar y operar dispositivos médicos IoT, las instituciones del sector deben tener en cuenta las siguientes instrucciones de seguridad:

- **Inventario y Gestión de Activos**: Implemente y mantenga un inventario de todos los dispositivos IoT médicos conectados a las redes institucionales. Este inventario debe registrar la ubicación física del dispositivo, el fabricante, modelo específico, versión de firmware instalada y el personal responsable de su gestión y mantenimiento.

- **Segmentación de Red y Accesos Controlados:** Implemente una arquitectura de red segmentada, tanto a nivel lógico (VLANs) como físico (aislamiento de puertos), para confinar los dispositivos IoT en redes separadas de otros sistemas críticos. Controle el acceso a estas redes mediante la configuración de listas de control de acceso (ACLs) y firewalls con reglas específicas que limiten la comunicación solo a los servicios y sistemas necesarios para su funcionamiento.

- **Control de Acceso y Autenticación Segura:** Establezca mecanismos de autenticación robustos para acceder a la configuración y la información de los dispositivos IoT. Deshabilite las credenciales predeterminadas de fábrica de manera inmediata y prohíba el uso de contraseñas débiles. Cuando las capacidades del dispositivo lo permitan, habilite la autenticación multifactor (MFA) para una mayor seguridad.

- **Gestión de Vulnerabilidades y Actualizaciones**: Requiera a los proveedores la entrega regular de parches de seguridad y actualizaciones de firmware para sus dispositivos, junto con la documentación de las pruebas de seguridad que hayan realizado. Las áreas de TI y clínica designadas deberán planificar, probar (en entornos no productivos cuando sea factible) e implementar estas actualizaciones, manteniendo un registro detallado del proceso.

- **Monitoreo y Registro de Actividades**: Implemente soluciones de monitoreo continuo del comportamiento de los dispositivos médicos IoT. Estas soluciones deben ser capaces de detectar accesos no autorizados, modificaciones en la configuración, patrones de tráfico anómalos y otros indicadores de compromiso. Asegure la generación y el almacenamiento seguro de registros de actividad (logs) detallados para facilitar auditorías y análisis forenses.

- **Cifrado de Datos y Comunicaciones**: Asegure que toda la información generada o transmitida por los dispositivos IoT médicos esté protegida mediante cifrado de extremo a extremo. Utilice estándares criptográficos reconocidos internacionalmente y robustos (por ejemplo, TLS 1.2 o superior para comunicaciones de red y AES-256 para datos en reposo cuando sea aplicable, acompañados de conjuntos de cifrados seguros).

DEPARTAMENTO TIC VISADO

- **Pruebas de Seguridad y Evaluaciones de Riesgo**: Antes de la puesta en operación de cualquier dispositivo médico IoT, realice pruebas de penetración y evaluaciones de riesgo específicas para identificar vulnerabilidades y evaluar su impacto potencial. Estas pruebas deben incluir la verificación de la interoperabilidad segura con otros sistemas clínicos o administrativos con los que el dispositivo interactúe.

- **Cumplimiento Normativo y Contratual**: Al establecer contratos con proveedores de dispositivos médicos IoT, incluya cláusulas explícitas que aborden los requisitos de ciberseguridad, en concordancia con la Ley N° 21.663, la Ley N° 21.541 (relativa a la calidad y seguridad de los dispositivos médicos) y las políticas y normativas vigentes del Ministerio de Salud.

- **Plan de Contingencia y Respuesta a Incidentes:** Integre los dispositivos médicos IoT dentro de los planes de continuidad operativa y respuesta a incidentes del establecimiento de salud. Asegure que existan procedimientos específicos para la identificación, contención, erradicación y recuperación de incidentes de seguridad que puedan afectar la disponibilidad o la integridad de estos dispositivos, manteniendo la trazabilidad y la comunicación oportuna de estos eventos.

11. SEGURIDAD EN TELEMEDICINA

La telemedicina, como prestación de servicios de salud a distancia a través de tecnologías de la información y la comunicación (TIC), se ha convertido en una parte fundamental del sector salud. Su uso no solo mejora el acceso a la atención médica, sino que también hace que los servicios sean más eficientes, permitiendo una atención más rápida, personalizada y ajustada a las necesidades de cada paciente.

Sin embargo, la telemedicina trae consigo nuevos retos en cuanto a la seguridad de la información y la ciberseguridad. Esto se debe a la criticidad de los datos de salud que se manejan, la variedad de tecnologías que se utilizan y los riesgos que conlleva la transmisión y el almacenamiento de esta información a distancia. Estos retos requieren una atención especial para garantizar la confidencialidad, integridad y disponibilidad de los datos.

Este capítulo detalla las pautas y controles de seguridad que las instituciones del sector salud deben poner en práctica para asegurar la protección de la información en el ámbito de la telemedicina. Esto abarca el cumplimiento de la Ley N° 21.541 y la NORMA TÉCNICA N° 237 del Minsal, que establecen los estándares relacionados con las acciones y servicios de salud a distancia y telemedicina.

11.1. Controles de Seguridad para la Telemedicina

Para asegurar la protección de la información en el ámbito de la telemedicina, las instituciones del sector salud deben considerar las siguientes directrices y controles de seguridad específicos:

Autenticación Robusta: Implementar autenticación multifactor (MFA) para todos los usuarios (pacientes, profesionales, administrativos) que accedan a las plataformas de telemedicina.

- Utilizar mecanismos de autenticación que cumplan con los estándares de seguridad establecidos por la normativa ministerial.
- Considerar la autenticación biométrica cuando sea apropiado y factible.

Autorización y Control de Acceso: Definir y aplicar políticas de control de acceso basadas en roles y privilegios mínimos, asegurando que cada usuario acceda solo a la información necesaria para su función.

- Gestionar los accesos de usuarios de manera centralizada y eficiente, incluyendo la creación, modificación y revocación de cuentas.
- Implementar mecanismos de bloqueo automático de sesión por inactividad.

Confidencialidad de la Información: Cifrar las comunicaciones de telemedicina de extremo a extremo, utilizando protocolos seguros y actualizados (ej., TLS 1.2 o superior).

- Proteger la información de salud transmitida y almacenada, tanto en reposo como en tránsito, mediante técnicas de cifrado adecuadas.
- Asegurar que las plataformas de telemedicina cumplan con los requisitos de confidencialidad establecidos en la Ley N° 19.628 (Protección de la Vida Privada) y otras normativas aplicables.

Integridad de la Información: Implementar mecanismos de verificación de la integridad de los datos para detectar cualquier alteración o manipulación no autorizada durante la transmisión y almacenamiento.

- Utilizar firmas digitales u otros mecanismos de autenticación de origen para validar la identidad del emisor de la información.
- Garantizar la integridad de los metadatos asociados a las transacciones de telemedicina.

Disponibilidad de los Servicios: Implementar medidas de redundancia y contingencia para asegurar la disponibilidad continua de los servicios de telemedicina.

- Establecer planes de recuperación ante desastres para minimizar el tiempo de inactividad en caso de fallos o incidentes.
- Monitorear el rendimiento y la disponibilidad de las plataformas de telemedicina y tomar medidas proactivas para prevenir interrupciones.

Videoconferencia Segura: Los sistemas de videoconferencia deben contar con protocolos seguros de acceso de usuario para minimizar riesgos de intrusiones y suplantaciones.

- Implementar cifrado robusto para la comunicación de video y voz, asegurando la inaccesibilidad de las conversaciones para terceros.
- Establecer mecanismos de verificación de la integridad de los datos en la comunicación de video y voz.
- Implementar protocolos de identificación de origen y destino en el enrutamiento de mensajes para validar la identidad del paciente y el profesional.

- Contar con servicios de registro y custodia segura de las videoconferencias para auditorías posteriores.

Almacenamiento Seguro de Datos: Almacenar los datos de telemedicina (incluyendo grabaciones, registros, etc.) en repositorios seguros, con controles de acceso estrictos y cifrado.

- Definir políticas de retención y eliminación de datos de acuerdo con la normativa vigente.
- Realizar copias de seguridad periódicas de los datos y almacenarlas en ubicaciones seguras.

Gestión de Incidentes: Establecer un plan de respuesta a incidentes de seguridad específico para la telemedicina, que incluya procedimientos para la detección, contención, erradicación, recuperación y notificación de incidentes.

- Definir los roles y responsabilidades del personal en la gestión de incidentes.
- Implementar mecanismos de monitoreo y alerta temprana para detectar posibles incidentes de seguridad.

Auditoría y Trazabilidad: Implementar registros de auditoría detallados de todas las actividades relevantes en las plataformas de telemedicina.

- Realizar auditorías periódicas para verificar el cumplimiento de las políticas y controles de seguridad.
- Conservar los registros de auditoría durante el tiempo requerido por la normativa.

Cumplimiento Normativo: Asegurar que las prácticas de telemedicina cumplan con la Ley N° 21.541, la Norma Técnica N° 237, la Ley N° 19.628, la Ley N° 21.663 y otras regulaciones aplicables.

- Mantenerse actualizado sobre los cambios en la normativa y adaptar las prácticas de seguridad en consecuencia.

12. INNOVACION Y TENDENCIAS EN CIBERSEGURIDAD

Es fundamental impulsar la adopción de nuevas tecnologías, enfoques y buenas prácticas de ciberseguridad en el sector salud, basándonos en normativas nacionales (Ley N° 21.663, Ley N° 21.719), estándares internacionales (ISO 27001, NIST, CIS v8) y marcos regulatorios como HIPAA.

Esto contribuirá a establecer una postura de seguridad que sea resiliente, anticipativa y sostenible. Para fortalecer la ciberseguridad institucional, anticipar amenazas emergentes y adoptar un enfoque proactivo ante los desafíos tecnológicos del entorno digital actual, es necesario considerar y aplicar las siguientes líneas de acción e innovación:

Detección y Respuesta Avanzada con Inteligencia Artificial y Automatización:

- Implementar Herramientas EDR/XDR con IA: Adopte soluciones de Detección y Respuesta en Endpoints (EDR) y Detección y Respuesta Extendida (XDR) que integren análisis de comportamiento basado en Inteligencia Artificial para identificar y responder a amenazas avanzadas de manera proactiva.
- Evaluar Plataformas SOAR: Analice e implemente plataformas de Orquestación, Automatización y Respuesta de Seguridad (SOAR) para automatizar los flujos de trabajo de respuesta a incidentes, mejorando la eficiencia y reduciendo los tiempos de reacción.
- Aplicar Aprendizaje Automático: Utilice técnicas de Machine Learning dentro de las herramientas de seguridad para optimizar la detección de amenazas y disminuir la cantidad de falsos positivos, permitiendo a los equipos de seguridad enfocarse en alertas genuinas.

Ciberinteligencia Predictiva y Táctica (TI/CTI):

- Anticipar Amenazas con Análisis de Tendencias: Establezca procesos para analizar tendencias de amenazas, datos de inteligencia y reportes del sector para anticipar posibles ataques dirigidos a las instituciones de salud.
- Integrar Plataformas CTI para Threat Hunting: Implemente y utilice plataformas de Ciberinteligencia (TI/CTI) que se integren con herramientas de "caza de amenazas" (Threat Hunting) para buscar proactivamente indicios de actividad maliciosa en la infraestructura.
- Monitorear y Correlacionar IoCs: Establezca mecanismos para monitorear y correlacionar Indicadores de Compromiso (IoCs) provenientes de diversas fuentes para detectar actividad sospechosa en tiempo real.
- Compartir Inteligencia de Amenazas: Participe activamente en el intercambio de información sobre amenazas con otros Servicios de Salud y entidades relevantes para fortalecer la defensa colectiva.

Exploración de Tecnologías Emergentes (Blockchain):

- Evaluar Uso de Tecnología Blockchain para Integridad y Trazabilidad: Investigue la viabilidad de utilizar la tecnología blockchain para asegurar la integridad, trazabilidad y transparencia en el manejo de datos clínicos y consentimientos informados.
- Probar Pilotos de Blockchain: Realice pruebas piloto para evaluar el uso de blockchain en escenarios como el intercambio seguro de historiales clínicos y la validación de la trazabilidad de consentimientos informados.
- Garantizar Interoperabilidad Segura: Asegure que cualquier implementación de blockchain sea interoperable y segura con los sistemas existentes.

Prevención de Suplantación Digital (Deepfakes y Phishing Avanzado):

- Mitigar Riesgos de Fraude Multimedia: Implemente medidas para mitigar los riesgos de fraude digital derivados de la manipulación multimedia (deepfakes).
- Aplicar Validación Biométrica y Antifraude: Utilice tecnologías de validación biométrica y soluciones antifraude avanzadas para verificar la identidad y prevenir la suplantación.
- Sensibilizar sobre Nuevas Tácticas de Phishing: Eduque al personal sobre las tácticas emergentes de phishing visual y de voz para aumentar su capacidad de detección.
- Monitorear Deepfakes e Imagen Institucional: Establezca procesos para monitorear la posible creación y uso indebido de deepfakes y la imagen institucional en línea.

Incorporación de Ciberinteligencia en la Gestión de Amenazas:

- Integrar Fuentes de Threat Intelligence: Incorpore fuentes de inteligencia de amenazas (Threat Intelligence) en los procesos de monitoreo y análisis de riesgos para obtener información contextual y oportuna sobre las amenazas.
- Participar en Comunidades de Intercambio: Únase y participe activamente en comunidades de intercambio de información sectorial (como los grupos WSSP del sector salud y foros nacionales de ciberseguridad) para compartir y recibir información relevante sobre amenazas y buenas prácticas

Identidad Digital y Autenticación Avanzada:

- Fortalecer Gestión de Identidad y Accesos (IAM): Optimice los sistemas de Gestión de Identidad y Accesos para asegurar un control granular sobre quién tiene acceso a qué recursos.
- Implementar Autenticación sin Contraseñas y Adaptativa: Explore e implemente métodos de autenticación sin contraseñas y autenticación adaptativa que consideren el riesgo del acceso en tiempo real.
- Establecer Roles y Privilegios Temporales: Implemente la asignación de roles y privilegios con duración limitada y mecanismos de trazabilidad para auditoría.
- Usar Identidad Federada (SSO): Explore la implementación de la federación de identidad (Single Sign-On - SSO) entre instituciones de salud para facilitar el acceso seguro y simplificado a recursos compartidos.

Implementación de la Arquitectura de Confianza Cero (Zero Trust Architecture - ZTA):

- Desarrollar Estrategia de Implementación ZTA: Elabore e implemente una estrategia gradual para adoptar el modelo de seguridad Zero Trust, implementando controles de acceso estrictos basados en la identidad del usuario, el contexto de la solicitud y la autenticación continua.
- Asegurar Microsegmentación y Monitoreo Continuo: Implemente la microsegmentación en redes clínicas y administrativas para limitar el radio de impacto de posibles brechas. Asegure la verificación continua de dispositivos y el monitoreo constante de los flujos de red internos.

- Aplicar Control de Acceso Basado en Identidad y Contexto: Implemente políticas de control de acceso dinámicas que consideren la identidad del usuario, su rol, la ubicación, el dispositivo utilizado y la sensibilidad de los datos a los que se intenta acceder.

Refuerzo de la Seguridad en Entornos Multicloud y Servicios SaaS:

- Incorporar Herramientas de Seguridad Cloud: Implemente herramientas de Gestión de Postura de Seguridad en la Nube (CSPM), Protección de Cargas de Trabajo en la Nube (CWPP) y Agentes de Seguridad de Acceso a la Nube (CASB) para asegurar la visibilidad y el control en entornos multicloud y servicios SaaS.
- Establecer Requisitos de Seguridad para Proveedores Cloud: Defina e imponga requisitos mínimos de seguridad para los proveedores de servicios en la nube, en cumplimiento con la Ley N° 21.663, HIPAA y otras normativas aplicables.

Fortalecimiento de la Protección de Tecnologías Operacionales (OT) y Dispositivos IoMT:

- Inventariar y Segmentar Activos IoMT/OT: Identifique, clasifique y mantenga un inventario actualizado de todos los activos de Tecnología Operacional (OT) y dispositivos de Internet de las Cosas Médicas (IoMT). Implemente redes segmentadas y aisladas para su operación.
- Incorporar Detección de Amenazas Específica: Implemente sistemas de detección de amenazas diseñados específicamente para entornos industriales y médicos conectados, que consideren los protocolos y las vulnerabilidades propias de estos sistemas.
- Implementar NAC e IDS para IoMT: Utilice soluciones de Control de Acceso a la Red (NAC) y Sistemas de Detección de Intrusiones (IDS) adaptadas a las características y necesidades de los dispositivos IoMT.
- Restringir Conexiones de Red Innecesarias: Minimice y controle estrictamente las conexiones de red salientes e innecesarias desde y hacia los dispositivos IoMT y OT.

Mejora de la Resiliencia Cibernética Institucional:

- Diseñar y Probar Planes de Continuidad y Recuperación: Desarrolle y pruebe exhaustivamente planes de continuidad operacional (BCP) y recuperación ante desastres (DRP) que consideren escenarios de ciberataques complejos, como ransomware y denegación de servicio distribuido (DDoS).
- Implementar Respaldo Inmutable y Recuperación Orquestada: Adopte soluciones de respaldo de datos inmutables para proteger la información crítica contra el cifrado o la eliminación maliciosa. Implemente y pruebe mecanismos de recuperación orquestada para restaurar los sistemas de manera eficiente tras un incidente.

13. CAPACITACION Y CONCIENTIZACION EN CIBERSEGURIDAD

DEPARTAMENTO TIC VISADO

Todas las instituciones del sector salud deben desarrollar e implementar un programa continuo de capacitación y concientización en ciberseguridad. Este programa debe enfocarse

en fortalecer la cultura de seguridad dentro de la organización, reducir el riesgo humano y garantizar el cumplimiento de las normativas vigentes.

13.1. Plan de Capacitación Anual en Ciberseguridad:

- **Desarrollo e Implementación:** El Área de Seguridad de la Información de la Institución, en colaboración con la Dirección y área de Recursos Humanos, deberá elaborar e implementar un Plan Anual de Capacitación en Ciberseguridad. Este plan cubrirá a la totalidad del personal, incluyendo funcionarios de planta, a contrata, honorarios y proveedores externos que tengan acceso a los sistemas de información institucionales.
- **Niveles de Profundidad Diferenciados:** El plan de capacitación deberá estructurarse en distintos niveles de profundidad, adaptados al perfil de riesgo y responsabilidades de cada grupo de usuarios:
    - Nivel Básico (Usuarios Generales): Módulos introductorios enfocados en la identificación de amenazas comunes y la adopción de prácticas seguras en el uso diario de las tecnologías institucionales.
    - Nivel Intermedio (Personal Técnico No Especializado): Formación que profundice en los conceptos de seguridad y proporcione herramientas prácticas para la protección de los sistemas y datos bajo su responsabilidad.
    - Nivel Avanzado (Personal Técnico Especializado): Capacitación técnica especializada en áreas como gestión de vulnerabilidades, seguridad en entornos cloud, hardening de sistemas, criptografía, implementación y gestión de sistemas de monitoreo de seguridad (SIEM), y procedimientos avanzados de gestión de incidentes.
    - Nivel Directivo: Sesiones informativas y talleres enfocados en el gobierno de la ciberseguridad, la gestión de riesgos cibernéticos, el cumplimiento normativo (Ley N° 21.663, Ley N° 21.719, HIPAA, etc.), y la toma de decisiones estratégicas ante incidentes de alto impacto.

13.2. Módulos Temáticos:

El Plan Anual de Capacitación deberá incluir, como mínimo, los siguientes módulos temáticos, adaptados al nivel de profundidad correspondiente:

- Fundamentos de Seguridad de la Información y Protección de Datos Personales: Introducción a los conceptos clave de confidencialidad, integridad y disponibilidad de la información, así como los principios y normativas fundamentales para la protección de datos personales (Ley N° 19.628 y Ley N° 21.719).
- Uso Seguro de Tecnologías y Redes Institucionales: Directrices para el uso seguro de equipos de escritorio, portátiles, dispositivos móviles, correo electrónico, navegación web, redes inalámbricas institucionales y el acceso remoto seguro.
- Gestión de Contraseñas y Autenticación Segura: Políticas de creación y gestión de contraseñas robustas, la importancia de la rotación periódica y la implementación y uso obligatorio de la Autenticación Multifactor (MFA) para el acceso a sistemas críticos.

- Prevención de Phishing, Ingeniería Social y Malware: Reconocimiento de las diferentes técnicas de phishing y otros ataques de ingeniería social, así como las medidas preventivas contra la infección por software malicioso (virus, ransomware, spyware, etc.).
- Normativa Vigente en Ciberseguridad y Privacidad: Revisión de las leyes, decretos, políticas y normativas internas y externas aplicables en materia de ciberseguridad y protección de la privacidad de los datos.
- Procedimientos de Respuesta ante Incidentes: Protocolos y pasos a seguir para la identificación, reporte y respuesta inicial ante incidentes de seguridad de la información y ciberseguridad, incluyendo los canales de comunicación internos y con la ANCI.

13.3. Capacitación Especializada para Equipos Técnicos y Directivos:

- **Equipos Técnicos:** Deberán recibir formación avanzada y práctica en:
  - Gestión integral de vulnerabilidades (identificación, evaluación, priorización y remediación).
  - Seguridad en la nube (configuración segura de servicios, gestión de identidades y accesos en la nube, cumplimiento).
  - Endurecimiento (hardening) de sistemas operativos, servidores, aplicaciones y dispositivos de red.
  - Implementación y gestión de soluciones de cifrado para datos en tránsito y en reposo.
  - Implementación, configuración y análisis de sistemas de monitoreo de seguridad (SIEM) para la detección y correlación de eventos.
  - Procedimientos avanzados de gestión y respuesta a incidentes complejos.
- **Directivos:** Deberán participar en sesiones de capacitación sobre:
  - Gobernanza de la ciberseguridad y su rol en la estrategia institucional.
  - Gestión de riesgos cibernéticos, incluyendo la evaluación del impacto financiero y reputacional.
  - Cumplimiento normativo y las implicaciones legales de los incidentes de seguridad.
  - Proceso de toma de decisiones estratégicas y comunicación en situaciones de incidentes de alto impacto.

13.3.1. Simulacros y Ejercicios de Ciberseguridad:

- Realización Anual Obligatoria: Se deberá planificar y ejecutar al menos un ejercicio o simulacro de respuesta a incidentes de seguridad por año. Estos simulacros deben involucrar a usuarios clave de diferentes áreas, personal técnico relevante y los responsables de la continuidad operativa.
- Escenarios Realistas: Los simulacros deben basarse en escenarios de amenazas realistas y relevantes para el Sector Salud (ej. ataques de ransomware, filtración de datos, denegación de servicio).

DEPARTAMENTO TIC VISADO

- Documentación y Mejora Continua: Los resultados de cada simulacro deberán ser exhaustivamente documentados, identificando las fortalezas y debilidades en los procesos de respuesta. Se deberán definir y ejecutar acciones de mejora continua basadas en las lecciones aprendidas.

13.3.2. Evaluación y Seguimiento del Aprendizaje:

- Evaluaciones Pre y Post Capacitación: Se implementarán evaluaciones diagnósticas al inicio y pruebas de conocimiento al finalizar cada módulo de capacitación para medir la efectividad del aprendizaje y la retención de la información.
- Registro de Participación: Se deberá mantener un registro centralizado y actualizado de la participación y el cumplimiento del Plan Anual de Capacitación por parte de todos los funcionarios. El cumplimiento de la capacitación será un requisito obligatorio.
- Indicadores de Desempeño y Madurez: Se incorporarán indicadores de desempeño relacionados con la participación en la capacitación y la adopción de prácticas seguras para evaluar la madurez de la cultura de ciberseguridad institucional a lo largo del tiempo.

13.3.3. Materiales y Canales de Difusión:

- Diversificación de Formatos: Se utilizarán diversos formatos de entrega de contenido para maximizar el alcance y la efectividad del aprendizaje, incluyendo sesiones presenciales, módulos de e-learning interactivos, cápsulas informativas concisas, newsletters periódicas con consejos de seguridad y videos explicativos.
- Uso de Medios Digitales Internos: Se aprovecharán los canales de comunicación digital internos (intranet, plataformas de colaboración, correo electrónico institucional) para la difusión continua de materiales educativos y recordatorios sobre las mejores prácticas de ciberseguridad.

13.3.4. Obligatoriedad y Registro Formal:

- Carácter Obligatorio: La participación en las actividades de capacitación en ciberseguridad será de carácter obligatorio para todo el personal y se considerará parte integral de sus obligaciones laborales. El incumplimiento podrá tener las implicaciones que defina la normativa interna.
- Sistema de Registro Centralizado: Se implementará un sistema formal y centralizado para el registro de todas las actividades de formación y concientización realizadas, incluyendo la fecha, el módulo cursado, la duración y el resultado de las evaluaciones (si aplica). Este registro deberá estar disponible para auditorías internas y externas.

14. ARQUITECTURA REFERENCIAL

Todo sistema desarrollado o implementado para el Sector Salud debe estar alineado con la Arquitectura Referencial Ministerial, la cual establece las directrices, estándares y lineamientos arquitectónicos de referencia. Esta arquitectura es clave para garantizar que las soluciones tecnológicas sean interoperables, escalables, seguras y fácilmente integrables en el ecosistema tecnológico institucional. Las instituciones del sector salud deberán considerar las siguientes directrices:

- Alineación con la Estrategia Tecnológica: Los sistemas deben diseñarse conforme a los objetivos estratégicos y tecnológicos definidos por el MINSAL, asegurando su contribución a la transformación digital del sector salud.
  - Uso de Estándares y Tecnologías Aprobadas: Todos los desarrollos deben seguir las tecnologías, plataformas, metodologías y patrones de diseño establecidos en la arquitectura referencial ministerial, asegurando uniformidad, robustez y sostenibilidad.
  - Revisión y Aprobación Arquitectónica: Cualquier cambio o excepción relevante a la arquitectura debe ser evaluado y aprobado por el equipo de gobernanza tecnológica institucional, asegurando su viabilidad, compatibilidad y control de riesgos.
  - Reutilización y Modularidad: Se debe promover el diseño modular y la reutilización de componentes tecnológicos, con el fin de reducir redundancias, acortar los plazos de desarrollo, mejorar la mantenibilidad y optimizar el uso de recursos.
  - Documentación Técnica Obligatoria: Toda solución tecnológica deberá contar con documentación arquitectónica actualizada que incluya la estructura del sistema, modelo de datos, diagramas de componentes, integraciones y configuraciones clave.

15. INTEROPERABILIDAD

Los sistemas y aplicaciones desarrollados para el sector salud deben cumplir con los requisitos de interoperabilidad definidos por el Ministerio, con el fin de garantizar la integración fluida entre sistemas internos y externos, mejorar la continuidad asistencial y optimizar la gestión clínica y administrativa. Para ello, se deben aplicar las siguientes directrices:

- Cumplimiento de Estándares HL7: Los sistemas deberán ser compatibles con los estándares HL7 vigentes, incluyendo HL7 v2.x y HL7 FHIR (R4 o superiores), promoviendo la interoperabilidad semántica y técnica entre sistemas de información de salud.
- Protocolos y Formatos de Intercambio Seguros: Se deberá emplear protocolos estandarizados como HTTPS, SFTP, REST, GraphQL y formatos como JSON o XML, asegurando una comunicación estructurada, confiable y protegida.
- Desarrollo de APIs Documentadas: Toda solución debe exponer APIs bien documentadas y estandarizadas que faciliten la integración funcional entre sistemas de salud, asegurando consistencia, trazabilidad y escalabilidad.

DEPARTAMENTO TIC VISADO

- Compatibilidad con la Arquitectura Empresarial: Los desarrollos deben ajustarse a la arquitectura empresarial institucional vigente, respetando las capas tecnológicas, dominios funcionales y plataformas habilitadoras establecidas.
- Gestión de Datos Normalizados: La interoperabilidad exige que los datos estén estructurados y normalizados conforme a catálogos, códigos y estándares reconocidos por el sector salud, preservando la integridad y consistencia clínica.
- Pruebas de Interoperabilidad: Es obligatorio realizar pruebas de interoperabilidad durante el ciclo de desarrollo, incluyendo pruebas funcionales, de seguridad y de rendimiento, asegurando una integración efectiva entre los distintos sistemas.

16. USO DE INTELIGENCIA ARTIFICIAL (IA)

El uso de la Inteligencia Artificial (IA) en el sector salud ofrece enormes ventajas, pero también plantea retos importantes en términos de seguridad, privacidad y ética. Es crucial que las instituciones sigan pautas claras y rigurosas para garantizar que la implementación de la IA sea segura, auditable y cumpla con la legislación vigente. La colaboración entre los proveedores de tecnología y las instituciones de salud es clave para alcanzar el éxito y fomentar la confianza en estos sistemas.

Cuando se trata de contratos o desarrollos tecnológicos en el ámbito de la salud que impliquen el uso de Inteligencia Artificial (IA), las instituciones del sector salud deben cumplir con los más altos estándares éticos, legales, técnicos y de seguridad.

Las siguientes directrices serán de cumplimiento obligatorio para los proveedores y responsables institucionales del proyecto:

- Auditabilidad y Explicabilidad: Los algoritmos utilizados deben ser auditables y explicables. El proveedor deberá garantizar que, ante requerimiento, se puedan comprender las decisiones automatizadas que afectan procesos clínicos o administrativos.
- Cumplimiento Normativo: La implementación de IA deberá cumplir con las leyes vigentes, incluyendo la Ley N° 21.663 sobre Ciberseguridad, la Ley N° 21.719 sobre Protección de Datos Personales, la Ley N° 21.541 sobre Telemedicina y la Circular N° 711/2023 de SEGPRES sobre uso de IA en el sector público.
- Evaluación y Gestión de Riesgos: Los proveedores deberán identificar y mitigar los riesgos relacionados con la seguridad, privacidad, equidad y sesgo algorítmico, a través de evaluaciones periódicas de impacto.
- Supervisión y Revisión de Resultados: Se deberán implementar mecanismos para la supervisión continua de los sistemas de IA, garantizando que sus resultados no sean discriminatorios ni generen impactos adversos en pacientes, usuarios o profesionales de la salud.

- Derechos de los Usuarios: Se debe permitir a los usuarios cuestionar, corregir o apelar decisiones tomadas por sistemas de IA, además de facilitar el ejercicio de los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) cuando corresponda.
- Responsabilidad y Remediación: El proveedor será responsable de los resultados generados por los sistemas de IA, debiendo corregir fallas, vulnerabilidades o impactos negativos derivados de su uso, asegurando la continuidad y confianza en los servicios digitales del sector salud.

16.1. Casos de Uso de la IA en el Sector Salud y los Riesgos Asociados

- IA para el Diagnóstico: Los sistemas de IA pueden ser utilizados para apoyar en el diagnóstico de enfermedades mediante el análisis de imágenes médicas o el procesamiento de datos de pacientes. Sin embargo, uno de los principales riesgos asociados es el sesgo en los algoritmos, lo que puede llevar a diagnósticos erróneos o a la falta de detección de ciertas condiciones. También existe el riesgo de falta de transparencia en cómo los algoritmos toman decisiones, lo que podría generar desconfianza en los profesionales de la salud.
- IA para el Tratamiento: Los sistemas de IA también pueden sugerir opciones de tratamiento basadas en los datos del paciente y en algoritmos predictivos. Sin embargo, los errores en las recomendaciones debido a la calidad deficiente de los datos o la falta de validación clínica pueden poner en peligro la seguridad del paciente. Es fundamental que las recomendaciones generadas por IA sean validadas por expertos médicos antes de ser implementadas.
- IA para la Gestión de la Salud Pública: En el ámbito de la gestión de la salud pública, la IA puede ayudar a predecir brotes de enfermedades y optimizar recursos. No obstante, existe el riesgo de uso indebido de los datos personales de los pacientes y preocupaciones sobre la privacidad. Los sistemas de IA deben estar diseñados para garantizar que la información de los pacientes se utilice de manera ética y legal.

16.2. Consideraciones de Seguridad y Privacidad en el Uso de IA en Salud

- Requisitos de Seguridad para los Datos Utilizados para Entrenar los Algoritmos de IA: Los datos utilizados para entrenar los algoritmos de IA deben ser almacenados y procesados de acuerdo con los más altos estándares de seguridad, garantizando su cifrado y protección contra accesos no autorizados. Esto incluye el uso de entornos seguros para el procesamiento de los datos y la implementación de controles de acceso estrictos.
- Mecanismos para Garantizar la Transparencia y Explicabilidad de los Algoritmos: Los proveedores de soluciones de IA deben implementar mecanismos que permitan la trazabilidad y auditabilidad de los algoritmos, lo que facilita que los resultados puedan ser explicados a los profesionales de la salud y pacientes cuando sea necesario.

- Medidas para Proteger la Privacidad de los Pacientes al Utilizar Sistemas de IA: Se deben adoptar medidas de anonimización y pseudonimización de los datos de los pacientes antes de ser utilizados para entrenar los algoritmos de IA. También deben implementarse políticas que regulen el consentimiento explícito de los pacientes para el uso de sus datos en estos sistemas.
- Consideraciones Éticas y Legales en el Uso de la IA en Salud: El uso de la IA debe estar alineado con principios éticos que respeten la dignidad y los derechos humanos de los pacientes. Además, se deben considerar las implicaciones legales de la implementación de IA, asegurando que el uso de los datos personales y de salud cumpla con las leyes de protección de datos y privacidad vigentes.

17. AUDITORÍA Y CUMPLIMIENTO DEL SGSI

La auditoría y el cumplimiento son fundamentales para asegurar que un Sistema de Gestión de Seguridad de la Información (SGSI) funcione de manera efectiva en las Instituciones del sector salud. Realizar auditorías de forma regular ayuda a detectar fallas en los controles de seguridad, a evaluar cómo se está cumpliendo con las políticas internas y las normativas externas, y a garantizar que siempre se esté mejorando en la protección de la información sensible de los pacientes.

A continuación, se presentan los tipos de auditorías que se recomiendan y las pautas para llevarlas a cabo, con el fin de asegurar que se cumplan las normativas, así como los estándares éticos y técnicos en la gestión de la seguridad de la información en el sector salud.

17.1. Tipos de Auditorías Recomendadas

- Auditorías Internas: Realizadas por el personal de la institución, con el fin de evaluar la efectividad de los controles de seguridad y detectar áreas de mejora.
- Auditorías Externas: Llevadas a cabo por auditores independientes para obtener una evaluación imparcial del SGSI.

Auditorías de Cumplimiento: Dirigidas a verificar el cumplimiento con regulaciones específicas, como la Ley N° 21.663 y otras normativas locales e internacionales.

17.2. Frecuencia de las Auditorías y Criterios para la Selección de Auditores

- Frecuencia: Las auditorías internas deben hacerse al menos una vez al año, mientras que las externas y de cumplimiento se realizan cada dos años o según las regulaciones pertinentes.

- Criterios para Selección de Auditores: Los auditores internos deben tener conocimientos en seguridad de la información, ser imparciales y contar con formación en auditoría. Los auditores externos deben ser profesionales independientes con experiencia en el sector salud y certificaciones adecuadas, mientras que los auditores de cumplimiento deben estar especializados en las normativas aplicables.

18. INDICADORES DE SEGURIDAD DE LA INFORMACION Y CIBERSEGURIDAD

La evaluación sistemática, el control efectivo y la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), así como de las medidas de ciberseguridad en las instituciones del sector salud, requieren un diseño, seguimiento y reporte bien estructurado de Indicadores Clave de Desempeño (KPI) e Indicadores Clave de Riesgo (KRI).

Estos indicadores ofrecen una visión objetiva, cuantificable y periódica sobre el estado de la seguridad de la información y la ciberseguridad a nivel institucional, lo que facilita la toma de decisiones estratégicas y operativas por parte de los responsables de seguridad y la Alta Dirección.

En este contexto, las instituciones del sector salud deben establecer e implementar un conjunto de indicadores que les ayuden a evaluar el nivel de madurez del Sistema de Gestión de Seguridad de la Información (SGSI), la eficiencia en la ejecución de controles, el grado de cumplimiento normativo (Ley N° 21.663, Ley N° 19.628, ISO/IEC 27001:2022, NIST, entre otros), y su capacidad de respuesta ante riesgos relacionados con la seguridad de la información y la ciberseguridad.

Cada indicador debe tener una definición clara, una unidad de medida, una frecuencia de evaluación y una persona responsable para su seguimiento. Los resultados de estas evaluaciones deben presentarse periódicamente al Comité de Seguridad de la Información y a la Alta Dirección, y, cuando sea necesario, informarse a la Agencia Nacional de Ciberseguridad.

Para una propuesta de indicadores aplicables, revisar la tabla contenida en el Anexo, punto 21.6.

19. MECANISMO DE DIFUSIÓN.

La comunicación del presente instructivo 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 el sitio web Minsal http://www.Minsal.cl/seguridad_de_la_informacion/
- Publicación en la intranet de Minsal http://isalud.Minsal.cl/
- Correo informativo.

20. CONTROL DE VERSIONES

Versión	Fecha	Pág. o Sección modificada	Motivo del cambio
01		Todas	Creación del documento
02	Abril 2025	Todas	Adaptación normativa nacional y estándares internacionales en materia de Seguridad de la Información y Ciberseguridad

21. ANEXOS

21.1. Definiciones y términos claves.

Para los efectos de la aplicación de este documento, los términos que a continuación se señalan tendrán el significado que se indica:

- **Activos de información:** toda información o recurso relacionado para la creación, almacenamiento, gestión o transmisión de dicha información. Podrán ser activos materiales (RRHH especializados, aparatos, equipos, redes, instalaciones, soportes y sistemas de almacenamiento) o intangibles (datos, aplicaciones, sistemas operativos, bases de datos, imagen, reputación, marcas de la organización).
- **Activo informático:** toda información almacenada en una red y sistema informático que tenga valor para una persona u organización.
- **Autenticación**: propiedad de la información que da cuenta de su origen legítimo.
- **Anonimización**: procedimiento irreversible en virtud del cual un dato personal no puede vincularse o asociarse a una persona determinada, ni permitir su identificación, por haberse destruido o eliminado el nexo con la información que vincula, asocia o identifica a esa persona. Un dato anonimizado deja de ser un dato personal.
- **Agencia**: la Agencia Nacional de Ciberseguridad, que se conocerá en forma abreviada como ANCI.
- **Auditorías de seguridad:** procesos de control destinados a revisar el cumplimiento de las políticas y procedimientos que se derivan del Sistema de Gestión de la Seguridad de la Información.
- **Seudonimización:** tratamiento de datos personales que se efectúa de manera tal que ya no puedan atribuirse a un titular sin utilizar información adicional que permita la re-identificación, la cual debe constar en medios seguros, gestionados por separado, y estar sujeta a medidas técnicas y organizativas destinadas a garantizar que accedan a ella personas sólo personal autorizado por el responsable del tratamiento.

- **Ciberespacio:** El ciberespacio es un ambiente complejo, soportado por hardware y las redes de comunicaciones, en el cual constan interacciones entre personas, software y servicios de Internet, destinados a la distribución mundial de información y comunicación" (ISO 27032).
- **Ciberataque:** Acción realizada con la finalidad de destruir, exponer, alterar, deshabilitar, o exfiltrar u obtener acceso o hacer uso no autorizado de un activo informático.
- **Ciberseguridad:** Preservación de la confidencialidad e integridad de la información y de la disponibilidad y resiliencia de las redes y sistemas informáticos, con el objetivo de proteger a las personas, la sociedad, las organizaciones o las naciones de incidentes de ciberseguridad.
- **Incidente de ciberseguridad**: Todo evento que perjudique o comprometa la confidencialidad o integridad de la información, la disponibilidad o resiliencia de las redes y sistemas informáticos, o la autenticación de los procesos ejecutados o implementados en las redes y sistemas informáticos.
- **Confidencialidad:** Propiedad que consiste en que la información no es accedida o entregada a individuos, entidades o procesos no autorizados.
- **Continuidad de servicios:** Capacidad de un organización para mantener la disponibilidad de sus servicios, reduciendo el riesgo de eventos que puedan dar lugar a una interrupción o inestabilidad en las operaciones de la entidad, manteniendo niveles aceptables de servicios, entendiendo por tales, las prestaciones básicas del sistema que sustentan las operaciones esenciales del servicios y propiciando la recuperación del nivel normal de servicios de tecnologías de la información (TI) en el menor tiempo posible.
- **Disponibilidad**: Propiedad que consiste en que la información es accesible y utilizable cuando es requerida por un individuo, entidad o proceso autorizado.
- **Datos Personales o datos de carácter personal:** los datos relativos a cualquier información concerniente a personas naturales, identificadas o identificables, con independencia de su soporte.
- **Datos Sensibles:** Datos personales que se refieren a características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, entre otros, los hábitos personales, origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.[6]
- **Equipo de Respuesta a Incidentes de Seguridad Informática o CSIRT:** Centros multidisciplinarios que tienen por objeto prevenir, detectar, gestionar y responder a

[6] La ley 21.719, que entrará en vigor el 01 de diciembre de 2026, sustituye la definición de datos sensibles por la siguiente: "Datos personales sensibles: tendrán esta condición aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, que revelen el origen étnico o racial, la afiliación política, sindical o gremial, la situación socioeconómica, las convicciones ideológicas o filosóficas, las creencias religiosas, los datos relativos a la salud, al perfil biológico humano, los datos biométricos, y la información relativa a la vida sexual, a la orientación sexual y a la identidad de género de una persona natural".

DEPARTAMENTO TIC VISADO

incidentes de ciberseguridad o ciberataques, en forma rápida y efectiva, y que actúan conforme a procedimientos y políticas predefinidas, ayudando a mitigar sus efectos.

- **Gestión de incidentes**: Procedimientos para la detección, análisis, manejo, contención y resolución de un incidente de ciberseguridad y responder ante ésta.
- **Incidente:** Evento inesperado o no deseado con consecuencias en detrimento de la seguridad de las redes, equipos y sistemas de información (véase también ciberincidente).
- **Infraestructura crítica**: las instalaciones, sistemas físicos o servicios esenciales y de utilidad pública, redes, servicios y equipos físicos y de tecnología de la información cuya afectación, degradación, denegación, interrupción o destrucción cause un grave daño a la salud o al abastecimiento de la población, a la actividad económica esencial, al medioambiente o a la seguridad del país. Se entiende por este concepto la infraestructura indispensable para la generación, transmisión, transporte, producción, almacenamiento y distribución de los servicios e insumos básicos para la población, tales como energía, gas, agua o telecomunicaciones; la relativa a la conexión vial, aérea, terrestre, marítima, portuaria o ferroviaria, y la correspondiente a servicios de utilidad pública, como los sistemas de asistencia sanitaria o de salud.
- **Integridad:** Propiedad que consiste en que la información no ha sido modificada o destruida sin autorización.
- **Nube privada:** La infraestructura de la nube se aprovisiona para uso exclusivo de una única organización aun cuando comprenda múltiples unidades de dicha organización. Puede ser propiedad, administrado y operado por la organización, un tercero o una combinación de ellos, y puede existir dentro o fuera de las instalaciones de la organización.
- **Nube pública:** La infraestructura y los recursos lógicos que forman parte del entorno se encuentran disponibles para el público en general a través de Internet. Suele ser propiedad de un Prestador de Servicios que gestiona la infraestructura y el servicio o servicios que se ofrecen.
- **Protección de los activos de información:** Adopción de las medidas que resguarden la seguridad física de los dispositivos, así como los accesos a éstos.
- **Red y sistema informático:** conjunto de dispositivos, cables, enlaces, enrutadores u otros equipos de comunicaciones o sistemas que almacenen, procesen o transmitan datos digitales.
- **Resiliencia:** Capacidad de las redes y sistemas informáticos para seguir operando luego de un incidente de ciberseguridad, aunque sea en un estado degradado, debilitado o segmentado, y la capacidad de las redes y sistemas informáticos para recuperar sus funciones después de un incidente de ciberseguridad.
- **Riesgo:** posibilidad de ocurrencia de un incidente de ciberseguridad; la magnitud de un riesgo es cuantificada en términos de la probabilidad de ocurrencia del incidente y del impacto de las consecuencias de este.
- **Riesgo de Ciberseguridad:** Toda circunstancia o hecho razonablemente identificable y previsible, que tenga un posible efecto adverso en la seguridad de las redes, equipos y sistemas de información. Se puede cuantificar como la probabilidad de materialización de

una de las amenazas antes mencionadas que produzca un impacto en términos de operatividad, o de integridad, confidencialidad o disponibilidad de datos.

- **Seguridad de la información:** Conjunto de medidas preventivas y reactivas de los organismos administradores y sus respectivos sistemas tecnológicos, que tienen por objeto resguardar y proteger la información, asegurando la confidencialidad, integridad, autenticidad y disponibilidad de los datos, continuidad de servicios y protección de activos de información.
- **Tratamiento de datos:** cualquier operación o conjunto de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan de cualquier forma recolectar, procesar, almacenar, comunicar, transmitir o utilizar datos personales o conjuntos de datos personales.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotado por una o más amenazas informáticas.

21.2. Normativa sobre seguridad de la información.

21.2.1. Normativa del sector salud:

- DFL Nº 1, de 24 de abril de 2006, Ministerio de Salud, que fija el texto refundido, coordinado y sistematizado del Decreto Ley Nº 2.763, de 1979 y de las leyes Nº 18.933 y 18.469;
- DFL Nº 725, Ministerio de Salud, Código Sanitario;
- Ley N°19.966, de 2004, que establece un régimen de garantías de salud;
- Ley N° 19.650, que perfecciona normas del área de la salud;
- Ley N° 20.120 de 22 de septiembre de 2006, sobre la investigación científica en el ser humano, su genoma, y prohíbe la clonación humana y demás normativa del área de la salud.
- Ley N°20.584, referida a Deberes y Derechos que tienen las Personas en relación con acciones vinculadas a su Atención de Salud;
- Ley N° 20.724, de 2014, que modifica el Código Sanitario en materia de regulación de medicamentos;
- Ley N° 20.850, de 2016, que crea un sistema de protección financiera para diagnósticos y tratamientos de alto costo y rinde homenaje póstumo a don Luis Ricarte Soto Gallegos;
- Ley N° 21.258, de 2020, que crea la ley nacional del cáncer, que rinde homenaje póstumo al doctor Claudio Mora.
- Ley 21.541, de 17 de marzo de 2023, que modifica la normativa que indica para autorizar a los prestadores de salud a efectuar atenciones mediante telemedicina.
- Decreto Nº 41, de 24 de julio de 2012, del Ministerio de Salud, Reglamento de Ficha Clínica;
- Decreto Nº 31 de 15 de junio de 2012, del Ministerio de Salud, Reglamento sobre entrega de información y expresión de consentimiento informado en las atenciones de salud;
- Decreto N° 38, de 2005, del Ministerio de Salud, Reglamento Orgánico de los establecimientos de salud de menor complejidad y de los establecimientos de autogestión en red.

- Decreto N° 38, de 26 de diciembre de 2012, del Ministerio de Salud, que aprueba Reglamento sobre derechos y deberes de las personas en relación con las actividades vinculadas con su atención de salud.
- Decreto N° 38, de 2013, del Ministerio de Salud, que modifica decreto N° 466 de 1984, Reglamento de Farmacias, Droguerías, almacenes farmacéuticos, botiquines y depósitos autorizados.
- Decreto N° 6, de 16 de abril de 2021, del Ministerio de Salud, Reglamento sobre acciones de vinculadas a la atención de salud realizadas a distancia.
- Decreto N° 820, 2011, Ministerio de Salud.

21.2.2. En materia de documentos electrónicos:

- Ley N°19.880/2003: Ley que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la administración del Estado. Esta ley es importante porque establece condiciones sobre los plazos y la forma en que los servicios públicos deben responder frente a requerimientos de ciudadanos y de otros servicios públicos.
- Ley N° 21.180, de transformación digital del Estado.
- Ley N° 19.799 de 12 de abril de 2002, de firmas y documentos electrónicos.
- Decreto N° 181, que aprueba Reglamento de la ley N° 19799 sobre documentos electrónicos. Firma electrónica y la certificación de dicha firma.
- Decreto N°83, de 2005, del Ministerio secretaría General de la Presidencia,
- Decreto Nº 14, de 2014, del Ministerio secretaría General de la Presidencia, el decreto Nº 1 de 2015, del Ministerio secretaría General de la Presidencia.
- Decreto N° 4, 2021, Ministerio Secretaría General de la Presidencia, Reglamento que regula la forma en que los procedimientos administrativos deberán expresarse a través de medios electrónicos, en las materias que indica, según lo dispuesto en la ley Nº 21.180 sobre transformación digital del estado.
- Decreto N° 24, 2019, Ministerio de Economía, que aprueba norma técnica para la prestación del servicio de certificación de firma electrónica avanzada.
- Decreto N° 1, 2015, Ministerio Secretaría General de la Presidencia, aprueba norma técnica sobre sistemas y sitios web de los órganos de la administración del estado.

21.2.3. En materia de seguridad de la información:

- Ley N° 21.663 sobre Marco de Ciberseguridad, esta ley proporciona un marco para asegurar la ciberseguridad de infraestructuras críticas.
- Decreto N° 295, de 2024, del Ministerio del Interior y Seguridad Pública: Aprueba reglamento de reporte de incidentes de ciberseguridad de la ley N° 21.633.
- Decreto N°483, de 2024, del Ministerio del Interior y Seguridad Pública: Aprueba Reglamento que determina la estructura interna de la Agencia Nacional de Ciberseguridad.
- Decreto N°164, de 2023, del Ministerio del Interior y Seguridad Pública: Aprueba Política Nacional de Ciberseguridad 2023-2028.

- Decreto Supremo N° 7, 2023, Ministerio secretaría General de la Presidencia, que establece una Norma Técnica de Seguridad de la Información y Ciberseguridad, en concordancia con la Ley Nº 21.180
- Decreto Supremo N° 83, 2005, Aprueba norma técnica para los órganos de la administración del estado, sobre seguridad y confidencialidad de los documentos electrónicos.
- Decreto N°273, 2022, Ministerio del Interior y Seguridad Pública, Establece obligación de reportar incidentes de ciberseguridad.
- Circular N° 711/2023 establece lineamientos sobre el uso de herramientas de inteligencia artificial (IA) en el sector público de Chile, proporcionando directrices para una implementación ética, segura y transparente de estas tecnologías en servicios gubernamentales. Con el objetivo de asegurar que las aplicaciones de IA en el sector público se alineen con los valores de protección de derechos, transparencia y seguridad de la información, además de fomentar la eficiencia y mejorar la calidad de los servicios público.
- Resolución Exenta N°372/2025 que aprueba texto de las recomendaciones del Consejo para la Transparencia sobre Transparencia Algorítmica y Oficio N°7286/2025 Guía del Consejo para la Transparencia para la adopción de las Recomendaciones sobre Transparencia Algorítmica.

21.2.4. En materia de protección de datos personales:

- Art. 19 Nos. 1 y 4 de la Constitución Política de la República.
- Ley N°19.628/1999: Sobre protección de la vida privada, que define dato personal, dato personal sensible, y establece las condiciones debe cumplir toda entidad que maneje estos datos.
- Ley N° 21.719/2024: Que modifica la ley N° 19.628, sustituyendo su nombre por "Ley de Protección de Datos Personales" y actualiza las normas de este cuerpo normativo de acuerdo con los estándares actualmente vigentes. Esta ley entra en vigor el 1 de diciembre de 2026.
- Ley N° 20.575 sobre el principio de finalidad en el tratamiento de datos personales.
- Decreto N° 779, de 2000, que Aprueba Reglamento del Registro de Bancos de Datos Personales a cargo de organismos públicos.
- Resolución Exenta N° 489, 2022, Consejo para la Transparencia, Aprueba procedimiento para la tramitación de solicitudes de ejercicio de derechos de la ley N° 19.628, sobre protección a la vida privada.

21.2.5. En materia de delitos informáticos:

DEPARTAMENTO TIC VISADO

- Ley N°21.459/2022: 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. Esta ley establece los delitos informáticos reconocidos en Chile.
- Ley N°20.009, sobre clonación de tarjetas de crédito.
- Decreto N° 83, de 2017, que promulgó el Convenio de Budapest en Chile. Tratado internacional de combate contra la ciberdelincuencia.

21.2.6. En materia de propiedad Intelectual:

- Ley N° 19.039, de Propiedad Industrial
- Ley N° 17.336, de Propiedad Intelectual. Fija condiciones para la protección de los programas computacionales como propiedad intelectual de sus autores.

21.2.7. Normas de aplicación general:

- Ley 21.542, Que modifica la carta fundamental con el objeto de permitir la protección de infraestructura crítica por parte de las fuerzas armadas, en caso de peligro grave o inminente
- Ley N° 21.180, de transformación digital del Estado;
- Ley N° 19.880 de bases de los procedimientos administrativos;
- Ley N° 20.285 de transparencia y acceso a la información pública;
- Ley N° 19.886 de compras públicas.
- Decreto N° 661 que aprueba reglamento de la Ley N° 19.886, de bases sobre contratos administrativos de suministro y prestación de servicios, y deja sin efecto el decreto supremo nº 250, de 2004, del Ministerio de Hacienda
- Resolución Exenta Nº 619 – B de 26 de noviembre de 2018, de la Dirección de Compras y Contratación Pública.

21.3. Estándares Internacionales y Normativa Nacional en Seguridad de la Información y Ciberseguridad

TEMA	NOMBRE	DESCRIPCIÓN
Seguridad de la información	ISO 27001:2022	Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI).
Seguridad de la información	ISO 27002:2022	Ofrece un conjunto de controles y mejores prácticas para establecer, implementar, mantener y mejorar un sistema de gestión de la seguridad de la información
Seguridad de la información	NIST SP 800-53	La publicación especial 800-53 del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) es un estándar de seguridad

TEMA	NOMBRE	DESCRIPCIÓN
		de la información que proporciona un catálogo de controles de privacidad y seguridad para sistemas de información. Originalmente destinado a agencias federales de EE.
Seguridad de la información	ISO/IEC 27799:2016 (alineada con prácticas europeas)	Aplica los principios de la ISO/IEC 27002 al ámbito de la salud, proporcionando guías específicas para proteger la información de salud personal.
Gestión de riesgos	ISO 31000	Estándar que proporciona principios y directrices para la gestión de riesgos aplicables a cualquier tipo de organización.
Continuidad del negocio	ISO 22301	Define requisitos para establecer y mantener un sistema de gestión de continuidad del negocio ante eventos disruptivos.
Protección de datos	HIPAA (EE.UU.)	Health Insurance Portability and Accountability Act. Ley estadounidense que regula la protección y privacidad de la información de salud en formato electrónico.
Protección de datos	Reglamento General de Protección de Datos (GDPR) - UE 2016/679	Reglamento obligatorio para todos los países de la UE que establece normas estrictas sobre cómo deben manejarse y protegerse los datos personales
Protección de datos	EHRxF (European Electronic Health Record Exchange Format)	Marco promovido por la Comisión Europea para el intercambio de registros electrónicos de salud con interoperabilidad y seguridad.
Protección de datos	Ley N° 19.628	Ley chilena sobre Protección de la Vida Privada, regula el tratamiento de datos personales.
Protección de datos	Ley N° 21.719	Modifica la Ley N° 19.628, incorporando estándares modernos de protección de datos personales.
Protección de datos	European Data Governance Act (DGA)	Establece un marco para el intercambio seguro de datos dentro de la UE, fomentando la reutilización de datos sensibles de forma segura, incluidos los de salud.
Ciberseguridad	NIST Cybersecurity Framework	Marco basado en cinco funciones clave (Identificar, Proteger, Detectar, Responder y Recuperar) para gestionar riesgos de ciberseguridad.
Ciberseguridad	CIS Controls v8	Conjunto de controles priorizados para defenderse contra las amenazas cibernéticas más comunes. Útil para establecer una base mínima de ciberseguridad
Ciberseguridad	ISO/IEC 27035	Proporciona directrices para la gestión de incidentes de seguridad de la información, incluyendo la planificación, detección, respuesta y lecciones aprendidas.
Ciberseguridad	Directiva NIS 2 - UE 2022/2555	Reemplaza la Directiva NIS original, reforzando los requisitos de ciberseguridad para sectores

TEMA	NOMBRE	DESCRIPCIÓN
		críticos, incluyendo salud, con obligaciones más estrictas.
Ciberseguridad	ENISA (Agencia de la Unión Europea para la Ciberseguridad)	Desarrolla buenas prácticas, marcos y herramientas para mejorar la ciberseguridad a nivel europeo; promueve la cooperación entre estados miembros.
Ciberseguridad	Ley N° 21.663	Ley Marco de Ciberseguridad de Chile, establece lineamientos, gobernanza y obligaciones para organizaciones públicas y privadas
Seguridad de redes	ISO/IEC 27033	Proporciona directrices detalladas para implementar la seguridad en redes, incluyendo diseño, gestión y protección de la infraestructura de red.
Salud digital	Ley N° 21.541	Regula la atención médica por medios digitales (telemedicina), incluyendo requisitos de ciberseguridad y protección de datos.
IA y Ética	Circular N° 711/2023 (SEGPRES)	Lineamientos para el uso ético y seguro de herramientas de inteligencia artificial en organismos públicos de Chile.
IA y Ética	AI Act (propuesta)	Marco legal propuesto por la Comisión Europea para regular el desarrollo y uso de sistemas de inteligencia artificial, con foco en ética, transparencia y riesgo.
IA y Ética	Transparencia Algorítmica sobre Sistemas de decisiones automatizadas y semiautomatizadas (SDA)	Recomendaciones del Consejo para la Transparencia sobre Transparencia Algorítmica aprobadas en Resolución Exenta N°372/2025 y Oficio N°7286/2025 Guía del Consejo para la Transparencia para la adopción de las Recomendaciones sobre Transparencia Algorítmica.

21.4. Matriz de Riesgos de Seguridad de la Información en el Sector Salud (ejemplo)

Amenaza	Vulnerabilidad	Impacto Potencial	Control Preventivo	Control Correctivo
Ataques de ransomware	Sistemas desactualizados, falta de parches de seguridad	Inaccesibilidad a datos clínicos críticos, interrupción de servicios de salud	- Actualización periódica de software - Implementación de EDR y antivirus de nueva generación - Segmentación de redes críticas	- Plan de recuperación ante incidentes (IRP) - Restauración desde respaldos verificados

Pérdida o robo de dispositivos móviles	Falta de cifrado de dispositivos, ausencia de MDM (Mobile Device Management)	Fuga de información sensible de pacientes	- Cifrado completo de dispositivos móviles - Gestión de dispositivos móviles (MDM) - Autenticación multifactor	- Borrado remoto de datos - Investigación de incidente y notificación a la autoridad (en caso de ser requerido por la normativa)
Acceso no autorizado a sistemas clínicos	Políticas de acceso débiles, contraseñas compartidas o no robustas	Modificación o exfiltración de datos de pacientes, daño reputacional	- Políticas de control de acceso basadas en roles (RBAC) - Autenticación multifactor (MFA) - Revisiones periódicas de cuentas y permisos	- Bloqueo inmediato de cuentas comprometidas - Análisis forense de acceso y remediación de brechas
Phishing dirigido a personal administrativo o clínico	Falta de capacitación en ciberseguridad, filtros de correo inadecuados	Compromiso de credenciales, infección de malware	- Programas de concienciación en ciberseguridad - Filtros avanzados de correo (antiphishing, antispam)	- Restablecimiento inmediato de contraseñas - Análisis de dispositivos y contención de malware
Fallas en disponibilidad de sistemas críticos (HIS, PACS, LIS)	Ausencia de alta disponibilidad y respaldo de sistemas	Interrupción en diagnósticos, tratamientos, procedimientos clínicos	- Implementación de arquitecturas de alta disponibilidad (HA) - Sistemas de respaldo en caliente y pruebas de recuperación	- Activación de procedimientos de continuidad operativa - Recuperación de servicios desde entornos alternativos

21.5. Estructura de Políticas y Procedimientos (ejemplo)

Categoría ISO/IEC 27001:2022	Política / Procedimiento	Descripción	Procedimientos Asociados
Políticas de Seguridad	Política General de Seguridad de la Información	Establece el marco general de gestión de la seguridad de la información y el compromiso institucional.	Procedimiento de revisión y aprobación de políticas. Procedimiento de difusión institucional.
Organización de la Seguridad	Política de Control de Accesos	Regula el acceso físico y lógico a los sistemas y la información.	Procedimiento de gestión de cuentas de usuario. Procedimiento de revisión periódica de accesos.
Políticas de Seguridad	Política de Uso Aceptable de Recursos	Establece normas para el uso correcto de los recursos tecnológicos institucionales.	Procedimiento de monitoreo del uso de recursos. Procedimiento de sanción por mal uso.
Gestión de Activos	Política de Gestión de Activos	Define cómo identificar, clasificar y proteger los activos de información.	Procedimiento de inventario. Procedimiento de clasificación y etiquetado.
Gestión de Activos	Política de Clasificación y Manejo de la Información	Establece criterios para el uso y protección de la información según su sensibilidad.	Procedimiento de clasificación. Procedimiento de destrucción segura.
Operación	Política de Respaldo y Recuperación	Establece directrices para respaldar y restaurar información crítica.	Procedimiento de respaldos. Procedimiento de prueba de restauración.
Continuidad	Política de Continuidad Operacional y DRP	Asegura disponibilidad frente a interrupciones.	Procedimiento de activación del plan. Procedimiento de pruebas de continuidad.
Seguridad Física y del Entorno	Política de Seguridad Física y Ambiental	Controla acceso físico y protección del entorno.	Procedimiento de control físico. Procedimiento de contingencias ambientales.
Adquisición, desarrollo y mantenimiento	Política de Seguridad en el Ciclo de Vida de los Sistemas	Integra seguridad desde el diseño hasta el retiro de sistemas.	Procedimiento de desarrollo seguro. Pruebas de aceptación.
Relación con Proveedores	Política de Relación con Proveedores	Establece requisitos de seguridad para terceros y contratistas.	Evaluación de proveedores. Acuerdos de confidencialidad.
Gestión de Incidentes	Política de Gestión de Incidentes de Seguridad	Define cómo responder y aprender de incidentes.	Procedimiento de notificación. Análisis post-incidente.

Categoría ISO/IEC 27001:2022	Política / Procedimiento	Descripción	Procedimientos Asociados
Cumplimiento normativo	Política de Protección de Datos Personales	Garantiza cumplimiento de Ley 19.628 en tratamiento de datos.	Procedimiento de gestión de consentimientos. Anonimización.
Comunicaciones	Política de Correos Electrónicos	Normas de uso seguro y profesional del correo institucional.	Prevención de phishing. Cifrado de correos.
Criptografía	Política de Uso de Criptografía	Determina mecanismos de cifrado aceptados para proteger la información.	Procedimiento de cifrado. Gestión de llaves.
Transversal	Procedimientos e Instructivos Técnicos	Instrumentos que detallan cómo implementar los controles definidos por las políticas.	Revisión de cumplimiento técnico. Auditorías internas.

21.6. Indicadores Clave de Desempeño e Indicadores Clave de Riesgo (ejemplo)

Proporciona una lista de ejemplos de métricas de seguridad, tanto a nivel técnico como de gestión:

Categoría / Área	Nombre del Indicador	Objetivo	Fórmula / Métrica	Unidad de Medida	Frecuencia	Meta / Umbral	Umbral de Alerta	Responsable
Capa Física	Porcentaje de cumplimiento de políticas de acceso físico	Evaluar el cumplimiento de normas de acceso físico a zonas críticas	% de áreas críticas con cumplimiento total	%	Mensual	100%	< 95%	Encargado de Infraestructura
	Número de incidentes de seguridad física	Detectar accesos no autorizados, robos o vandalismo	Nº de eventos registrados	Nº	Mensual	0	> 0	Seguridad Física
Capa Perimetral	Tasa de bloqueo de intentos de intrusión	Medir la eficacia de las barreras perimetrales	(% intentos bloqueados / total intentos) x 100	%	Semanal	≥ 99.9%	< 99.5%	Red/Firewall Admin
	Número de alertas críticas del IDS/IPS	Supervisar anomalías y amenazas externas	Nº de alertas críticas generadas	Nº	Diario	≤ 2	> 2	Encargado de SOC
Capa de Red	Porcentaje de cumplimiento de	Evaluar la implementación de una	% de segmentos implementados	%	Trimestral	100%	< 90%	Arquitecto de Red

DEPARTAMENTO TIC VISADO

Categoría / Área	Nombre del Indicador	Objetivo	Fórmula / Métrica	Unidad de Medida	Frecuencia	Meta / Umbral	Umbral de Alerta	Responsable
	segmentación de red	arquitectura segura						
	Número de incidentes de seguridad interna	Controlar accesos indebidos entre zonas de red	Nº de incidentes entre segmentos	Nº	Mensual	0	> 0	Encargado de Seguridad
Capa End Point	Endpoints con software de seguridad actualizado	Verificar cobertura de antivirus/EDR	(% endpoints protegidos / total) x 100	%	Semanal	≥ 98%	< 95%	Soporte Técnico
	Detecciones de malware en endpoints	Monitorear infecciones en equipos de usuario	Nº de detecciones confirmadas	Nº	Semanal	≤ 5	> 5	SOC o EDR Admin
Capa de Aplicación	Vulnerabilidades críticas sin corregir	Identificar riesgos graves en software	Nº de vulnerabilidades abiertas > 30 días	Nº	Mensual	0	> 0	Desarrollo / Seguridad App
	Aplicaciones con pruebas de seguridad aplicadas	Garantizar verificación de seguridad en sistemas críticos	% apps críticas con SAST/DAST	%	Trimestral	≥ 90%	< 80%	QA / DevSecOps
Capa de Datos	Porcentaje de datos cifrados en reposo	Asegurar confidencialidad de datos sensibles	(% bases/archivos cifrados / total) x 100	%	Trimestral	≥ 95%	< 90%	DBA / Seguridad
	Incidentes de fuga de datos	Medir exfiltraciones o pérdidas de datos	Nº de incidentes validados	Nº	Anual	0	> 0	Responsable de Protección de Datos
Capa Administrativa	Personal capacitado en seguridad	Asegurar conocimiento básico de ciberseguridad	(% personal capacitado / total) x 100	%	Anual	≥ 95%	< 90%	Área de Formación
	Incumplimientos de políticas de seguridad	Detectar acciones contrarias a normativas internas	Nº de violaciones documentadas	Nº	Mensual	≤ 3	> 3	Comité de Seguridad
Gestión de Identidades	Cuentas inactivas deshabilitadas	Prevenir accesos indebidos por cuentas obsoletas	(% deshabilitadas / detectadas) x 100	%	Mensual	≥ 95%	< 90%	Administrador IAM

Categoría / Área	Nombre del Indicador	Objetivo	Fórmula / Métrica	Unidad de Medida	Frecuencia	Meta / Umbral	Umbral de Alerta	Responsable
Gestión de Vulnerabilidades	Tasa de vulnerabilidades críticas sin mitigar (>30 días)	Reducir exposición prolongada a riesgos graves	(% sin mitigar / total críticas) x 100	%	Mensual	≤ 5%	> 10%	Encargado de Infraestructura
Respuesta a Incidentes	Tiempo medio de respuesta ante incidentes	Mejorar eficiencia en contener amenazas	Σ tiempo de respuesta / Nº incidentes	Horas	Trimestral	≤ 8h	> 12h	CSIRT local
	Tiempo medio de detección de incidentes	Reducir latencia desde ocurrencia hasta detección	Σ tiempo de detección / Nº incidentes	Horas	Mensual	≤ 1h	> 4h	SOC / SIEM Admin
Cumplimiento Normativo	Cumplimiento con normativas y leyes	Asegurar alineación con Ley 21.663, 19.628, ISO 27001:2022, etc.	(% controles implementados / requeridos) x 100	%	Anual	100%	< 95%	Oficial de Cumplimiento

Consideraciones para la Implementación:

- Esta tabla es un ejemplo. Deberás adaptar los indicadores a las necesidades específicas, los activos críticos y los riesgos particulares de cada institución del sector salud.
- Asegúrate de que los indicadores sean relevantes para los objetivos de seguridad y las prioridades de la organización.
- Los indicadores deben ser cuantificables y fáciles de medir.
- Los resultados de los indicadores deben permitir la toma de decisiones informadas y la implementación de acciones correctivas.
- Los indicadores deben revisarse y ajustarse periódicamente para asegurar su continua relevancia y efectividad.
- Considera la implementación de herramientas de gestión de seguridad de la información (SIEM, paneles de control de seguridad) para facilitar la recopilación, el análisis y la visualización de estos indicadores.