POLÍTICA DE CIBERSEGURIDAD
CLÍNICA LAS CONDES

ELABORACIÓN	REVISIÓN	AUTORIZACIÓN
Nombre:Diego Allende Triviño Cargo:Jefe Seguridad de la Información Fecha: Agosto 2025	Nombre:Jaime Hagel Cargo:Gerente Operaciones y TI Fecha: Agosto 2025	Nombre: Pablo Yarmuch Cargo: Gerente General Fecha: Agosto 2025

1. OBJETIVO

El objetivo de esta política es establecer las directrices de gobernanza para la gestión de los riesgos de ciberseguridad que amenazan a Clínica Las Condes. Su propósito es asegurar la resiliencia de los servicios clínicos y administrativos protegiendo la infraestructura tecnológica y los activos de información digitales contra ciberataques. De esta forma, se busca salvaguardar la continuidad operacional, la integridad de los datos de los pacientes y la confianza depositada en Clínica Las Condes, minimizando el impacto de potenciales incidentes.

1.1 OBJETIVOS ESPECÍFICOS

- Diseñar, formalizar e implementar un marco de controles técnicos para identificar, proteger, detectar, responder y recuperarse de amenazas cibernéticas.
- Diseñar, formalizar e implementar una metodología de gestión de incidentes de ciberseguridad.
- Gestionar y mitigar las vulnerabilidades técnicas en la infraestructura y aplicaciones de la organización.
- Fomentar y mantener una cultura de ciberseguridad en toda la organización, donde los colaboradores y terceros relevantes comprendan su rol y responsabilidad para identificar y reportar amenazas que pongan en riesgo la información y los sistemas de Clínica Las Condes.
- Asegurar que los proveedores con acceso a los sistemas de Clínica Las Condes cumplan con los estándares de ciberseguridad requeridos.

2. ALCANCE

Esta política es aplicable a todos los colaboradores, directivos, administradores y filiales de Clínica Las Condes, sus proveedores y externos que presten servicios, que tengan relación con:

- Administración de activos de información o datos clasificados como sensibles.
- La seguridad lógica y física de la información en medios digitales.
- Controles de acceso a los datos e información.
- El gobierno y la gestión de la infraestructura tecnológica.
- Los controles de acceso a los datos e información en sistemas y redes.
- La administración de incidentes de ciberseguridad.
- La continuidad del negocio y resiliencia cibernética.
- El cumplimiento de requisitos normativos y legales en el ámbito digital.

3. DEFINICIONES

- **Ciberseguridad:** Práctica de defender equipos tecnológicos, servidores, dispositivos móviles, sistemas electrónicos, redes y datos de ataques maliciosos.
- **Amenaza**: Causa potencial de un incidente cibernético, que puede resultar en daño a un sistema o a la Compañía (ej. malware, phishing, denegación de servicio).
- **Vulnerabilidad**: Debilidad presente en un activo o control tecnológico que puede ser explotada por una amenaza.
- **Incidente de Ciberseguridad**: Evento que compromete la confidencialidad, integridad o disponibilidad de un activo de información digital, como resultado de un ataque o falla de un control de ciberseguridad.
- **Activo**: Todo lo que tiene valor para la Compañía. Por ejemplo, documentos, personas, oficinas, datos, etc.

4. MARCO NORMATIVO Y REFERENCIAS

- Marco de referencia NIST.
- CIS Controls.
- Política de Seguridad de la Información de Clínica Las Condes.
- Legislación Chilena Aplicable (Ley 21.663).
- Reglamento Interno de Orden, Higiene y Seguridad de Clínica Las Condes.

5. PRINCIPIOS Y DIRECTRICES

Clínica Las Condes asume el compromiso de desarrollar sus actividades de acuerdo con los lineamientos de Ciberseguridad para proteger su infraestructura tecnológica y activos digitales. El objetivo es contar con un ambiente robusto que permita defender activamente a la organización contra ciberamenazas, asegurando la resiliencia de los procesos críticos del negocio.

Lo anterior se llevará a cabo mediante la implementación y mantenimiento de un programa de ciberseguridad basado en marcos de referencia y estándares internacionales como NIST Cybersecurity Framework (CSF) y Controles CIS.

Para el cumplimiento de esta política, Clínica Las Condes establece los siguientes lineamientos:

Uso Aceptable de Activos: Todo el personal de Clínica Las Condes y Filiales debe hacer un uso responsable y seguro de los activos tecnológicos de la empresa (equipos tecnológicos, correo electrónico, internet).

Control de Acceso Lógico: El acceso a sistemas y aplicaciones se gestionará mediante identificadores únicos, contraseñas robustas y, cuando aplique, múltiples factores de autenticación, siguiendo el principio de mínimo privilegio.

Protección de Redes: Se implementarán controles como firewalls, segmentación de redes y sistemas de detección de intrusos para proteger el perímetro y las redes internas.

Protección contra Malware: Todos los servidores y equipos de usuario final deberán contar con software de protección contra código malicioso, el cual deberá mantenerse actualizado.

Gestión de Vulnerabilidades: Clínica Las Condes establecerá un proceso para identificar, evaluar y remediar vulnerabilidades técnicas en sus sistemas de manera oportuna.

Gestión de Incidentes de Ciberseguridad: Se implementará un plan de respuesta a incidentes para asegurar la detección, contención, erradicación y recuperación efectiva ante ciberataques.

Resiliencia Cibernética: Se realizarán copias de seguridad periódicas de la información crítica y se probarán planes de recuperación de desastres tecnológicos para minimizar la interrupción del negocio.

Concientización y Capacitación: Se realizarán campañas y entrenamientos periódicos para educar a los usuarios sobre las ciber amenazas actuales y cómo reconocerlas.

Mejora Continua: Clínica Las Condes promoverá la mejora continua de la Ciberseguridad mediante un proceso formal.

6. SEGUIMIENTO Y CUMPLIMIENTO

6.1 COMITÉ DE CIBERSEGURIDAD

Se establece el Comité de Ciberseguridad (que podrá ser el mismo Comité de Seguridad de la Información) de la Administración como ente de gobernanza para la supervisión de la estrategia de ciberseguridad de Clínica Las Condes.

Propósito: Evaluar el panorama de ciberamenazas, supervisar la postura de ciberseguridad de Clínica Las Condes y Filiales, aprobar la implementación de nuevas tecnologías de defensa y asegurar una respuesta coordinada ante incidentes críticos.

Miembros: El comité estará compuesto por el Oficial de Seguridad de la Información, el Gerente de Tecnología, líderes de infraestructura y redes, y otros roles técnicos relevantes o sus respectivos representantes.

Frecuencia: El comité se reunirá con una frecuencia periódica definida en su acta de constitución.

6.2 METODOLOGÍA

Para garantizar la aplicación efectiva de los controles de ciberseguridad, se implementará un programa de monitoreo técnico que incluye:

Evaluaciones de Vulnerabilidades y Pruebas de Penetración: Se ejecutarán análisis de vulnerabilidades de forma periódica y pruebas de penetración (pentesting) al menos una vez al año sobre los sistemas críticos para identificar y remediar debilidades técnicas.

Monitoreo de Seguridad Continuo (SOC/SIEM): Se monitorearán los eventos de seguridad en la infraestructura tecnológica para la detección temprana y respuesta a actividades anómalas o maliciosas.

Reportes Técnicos: El equipo de TI y Ciberseguridad presentará informes técnicos al Comité sobre el estado de la gestión de vulnerabilidades, los intentos de ataque bloqueados y la eficacia de los controles de ciberseguridad.

7. ROLES Y RESPONSABILIDADES

Dentro de las principales responsabilidades del personal que contempla la Seguridad de la Información y Ciberseguridad, se encuentran:

Cargo	Responsabilidades
Dirección de Clínica Las Condes	Apoyar la cultura, inversión y la asignación de recursos necesarios para mantener una postura de ciberseguridad robusta.
Oficial de Seguridad de la Información	Supervisar la implementación y efectividad de los controles de ciberseguridad y liderar la respuesta a incidentes críticos.
Dueños de procesos y responsables de controles	Implementar y mantener los controles técnicos de ciberseguridad definidos en esta política y sus procedimientos asociados.
Personal de Clínica Las Condes y Filiales	Entender, aplicar y cumplir los principios de la Política de Ciberseguridad.

8. REVISIÓN Y ACTUALIZACIÓN

Esta Política será revisada y actualizada anualmente, o cuando existan cambios importantes en el modelo de negocios de la Compañía o en factores externos, que ameriten su revisión antes del período anual. Corresponderá al Comité de Ciberseguridad, revisar la política y proponer al Directorio de la Compañía las modificaciones que se consideren necesarias.

9. CONTROL DE CAMBIOS

Fecha	Versión	Modificado por:	Observaciones
22-09-2025	V1	Comité de Seguridad de la Información	Aprueba la primera versión de la Política de Ciberseguridad.
27-11-2025	V1	Directorio CLC	Aprueba la primera versión de la Política de Ciberseguridad.

10. APROBACIÓN

Esta política fue aprobada por el Comité de Seguridad de la Información durante su reunión del 22 de septiembre de 2025 y aprobada por el directorio en sesión del día 27 de noviembre de 2025, garantizando su alineación con los estándares y objetivos de la organización.