Política

De Seguridad de la Información Corporativa

1. Objetivo

La presente "Política de Seguridad de la Información Corporativa", tiene por objetivo establecer el lineamento de la empresa respecto de la responsabilidad, resguardo y gestión de riesgos de la información, así como entregar directrices generales sobre el acceso, manipulación, procesamiento, transmisión, protección, almacenamiento o cualquier otro tratamiento que se realice sobre los activos de información de Clínica Ciudad del Mar y sus centros médicos, en adelante, Clínica Ciudad del Mar.

En consecuencia, a través de la "Política de Seguridad de la Información Corporativa", se buscar dar cumplimiento a lo siguiente:

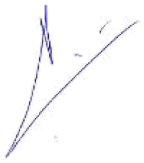
a) Establecer un programa de seguridad de la información y los lineamientos generales de seguridad de la información para la infraestructura tecnológica y operación de la organización.
b) Dar cumplimiento de los requisitos legales y contractuales vigentes y aplicables a la organización en materia de seguridad de la información.
c) Velar por que todos(as) los(as) colaboradores(as) de Clínica Ciudad del Mar cumplan con la "Política de Seguridad de la Información Corporativa".
d) Hacer de conocimiento de todos(as) los(as) colaboradores(as) de la organización el impacto relacionado al incumplimiento de la "Política de Seguridad de la información Corporativa".

2. Alcance

Esta Política aplica a todas las operaciones, sistemas, personas e infraestructura tecnológica que constituyen los sistemas de información de Clínica Ciudad del Mar y que dan soporte a los procesos y servicios considerados dentro del alcance del Sistema de Gestión de Seguridad de la Información (en adelante SGSI), esto incluye:

- Todas las instalaciones físicas donde se llevan a cabo estos procesos.
- Todo el personal involucrado en la entrega y gestión de estos servicios, incluyendo miembros del directorio, ejecutivos, colaboradores(as), contratistas y terceros relevantes.

3. Control de Cambios

No. DE VERSIÓN	REVISADO POR	APROBADO POR
1.0	**Nombre**: Estefanía Pardo Vergara **Cargo**: Analista de Riesgos **Fecha**: 03-09-2025 **Firma**: 	**Nombre:** Víctor Valle Rohde **Cargo:** Gerente General **Fecha:** **Firma:**  **Nombre:** Sergio Mella Toledo **Cargo:** CISO Empresas Banmédica Prestadores **Fecha:** 03-09-2025 **Firma:** 

MODIFICACIONES			
No. DE VERSIÓN	**FECHA**	**DESCRIPCIÓN**	**AUTOR**
1.0	30-11-2020	Versión inicial.	Gerencia de Seguridad de la Información Corporativa
2.0	26-08-2024	Se incorpora alcance y actualización de formato	Gerencia de Seguridad de la Información Corporativa
3.0	25-08-2025	Se actualiza formato y se incorpora control de equipos médicos en 9.6.5 Seguridad de Operaciones. Adaptación a formato prestadores.	Gerencia de Seguridad de la Información Corporativa

Contenido

4. Evaluación y Revisión

La "Política de Seguridad de la Información Corporativa" será revisada con una frecuencia anual desde su aprobación, sin embargo, ante cambios significativos que modifiquen el nivel de riesgo del presente documento, la presente política podrá ser analizada, evaluada y actualizada.

Entre los cambios que hacen necesaria la revisión de la política, se destacan los siguientes:

- Cambios en las leyes y/o reglamentos que afecten a la organización.
- Incorporación o modificaciones importantes de procesos críticos del negocio.
- Cambios significativos en el soporte tecnológico.
- Cambios significativos en las amenazas a que se expone la información de la organización.
- Resultados de la Revisión por la Dirección y/o Auditorías.

Esta Política debe ser revisada y presentada para su aprobación, por el Comité de Seguridad de la Información (CSI).

5. Mecanismos de Difusión

Con el fin de asegurar que todos(as) los(as) Gerentes(as), Jefaturas y Colaboradores(as) de la organización estén debidamente informados, la presente "Política de Seguridad de la Información Corporativa" será distribuida y difundida a través de los canales de comunicación definidos por Clínica Ciudad del Mar: correo electrónico y/o a través de su publicación en el sitio web.

Además, este documento se publicará y mantendrá accesible para todas las partes interesadas relevantes a través de los siguientes medios:

- Gestor Documental definido por la Organización
- Sitio web de Clínica Ciudad del Mar.

6. Roles y Responsabilidades

Para efectos de cumplir con la presente "Política de Seguridad de la Información Corporativa", los(as) directores(as), Gerencias, funcionarios(as) y los(as) colaboradores(as) en general de Clínica Ciudad del Mar tendrán las siguientes responsabilidades y roles:

- **Área de Comunicaciones Internas:** Colabora en la redacción y diseño de las versiones resumidas y visuales del alcance de la política.
- **CISO:** Es responsable de supervisar el proceso de publicación y actualización del SGSI incluyendo la Política de Seguridad de la Información Corporativa.
- **Colaboradores(as) de Clínica Ciudad Del Mar:** Son responsables de utilizar la versión más reciente de la Política.
- **Comité de Seguridad de la Información:** Se encuentra compuesto por la Gerencia de Seguridad de la Información Corporativa, el(la) CISO y Gerencia de Clínica Ciudad Del Mar. Este comité es el responsable de mantener, implementar y dirigir el SGSI, asegurar que los objetivos establecidos cumplan con los requisitos de la norma ISO 27001:2022 y proponer ajustes en los indicadores o metas del sistema.
- **Directorio:** Debe realizar las acciones necesarias a fin de que se adopten las medidas para asegurar el cumplimiento de la "Política de Seguridad de la Información Corporativa" y se asegure el monitoreo periódico del cumplimiento de los controles y procedimientos que implementen para tal fin.
- **Gerencia de Operaciones:** Es responsable de mantener la infraestructura técnica necesaria para sustentar los procesos de la compañía que se alinean a esta Política.
- **Gerencias de Clínica Ciudad del Mar:** Deben alinear sus procedimientos a la política y adoptar las medidas necesarias para asegurar que el personal a su cargo las conozca y aplique, por lo que deberá ejecutar y/o coordinar las correspondientes acciones de difusión y fiscalización.
- **Responsable de Seguridad de la Información de Clínica Ciudad del Mar:** Deberá:
  a) Informar al Directorio sobre cualquier tema de interés relacionado al cumplimiento de la política.
  b) Identificar y asegurar la correcta aplicación de:
     - Los marcos regulatorios legales vigentes y aplicables en materia de seguridad de la información.
     - Los lineamientos de seguridad para las aplicaciones que realizan tratamiento de datos fuera de las instalaciones de Clínica Ciudad del Mar.
     - Los lineamientos de seguridad de la información para el envío de datos por medios de soporte informático.
     - Los lineamientos para mantenimiento de registros de auditoría.
     - Los lineamientos para transferencias por correo electrónico.
     - Los lineamientos para que las App No IT y documentos digitales cumplan con la seguridad de la información.
  c) Brindar soporte de entendimiento para la aplicación de la "Política de Seguridad de la Información Corporativa".
  d) Desarrollar y mantener los roles y responsabilidades del programa de seguridad de la información corporativo.
- **Responsable de Seguridad de la Información y los(as) encargados(as) pertinentes:** Deberán:
  a) Asegurar el cumplimiento de la política.

b) Incorporar en la cultura de la organización las obligaciones asociadas con la seguridad de la información, sustentadas en la política.
c) Asegurar el monitoreo e investigación para el cumplimiento de la política.
d) Coordinar y aplicar las sanciones por el incumplimiento de la política.
e) Asegurar el desarrollo e implementación de procedimientos que permitan el cumplimiento de la "Política de Seguridad de la Información Corporativa".
f) Adoptar la Seguridad de la Información como un elemento integral del ciclo de vida de proyectos.
g) Asegurar la madurez de la Seguridad de la Información con alineación a la política.
h) Definir las líneas base de seguridad para la infraestructura donde residen las aplicaciones.
i) Ejecutar capacitaciones para que los(as) colaboradores(as) conozcan las normas internas de seguridad de la información.

7. Términos y Definiciones

- **Activo de información:** Todo documento físico (DF), documento digital (DD) y aplicativos informáticos (APP) que tengan un valor para la empresa y/o soporten o sean parte de la actividad, proceso o giro de negocio de la organización.
- **Aplicativo informático fuera de la custodia de la unidad de sistemas (APPnoIT):** Todo activo de información orientado al procesamiento y administración de datos que se encuentre administrado por una unidad, y además se encuentre alojado en la misma unidad o en la unidad de sistemas. Se incluye a esta definición los archivos digitales con lógica de programación en su contenido, como, por ejemplo: macros en Excel, bases de datos en Access, flujos de trabajo en SharePoint, entre otros.
- **Áreas seguras:** Áreas donde se requiere un segundo nivel de autorización para obtener acceso físico. Áreas de servidores, centro de datos, closets de cableado, son ejemplos específicos de áreas seguras.
- **Autenticación:** La autenticación se refiere a la verificación de la autenticidad, sea de la persona o de la información, por ejemplo, un mensaje puede ser autentificado que efectivamente ha sido generado por el origen declarado. Las técnicas de autenticación usualmente conforman las bases para todas las formas de control de acceso a los sistemas de información y/o datos y serán determinadas y comunicadas de tiempo en tiempo al interior de la organización por parte de la Gerencia de Seguridad de la Información Corporativa en Clínica Ciudad del Mar.
- **Control de acceso:** El control de acceso se refiere a las reglas y mecanismos determinados por el Gerencia de Seguridad de la Información Corporativa en Clínica Ciudad del Mar, desplegados al interior de la organización y que controlan el acceso a los sistemas de información y activos de información, así como el acceso físico a las instalaciones y dispositivos donde aquellos se encuentran. La seguridad de la información está sustentada en el control de acceso, sin el cual, la seguridad de la información, por definición, no podría existir.

- **Confidencialidad:** Obligación de guardar reserva y secreto respecto de los activos de información, de los sistemas de tecnología de la información y, en general, de la información de la organización que se identifique como confidencial o que por su naturaleza requiera trato confidencial; y de asegurar que dicha información es únicamente compartida entre las personas autorizadas en conformidad a esta política.
- **Disponibilidad:** Asegurar que los sistemas de tecnología de la información y los activos de información necesarios están disponibles para ser utilizados en el momento que son requeridos únicamente para las personas autorizadas.
- **Integridad:** Asegurar que la información es auténtica y completa. Proveer el suficiente nivel de confianza de que la información es lo suficientemente precisa para el propósito requerido.
- **Documento digital (DD):** Toda representación de hecho, imagen o idea, incluyendo activos de información, que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior. Se excluye de esta definición a todo archivo digital que contenga lógica de programación en su contenido, como por ejemplo macros en Excel.
- **Documento físico (DF):** Todo activo de información que contenga datos registrados por escrito y en soporte de papel, tales como comprobantes de caja, documentos de control operativo, documentos activos, documentos pasivos, documentos para archivo físico, entre otros.
- **Segundo nivel de autorización:** Autorización adicional obligatoria requerida para poder ganar acceso a áreas restringidas.
- **Seguridad de la Información:** Preservación de la confidencialidad, la integridad y la disponibilidad de la información.
- **Usuarios:** Personas naturales que pueden hacer uso de ciertos servicios que ofrece Clínica Ciudad del Mar, sea en su condición de pacientes, afiliados(as) o por cualquier otra razón.

8. Referencias

- Alcance del SGSI.
- Reglamento Interno de Orden, Higiene y Seguridad.
- Objetivos del Sistema de Gestión de Seguridad de la Información.
- ISO 27001: 2022
- ISO 27000:2019

9. Generalidades

9.1. Introducción

Clínica Ciudad del Mar, prestadora de servicios de salud, ha elaborado la siguiente "Política de Seguridad de la Información Corporativa", en conjunto con las Normas de Seguridad de la Información, que definen los controles de seguridad requeridos colectivamente para dar cumplimiento al marco normativo vigente en lo que respecta al gobierno de seguridad de la información basado en ISO 27001:2022.

Los objetivos de la presente "Política de Seguridad de la Información Corporativa" comprenden los siguientes aspectos:

- La gestión de riesgos (10.1.a)
- La gestión de políticas y compromiso organizacional (10.2.b).
- La gestión de los activos de información (10.1.b).
- Auditoria y evaluación (10.2.a)
- La comunicación y concientización de la organización (10.3.a)
- La mejora continua del SGSI (10.4.a).

Todo esto en concordancia con el documento de "Objetivos del Sistema de Gestión de Seguridad de la Información" ya referenciado.

9.2. Cumplimiento de la Política

Considerando la importancia que reviste para Clínica Ciudad del Mar el cumplimiento del marco normativo y lineamientos institucionales en materia de seguridad de la información, si la organización determina que un(a) colaborador(a) ha violado esta política, este(a) puede estar sujeto(a) a sanciones laborales según lo establecido en el "Reglamento Interno de Orden, Higiene y Seguridad", las que, según la gravedad de la infracción cometida, pueden incluir la terminación del contrato individual de trabajo respectivo. Lo anterior, sin perjuicio de las acciones judiciales que puedan dirigirse contra el(la) transgresor(a) para hacer efectiva su responsabilidad tanto civil como penal.

Los factores para tener en cuenta al evaluar las posibles sanciones incluyen, pero no se limitan, a los siguientes:

- El alcance de la violación.
- La naturaleza de la violación (conducta accidental, inadvertida o intencional).
- El daño o riesgo potencial creado por la divulgación para las personas cuya información fue liberada, la entidad o personas afectadas (considerándose particularmente graves las infracciones que conciernan a información de afiliados(as) o pacientes o que de alguna forma comprometa información comercialmente sensible de la organización).
- El hecho de que el(la) colaborador(a) haya informado de la situación a los(as) encargados(as) correspondientes tan pronto tuvo conocimiento de los hechos y si colabora en las auditorías o investigaciones internas que puedan iniciarse en relación con los hechos informados.
- Eventual reiteración, en caso de haberse registrado por parte del(la) colaborador(a) una conducta errónea repetida o intencional o violaciones de las políticas y procedimientos de la organización.

Los(as) colaboradores(as) son responsables de plantear con prontitud cualquier preocupación sobre posibles violaciones de esta política. Si un(a) empleado(a) es consciente de una situación que él(ella) cree que puede estar violando esta política o que de alguna otra manera puede resultar contraria a la ley o la normativa aplicable, debe ponerse inmediatamente en contacto con cualquiera de los siguientes recursos:

- Responsable de la Seguridad de la Información (CISO).
- Responsable de Cumplimiento (Compliance).
- Gerencia de Seguridad de la Información Corporativa.
- También puede notificar mediante un correo electrónico a las casillas infosec@ccdm.cl y csirt@ccdm.cl.

Los casos reales o sospechosos de posibles incidentes de seguridad se deben notificar al(la) Responsable de Seguridad de la Información para la respuesta a incidentes de seguridad en conformidad al programa de gestión de riesgos de la Gerencia de Seguridad de la Información Corporativa de Clínica Ciudad del Mar y los planes de continuidad del negocio y recuperación ante desastres, para su investigación y seguimiento.

9.3. Roles y responsabilidades del SGSI

Los roles y responsabilidades sobre el SGSI son los siguientes:

RESPONDABILIDADES POR ROL
Rol: EJECUTOR(A) DEL SGSI
a. Garantizar que el SGSI se adapte a los requisitos de las normas correspondientes. b. Apoyar a los responsables de procesos en la identificación de activos y riesgos. c. Mantener actualizada la declaración de aplicabilidad (SGSI). d. Concientizar al personal respecto a la importancia del SGSI. e. Mantener actualizada la información documentada del SGSI. f. Asegurar la integración de los requisitos del SGSI en los procesos de Clínica Ciudad del Mar.
Rol: RESPONSABLE DEL SGSI
a. Garantizar que el SGSI se adapte a los requisitos de las normas correspondientes. b. Responsable del SGSI ante la organización y entidades externas. c. Informar acerca del desempeño del SGSI a la Alta Dirección a intervalos planificados. d. Reportar a la Alta Dirección el estado del SGSI. e. Apoyar a los responsables de procesos en la identificación de activos y riesgos. f. Programar las auditorías del SGSI. g. Dar seguimiento a los hallazgos de auditorías con los responsables de procesos. h. Asegurar la integración de los requisitos del SGSI en los procesos de Clínica Ciudad del Mar. i. Promover la mejora continua del SGSI.
Rol: CISO
a. Asegurar el establecimiento de la política y objetivos del SGSI. b. Asegurar la integración de los requisitos del SGSI en los procesos de Clínica Ciudad del Mar.

c. Proporcionar recursos para el establecimiento, implementación, mantenimiento y mejora del SGSI.
d. Asegurar que la responsabilidad y autoridad para los roles pertinentes al SGSI se asignen y comuniquen.
e. Promover la mejora continua.
f. Dirigir y apoyar a las personas para contribuir a la eficacia del SGSI.
g. Comunicar la importancia de una gestión eficaz de Seguridad de la Información y la conformidad con los requisitos del SGSI.
h. Revisar el SGSI a intervalos planificados para asegurar su idoneidad, adecuación y eficacia.
i. Decidir las oportunidades de mejora y necesidad de cambios del SGSI.
j. Participar activamente en las auditorías del SGSI.
k. Controlar los cambios en la organización, procesos del negocio, instalaciones de procesamiento de información y los sistemas que afectan la Seguridad de la Información.
l. Mantener contacto con las autoridades pertinentes para conocer cambios que se originen a nivel de obligaciones legales, regulatorias o contractuales.

Rol: USUARIO(A) DEL SGSI

a. Conocer y aplicar la responsabilidad y autoridad de su cargo.
b. Conocer los objetivos del SGSI.
c. Conocer y cumplir la "Política de Seguridad de la Información Corporativa".
d. Conocer como sus tareas contribuyen a la eficacia del SGSI, incluyendo los beneficios de la mejora del desempeño de la Seguridad de la Información.
e. Conocer las consecuencias de no actuar en conformidad con los requerimientos del SGSI.
f. Colaborar activamente en las actividades relacionadas al SGSI en las cuales se los haya involucrado.
g. Utilizar la información, activos, sistemas y servicios tecnológicos de la empresa únicamente para los propósitos autorizados y relacionados al desempeño de sus funciones.
h. Cumplir con los términos y condiciones de su contrato de trabajo.
i. Reportar debilidades, eventos o incidentes de Seguridad de la Información.
j. Conocer y aplicar las políticas, procesos y procedimientos establecidos en Clínica Ciudad del Mar relacionados a SGSI y a su cargo.

Rol: ALTA DIRECCIÓN

a. Asegurar el establecimiento de la política y objetivos del SGSI.
b. Proporcionar recursos para el establecimiento, implementación, mantenimiento y mejora del SGSI.
c. Asegurar que la responsabilidad y autoridad para los roles pertinentes al SGSI se asignen y comuniquen.
d. Promover la mejora continua.
e. Comunicar la importancia de una gestión eficaz de Seguridad de la Información y la conformidad con los requisitos del SGSI.
f. Revisar el SGSI a intervalos planificados para asegurar su idoneidad, adecuación y eficacia.
g. Participar activamente en las auditorías del SGSI.

Rol: DUEÑO(A) DEL PROCESO

a. Concientizar al personal a su cargo la importancia del SGSI.
b. Revisar regularmente el cumplimiento de procedimientos y procesamiento de información dentro de su área de responsabilidad, de acuerdo con las políticas, normas de seguridad y a cualquier otro requisito de seguridad.
c. Mantener el inventario de activos actualizado.
d. Identificar y gestionar los riesgos relacionados con sus procesos.
e. Aprobar los planes de tratamiento de riesgos y aceptar los riesgos residuales.
f. Cumplir y hacer cumplir las políticas de Seguridad de la Información.
g. Participar en las auditorías del SGSI y establecer acciones para atender los hallazgos identificados.
h. Asegurar la implementación de planes de tratamiento de riesgos cuando aplique.
i. Definir y mantener actualizada la información documentada relacionada con sus actividades y procesos.

j. Gestionar los accesos a los sistemas para la asignación de nuevo personal o revocar en caso de desvinculación o cambio de cargo.
Rol: RESPONSABLE DE LA OPERACIÓN
a. Cumplir y hacer cumplir la "Política de Seguridad de la Información Corporativa". b. Asegurar la disponibilidad de la infraestructura tecnológica. c. Gestionar las vulnerabilidades técnicas. d. Reportar y mitigar las debilidades, eventos, incidentes de seguridad reportados. e. Gestionar la capacidad de la infraestructura tecnológica. f. Planificar los cambios en la infraestructura de modo que no impacten la operación. g. Obtener respaldos y realizar pruebas de los mismos. h. Participar en las auditorías del SGSI y establecer acciones para atender los hallazgos. i. Definir y mantener actualizada la información documentada relacionada con sus actividades y procesos. j. Asignar accesos y privilegios a los sistemas de información de acuerdo con los perfiles definidos.
Rol: TERCERAS PARTES
a. Cumplir con lo establecido en la "Política de Seguridad de la Información Corporativa". b. Reportar debilidades, eventos o incidentes de seguridad de la información. c. Cumplir con los acuerdos de nivel de servicio y cláusula de confidencialidad.

9.4. Compromiso de Cumplimiento

La Clínica Ciudad del Mar, se compromete a crear, aplicar y mantener los controles de seguridad adecuados para proteger la confidencialidad, integridad y disponibilidad de la información, incluyendo, pero no limitado a información y datos relativos a:

- Los(as) colaboradores(as), personas y pacientes a los que Clínica Ciudad del Mar prestan servicios y la organización.
- Sistemas de TI, sitios web, aplicaciones, infraestructura, equipos médicos, teléfono, correo de voz, hardware, software, así como el uso de sistemas de tecnología de la información de la Clínica y comunicaciones electrónicas como correo electrónico, intranet, internet y redes, como topología, protocolo y arquitectura (en lo sucesivo denominados conjuntamente "sistemas de tecnología de la información de la empresa").

Adicionalmente, Clínica Ciudad del Mar conscientes de la importancia de la seguridad de la información para llevar a cabo con éxito sus objetivos de negocio consideran:

- Cumplir con los requisitos legales, reglamentarios, contractuales y otros aplicables al SGSI.
- Promover una cultura organizacional basada en la mejora continua y la alineación con los objetivos del SGSI y los principios de la norma ISO/IEC 27001.
- Proveer los recursos necesarios, asegurando la correcta asignación de los recursos humanos, tecnológicos y financieros necesarios para implementar y demás mantener el SGSI.
- Garantizar el respaldo y liderazgo activo de la Alta Dirección para asegurar el cumplimiento de los compromisos asumidos.

- Impulsar la divulgación y la concienciación de la Política de Seguridad de la Información entre todos los funcionarios.

9.5. Restricciones Particulares o Especiales

Al haber distintas funciones y roles que manejan información confidencial, las gerencias podrán disponer, en caso de que lo estimen necesario, mayores restricciones en su unidad o área que las disposiciones de esta política, en cuyo caso prevalecerá la más exigente.

9.6. Disposiciones de la Política

9.6.1. Gestión del Programa de Seguridad

- La Gerencia Seguridad de la Información Corporativa tiene la responsabilidad de desarrollar, documentar, mantener y comunicar un programa integral de seguridad de la información corporativo. La autoridad y la responsabilidad de administrar el programa de seguridad de la información corporativo se delegan en el(la) Director(a) de Seguridad de la Información (CISO).
- La misión de la Gerencia de Seguridad de la Información Corporativa es proteger la confidencialidad, integridad y disponibilidad de la información de la organización. Esto incluye crear, administrar, comunicar y supervisar la política.

9.6.2. Evaluación y Gestión de Riesgos

- El programa de gestión de riesgos de la Gerencia de Seguridad de la Información Corporativa proporciona información de análisis de riesgos precisa y relevante que facilita la toma de decisiones consistentes de gestión de riesgos. Las decisiones de gestión de riesgos se tomarán en colaboración con el liderazgo legal, empresarial, de tecnologías de la información y de la Gerencia de Seguridad de la Información Corporativa para optimizar el equilibrio entre las necesidades operativas del negocio y los requisitos legales, reglamentarios, de cliente(a) y de seguridad.
- Las evaluaciones de riesgos se realizan para determinar los controles de seguridad requeridos en función del uso y el riesgo, así como la normativa legal, reglamentaria, de seguridad del cliente y de seguridad de la información aplicable.

9.6.3. Seguridad del Personal

- Las responsabilidades de seguridad y de los(as) colaboradores(as) se deben definir, comunicar, evaluar y supervisar adecuadamente para mitigar el riesgo de error, robo, fraude, pérdida o uso indebido de la información de la empresa y de los sistemas de tecnología de la información de la empresa.

- Los(as) colaboradores(as) deben cumplir con la "Política de Seguridad de la Información Corporativa", incluidos los requisitos de las normas de seguridad para un uso aceptable de los sistemas de tecnología de la información de la empresa.
- De forma regular, los(as) colaboradores(as) deben reconocer sus responsabilidades de seguridad, tal como se define en la "Política de Seguridad de la Información Corporativa".
- Se supervisa, de acuerdo con las leyes vigentes y aplicables, todas las actividades en los sistemas de tecnología de la información de la empresa.

9.6.4. Seguridad Física

- La información de la organización, los sistemas de tecnología de la información de la empresa y las áreas seguras deben estar protegidas contra el acceso físico no autorizado.
- La Gerencia de Seguridad de la Información Corporativa en conjunto con las áreas pertinentes definirán los controles para proteger la infraestructura tecnológica ubicada en instalaciones bajo el control de la organización contra riesgos ambientales razonables, para preservar la salud y la seguridad de los(as) colaboradores(as) y terceros de la compañía.
- La Gerencia de Seguridad de la Información Corporativa en conjunto con las áreas pertinentes implementarán controles ambientales adecuados para el correcto funcionamiento y disponibilidad de la información de la empresa, de los activos de información y de los sistemas de tecnología de la información de la empresa.

9.6.5. Seguridad de Operaciones

- Los sistemas de tecnología de la información de la empresa se deben configurar, operar y administrar de manera controlada para proteger la confidencialidad, integridad y disponibilidad de la información de Clínica Ciudad del Mar.
- Los hardware y software que deben ser aprobados antes de su uso dentro de la organización por parte de la Gerencia de Seguridad de la Información Corporativa.
- El hardware y el software deben ser soportados formalmente a través del Área de Infraestructura Corporativa, incluyendo el mantenimiento regular y las actualizaciones periódicas.
- El hardware y el software de equipos médicos deben ser soportados formalmente a través del Área de Equipos Médicos, incluyendo el mantenimiento regular y las actualizaciones periódicas.

9.6.6. Registro, Monitoreo y Gestión de Incidentes

- Los sistemas de tecnología de la información de la empresa se deben supervisar para detectar eventos operativos, de seguridad y de sistema que puedan afectar la confidencialidad, integridad y disponibilidad de la información de la organización.
- Los incidentes de seguridad se deben administrar mediante una capacidad de respuesta documentada, que incluye procedimientos para notificar, analizar, escalar, investigar y resolver incidentes de seguridad de manera oportuna, todo en conformidad al programa de gestión de

riesgos de la Gerencia de Seguridad de la Información Corporativa y los planes de continuidad del negocio y recuperación ante desastres de la organización.

9.6.7. Seguridad de la Comunicación

- La confidencialidad, integridad y disponibilidad de la información de la organización y activos de información se deben proteger, cuando se comunique, a través de las técnicas y mecanismos determinados e informados de tiempo en tiempo al interior de la organización por parte de la Gerencia de Seguridad de la Información Corporativa.
- La transmisión de la información de la organización se debe realizar de acuerdo con los requisitos normativos y contractuales que se encuentran vigentes y son aplicables, además la "Política de Seguridad de la Información Corporativa".

9.6.8. Control de Acceso, Administración de Acceso e Identificación y Autenticación

- El acceso a la información de la organización y a los sistemas de tecnología de la información de la organización y a los activos de información de la organización deben ser sujeto a control de acceso y autenticación.
- El acceso se debe limitar a la cantidad mínima necesaria para realizar las tareas asignadas.

9.6.9. Seguridad de la Red

- Las redes de la organización, y la capacidad de conectarse a los sistemas de tecnología de la información de la organización, deben ser administradas y controladas.
- Todas las conexiones a sistemas de tecnología de la información que no sean de la empresa deben estar aprobadas por la Gerencia de Seguridad de la Información Corporativa y cumplir con los requisitos de seguridad que éste determine y comunique como aplicables al interior de la organización.

9.6.10. Seguridad de Partes Externas o Terceros

- Las redes de la organización, y la capacidad de conectarse a los sistemas de tecnología de la información de la organización, deben ser administradas y controladas.
- La organización debe gestionar los riesgos presentados al permitir que entidades externas que no sean afiliadas de la organización ("Partes Externas" o "Terceros") accedan a la información de la organización o a los sistemas de tecnología de la información.
- Las partes externas o terceros podrán acceder a la información de la organización, a los activos de información o a los sistemas de tecnología de la información de la organización en el contexto de un acuerdo contractual formal que establezca los requisitos y responsabilidades de seguridad apropiados de la parte externa o tercero, los cuales no podrán ser inferiores a los establecidos en esta política.

- Los dispositivos en uso por las partes externas o terceros deben ser revisados y aprobados por la Gerencia de Seguridad de la Información Corporativa antes de estar conectados a los sistemas de tecnología de la información de la organización.

9.6.11. Seguridad en el Desarrollo de Aplicaciones

- Las aplicaciones de la organización se deben diseñar, implementar y administrar para proteger la confidencialidad, integridad y disponibilidad de los sistemas de tecnología de la información de la organización, los activos de información y la información.
- El software y el código de la aplicación deben estar protegidos contra modificaciones no autorizadas.

9.6.12. Continuidad del Negocio y Recuperación Ante Desastres

- La organización debe desarrollar, probar y mantener planes de continuidad del negocio y recuperación ante desastres con el fin de mitigar el impacto causado por interrupciones en las operaciones críticas del negocio, y para permitir una recuperación eficiente y efectiva. Los planes de continuidad del negocio y recuperación ante desastres incluirán procesos y controles para proteger el negocio de la organización, la vida y la seguridad de los(as) colaboradores(as), así como para proteger la imagen, la reputación, los activos y los recursos de la organización.
- Los requisitos de continuidad del negocio y recuperación ante desastres están determinados por los riesgos empresariales, las obligaciones legales, reglamentarias y contractuales y los posibles impactos comerciales de las interrupciones del servicio, entre otros que determine el Directorio.

9.6.13. Clasificación y Protección de Datos

- La información utilizada o mantenida por la organización debe ser recopilada, utilizada, mantenida y divulgada solo por las personas autorizadas y solo en las oportunidades y medida permitidas, siempre de acuerdo con todas las leyes y regulaciones vigentes y aplicables, las políticas de la organización y, si también es aplicable, autorizaciones individuales más estrictas o contratos con pacientes.
- La información utilizada o mantenida por la organización se debe clasificar de acuerdo con las definiciones de nivel de clasificación de datos de la organización. Estas definiciones proporcionan orientación sobre las formas apropiadas de manejar y proteger la información de la empresa con el fin de proteger su confidencialidad, integridad y disponibilidad.

9.6.14. Seguridad en la Nube

- La organización debe asegurar que cuando se adquiera un servicio en la nube, este cumpla con los requisitos comerciales, con las leyes y regulaciones vigentes y aplicables, además de la “Política de Seguridad de la Información Corporativa”. Se debe establecer dónde implementar los controles

de seguridad, además de los requisitos adicionales para poder respaldar y gestionar los riesgos presentes en los entornos en la nube.

9.7. Aspectos de Control

De acuerdo con la definición estratégica de Clínica Ciudad del Mar, la presente política se adopta como apoyo al cumplimiento del marco normativo de Seguridad de la Información, la evaluación anual de los controles de seguridad definidos en la política y normas de seguridad de la información, con la finalidad de fortalecer de manera continua el SGSI.

9.8. Alcance del SGSI

9.8.1. Proceso de Actualización

Para garantizar que el "Alcance del SGSI" se mantenga actualizado se efectuarán las siguientes gestiones:

- **Revisión periódica de la política:** El(la) Responsable de Seguridad de la Información (CISO) revisará el contenido publicado al menos una vez al año.
- **Actualización por cambios:** Cualquier modificación en el alcance del SGSI desencadenará una actualización inmediata en todos los medios de publicación.
- **Proceso de aprobación:** Todas las actualizaciones del alcance publicado deberán ser aprobadas por la Alta Dirección antes de su difusión.
- **Notificación de cambios:** Se implementará un sistema de notificación para informar a las partes interesadas sobre cualquier actualización significativa en el alcance del SGSI.
- **Registro de versiones:** Se mantendrá un registro las versiones anteriores del alcance publicado, incluyendo las fechas de vigencia y los cambios realizados.
- **Feedback:** Se establecerá un mecanismo para que las partes interesadas puedan proporcionar comentarios o solicitar aclaraciones sobre el alcance publicado.

9.8.2. Toma de Conciencia del SGSI

El programa de toma de conciencia del SGSI de Clínica Ciudad del Mar tiene como objetivos:

- Asegurar que todos(as) los(as) colaboradores(as) y partes interesadas relevantes comprendan la importancia del SGSI.
- Promover la comprensión de la contribución individual a la eficacia del SGSI.
- Fomentar una cultura de seguridad de la información en toda la organización.
- Reducir los incidentes de seguridad causados por falta de conocimiento o negligencia.

9.8.3. Medios de Concientización

Se implementarán los siguientes métodos para fomentar la toma de conciencia sobre el SGSI:

CAPACITACIONES:

- Inducción para nuevos(as) colaboradores(as) sobre el SGSI.
- Cursos normativos e-learning anuales de actualización para todos(as) los(as) colaboradores(as).

COMUNICACIONES INTERNAS:

- Correos electrónicos mensuales con consejos y recordatorios sobre prácticas seguras, los cuales serán trabajados entre el Área de Comunicaciones Internas y la Gerencia de Seguridad de la Información Corporativa.
- Publicación de infografías y posters en áreas comunes.

SIMULACROS Y EJERCICIOS PRÁCTICOS:

- Simulaciones de phishing para evaluar la conciencia de seguridad.
- Ejercicios de respuesta a incidentes.

10. Objetivos de Seguridad de la Información

Los objetivos de seguridad de la información se establecen para garantizar que la organización cumple con sus propósitos estratégicos, protege sus activos de información y satisface los requisitos legales, contractuales y normativos aplicables. Estos objetivos son medibles y se revisan periódicamente para garantizar su vigencia y alineación con los objetivos generales de la organización. Los objetivos son los siguientes:

10.1. Garantizar la confidencialidad, integridad y disponibilidad de los activos de información

a. Implementar y/o actualizar los controles que reduzcan los riesgos identificados en un 90% antes del cierre del próximo ciclo anual.
b. Mantener un tiempo máximo de inactividad no planificada de los sistemas críticos de acuerdo con lo establecido en el plan de continuidad de negocio.

10.2. Cumplir con los requisitos legales y normativos aplicables

a. Realizar auditorías anuales de cumplimiento normativo. Su objetivo debe ser el 100% de cumplimiento.
b. Actualizar las políticas y normas internas en un plazo de 30 días tras cualquier cambio legislativo relevante.

10.3. Incrementar la concientización sobre seguridad entre los(as) colaboradores(as)

a. Lograr que al menos el 90% del personal complete la capacitación anual en seguridad de la información.

10.4. Mejorar continuamente la seguridad de los sistemas

a. Mantener la efectividad de los controles de seguridad a un 90% medido a través de auditorías internas, para el próximo período anual.

11. Excepciones

Para la "Política de Seguridad de la Información Corporativa" no se presentan excepciones para su cumplimiento.