CALIDAD
NOS CONECTA

POLÍTICA
de Seguridad de la Información Corporativa

Clínica Santa María
Especialistas en ti

ÍNDICE

1. OBJETIVO

La presente “Política de Seguridad de la Información Corporativa” tiene por objetivo establecer los lineamientos generales para la responsabilidad, resguardo, gestión de riesgos y protección de la información de la organización, incluyendo sus activos de información, redes, sistemas, aplicaciones, documentos físicos y digitales, datos personales y datos personales sensibles. Asimismo, establece directrices generales sobre el acceso, recolección, uso, consulta, comunicación, transmisión, almacenamiento, conservación, eliminación, anonimización, respaldo, recuperación y cualquier otra operación de tratamiento de información, con el objeto de preservar su confidencialidad, integridad, disponibilidad y resiliencia de los sistemas que procesan la información.

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, especialmente al cumplimiento de las obligaciones aplicables en materia de protección de datos personales, incluyendo el deber de seguridad, confidencialidad, protección desde el diseño y por defecto, gestión de vulneraciones a las medidas de seguridad y conservación de evidencia suficiente para acreditar la existencia y funcionamiento de las medidas adoptadas y, asimismo, contribuir al cumplimiento de las obligaciones de ciberseguridad aplicables a la organización, incluyendo la prevención, detección, contención, respuesta, recuperación y reporte de incidentes de ciberseguridad, cuando corresponda.

c) Velar porque todos(as) los(as) colaboradores(as), directores, miembros de consejos consultivos, ejecutivos, contratistas y proveedores de la compañía 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 la organización, y que dan soporte a los procesos y servicios considerados dentro del alcance del Sistema de Gestión de Seguridad de la Información ("SGSI"). Lo anterior comprende el acceso, uso, tratamiento, almacenamiento, transmisión, comunicación, conservación, respaldo, eliminación y protección de activos de información, información corporativa, información confidencial, datos personales, y datos personales sensibles, sin alterar la calidad de responsable, encargado o tercero que corresponda a cada entidad conforme a la normativa aplicable.

Quedan comprendidas dentro del ámbito de aplicación de esta política:

- Todas las instalaciones físicas donde se llevan a cabo los procesos descritos en el presente numeral.

- Todos los sistemas, redes, aplicaciones, bases de datos, documentos físicos y digitales, servicios en la nube, dispositivos, soportes tecnológicos e infraestructura que permitan almacenar, procesar, transmitir o acceder a información de la compañía.

- Todo el personal involucrado en la entrega, gestión, soporte o control de estos procesos y servicios, incluyendo miembros de directorios y consejos consultivos, ejecutivos, colaboradores(as), contratistas, proveedores y terceros relevantes.

- Los terceros que, en virtud de una relación contractual o de servicios, accedan, traten, almacenen, transmitan o administren información de la compañía, incluidos datos personales o datos personales sensibles, en la medida que corresponda según el servicio contratado.

3. EVALUACIÓN Y REVISIÓN

La “Política de Seguridad de la Información Corporativa” será revisada periódicamente y, al menos, una vez al año. También será revisada ante cambios significativos que modifiquen o puedan modificar el nivel de riesgo de la organización, de sus sistemas de información, de sus activos de información o de los tratamientos de datos personales comprendidos en su alcance, incluyendo, entre otros, los siguientes:

- Cambios en las leyes, reglamentos, instrucciones o criterios de autoridad que afecten a la organización en materia de seguridad de la información, ciberseguridad o protección de datos personales.

- Incorporación o modificación relevante de procesos críticos del negocio, servicios, sistemas, aplicaciones, bases de datos o tratamientos de datos personales.

- Cambios significativos en el soporte tecnológico, infraestructura, arquitectura, servicios en la nube, proveedores tecnológicos o integraciones relevantes.

- Cambios significativos en las amenazas, vulnerabilidades o riesgos a que se expone la información de la organización, incluyendo datos personales y datos personales sensibles.

- Resultados de auditorías, revisiones internas, revisiones de cumplimiento, ejercicios de continuidad, pruebas de recuperación, investigaciones de incidentes, evaluaciones de impacto en protección de datos personales o revisiones de la organización.

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

4. MECANISMOS DE DIFUSIÓN

La presente "Política de Seguridad de la Información Corporativa" será distribuida y difundida a través de los canales de comunicación definidos por la compañía: correo electrónico y/o a través de su publicación en el sitio web o portal interno.

La presente política será también incluida en los correspondiente Reglamentos de Orden, Higiene y Seguridad.

5. ROLES Y RESPONSABILIDADES

Para efectos del cumplimiento con la presente "Política de Seguridad de la Información Corporativa", se consideran las siguientes unidades o áreas responsables y roles al interior de la organización:

- **Área de Comunicaciones Internas:** Colabora en la redacción y diseño de las versiones resumidas y visuales del alcance de la política.

- **Encargado de Seguridad de la información o CISO:** Responsable de supervisar el proceso de publicación y actualización del SGSI incluyendo la Política de Seguridad de la Información Corporativa.

Entre otras que pudieran corresponder, serán responsabilidad del Encargado de Seguridad de la Información o CISO las siguientes:

I. Asegurar el desarrollo e implementación de procedimientos que permitan el cumplimiento de la "Política de Seguridad de la Información Corporativa", así como promover el cumplimiento de la misma.

II. Incorporar en la cultura de la organización las obligaciones asociadas con la seguridad de la información, sustentadas en la política. Adoptar la Seguridad de la Información como un elemento integral del ciclo de vida de proyectos.

III. Asegurar el monitoreo e investigación para el cumplimiento de la política.

IV. Identificar y asegurar la correcta aplicación de:

- Los leyes y normas 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 la organización.
- 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.

V. Reportar los incumplimientos relevantes a las áreas de Personas y/o Compliance, según corresponda, para que éstas evalúen las medidas laborales, contractuales, disciplinarias o correctivas aplicables conforme al Reglamento Interno de Orden, Higiene y Seguridad, los contratos vigentes y la normativa aplicable.

VI. Asegurar la madurez de la Seguridad de la Información con alineación a la política.

VII. Ejecutar capacitaciones para que los(as) colaboradores(as) conozcan las normas internas de seguridad de la información.

VIII. Informar al directorio u órgano mayor de administración sobre temas de interés relacionado al cumplimiento de la política.

IX. Responder consultas y educar para una correcta aplicación de la "Política de Seguridad de la Información Corporativa".

X. Desarrollar y mantener los roles y responsabilidades del programa de seguridad de la información corporativo.

- **Colaboradores(as):** Son responsables de conocer y cumplir la versión más reciente de la Política.

- **Delegado de Protección de Datos Personales:** Es responsable de asesorar y apoyar a la organización en materias de protección de datos personales, revisar la consistencia de esta política con el programa de cumplimiento de datos personales, participar en la evaluación de riesgos que involucren datos personales, coordinar con el Encargado de la Seguridad de la Información o CISO y las áreas responsables la gestión de vulneraciones a las medidas de seguridad que afecten datos personales, y promover la documentación de evidencia necesaria para acreditar cumplimiento. Este rol no sustituye las responsabilidades técnicas del CISO ni las responsabilidades operacionales de las áreas dueñas de los procesos o sistemas.

- **Comité de Seguridad de la Información:** 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. Este comité estará compuesto por el Country Manager Chile, el Gerente General de Prestadores, el Fiscal Corporativo, el Oficial de Protección de Datos Personales y los gerentes generales de los prestadores de salud.

- **Directorio u órgano mayor de administración:** Debe realizar las acciones necesarias para 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:** Responsables de mantener la infraestructura técnica necesaria para sustentar los procesos de la compañía que se alinean a esta política.

- **Gerencias de la organización:** 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, según sea indicado por el directorio o la alta administración.

6. TÉRMINOS Y DEFINICIONES

Para efectos de la presente política y su aplicación, los siguientes conceptos tendrán el significado que en cada caso se señala.

- **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:** Verificación de la autenticidad de la persona o de la información. 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 Unidad de Seguridad de la Información Corporativa.

- **Control de acceso:** Reglas y mecanismos determinados por la Unidad de Seguridad de la Información Corporativa, 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:** Aseguramiento de 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:** Aseguramiento de que la información es auténtica y completa 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 la organización, sea en su condición de pacientes, afiliados(as) o por cualquier otra razón.

7. GENERALIDADES

7.1 Cumplimiento de la Política y sanciones por incumplimiento

Considerando la importancia que reviste para la compañía 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 o CISO.
- Delegado de Protección de Datos Personales.
- También puede notificar mediante un correo electrónico a las casillas infosec@empresasbanmedica.com y csirt@empresasbanmedica.com

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 y los planes de continuidad del negocio y recuperación ante desastres, para su investigación y seguimiento.

7.2 Compromiso de Cumplimiento

La organización, 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 la compañía 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 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, la organización consciente 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 27001:2022.
- 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.

7.3 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.

7.4 Disposiciones de la Política

7.4.1. Gestión del Programa de Seguridad

- La Unidad de 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 Encargado de Seguridad de la Información o CISO.

- La misión de la Unidad 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.

7.4.2. Evaluación y Gestión de Riesgos

- El programa de gestión de riesgos de la Unidad 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 Unidad 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.
- Las evaluaciones de riesgos deberán considerar, según corresponda, la criticidad del activo, la naturaleza de la información tratada, la existencia de datos personales o datos personales sensibles, el volumen de datos, las categorías de titulares, las finalidades del tratamiento, los terceros o encargados involucrados, las transferencias nacionales o internacionales, la exposición a amenazas, la probabilidad e impacto de incidentes, y los riesgos para los derechos y libertades de los titulares de datos. Cuando un tratamiento pueda generar alto riesgo, deberá evaluarse la necesidad de realizar una evaluación de impacto en protección de datos personales antes de iniciar el tratamiento o implementar cambios relevantes.

7.4.3. 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”.
- La organización podrá monitorear, registrar y revisar el uso de sus sistemas,redes, dispositivos, cuentas y activos de información, conforme a la ley, al Reglamento Interno de Orden, Higiene y Seguridad, a las políticas internas aplicables y a criterios de proporcionalidad, finalidad, necesidad y transparencia. Dicho monitoreo deberá orientarse a fines legítimos de seguridad, continuidad operacional, prevención de fraudes, investigación de incidentes, cumplimiento normativo y protección de la información.

7.4.4. 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 Unidad 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 Unidad 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.

7.4.5. 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 la organización.
- El hardware y software deben ser aprobados antes de su uso dentro de la organización por parte de la Unidad 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 de la organización, incluyendo el mantenimiento regular y las actualizaciones periódicas.

7.4.6. Registro, Monitoreo y Gestión de Incidentes

- Los sistemas de tecnología de la información de la empresa deberán ser supervisados para detectar eventos operativos, de seguridad y de sistema que puedan afectar la confidencialidad, integridad, disponibilidad o resiliencia de la información, de las redes, de los sistemas, de los activos informáticos y de los datos personales tratados por la organización.
- Los eventos, alertas, vulneraciones a las medidas de seguridad e incidentes de seguridad de la información o ciberseguridad deberán administrarse mediante una capacidad de respuesta documentada, que incluya procedimientos para su detección, registro, clasificación, notificación interna, análisis, escalamiento, investigación, contención, erradicación, recuperación, resolución, cierre y conservación de evidencia, de manera oportuna y conforme al programa de gestión de riesgos de la Unidad de Seguridad de la Información Corporativa, los planes de continuidad del negocio y recuperación ante desastres de la organización, y las obligaciones legales y regulatorias aplicables.
- Dichos procedimientos deberán considerar, según corresponda, si el evento o incidente: (i) compromete la confidencialidad, integridad,

disponibilidad o resiliencia de redes, sistemas o activos informáticos; (ii) afecta o puede afectar datos personales, datos personales sensibles o datos relativos a la salud; (iii) puede constituir una vulneración a las medidas de seguridad de datos personales; (iv) puede tener efectos significativos bajo la normativa de ciberseguridad; o (v) exige notificación a titulares, autoridades sectoriales, la Agencia de Protección de Datos Personales, el CSIRT Nacional u otra autoridad competente.

7.4.7. 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 Unidad 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".

7.4.8. 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 deberá limitarse al mínimo necesario para realizar las tareas asignadas, conforme a perfiles, roles y responsabilidades previamente aprobados. La organización deberá implementar controles proporcionales al riesgo, incluyendo autenticación robusta, autenticación multifactor cuando corresponda, gestión de altas, bajas y modificaciones de usuarios, revisión periódica de accesos, control reforzado de cuentas privilegiadas, segregación de funciones, trazabilidad de accesos y revocación oportuna de permisos cuando cese la necesidad de acceso.

7.4.9. 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 Unidad 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.

7.4.10. 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 sólo podrán acceder a información de la organización, activos de información, redes, sistemas, aplicaciones, infraestructura tecnológica, servicios, ambientes, documentación, información confidencial o datos personales en virtud de un acuerdo contractual formal y vigente que establezca, según corresponda, el alcance del servicio, las condiciones de acceso, uso y tratamiento de la información, las instrucciones aplicables, las obligaciones de confidencialidad, las medidas de seguridad exigibles, los niveles de servicio, las restricciones de subcontratación, los deberes de cooperación, auditoría y entrega de información, la obligación de reportar oportunamente incidentes, eventos de seguridad o vulneraciones, y las reglas de devolución, eliminación, anonimización o restitución de la información y activos al término del servicio.
- Cuando el tercero trate datos personales por cuenta de la compañía, o de alguna de sus filiales, el acuerdo respectivo deberá incorporar, además, las condiciones exigibles al tratamiento encargado de datos personales, incluyendo finalidad, duración, categorías de datos y titulares, instrucciones del responsable, asistencia en el ejercicio de derechos de los titulares, reglas sobre sub encargados, transferencias nacionales o internacionales, medidas de seguridad aplicables y deberes de colaboración frente a vulneraciones a las medidas de seguridad.
- Los requisitos de seguridad aplicables a terceros no podrán ser inferiores a los exigidos por esta política y deberán ser proporcionales al riesgo del servicio, al nivel de acceso concedido,

a la criticidad de los activos involucrados y a la naturaleza de la información tratada.

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

7.4.11. Seguridad en el Desarrollo de Aplicaciones

- Las aplicaciones de la organización deberán diseñarse, implementarse, probarse y administrarse incorporando seguridad y privacidad desde el diseño y por defecto, con controles proporcionales al riesgo, incluyendo gestión segura de requisitos, revisión de arquitectura, segregación de ambientes, control de cambios, pruebas de seguridad, revisión de código cuando corresponda gestión de vulnerabilidades, control de accesos, trazabilidad, minimización de datos personales y configuración segura por defecto.
- El software y el código de la aplicación deben estar protegidos contra modificaciones no autorizadas.

7.4.12. Continuidad del Negocio y Recuperación Ante Desastres

- La organización deberá desarrollar, probar, mantener y actualizar planes de continuidad del negocio, continuidad operacional, respaldo y recuperación ante desastres, con el fin de mitigar el impacto causado por interrupciones en operaciones críticas, servicios relevantes, sistemas que soporten procesos esenciales y tratamientos de información o datos personales, y permitir una recuperación eficiente y efectiva.
- Dichos planes deberán incluir procesos y controles para proteger la continuidad del negocio, la vida y seguridad de los(as) colaboradores(as), la imagen, reputación, activos y recursos de la organización, así como objetivos de tiempo y punto de recuperación, priorización de servicios críticos, pruebas periódicas, restauración oportuna de la disponibilidad y acceso a la información, y conservación de evidencia de las pruebas, resultados y mejoras implementadas.
- 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.

7.4.13. 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.
- Lo dispuesto en la presente política es sin perjuicio de lo establecido en las políticas o procedimientos aplicables a protección de datos personales adoptados por la organización.

7.4.14. Seguridad en la Nube

La organización deberá asegurar que la contratación, implementación y uso de servicios en la nube cumpla con los

requisitos comerciales, con las leyes y regulaciones vigentes y aplicables, además de la “Política de Seguridad de la Información Corporativa”. Para estos efectos, deberá someterse a una evaluación previa de riesgos, seguridad, continuidad, protección de datos personales, ubicación o regiones de almacenamiento, transferencias internacionales, subprocesadores, cifrado, gestión de identidades, registro de actividad, segregación de ambientes, respaldo, recuperación, portabilidad, eliminación segura y salida del proveedor. Asimismo, se deberá 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.

7.5 Aspectos de Control

La presente Política se adopta como instrumento de apoyo al cumplimiento del marco normativo de seguridad de la información, ciberseguridad y protección de datos personales, y como base para la evaluación anual de los controles definidos en la política y normas de seguridad de la información, con la finalidad de fortalecer de manera continua el SGSI.

8. EXCEPCIONES

No se admitirán excepciones a esta política que impliquen incumplimiento legal, regulatorio o contractual.

Cualquier excepción técnica u operativa deberá ser previamente autorizada por el Encargado de Seguridad de la Información o CISO, y deberá ser, en todo caso, excepcional, fundada, documentada, evaluada según riesgo, y contar con medidas compensatorias, plazo de vigencia definido y responsable de remediación. Las excepciones deberán registrarse y revisarse periódicamente por el Encargado de la Seguridad de la Información o CISO y, cuando involucren datos personales, conjuntamente con el Delegado de Protección de Datos personales.

9. CONTROL DE CAMBIOS

MODIFICACIONES

MODIFICACIONES			
N° DE VERSIÓN	FECHA	DESCRIPCIÓN	AUTOR
1.0	30-11-2020	Versión inicial	Unidad de Seguridad de la Información Corporativa
2.0	26-08-2024	Se incorpora alcance y actualización de formato y se agrega 9.5.14. Seguridad en la Nube	Unidad 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	Unidad de Seguridad de la Información Corporativa
4.0	11-05-2026	Se incorpora concepto relacionados a Ley Protección de Datos y se modifica formato de índice	Unidad de Seguridad de la Información Corporativa

Clínica
Santa María

Especialistas en ti