Política de Seguridad de la Información

CF | Seguros de Vida

Control de Cambios

Histórico de Versiones		
Versión	**Fecha**	**Resumen de los cambios producidos**
1	Abril 2020	Primera versión
2	Junio 2021	• Desglose de los lineamientos generales de la Política Seguridad de la Información. • Incorporación de responsabilidades del directorio, comité de riesgos y seguridad y del oficial de seguridad de la información, conforme a la Política de Riesgo Operacional y norma NCG 454 de la CMF.
3	Marzo 2022	• Incorporación de Lineamiento General asociado a la evaluación de riesgos cibernéticos dentro del proceso de gestión de cambios.
4	Junio 2023	• Se incorpora en el punto 5.2 la responsabilidad del área de Control Permanente y Riesgos en ejecutar anualmente la autoevaluación de Ciberseguridad bajo la norma NCG 545 de la CMF. • Se incorpora nuevo dominio de seguridad 6.15 Seguridad en la Nube • Se incluye la Política Corporativa de Seguridad de la Información dentro de las políticas relacionadas.
5	Marzo 2024	• Se incorpora nuevo dominio de seguridad 6.16 Gobierno del Dato. • Se actualizan cargos de la Sociedad. • Se actualiza registro de director para firma.
6	Marzo 2025	• Se actualiza registro para firma. • Se incorpora obligación del Oficial de Seguridad de la Información en el cumplimiento normativo, legal y contractual de notificación de incidentes.
7	Marzo 2026	• Se incorporan definiciones en el apartado de gobierno del dato y seguridad en la nube.

Responsabilidad	**Nombre**
Preparación	Jefe de Control Permanente y Riesgos
Revisión	Comité de Riesgos y Seguridad
Aprobación	Directorio CF Seguros de Vida

ÍNDICE

1. Introducción

El presente documento define la Política de Seguridad de la Información de **CF Seguros de Vida**, en consonancia con las directrices emitidas por su **Directorio**, recogiendo la filosofía y los principios de gobierno aplicables a toda la Organización, en materia de seguridad de la información y ciberseguridad, con el fin de resguardar la confidencialidad, integridad y disponibilidad de los activos de información.

La Política de Seguridad de la Información (en adelante la "Política") forma parte de un conjunto más amplio de documentos que componen el **Sistema de Gestión de Riesgos** para el negocio de seguros de vida. Así lo enuncia la NCG 325 que requiere la definición de un Sistema de Gestión de Riesgos a partir de dos componentes:

1. La **Estrategia de Gestión de Riesgos** de la entidad y,
2. Las **Políticas específicas** de cada Riesgo, requerimiento al que responde este documento.

Las empresas que presten servicios críticos para **CF Seguros de Vida**, y que tengan relación directa con los riesgos que aborda la Política, deberán acoger los puntos que se establezcan en el apartado ***6.10. Gestión de Proveedores*** de este documento, la Política de Gestión de Servicios Críticos Externalizados, así como en la **Estrategia de Gestión de Riesgos**.

2. Objetivo y Alcance

2.1. Objetivos

i. Establecer los lineamientos generales de seguridad de la información y de ciberseguridad que permitan asegurar la protección y uso adecuado de los activos de información de **CF Seguros de Vida**, en función de las directrices establecidas en las políticas corporativas.

ii. Representar los intereses del Directorio para la administración y utilización, que los usuarios o empleados internos y externos deben hacer de los activos de información de **CF Seguros de Vida**, así como las medidas que se adopten para proteger dichos recursos.

iii. Gestionar y controlar los riesgos de seguridad y ciberseguridad frente a las amenazas internas, externas y del ciberespacio que puedan comprometer los activos de información de **CF Seguros de Vida**, conforme a los apetitos y tolerancias definidos en la Política de Riesgo Operacional de la Compañía.

iv. Promover la cultura de seguridad de la información y ciberseguridad en la compañía, incluyendo la comprensión de sus responsabilidades sobre estas.

2.2. Alcance

La Política de Seguridad de la Información de **CF Seguros de Vida** es aplicable a todos los colaboradores de la compañía, incluyendo contratistas y empresas externas que presten servicios y que realicen tratamiento a los activos de información de la compañía que se encuentra en la red e internet, incluyendo los sistemas, dispositivos comunicacionales e infraestructuras críticas.

2.3. Políticas Relacionadas

- Estrategia de Gestión de Riesgos
- Política de Ciberseguridad
- Política de Continuidad del Negocio.
- Política de Gestión de Riesgo Operacional.
- Plan de Gestión y Comunicación en Crisis
- Política de Gestión de Riesgos de Externalizados de Servicios
- Política General de Seguridad de la Información Falabella S.A.

3. Marco Normativo

La Comisión para el Mercado Financiero (CMF) ha establecido su enfoque de supervisión adoptando un modelo de **Supervisión Basado en Riesgos** (SBR), lo anterior es consistente con las recomendaciones internacionales de la IAIS, OECD, Banco Mundial y FMI, concluyendo que la efectividad del gobierno corporativo es clave en un modelo de SBR. En este sentido, se han dictado **Normas de Carácter General** (NCG) que detallan requerimientos y propuestas que velen por satisfacer las necesidades antes expuestas.

De igual forma **CF Seguros de Vida** se alinea a los controles definidos en el Framework Corporativo de Seguridad de la Información, cuyo marco de referencia se basa en las mejores prácticas de las International Organization for Standardization (ISO), del Center for Internet Security (CIS) y del National Institute of Standards and Technology (NIST).

4. Definiciones

Activo de información: Conocimiento o datos que tienen valor para la organización, por lo tanto, deben ser protegidos, entre estos se consideran la información estratégica de negocio, datos personales, información operacional, información secreta, manuales, procedimientos, entre otros y que se representan en formato físico y/o digital.

Ciberespacio: Entorno virtual, en donde no existe forma física, sino más bien un entorno complejo que resulta de la interacción de personas, organizaciones y actividades de todo tipo de dispositivos tecnológicos y redes que se conectan a este entorno.

Ciberseguridad: Conjunto de acciones que la organización debe llevar a cabo para proteger los activos de la organización y a los usuarios a través de la prevención, detección y respuesta de ataques realizados en el ciberespacio.

Confidencialidad: Característica de la información que permite que sea accesible sólo a aquellas personas autorizadas.

Disponibilidad: Característica que permite que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, cada vez que lo requieran.

Incidente de seguridad de la información: Es cualquier hecho o evento que podría afectar a los activos de información de **CF Seguros de Vida** o la violación de alguno(s) de los controles de seguridad de la información definidos.

Información: La información es la interpretación que se da a los datos. En el caso de la Política, se entenderá como información a toda forma que contenga datos relacionados con **CF Seguros de Vida**, así como antecedentes proporcionados por los clientes en el contexto de la prestación de servicios.

Información Confidencial: Comprende los datos relacionados con el negocio, los antecedentes de los clientes, así como también información de planes estratégicos, metodologías, contratos y cualquier otra información cuyo propietario estime necesario un nivel de protección superior. Es toda aquella información, que, de ser mal utilizada, podría afectar en forma grave el prestigio de la empresa y su continuidad en el negocio.

Integridad: Característica que permite salvaguardar la exactitud y totalidad de la información.

Necesidad de Saber: Corresponde al principio de acceso a la información, que restringe su acceso, sólo al personal debidamente autorizado y sólo con acceso a la información que estrictamente necesita para realizar sus actividades y tareas.

Seguridad de información: Es la preservación y protección de la confidencialidad, integridad y disponibilidad de la información, de una amplia gama de amenazas, con el objetivo de minimizar el daño, asegurando la continuidad operacional y maximizar el retorno sobre las inversiones y las oportunidades de los negocios de la organización.

Tratamiento de información: Es cualquier acción que los usuarios autorizados pueden realizar sobre los activos de información de **CF Seguros de Vida**, de las cuales incluye**:** creación, eliminación, modificación, almacenamiento, procesamiento, transferencia, destrucción u otra acción que involucre el uso del activo.

5. Gobierno de Seguridad de la Información

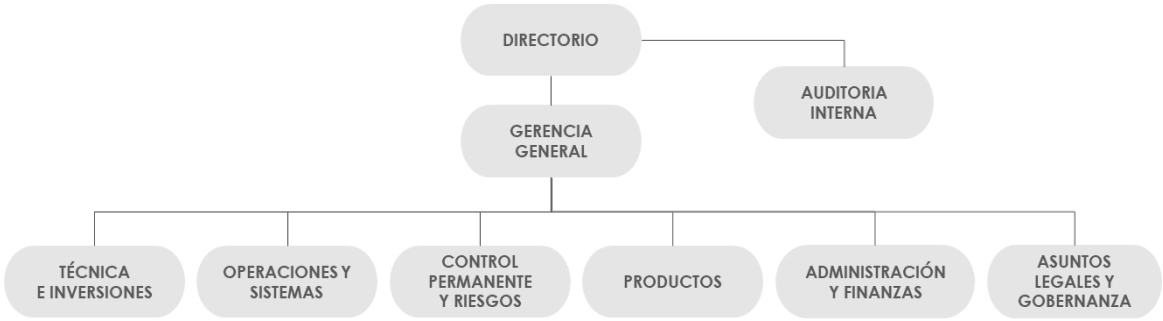
5.1. Modelo de Gobierno

Considerando que los riesgos sobre de activos de la información son **inherentes a todos los productos, actividades, procesos, datos, personas y tecnologías y se genera en todas las áreas de la compañía**, se entiende que todos los empleados [1] son responsables de gestionar y controlar los riesgos sobre activos de la información generados en su ámbito de actuación.

La documentación de la Política complementa el principio de **Gestión Integral** que comprende la **planificación, identificación, evaluación y seguimiento de los riesgos, la aplicación de medidas de mitigación y finalmente el reporte o comunicación de los aspectos pertinentes.**

La elaboración e interpretación de la Política corresponde al área de **Control Permanente y Riesgos** la cual deberá ser aprobada por el Directorio. La gestión de riesgos de seguridad y ciberseguridad será responsabilidad del Jefe de Control Permanente y Riesgos quien asume el rol **Oficial de Seguridad de la Información (OSI)** de **CF Seguros de Vida**.

1 Esto considera a los responsables de las unidades organizativas del Grupo.



La función de riesgos de seguridad de la información y de ciberseguridad se estructura en **tres líneas de defensa**. Los roles y responsabilidades de dichas líneas se concretan en el ámbito de la gestión y el control del riesgo, y se alinean con la **Política de Gestión de Riego Operacional** de la compañía, tal como se detalla a continuación:

I. Primera Línea de Defensa

La primera línea de defensa comprende todas las áreas de **CF Seguros de Vida** y son responsables, tanto de las actividades (internas o tercerizadas) que se realizan, como la gestión de sus riesgos, en los siguientes aspectos:

i. Identificar, medir, gestionar, monitorear y reportar los riesgos de los activos de información que surja de las actividades operativas e iniciativas.

ii. Analizar y reportar el riesgo residual que no es mitigado por los controles, incluidos los riesgos sobre los activos de información, las deficiencias de control, los recursos humanos, los procesos y las deficiencias de la gestión del riesgo.

iii. Promover un entorno de gestión que permita la identificación de todos los eventos y factores que son susceptibles de generar riesgos sobre los activos de información de forma que se pueda llevar a cabo una adecuada evaluación de sus posibles consecuencias. Por ellos es relevante que:

   1. Analicen los riesgos materializados y monitoreen la evolución de sus indicadores.
   2. Definan medidas de tratamiento al riesgo cuando sean necesarias.
   3. Informen de cambios en procesos, productos, externalizaciones, etc. que pudieran generar potenciales exposiciones de riesgos de seguridad de la información y de ciberseguridad.

iv. Establecer mecanismos de control y seguimiento que permitan una adecuada monitorización del riesgo, permitiendo asegurar que los riesgos de seguridad de la información y ciberseguridad se mantienen dentro de la tolerancia al riesgo definida.

v. Impulsar la participación de todos los colaboradores en la identificación de los activos de información y en la gestión de riesgos de seguridad de la información y de ciberseguridad de acuerdo con los objetivos y funciones desempeñadas.

vi. Utilizar las líneas de comunicación continuas con la segunda línea de defensa y la alta dirección que permitan reaccionar con la anticipación suficiente ante posibles situaciones de riesgo detectadas.

vii. Desarrollar e implementar, de manera oportuna, acciones correctivas para los riesgos de seguridad de la información y ciberseguridad que se han identificado.

viii. Participar de las actividades de capacitación asociadas a la gestión de riesgos de seguridad de la información y de ciberseguridad, aplicando los contenidos en su ámbito de acción.

II. Segunda Línea de Defensa

La segunda línea de defensa es responsable de proporcionar una metodología común y probada para identificar, medir y mitigar los riesgos, así como también, supervisar el control efectivo de los riesgos de seguridad de la información y de ciberseguridad cumpliendo con los niveles de tolerancia definido en la Política de Riesgo Operacional.

La segunda línea de defensa es una **función independiente realizada por el Oficial de Seguridad de la Información (OSI)** y complementa las funciones de gestión y control de la primera línea de defensa de la siguiente manera:

i. Promoviendo el desarrollo de una cultura de riesgos de seguridad de la información y de ciberseguridad en la compañía.

ii. Diseñando y ejecutando programas de capacitación que permitan a los integrantes del negocio comprender y aplicar sus responsabilidades en la gestión de riesgos.

iii. Alineando los apetito y tolerancia de riesgos conforme a la Política de Riesgo Operacional de la compañía.

iv. Supervisando la gestión y control de los riesgos de seguridad de la información y de ciberseguridad en las diferentes áreas de negocio y de soporte.

v. Reportando el perfil de riesgos y los resultados de la gestión a la alta dirección y a los órganos de administración por medio de las instancias definidas.

vi. Evaluando el impacto de cambios regulatorios en el modelo de gestión de riesgos, y gatillando la adecuación de éste cuando así se requiera.

III. Tercera Línea de Defensa

La tercera línea de defensa está constituida por Auditoría Interna quién en su labor de última capa de control y que, en función al plan de auditoría anual aprobado por el Directorio, debe evaluar periódicamente que las políticas, métodos y procedimientos son adecuados y comprobar que están implementados efectivamente en la gestión. Los resultados de sus revisiones deben ser presentados en Comité de Auditoría de la Compañía.

5.2. Roles y Responsabilidades

A continuación, en la siguiente tabla se describen los roles y responsabilidades de las distintas áreas de **CF Seguros de Vida**:

Rol	Responsabilidad
Directorio	• Aprobar la Política de Seguridad de la Información. • Aprobar apetito y tolerancia de riesgo definido en la Política de Riesgo Operacional, que considera el riesgo de seguridad de la información y ciberseguridad. • Informarse adecuada y periódicamente respecto de la gestión y estado de la gestión de riesgos de seguridad de la información y de ciberseguridad, y solicitar acciones adicionales si lo considera necesario. • Asignar los fondos adecuados y recursos suficientes para evaluar y mitigar los riesgos de seguridad de la información y de ciberseguridad, a fin de contar con políticas, personal, procesos, metodología y practicas apropiadas. • Tomar conocimiento de la necesidad de capital suficiente, para enfrentar los riesgos a los que se está expuesto, estableciendo las acciones para cumplir los requerimientos regulatorios de manera apropiada.

Comité de Riesgos y Seguridad	• Velar por el cumplimiento de la Política y los procedimientos asociados a la gestión de riesgo de seguridad de la información y de ciberseguridad. • Revisar que el apetito y tolerancia de riesgo definida en la Política de Riesgo Operacional considera el riesgo de seguridad de la información y ciberseguridad, y proponerlos al Directorio para su aprobación. • Revisar al menos una vez al año la Política y proponerla al Directorio para su aprobación. • Revisar periódicamente respecto de la gestión y estado de la gestión de riesgos de seguridad de la información y de ciberseguridad, y solicitar acciones adicionales si lo considera necesario. • Identificar, priorizar y fijar estrategias para mitigar los principales riesgos de seguridad de la información y de ciberseguridad identificados. • Aprobar reprogramaciones de planes de acción asociadas a los principales riesgos del negocio. • Promover una cultura de gestión de riesgos de seguridad de la información y de ciberseguridad. • Conocer los riesgos de seguridad de la información y de ciberseguridad, y las acciones necesarias para la mitigación de estos, en función a los niveles de tolerancia al riesgo y a los grados de exposición asumidos. • Proponer mejoras en la gestión de riesgo de seguridad de la información y de ciberseguridad. • Revisar el avance del plan de trabajo de seguridad de la información y ciberseguridad. • Estar en conocimiento de los procesos de supervisión y/o auditorias por parte del regulador en el ámbito de seguridad de la información y de ciberseguridad.
Oficial de Seguridad de la Información	• Informar al Directorio, comités respectivos y a las áreas de decisión correspondientes, sobre los riesgos de seguridad de la información y de ciberseguridad, el grado de exposición al riesgo y la gestión de éstos. • Evaluar la suficiencia de recursos y proponer las necesidades de capacitación del personal, para una adecuada gestión de los riesgos. • Velar por el cumplimiento de las políticas y procedimientos establecidos para la gestión de riesgos de seguridad de la información y de ciberseguridad • Definir y actualizar la Política y los documentos asociados a ella, gestionando su aprobación en las instancias que corresponde. • Difundir la Política y documentos asociados dentro de la compañía. • Cumplir con las actividades de segunda línea de defensa establecidas en la Política. • Desarrollar metodologías para la gestión de riesgos de seguridad de la información y ciberseguridad. • Apoyar y asistir a las demás unidades de negocio en la aplicación de la metodología de gestión de riesgos de seguridad de la información y de ciberseguridad, promoviendo el alineamiento de las medidas de tratamiento de los riesgos residuales, con los niveles de apetito y tolerancia aprobadas por el Directorio. • Informar al Comité del Riesgos y Seguridad, los resultados de las evaluaciones de riesgos asociados a los activos de información; así como las medidas de tratamiento propuestas o implementadas. • Velar por el cumplimiento de las funciones y responsabilidades asignadas a los dueños de los activos de información, con relación a la gestión de riesgos de seguridad de la información y ciberseguridad. • Identificar las necesidades de capacitación y difusión para una adecuada gestión de riesgos. • Desarrollar el plan anual de trabajo y presentar el estado de avance en el Comité de Riesgos y Seguridad, así mismo, el estado de planes de tratamiento de riesgos. • Establecer indicadores y controles claves de seguridad de la información y ciberseguridad inherentes a la compañía. • Evaluar escenarios de riesgo de ciberataques que se pueden materializar en la compañía, junto con las acciones mitigatorias e identificar posibles brechas.

	• Supervisar y cuestionar la identificación, adecuación y remediación de las acciones, como resultado de incidentes de seguridad de la información o de ciberseguridad y evaluaciones de riesgo. • Realizar anualmente la Autoevaluación de Ciberseguridad conforme a la norma NCG 454 de la CMF. • Cumplir con las obligaciones normativas, legales y contractuales vigentes relacionado a la notificación de incidentes de ciberseguridad.
Gerencias	• Cumplir con las actividades de la primera línea de defensa descritas en la Política. • Promover el cumplimiento de la Política y propiciar la cultura de riesgos dentro de las áreas bajo su responsabilidad. • Gestionar los riesgos de seguridad de la información y de ciberseguridad en su ámbito de acción dentro de las áreas bajo su responsabilidad. • Informar y evaluar los riesgos asociados a nuevos productos, tecnologías y a cambios importantes en el ambiente de negocio. • Identificar e informar los incidentes que pueden generar pérdidas por la materialización del riesgo de seguridad de la información o de ciberseguridad. • Proponer, gestionar y realizar el seguimiento de los planes de acción a fin de mitigar el riesgo, hasta su implementación. • Asegurar el cumplimiento de planes de acción.
Auditoría Interna	• Cumplir con las actividades de la tercera línea de defensa, descritas en este documento. • Evaluar el cumplimiento de los procedimientos utilizados para la gestión de los riesgos de seguridad de la información y de ciberseguridad. • Incluir en el Plan Anual de Auditoria las actividades de evaluación y control referidos a la función de riesgos de seguridad de la información y de ciberseguridad, generando los informes y recomendaciones que se deriven de la misma. • Comunicar al Oficial de Seguridad de la Información (OSI), la información relacionada con eventos de riesgos de seguridad de la información y de ciberseguridad que obtengan de sus respectivos análisis. • Evaluar el cumplimiento de los controles asociados a los riesgos de seguridad de la información y ciberseguridad de acuerdo con su plan anual de trabajo • Informar los resultados de la evaluación sobre la gestión de riesgo al Directorio, así como el seguimiento de las observaciones de Auditoría Interna y Externa.

6. Política de Seguridad de la Información

6.1. Lineamientos Generales

- **CF Seguros de Vida** entiende la seguridad de la información como la preservación y protección de la confidencialidad, integridad y disponibilidad de la información.
- Todas las áreas de **CF Seguros de Vida** deben proteger la información que manejan, de forma apropiada, según su valor y sensibilidad, independiente de los medios que la contengan y velando especialmente por su confidencialidad, integridad y disponibilidad.
- **CF Seguros de Vida** debe cumplir con todas las regulaciones, leyes y normativas de seguridad y de ciberseguridad vigentes en el país que opera.

- **CF Seguros de Vida** debe invertir en función de la evolución del negocio, en tecnologías, procesos, recursos y personal necesario para proteger la información confidencial de la compañía.
- **CF Seguros de Vida** debe implementar medidas de control consistentes y que permitan mitigar los riesgos de seguridad de la información y de ciberseguridad identificados.
- **CF Seguros de Vida** debe realizar periódicamente análisis de riesgos de seguridad y de ciberseguridad, de modo, que éstos se gestionen y traten de forma adecuada mitigando sus impactos.
- **CF Seguros de Vida** debe considerar los riesgos de seguridad y de ciberseguridad dentro de la evaluación de riesgos de la Gestión del Cambio, minimizando el impacto sobre la confidencialidad, integridad y disponibilidad de la información.
- **CF Seguros de Vida** a través de la gerencia general y los gerentes de primera línea, deberán velar por la implementación y cumplimiento de la Política.
- **CF Seguros de Vida** debe elaborar, gestionar y probar todos sus procedimientos de continuidad de negocio, a modo de asegurar la operación de todos sus procesos críticos de negocio, ante eventos de desastres o ciberataque que afecten la disponibilidad o correcto funcionamiento.
- Todos los empleados de **CF Seguros de Vida** son responsables por la custodia y protección de la información que manejan en relación con el desempeño de sus funciones.
- Todos los empleados de CF Seguros de Vida deben participar de las actividades de inducción, capacitación y concientización en temas de seguridad de la información y ciberseguridad.
- La Política debe ser aplicada, difundida y conocida por todo el personal de **CF Seguros de Vida** y su incumplimiento constituye una falta grave, la que será sancionada como tal. Por lo mismo, se debe realizar al menos anualmente el respectivo proceso de sensibilización y capacitación.
- **CF Seguros de Vida** debe alinearse al cumplimiento de la Política General de Seguridad de la Información de Falabella S.A.

6.2. Seguridad de recursos humanos

CF Seguros de Vida debe considerar la protección de la información durante todo el ciclo de vida del colaborador, desde los procesos de reclutamiento, selección y contratación, durante el vínculo contractual y en el término de la relación laboral; mediante cláusulas de confidencialidad en los contratos; educación sobre las responsabilidades en la protección de información y cumplimiento de la Política de Seguridad de la Información; y contar con procedimientos de asignación y revocación de accesos a la información.

6.3. Gestión de activos de información

CF Seguros de Vida debe identificar y mantener una adecuada protección de los activos de información conforme a su sensibilidad e importancia. Dentro de las actividades incluye la mantención de un inventario actualizado que permita identificar a los propietarios, ubicación, tipo, clasificación y custodios de los activos de información.; asignación de las responsabilidades del tratamiento y uso aceptable de la información; y mantener los mecanismos de protección frente a los riesgos identificados.

6.4. Criptografía

CF Seguros de Vida debe mantener una gestión y uso seguro de las claves criptográficas durante todo el ciclo de vida, asegurando la confidencialidad, autenticidad y/o integridad de la información, estableciendo las definiciones sobre el uso, las responsabilidades, la custodia, el nivel de protección y recuperación de las claves criptográficas.

6.5. Control de acceso lógico

CF Seguros de Vida debe contar con los procedimientos y controles que permitan proteger la información de la compañía frente al acceso no autorizado, salvaguardando la confidencialidad e integridad, alineándose al principio de "Necesidad de Saber". Dentro de las actividades incluyen la gestión de cuentas, gestión de privilegios y perfiles de acceso de usuarios hacia a los sistemas de información, redes de comunicación y equipos computacionales.

6.6. Seguridad física y ambiental

CF Seguros de Vida debe contar con las medidas y controles de seguridad física y ambiental necesarios que permitan proteger la vida de las personas y/o disminuir daños frente a las amenazas de tipo catástrofe naturales o incendios dentro de las dependencias y áreas restringidas de la compañía. Adicionalmente dentro de las dependencias y áreas restringidas, **CF Seguros de Vida** debe contar con mecanismos y controles de acceso físico necesarios que permitan asegurar que sólo el personal autorizado pueda acceder.

6.7. Gestión de las operaciones

CF Seguros de Vida debe contar con los controles de seguridad que permitan asegurar la operación correcta de los sistemas de información de la compañía, así también, evitar la divulgación no autorizada, la corrupción y pérdida de disponibilidad. Dentro de los controles de seguridad incluyen:

- controles de acceso al entorno operativo.
- documentación de las actividades operacionales y de los sistemas de información.
- controles de detección y prevención frente al código malicioso.
- gestión de respaldos, retención y recuperación de datos.
- gestión de cambios efectuados en sistemas críticos.
- gestión de vulnerabilidades sobre los activos tecnológicos que procesan información.

6.8. Gestión de las comunicaciones

CF Seguros de Vida debe contar con controles permitan proteger la confidencialidad e integridad de la información que se encuentra en las redes y en las instalaciones de procesamiento de información de la compañía, así también, en la transferencia de información. Dentro de los controles de seguridad incluyen: uso de herramientas o mecanismos que permitan proteger la información electrónica en tránsito frente al código malicioso; actividades de concientización hacia los colaboradores sobre el manejo y transmisión de información confidencial; acuerdos de confidencialidad y no divulgación en los contratos para la protección de la información.

6.9. Adquisición, desarrollo y mantenimiento de los sistemas

CF Seguros de Vida debe considerar la seguridad de la información desde la adquisición, desarrollo y mantenimiento de los sistemas desarrollados internamente hasta el término de su vida útil, mediante procedimientos y controles que incluyan: levantamiento de requerimientos de seguridad, validación del procesamiento correcto de datos, gestión de cambios, desarrollo seguro y protección del código fuente en los casos que apliquen y gestión sobre los ambientes de desarrollo, pruebas y producción.

6.10. Gestión de proveedores de servicios críticos

CF Seguros de Vida debe realizar las actividades de revisión y monitoreo que permitan asegurar la protección de la información confidencial que es accesible por proveedores que prestan servicios críticos a la compañía, evitando la divulgación de información no autorizada, la corrupción y pérdida de información. Dentro de las actividades de revisión y monitoreo hacia los proveedores críticos incluyen (en los casos que apliquen):

- incorporación de cláusulas de confidencialidad, de seguridad de la información y ciberseguridad, de propiedad de la información.
- incorporación de procedimientos y/o cláusulas que aseguren la notificación de incidentes de seguridad la información y ciberseguridad.
- incorporación de indicadores claves de seguridad y ciberseguridad.
- seguimiento de proyectos o planes de acción producto de riesgos de seguridad de la información y ciberseguridad residuales identificados.

6.11. Gestión de incidentes

CF Seguros de Vida debe contar con procedimientos que permitan gestionar de forma eficiente los incidentes de seguridad de la información y de ciberseguridad que pudieran materializarse en la compañía, considerando las actividades de detección, identificación, mitigación y recuperación de las operaciones. El procedimiento debe contar con los canales formales de notificación, registro de incidentes, roles, responsabilidades, actividades en la gestión del incidente y gestión de evidencias.

6.12. Gestión de seguridad en continuidad del negocio

CF Seguros de Vida debe contar con los planes continuidad operacional y planes de recuperación ante desastres a modo de resguardar la operación de todos los procesos críticos del negocio frente a incidentes de seguridad y de ciberseguridad que afecten la disponibilidad o el correcto funcionamiento.

6.13. Gestión de cumplimiento

CF Seguros de Vida debe velar por el cumplimiento de las leyes, normas regulatorias y responsabilidades contractuales vigentes que tengan relación con el trato correcto la información o los sistemas donde se procesa, mediante la identificación de los requisitos regulatorios, de legislación y contractuales relacionados a seguridad de la información y ciberseguridad con el cual deben ser difundidos y conocidos por los interesados.

6.14. Ciberseguridad

CF Seguros de Vida debe establecer las actividades e iniciativas necesarias para resguardar la confidencialidad, integridad y disponibilidad de la información que se encuentra en el ciberespacio. Para esto, la compañía deberá realizar procesos de evaluación y gestión de riesgos de ciberseguridad que permitan identificar las principales vulnerabilidades, amenazas y riesgos que puedan comprometer la información confidencial; contar con procesos de monitoreo que permitan detectar incidentes cibernéticos; contar con procesos de respuesta ante incidentes cibernéticos; contar con procesos de recuperación frente a la materialización de un ataque cibernético; contar con procesos para recopilar y analizar las amenazas cibernéticas; y contar con procesos de mejora continua desde el foco de los principales riesgos cibernéticos que puedan comprometer a la compañía.

6.15. Seguridad en la Nube

CF Seguros de Vida debe establecer los lineamientos y buenas prácticas de seguridad para resguardar la información de la Compañía en los servicios en la Nube, así como asegurar la correcta operación y manipulación de recursos en ambientes en la Nube. Para esto, se deberá implementar controles para proteger los recursos en la nube frente al acceso no autorizado y las amenazas del ciberespacio como son el robo de información, denegación de servicios, infección de malware entre otros; implementar controles para proteger el acceso y la información contenida en servicios PaaS (Plataformas como Servicio) como son las bases de datos y servidores; implementar controles para proteger el acceso y la información contenida en servicios IaaS (Infraestructura como Servicio) como son las máquinas virtuales de datos y servidores mediante procesos de parchado de seguridad, gestión de vulnerabilidades, multifactor de autenticación, control antimalware, e imágenes seguras; implementar controles para resguardar la privacidad de los datos mediante cifrado de datos, procedimiento de respaldo y restauración de datos, registros de auditoría, control de acceso lógico, monitoreo de los eventos de ciber amenazas y evaluación de riesgos asociado a la privacidad y sensibilidad de los datos e información.

Asimismo, se deberán realizar respaldos periódicos de la información contenida en las bases de datos y en las máquinas virtuales que soportan los servicios de la Compañía, asegurando que dichos respaldos cumplan con los estándares de seguridad y retención establecidos en las Políticas Corporativas y/o lo que determine la legislación vigente o ente regulador. Los respaldos deberán someterse a pruebas de restauración periódicas, con el fin de verificar su integridad, disponibilidad y eficacia, y asegurar la continuidad operativa ante incidentes, fallas o pérdidas de información.

6.16. Gobierno del Dato

CF Seguros de Vida se adhiere a los lineamientos de gobierno del dato establecidos en la Política General de Gobierno del Dato de Falabella Financiero. Los lineamientos generales de gobierno del dato deben ser cumplido por todos los colaboradores que traten los datos en nubes administradas por **CF Seguros de Vida** y terceros que tengan acceso a los activos de información de la Compañía. La Gobernanza de Datos establece los lineamientos sobre la gestión de los datos, entendiendo a estos como un activo estratégico para la Compañía. La misión de Gobierno de Datos está sustentada en 8 principios adheridos en la política corporativa:

- **El Dato es un activo:** La Compañía entiende que el dato es un activo que posee un valor real y cuantificable asociado a los objetivos con los que se utiliza. Por ello, son tratados como un activo dentro la compañía y se gestionan y protegen acorde a ello. Debe incrementarse y resguardarse su valor y simultáneamente facilitar un mejor uso de este, sin desatender la seguridad y protección.

  Respecto a los datos personales, el tratamiento de los datos deberá siempre sustentarse en una base legal válida, respetando los principios de licitud, finalidad, proporcionalidad y minimización definidos por la Ley 21.719 que regula la protección y el tratamiento de los datos personales.

- **Datos Gobernados:** La Compañía debe contar con Datos Gobernados. Los datos deben ser gobernados a través de una gestión eficiente y transparente. Busca disminuir la entropía en la toma de decisiones sobre los datos, para lo cual potencia roles transversales, mejorando los procesos a lo largo de todo el ciclo de vida del dato. Para ello, la Compañía contará con roles formales responsables de la definición, calidad, protección y uso autorizado del dato, asegurando trazabilidad, responsabilidad y cumplimiento regulatorio.

- **Granularidad del Dato:** En la Compañía los datos deben ser recolectados o recibidos desde su origen con el máximo nivel de granularidad posible, para así maximizar potenciales usos del dato en el corto y largo plazo. La granularidad deberá mantenerse dentro de criterios de necesidad y proporcionalidad, evitando recopilar o almacenar datos no estrictamente requeridos para la finalidad declarada del tratamiento.
- **Datos Protegidos:** En la Compañía los datos deben ser protegidos, auditables y cumplir con las regulaciones vigentes. Se debe reducir los riesgos de acceso y uso indebido de los datos, así como potenciales multas por incumplimiento de regulaciones vigentes. Los datos se clasifican de acuerdo con su nivel de sensibilidad definidos de acuerdo con la gestión de activos.
- **Definición Única:** En la Compañía los datos y cada uno de sus elementos deben existir bajo una definición única. Se debe reducir el riesgo de confusiones e inconsistencias en la toma de decisiones sobre los datos. Esto se implementará mediante un Catálogo de Datos Corporativo que incluya definiciones, metadatos, clasificaciones, reglas de calidad y linaje del dato.
- **Data Integrada:** Los datos deben poder integrarse entre sí para obtener el máximo valor a través de la relación entre los distintos dominios de datos de la compañía.
- **Datos confiables:** Los datos deben ser confiables, oportunos y representar la realidad. Se debe asegurar la calidad de la información y el cumplimiento de normativas y regulaciones que apliquen.
- **Democratización de Datos:** Falabella Financiero espera que los datos sean accesibles y pueden ser utilizados por todos los empleados de la compañía según la necesidad del rol que desempeña y objetivos de negocio. Se busca democratizar el acceso y uso de los datos en la organización.

La Compañía debe establecer la responsabilidad general de identificar y reportar problemas con los datos y colaborar en las diferentes tareas del proceso de gestión del dato de acuerdo con su área de conocimiento y ámbito de responsabilidad. Los roles y responsabilidades para las tareas de Gobierno de Datos se separan en:

- Dueño del Dato: responsable del dato en la Compañía, define su finalidad, reglas de acceso, calidad esperada, clasificación y plazos de conservación del dato, asegurando su cumplimiento normativo.
- Custodio del Dato: responsable del dato en TI, implementará controles tecnológicos de seguridad, integridad, disponibilidad y trazabilidad conforme a las exigencias regulatorias y de ciberseguridad.

7. Actualización de la Política

La Política será **actualizado y adaptado constantemente** a la situación que afecta en cada momento a la realidad de **CF Seguros de Vida**. Esta actualización y adaptación se deriva tanto de cambios experimentados en su operativa diaria como por modificaciones en la infraestructura existente.

La actualización de la Política será responsabilidad del área de Control Permanente y Riesgos. La periodicidad de su revisión será anual y/o cuando las condiciones del entorno lo ameriten. La Política, así como cualquier modificación a esta, deberá ser aprobada por el Directorio de **CF Seguros de Vida**.

A su vez, el área de Control Permanente y Riesgos será la responsable de la distribución de dicho documento a todas las áreas/unidades afectas.

El proceso de mantenimiento y/o actualización puede originarse por distintos motivos:

- Revisión periódica: Se realiza con una **periodicidad mínima anual**, siguiendo un procedimiento de control por confirmación. A través de este proceso de validación, las distintas áreas/unidades afectadas confirmarán la vigencia del contenido de la Política y su consistencia con la normativa vigente en el Grupo.
- Revisión a petición: El procedimiento se revisa a petición de cualquiera de las áreas/unidades afectas a la Política que hayan identificado la necesidad de su modificación en cualquier momento del tiempo.