Manual de Seguridad de la Información y Ciberseguridad

Administración del Documento	Responsable Seguridad de la Información y Ciberseguridad
Versión:	02
Fecha de la versión:	Octubre 2025
Creado por:	Responsable Seguridad de la Información y Ciberseguridad
Aprobado por:	Directorio
Fecha Aprobación	28-10-2025

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
Mayo 2025	01	Responsable Seguridad de la Información y Ciberseguridad	Creación Manual
Octubre 2025	02	Responsable Seguridad de la Información y Ciberseguridad	Las modificaciones consolidan la gobernanza de la Sociedad (roles y responsabilidades; segregación de funciones); fortalecen la gestión de riesgos, controles y continuidad operacional; establecen directrices de respuesta a incidentes y notificación a autoridades; y precisan lineamientos específicos para servicios en la nube, seguridad de redes y resguardo de las personas, proveedores y terceros

1. PRESENTACIÓN INSTITUCIONAL

1.1. Descripción de la Organización

FALCOM AGF es una institución financiera dedicada a la administración de activos, cuyo compromiso con la excelencia se refleja en la gestión integral de inversiones y en la oferta de productos financieros diseñados para satisfacer las necesidades de sus clientes en un entorno dinámico y altamente regulado. La organización opera con una visión estratégica que integra la innovación, la gestión del riesgo y la responsabilidad fiduciaria, consolidándose como un referente en el sector financiero.

Misión
La misión de FALCOM AGF es proporcionar soluciones de inversión seguras, eficientes y adaptadas a los objetivos de sus clientes, asegurando la sostenibilidad a largo plazo mediante prácticas éticas y una gestión prudente de los riesgos. La organización busca maximizar el valor para sus stakeholders, promoviendo la transparencia, la integridad y la responsabilidad en todas sus operaciones.

Estructura Organizativa
FALCOM AGF cuenta con una estructura organizativa robusta y flexible que permite una gestión eficiente de sus operaciones y una respuesta ágil ante los desafíos del entorno financiero. Esta estructura está compuesta por:

- **Alta Dirección:** Responsable de la definición de la estrategia corporativa y la supervisión del cumplimiento de los objetivos organizacionales.
- **Comités de Gobierno Corporativo:** Incluyen el Comité de Riesgos, el Comité de Auditoría y el Comité de Sistemas y Ciberseguridad, encargados de velar por la adecuada gestión de los riesgos y el cumplimiento normativo.
- **Áreas Operativas y de Soporte:** Gestión de inversiones, análisis financiero, tecnologías de la información, cumplimiento regulatorio, entre otras, que trabajan de manera coordinada para garantizar la eficacia operativa y la seguridad de la información.

Contexto Operativo
La organización opera en un entorno regulatorio complejo, bajo la supervisión de la **Comisión para el Mercado Financiero (CMF)**, y en conformidad con normativas nacionales e internacionales en materia de gestión de riesgos, seguridad de la información y ciberseguridad. La creciente digitalización de los servicios financieros y la evolución de las amenazas cibernéticas exigen un enfoque integral de seguridad que permita proteger los activos de información y garantizar la continuidad del negocio.

1.2. Visión

"Operamos con un denominador común: entender al cliente en todas las dimensiones posibles que influyen en sus decisiones financieras. Ponemos al cliente en el centro de nuestra gestión, buscando resultados sostenibles en el largo plazo."

La visión de FALCOM AGF refleja su compromiso con la creación de valor a largo plazo, tanto para sus clientes como para la sociedad en su conjunto. En el ámbito de la seguridad de la información, esta visión se traduce en la implementación de prácticas de ciberseguridad que no solo protejan los activos críticos, sino que también fortalezcan la confianza de los clientes y otros stakeholders en la integridad y resiliencia de la organización.

1.3. Filosofía y Valores

La filosofía corporativa de FALCOM AGF se basa en principios fundamentales que orientan la toma de decisiones y la gestión de riesgos en todos los niveles de la organización. Estos principios se reflejan en una cultura organizacional que promueve la ética, la responsabilidad y la mejora continua.

Principios Rectores:

- **Independencia:** FALCOM AGF prioriza la independencia en la toma de decisiones, garantizando que las recomendaciones y estrategias de inversión estén alineadas con los intereses de los clientes.
- **Transparencia:** La organización se compromete a actuar con transparencia en todas sus operaciones, promoviendo la rendición de cuentas y la comunicación abierta con los stakeholders.
- **Resiliencia:** La capacidad de adaptarse a cambios y gestionar eficazmente situaciones de crisis es un pilar fundamental en la filosofía de FALCOM AGF. La resiliencia se construye a través de una gestión proactiva de riesgos, planes de continuidad del negocio y una cultura de ciberseguridad arraigada en toda la organización.
- **Compromiso con la Excelencia:** La organización busca la excelencia en todas sus actividades, impulsando la innovación, la eficiencia operativa y el desarrollo profesional de sus colaboradores.

Valores Corporativos:

- **Ética e Integridad:** Actuar con honestidad y responsabilidad en todas las interacciones.
- **Orientación al Cliente:** Poner las necesidades del cliente en el centro de la estrategia organizacional.
- **Gestión del Conocimiento:** Fomentar el aprendizaje continuo y la actualización de competencias en un entorno tecnológico en constante evolución.
- **Responsabilidad Social:** Contribuir al desarrollo sostenible, considerando el impacto de las decisiones empresariales en la sociedad y el medio ambiente.

Estos valores son la base sobre la cual se construyen las políticas y procedimientos de seguridad de la información y ciberseguridad, asegurando que la protección de los activos de información esté alineada con la misión y visión de FALCOM AGF.

2. INTRODUCCIÓN

La seguridad de la información y la ciberseguridad son pilares fundamentales para garantizar la integridad, confidencialidad y disponibilidad de los activos de información en el entorno financiero actual. La creciente dependencia de la tecnología, la complejidad de las operaciones digitales y el aumento de las amenazas cibernéticas exigen un enfoque estratégico que permita gestionar eficazmente los riesgos asociados a la información.

El presente **Manual de Seguridad de la Información y Ciberseguridad** de FALCOM AGF tiene como propósito establecer los principios, políticas y directrices que rigen la gestión de la seguridad de la información en la organización. Este manual se alinea con la **Norma de Carácter General N°510 (NCG 510)** emitida por la **Comisión para el Mercado Financiero (CMF)**, así como con estándares internacionales de referencia, como la **ISO/IEC 27001:2022**, **ISO/IEC 27002:2022**, y el **NIST SP 800-37r2**.

2.1. Objetivo del Manual

El objetivo principal de este manual es proporcionar un marco integral para la gestión de la seguridad de la información y la ciberseguridad en FALCOM AGF. A través de la implementación de políticas, procedimientos y controles específicos, se busca:

- **Proteger la información** contra amenazas internas y externas, accidentales o deliberadas, garantizando su confidencialidad, integridad y disponibilidad.
- **Establecer lineamientos claros** para la gestión de riesgos de seguridad de la información, alineados con la estrategia corporativa y los requisitos regulatorios.
- **Fomentar una cultura organizacional** orientada a la ciberseguridad, donde todos los colaboradores comprendan sus responsabilidades en la protección de los activos de información.
- **Cumplir con las obligaciones regulatorias**, incluyendo la NCG 510, la Ley Marco de Ciberseguridad y otros marcos normativos aplicables.
- **Asegurar la continuidad del negocio**, mediante la gestión proactiva de incidentes de seguridad y la implementación de planes de recuperación ante desastres.

Este manual está diseñado para ser un documento vivo, sujeto a actualizaciones periódicas que reflejen la evolución de las amenazas, los cambios tecnológicos y las mejores prácticas internacionales en ciberseguridad.

2.2. Alcance

El alcance de este manual abarca todos los aspectos relacionados con la seguridad de la información y la ciberseguridad dentro de FALCOM AGF. Incluye, pero no se limita a:

Ámbitos de Aplicación:

- **Áreas Funcionales:** Todas las unidades de negocio, áreas operativas, departamentos de soporte y funciones estratégicas de la organización.
- **Procesos Críticos:** Procesos relacionados con la gestión de inversiones, análisis financiero, operaciones de back-office, gestión de riesgos, cumplimiento normativo y atención al cliente.
- **Sistemas de Información:** Infraestructura tecnológica, redes de comunicaciones, aplicaciones corporativas, bases de datos, servicios en la nube y dispositivos móviles utilizados para el procesamiento y almacenamiento de información.
- **Activos de Información:** Incluye información confidencial, datos personales, registros financieros, documentación interna, y cualquier otro activo que sea relevante para la operación de FALCOM AGF.

Cobertura de Usuarios:

Este manual aplica a todas las personas que, de forma directa o indirecta, interactúan con los sistemas de información de FALCOM AGF, incluyendo:

- **Directivos y Ejecutivos:** Responsables de la toma de decisiones estratégicas en materia de seguridad de la información.
- **Empleados:** Independientemente de su nivel jerárquico o área de trabajo, todos los colaboradores tienen responsabilidades específicas en la protección de la información.
- **Contratistas y Proveedores:** Terceros que prestan servicios a la organización y que tienen acceso a los sistemas o datos corporativos.
- **Clientes y Usuarios Externos:** En la medida en que interactúan con las plataformas digitales de FALCOM AGF, deben cumplir con las políticas de seguridad establecidas.

El alcance de este manual se extiende a las operaciones locales e internacionales de FALCOM AGF, considerando las particularidades regulatorias de cada jurisdicción en la que la organización opera.

2.3. Marco Normativo

El marco normativo que sustenta este manual está compuesto por regulaciones nacionales e internacionales, estándares de mejores prácticas y directrices internas de FALCOM AGF. Este enfoque integral garantiza la alineación con los requisitos legales y regulatorios, así como con las expectativas del mercado en materia de seguridad de la información y ciberseguridad.

Normativas Regulatorias:

- **NCG 510 de la Comisión para el Mercado Financiero (CMF):** Establece los lineamientos para la gestión de riesgos operacionales, incluyendo la seguridad de la información, la continuidad del negocio y la gestión de servicios externalizados.
- **Ley N° 21.663 - Ley Marco de Ciberseguridad:** Define el marco legal para la protección de infraestructuras críticas y la gestión de incidentes de ciberseguridad en Chile.
- **Reglamento General de Protección de Datos (RGPD) - Unión Europea:** Aplicable en contextos internacionales donde se gestionen datos personales de ciudadanos de la UE.

Estándares Internacionales:

- **ISO/IEC 27001:2022 - Sistema de Gestión de Seguridad de la Información (SGSI):** Establece los requisitos para implementar, mantener y mejorar un SGSI efectivo.
- **ISO/IEC 27002:2022 - Código de Prácticas para Controles de Seguridad de la Información:** Proporciona directrices para la implementación de controles de seguridad específicos.
- **NIST SP 800-37r2 - Risk Management Framework (RMF):** Marco de gestión de riesgos que integra la seguridad de la información y la privacidad en el ciclo de vida de los sistemas.

Políticas y Directrices Internas:

- **Política General de Seguridad de la Información y Ciberseguridad**
- **Política de Seguridad en la Nube**
- **Política de Seguridad de Proveedores**
- **Política de Seguridad de Redes**
- **Política de Seguridad de Personas**

Estas normativas y estándares constituyen la base sobre la cual se desarrolla la estrategia de ciberseguridad de FALCOM AGF, asegurando la coherencia y la eficacia de los controles implementados.

2.4. Definiciones y Glosario de Términos Clave

Para una mejor comprensión de los conceptos utilizados en este manual, se incluye un glosario de términos clave relacionados con la seguridad de la información y la ciberseguridad. Este glosario será ampliado en los anexos del documento, pero a continuación se presentan algunas definiciones fundamentales:

- **Activo de Información:** Cualquier dato, sistema, recurso tecnológico o proceso que tenga valor para la organización.
- **Amenaza:** Cualquier circunstancia o evento que pueda explotar una vulnerabilidad y causar daño a un activo de información.
- **Confidencialidad:** Propiedad que garantiza que la información solo sea accesible por personas autorizadas.
- **Disponibilidad:** Aseguramiento de que la información y los sistemas estén accesibles y operativos cuando se necesiten.
- **Integridad:** Garantía de que la información es precisa, completa y no ha sido alterada de forma no autorizada.
- **Incidente de Seguridad:** Evento que compromete o tiene el potencial de comprometer la seguridad de la información.
- **Riesgo:** Combinación de la probabilidad de que ocurra un evento de seguridad y el impacto asociado.
- **Vulnerabilidad:** Debilidad en un sistema, proceso o control que puede ser explotada por una amenaza para comprometer la seguridad de la información.
- **Ciberseguridad:** Conjunto de políticas, tecnologías y procesos diseñados para proteger sistemas de información contra ciberamenazas.
- **Gestión de Riesgos:** Proceso sistemático para identificar, evaluar, tratar y monitorear riesgos que afectan la seguridad de la información.

Este glosario se actualizará de forma continua para reflejar la evolución de la terminología en el ámbito de la ciberseguridad y la gestión de riesgos.

3. Gobernanza de la Seguridad de la Información

La **gobernanza de la seguridad de la información** constituye el marco estratégico que permite a FALCOM AGF garantizar que la seguridad de la información sea gestionada de manera efectiva y alineada con los objetivos corporativos. Este marco asegura que los recursos, las políticas y los controles de seguridad estén diseñados

e implementados de forma coherente para proteger los activos de información de la organización, cumplir con las regulaciones aplicables y gestionar los riesgos de manera proactiva.

La gobernanza de la seguridad de la información se basa en principios de **responsabilidad, rendición de cuentas, transparencia y mejora continua**, promoviendo una cultura organizacional que considera la ciberseguridad como un factor crítico para el éxito del negocio.

3.1. Políticas de Seguridad de la Información y Ciberseguridad

Las **políticas de seguridad de la información y ciberseguridad** son el pilar fundamental de la gobernanza en FALCOM AGF. Estas políticas establecen las directrices y los principios que orientan la gestión de la seguridad, definiendo el comportamiento esperado de los empleados, proveedores y otras partes interesadas en relación con la protección de la información.

Política General de Seguridad de la Información y Ciberseguridad

Esta política define el compromiso de FALCOM AGF con la protección de la información en todas sus formas, abarcando tanto los entornos tecnológicos como los procesos de negocio. Sus objetivos principales son:

- **Proteger la confidencialidad, integridad y disponibilidad de la información** en todos los sistemas y procesos de la organización.
- **Establecer un marco de gestión de riesgos de seguridad de la información** que permita identificar, evaluar y mitigar amenazas de forma proactiva.
- **Asegurar el cumplimiento de la normativa legal y regulatoria**, incluyendo la NCG 510 de la CMF, la Ley Marco de Ciberseguridad y estándares internacionales como ISO 27001 e ISO 27002.
- **Fomentar una cultura de ciberseguridad**, mediante la concienciación y la capacitación continua del personal.

Políticas Específicas Complementarias

Además de la política general, FALCOM AGF cuenta con políticas específicas que abordan áreas críticas de la seguridad de la información, tales como:

- **Política de Seguridad en la Nube:** Establece los controles para la gestión segura de servicios y datos en entornos de computación en la nube.
- **Política de Seguridad de Proveedores:** Define los requisitos de seguridad para la gestión de relaciones con terceros y proveedores críticos.
- **Política de Seguridad de Redes:** Regula la protección de las infraestructuras de red, incluyendo el control de accesos, la segmentación y la monitorización de tráfico.
- **Política de Seguridad de Personas:** Enfocada en la gestión de la seguridad en relación con el factor humano, incluyendo la capacitación y la gestión de identidades.

Estas políticas son revisadas y actualizadas de manera periódica para garantizar su vigencia y eficacia frente a la evolución de las amenazas y los cambios en el entorno regulatorio.

3.2. Roles y Responsabilidades

La gestión de la seguridad de la información en FALCOM AGF se sustenta en una **estructura organizativa clara**, con roles y responsabilidades bien definidos que aseguran una gobernanza efectiva y una adecuada segregación de funciones. La asignación de responsabilidades se basa en el principio de **"accountability"**, garantizando que cada actor en la organización entienda su papel en la protección de la información.

Alta Dirección

- **Directorio:** Responsable último de la seguridad de la información. Aprueba la estrategia de ciberseguridad, las políticas y la asignación de recursos necesarios para su implementación.

- **Gerencia:** Supervisa la ejecución de la estrategia de seguridad de la información, asegurando su alineación con los objetivos del negocio.

Comité de Sistemas y Ciberseguridad
El **Comité de Sistemas y Ciberseguridad** es el órgano colegiado encargado de la supervisión y el seguimiento de la gestión de la seguridad en la organización. Sus funciones incluyen:

- Definir y revisar la estrategia de seguridad de la información.
- Evaluar los riesgos de seguridad y aprobar planes de mitigación.
- Monitorear el cumplimiento de las políticas y regulaciones.
- Revisar informes de incidentes de seguridad y coordinar la respuesta ante crisis cibernéticas.

Responsable de Seguridad de la Información y Ciberseguridad
Es el responsable de liderar la gestión de la seguridad de la información en FALCOM AGF. Su rol es estratégico y operativo, con funciones que incluyen:

- Desarrollar e implementar la estrategia de ciberseguridad de la organización.
- Identificar y gestionar los riesgos de seguridad de la información.
- Coordinar las actividades de respuesta ante incidentes de seguridad.
- Promover la concienciación en ciberseguridad en toda la organización.
- Actuar como punto de contacto con los reguladores en materia de seguridad de la información.

Áreas de Tecnología de la Información (TI)

- Implementación de controles técnicos de seguridad en la infraestructura tecnológica.
- Gestión de accesos, seguridad de redes, cifrado de datos y monitoreo de eventos de seguridad.
- Soporte en la investigación y análisis de incidentes de ciberseguridad.

Áreas de Cumplimiento y Riesgos

- Asegurar el cumplimiento de las normativas legales y regulatorias relacionadas con la seguridad de la información.
- Integrar la gestión de riesgos de seguridad de la información en el marco de riesgos corporativos.

Todos los Empleados
La seguridad de la información es una responsabilidad compartida. Todos los empleados de FALCOM AGF deben:

- Conocer y cumplir con las políticas y procedimientos de seguridad.
- Participar en programas de formación y concienciación en ciberseguridad.
- Reportar de manera inmediata cualquier incidente de seguridad o vulnerabilidad detectada.

3.3. Gestión del Apetito por el Riesgo
El **apetito por el riesgo** define el nivel de riesgo que FALCOM AGF está dispuesta a aceptar en relación con la seguridad de la información, en función de su estrategia de negocio, su capacidad para gestionar riesgos y su entorno regulatorio.

Definición del Apetito por el Riesgo
El apetito por el riesgo en ciberseguridad se establece considerando:

- **Impacto Potencial:** Consecuencias financieras, operativas, legales y reputacionales de los incidentes de seguridad.
- **Probabilidad de Ocurrencia:** Evaluación de la frecuencia con la que podrían materializarse amenazas específicas.

- **Capacidades de Mitigación:** Controles y recursos disponibles para prevenir, detectar y responder a incidentes de seguridad.

Categorías de Apetito por el Riesgo:

- **Riesgo Inaceptable:** Situaciones que la organización no está dispuesta a tolerar bajo ninguna circunstancia (por ejemplo, pérdida de datos confidenciales críticos sin cifrado).
- **Riesgo Condicional:** Riesgos que pueden ser aceptados si se implementan controles de mitigación adecuados.
- **Riesgo Aceptable:** Riesgos menores que se consideran tolerables debido a su bajo impacto y probabilidad.

La gestión del apetito por el riesgo se revisa de forma periódica y se adapta a los cambios en el entorno operativo, regulatorio y tecnológico.

3.4. Estructura de Reporte y Toma de Decisiones

Una **estructura de reporte y toma de decisiones clara y eficiente** es fundamental para la gestión eficaz de la seguridad de la información. En FALCOM AGF, esta estructura está diseñada para garantizar que la información relevante sobre riesgos, incidentes y controles de seguridad llegue de manera oportuna a los niveles adecuados de la organización.

Flujos de Información:

- **Reporte de Incidentes de Seguridad:** Todos los empleados deben reportar incidentes de seguridad de manera inmediata al equipo de ciberseguridad o al Responsable de Seguridad de la Información y Ciberseguridad.
- **Informes Periódicos de Seguridad:** El Responsable de Seguridad de la Información Y Ciberseguridad presenta informes regulares al Comité de Tecnología y Ciberseguridad y a la Alta Dirección, incluyendo análisis de riesgos, incidentes relevantes y recomendaciones de mejora.
- **Escalamiento de Incidentes Críticos:** En caso de incidentes de alta criticidad (por ejemplo, brechas de datos o ciberataques significativos), se activa un protocolo de escalamiento rápido que involucra al Comité de Crisis y, si es necesario, a las autoridades regulatorias.

Toma de Decisiones:

Las decisiones estratégicas en materia de seguridad de la información, como la aprobación de políticas, asignación de recursos o respuesta a incidentes críticos, son responsabilidad del Comité de Tecnología y Ciberseguridad y de la Alta Dirección. Estas decisiones se basan en:

- Análisis de riesgos detallados.
- Evaluación del impacto en el negocio.
- Cumplimiento de requisitos regulatorios.
- Recomendaciones del Responsable de Seguridad de la Información Y Ciberseguridad, y de los equipos técnicos.

4. GESTIÓN DEL RIESGO OPERACIONAL (CONFORME A NCG 510)

La **gestión del riesgo operacional** es un componente esencial de la estrategia de seguridad de FALCOM AGF, ya que permite identificar, evaluar, mitigar y monitorear los riesgos que pueden afectar la operación continua de la organización. Según la **Norma de Carácter General N°510 (NCG 510)** de la **Comisión para el Mercado Financiero (CMF)**, la gestión del riesgo operacional debe estar integrada en el marco de control interno de las instituciones financieras, considerando factores tecnológicos, humanos, organizativos y externos.

El objetivo de esta sección es establecer los principios, procesos y responsabilidades para una gestión proactiva de los riesgos operacionales, especialmente aquellos relacionados con la seguridad de la información y la ciberseguridad.

4.1. Metodología de Identificación, Evaluación y Tratamiento del Riesgo

La gestión del riesgo operacional en FALCOM AGF se basa en un enfoque sistemático y estructurado, que sigue las mejores prácticas internacionales, como las definidas en la **ISO 31000:2018** y el **NIST SP 800-37r2**. Este enfoque abarca cuatro fases principales:

a. Identificación del Riesgo

La identificación de riesgos tiene como objetivo reconocer de manera temprana los eventos, amenazas o vulnerabilidades que podrían afectar los procesos críticos de la organización. Se consideran riesgos asociados a:

- **Tecnologías de la Información:** Fallos de sistemas, ataques cibernéticos, vulnerabilidades de software, brechas de seguridad.
- **Factores Humanos:** Errores operativos, falta de capacitación, accesos no autorizados, ingeniería social.
- **Procesos Internos:** Inadecuadas segregaciones de funciones, deficiencias en controles internos, fraudes internos.
- **Factores Externos:** Desastres naturales, cambios regulatorios, incidentes en la cadena de suministro, dependencia de terceros críticos.

Se utilizan herramientas y técnicas como:

- **Mapeo de Procesos:** Identificación de puntos críticos en los flujos de trabajo.
- **Análisis de Incidentes Pasados:** Revisión de eventos históricos para identificar patrones de riesgo.
- **Evaluaciones de Vulnerabilidades:** Pruebas de seguridad, análisis de brechas y auditorías técnicas.
- **Entrevistas y Talleres de Riesgos:** Involucramiento de expertos internos para identificar riesgos emergentes.

b. Evaluación del Riesgo

Una vez identificados, los riesgos se evalúan en términos de su **probabilidad de ocurrencia** y su **impacto potencial** sobre la organización. La evaluación se realiza mediante:

- **Matriz de Riesgos:** Herramienta que permite clasificar los riesgos según su severidad (bajo, moderado, alto, crítico).
- **Análisis Cualitativo:** Evaluación basada en juicios de expertos para identificar riesgos significativos.
- **Análisis Cuantitativo:** Aplicación de modelos matemáticos o estadísticos para cuantificar el impacto financiero o operativo de los riesgos.

c. Tratamiento del Riesgo

El tratamiento de los riesgos identificados se lleva a cabo mediante la implementación de estrategias que buscan reducir la probabilidad de ocurrencia o el impacto de los eventos adversos. Las opciones de tratamiento incluyen:

- **Mitigación:** Implementación de controles técnicos, organizativos o procedimentales para reducir el riesgo (por ejemplo, firewalls, autenticación multifactor, planes de continuidad del negocio).
- **Transferencia:** Transferencia del riesgo a terceros mediante seguros o acuerdos contractuales (por ejemplo, ciberseguros, outsourcing de servicios críticos con cláusulas de seguridad).

- **Aceptación:** Aceptación del riesgo cuando su impacto es tolerable y el costo de mitigación supera el beneficio esperado.
- **Evitar el Riesgo:** Modificación o eliminación de procesos, tecnologías o actividades que generen riesgos inaceptables.

d. Monitoreo y Revisión del Riesgo
La gestión del riesgo es un proceso continuo. Por ello, FALCOM AGF establece mecanismos de monitoreo y revisión para:

- Evaluar la efectividad de los controles implementados.
- Identificar cambios en el entorno interno o externo que puedan generar nuevos riesgos.
- Asegurar que los riesgos residuales se mantengan dentro del apetito por el riesgo definido por la organización.

4.2. Integración con la Gestión de Riesgos Corporativos
La gestión del riesgo operacional en FALCOM AGF está plenamente integrada en el **marco de gestión de riesgos corporativos**, lo que permite un enfoque holístico y coordinado en la identificación, evaluación y tratamiento de los riesgos que afectan a la organización.
Principios de Integración:

- **Visión Integral del Riesgo:** Los riesgos operacionales, tecnológicos, de ciberseguridad, legales, financieros y reputacionales se gestionan de manera integrada, considerando sus interrelaciones.
- **Gobernanza Estructurada:** La gestión del riesgo es responsabilidad de toda la organización, con roles claramente definidos para la Alta Dirección, los comités de riesgos y las áreas operativas.
- **Toma de Decisiones Basada en el Riesgo:** Las decisiones estratégicas se fundamentan en el análisis de riesgos, permitiendo priorizar recursos y esfuerzos en función del impacto potencial.

Interconexión de Riesgos:

- **Riesgo Operacional y Ciberseguridad:** Los ciberataques pueden generar riesgos operacionales significativos, como interrupciones en los servicios críticos o pérdida de datos confidenciales.
- **Riesgo de Terceros:** La dependencia de proveedores críticos introduce riesgos operacionales que deben ser evaluados y gestionados mediante contratos robustos y auditorías de seguridad.
- **Riesgo Regulatorio:** El incumplimiento de normativas de seguridad de la información puede derivar en sanciones legales y daños reputacionales.

Esta integración permite a FALCOM AGF anticiparse a los desafíos emergentes y responder de manera eficaz a incidentes que puedan afectar la continuidad del negocio.

4.3. Indicadores Clave de Riesgo (KRI)
Los **Indicadores Clave de Riesgo (KRI)** son métricas que permiten monitorear de forma proactiva la exposición de la organización a riesgos operacionales y de seguridad de la información. Estos indicadores proporcionan señales de alerta temprana que facilitan la toma de decisiones y la adopción de medidas preventivas antes de que se materialicen eventos adversos.

Características de los KRIs Efectivos:

- **Relevancia:** Deben estar alineados con los objetivos estratégicos de la organización y con los riesgos críticos identificados.

- **Medibilidad:** Deben basarse en datos objetivos y cuantificables para facilitar su análisis y seguimiento.
- **Claridad:** Deben ser comprensibles para todos los niveles de la organización.
- **Capacidad Predictiva:** Deben permitir anticipar la ocurrencia de eventos de riesgo antes de que se materialicen.

Ejemplos de KRIs en Seguridad de la Información:

- **Número de Incidentes de Seguridad Registrados:** Frecuencia de eventos que comprometen la seguridad de la información.
- **Tiempos de Respuesta a Incidentes (MTTR):** Tiempo medio necesario para identificar, contener y resolver incidentes de ciberseguridad.
- **Porcentaje de Parches de Seguridad Aplicados a Tiempo:** Nivel de cumplimiento en la gestión de vulnerabilidades.
- **Tasa de Éxito en Simulacros de Phishing:** Porcentaje de empleados que identifican correctamente intentos de phishing en pruebas controladas.
- **Disponibilidad de Sistemas Críticos:** Medición de la continuidad operativa de los sistemas esenciales para el negocio.

Estos indicadores se revisan de forma periódica en los comités de riesgos y seguridad de la información, y sus resultados se utilizan para mejorar continuamente los controles de seguridad.

4.4. Registro y Reporte de Incidentes Operacionales

El **registro y reporte de incidentes operacionales** es fundamental para la gestión del riesgo en FALCOM AGF, ya que permite documentar, analizar y aprender de los eventos adversos que puedan afectar la seguridad de la información o la continuidad del negocio.

Definición de Incidente Operacional:

Se considera incidente operacional cualquier evento que pueda interrumpir, degradar o comprometer la operatividad de la organización, incluyendo:

- **Fallas Tecnológicas:** Caídas de sistemas críticos, interrupciones en servicios en la nube, pérdida de datos.
- **Ciberincidentes:** Ataques de malware, ransomware, accesos no autorizados, violaciones de datos.
- **Errores Humanos:** Configuraciones incorrectas, errores en el procesamiento de transacciones, incumplimiento de procedimientos de seguridad.
- **Incidentes Físicos:** Desastres naturales, fallos en infraestructuras críticas, robos o accesos no autorizados a instalaciones.

Proceso de Gestión de Incidentes:

- **Detección:** Identificación temprana del incidente mediante sistemas de monitoreo, alertas automáticas o reportes del personal.
- **Notificación:** Comunicación inmediata del incidente a los equipos responsables, siguiendo los canales de reporte definidos.
- **Registro:** Documentación detallada del incidente, incluyendo la descripción del evento, su impacto, las causas identificadas y las acciones de respuesta implementadas.
- **Análisis:** Evaluación del incidente para identificar lecciones aprendidas, causas raíz y oportunidades de mejora en los controles existentes.
- **Reporte a Autoridades Regulatorias:** En caso de incidentes significativos, se notificará a la CMF y a otras autoridades pertinentes, cumpliendo con los plazos y requisitos establecidos por la NCG 510.

Cultura de Reporte:

FALCOM AGF promueve una **cultura de reporte proactiva**, donde todos los empleados se sientan responsables de informar sobre incidentes de seguridad sin temor a represalias. Esto contribuye a fortalecer la resiliencia organizacional y la capacidad de respuesta ante crisis.

5. SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD (NCG 510 - SECCIÓN A)

La **seguridad de la información y la ciberseguridad** son componentes críticos de la estrategia de gestión de riesgos de FALCOM AGF. En un entorno financiero caracterizado por una creciente digitalización y sofisticación de las amenazas cibernéticas, proteger los activos de información no solo es una exigencia regulatoria establecida por la **NCG 510 de la CMF**, sino también una prioridad estratégica para garantizar la continuidad del negocio, la confianza de los clientes y la integridad de las operaciones financieras.

El enfoque de FALCOM AGF en materia de ciberseguridad se basa en principios de **protección proactiva**, **resiliencia organizacional** y **mejora continua**, integrando controles técnicos, administrativos y físicos para mitigar los riesgos asociados a la seguridad de la información.

5.1. Política de Seguridad de la Información y Ciberseguridad
La **Política de Seguridad de la Información y Ciberseguridad** de FALCOM AGF es el documento rector que establece los principios, objetivos y directrices para la gestión de la seguridad de la información en toda la organización. Esta política refleja el compromiso de la Alta Dirección con la protección de los activos de información y el cumplimiento de las normativas vigentes.

Objetivos de la Política:
- **Proteger la confidencialidad, integridad y disponibilidad** de la información gestionada por la organización.
- **Prevenir, detectar, responder y recuperar** ante incidentes de seguridad de la información y ciberataques.
- **Asegurar el cumplimiento** de las normativas nacionales e internacionales aplicables en materia de ciberseguridad, como la NCG 510, ISO 27001 e ISO 27002.
- **Fomentar una cultura organizacional** orientada a la gestión de riesgos de seguridad de la información, con un enfoque en la concienciación y la responsabilidad compartida.

Actualización y Revisión de la Política:
La política se revisa de forma periódica, al menos una vez al año o cuando se produzcan cambios significativos en el entorno tecnológico, regulatorio o de amenazas. Las actualizaciones deben ser aprobadas por el **Consejo de Administración** y el **Comité de Tecnología y Ciberseguridad**, garantizando su alineación con la estrategia corporativa.

Aprobación y Compromiso del Directorio:
El Directorio de FALCOM AGF es responsable de aprobar la política y de supervisar su implementación efectiva. Este compromiso se refleja en la asignación de recursos adecuados, la definición de roles y responsabilidades, y la integración de la ciberseguridad en la toma de decisiones estratégicas.

5.2. Gestión de Activos de Información
La **gestión de activos de información** tiene como objetivo identificar, clasificar, proteger y administrar de manera adecuada todos los activos que poseen valor para FALCOM AGF, incluyendo datos, sistemas, aplicaciones, infraestructura tecnológica y recursos humanos.

Inventario de Activos:
FALCOM AGF mantiene un **inventario actualizado de activos de información**, que incluye:
- **Activos Físicos:** Equipos informáticos, servidores, dispositivos móviles, medios de almacenamiento.
- **Activos Lógicos:** Bases de datos, aplicaciones, sistemas operativos, software de seguridad.
- **Información:** Datos financieros, registros de clientes, información confidencial, propiedad intelectual.
- **Servicios en la Nube:** Infraestructura, plataformas y aplicaciones gestionadas en entornos de nube.

El inventario debe contener información detallada sobre la ubicación del activo, su propietario, su clasificación de seguridad y su criticidad para la organización.

Clasificación de la Información:
La información se clasifica en función de su sensibilidad y su impacto potencial en caso de una brecha de seguridad:
- **Confidencial:** Información altamente sensible cuyo acceso está restringido a personal autorizado (ej. datos financieros, credenciales de acceso).

- **Interna:** Información utilizada dentro de la organización, pero que no requiere medidas extremas de protección.
- **Pública:** Información que puede ser compartida libremente sin riesgo para la organización.

Propietarios de Activos:
Cada activo de información tiene un **propietario designado**, responsable de:
- Definir los requisitos de seguridad del activo.
- Asegurar que se apliquen controles de protección adecuados.
- Gestionar el ciclo de vida del activo, incluyendo su creación, uso, almacenamiento y eliminación segura.

5.3. Control de Accesos
El **control de accesos** es un componente esencial de la seguridad de la información, ya que permite garantizar que solo las personas autorizadas puedan acceder a los recursos de la organización, y únicamente en la medida necesaria para el desempeño de sus funciones.

Gestión de Identidades y Accesos (IAM):
FALCOM AGF implementa un sistema de **Gestión de Identidades y Accesos (IAM)** que abarca:
- **Creación y Gestión de Cuentas:** Procedimientos para el alta, modificación y baja de cuentas de usuario, tanto internas como de terceros.
- **Principio de Privilegio Mínimo:** Los usuarios solo tienen acceso a la información y los recursos necesarios para realizar su trabajo.
- **Segregación de Funciones:** Diseño de controles para evitar conflictos de interés y reducir el riesgo de fraude o errores operativos.

Autenticación Multifactor (MFA):
Se requiere el uso de **autenticación multifactor (MFA)** para acceder a sistemas críticos, aplicaciones sensibles y entornos en la nube. Esto incluye una combinación de:
- **Algo que sabes:** Contraseñas seguras.
- **Algo que tienes:** Tokens, dispositivos móviles para autenticación.
- **Algo que eres:** Datos biométricos, como huellas dactilares o reconocimiento facial.

Gestión de Accesos Remotos:
El acceso remoto a los sistemas de FALCOM AGF se realiza a través de canales seguros, utilizando:
- **Redes Privadas Virtuales (VPN)** cifradas.
- **Controles de Seguridad Adicionales:** Autenticación reforzada, monitoreo de conexiones y restricciones de acceso basadas en la ubicación.

Revisión y Auditoría de Accesos:
Se realizan auditorías periódicas para revisar los permisos de acceso, identificar accesos innecesarios o inadecuados y detectar posibles anomalías o actividades sospechosas.

5.4. Protección de Infraestructura y Redes
La **protección de la infraestructura tecnológica y las redes de comunicación** es fundamental para garantizar la resiliencia de los sistemas de FALCOM AGF frente a amenazas internas y externas.

Segmentación de Redes:
La red de la organización está segmentada en diferentes zonas de seguridad, como:
- **Zona de Usuario:** Redes internas para operaciones diarias.
- **Zona DMZ (Zona Desmilitarizada):** Para exponer servicios externos de forma controlada, minimizando el riesgo de acceso directo a la red interna.

- **Redes Críticas:** Segmentadas con controles adicionales para proteger sistemas sensibles, como aplicaciones financieras y bases de datos.

Seguridad Física:
Los centros de datos y las instalaciones críticas cuentan con medidas de **seguridad física**, que incluyen:
- Control de acceso mediante tarjetas de identificación, biometría y vigilancia por CCTV.
- Sistemas de detección de incendios, control de temperatura y redundancia eléctrica.
- Protocolos de acceso restringido para personal autorizado.

Seguridad Lógica:
Se implementan controles de seguridad lógica para proteger la infraestructura tecnológica, tales como:
- **Firewalls de Nueva Generación:** Para filtrar tráfico de red y prevenir accesos no autorizados.
- **Sistemas de Detección y Prevención de Intrusiones (IDS/IPS):** Para identificar y bloquear actividades maliciosas en tiempo real.
- **Cifrado de Comunicaciones:** Utilización de protocolos seguros (TLS/SSL) para proteger la integridad y la confidencialidad de los datos en tránsito.

5.5. Gestión de Vulnerabilidades
La **gestión de vulnerabilidades** es un proceso continuo que permite identificar, evaluar, priorizar y mitigar debilidades en los sistemas de información antes de que puedan ser explotadas por actores malintencionados.

Evaluaciones de Vulnerabilidades:
Se realizan evaluaciones periódicas utilizando herramientas automatizadas y análisis manuales para identificar:
- Vulnerabilidades de software, configuraciones incorrectas, puertos abiertos y otros riesgos técnicos.
- Exposiciones en aplicaciones web y servicios en la nube.

Pruebas de Penetración (Pentesting):
Se llevan a cabo **pruebas de penetración** internas y externas para simular ataques reales y evaluar la eficacia de los controles de seguridad existentes. Estas pruebas permiten identificar brechas de seguridad y validar la resiliencia de la organización frente a amenazas avanzadas.

Gestión de Parches:
Se implementa un proceso formal de **gestión de parches de seguridad**, que incluye:
- Evaluación de actualizaciones críticas publicadas por proveedores de software.
- Aplicación oportuna de parches en sistemas críticos.
- Pruebas de validación para garantizar la estabilidad operativa tras la implementación de parches.

5.6. Concienciación y Capacitación en Ciberseguridad
La **concienciación y la capacitación en ciberseguridad** son fundamentales para fortalecer la resiliencia de FALCOM AGF frente a amenazas cibernéticas, ya que el factor humano es a menudo el eslabón más débil en la cadena de seguridad.

Programas de Formación Continua:
FALCOM AGF desarrolla programas de formación adaptados a diferentes perfiles de la organización, que incluyen:
- **Capacitación Básica:** Para todos los empleados, cubriendo temas como buenas prácticas en el uso de contraseñas, seguridad en el correo electrónico, protección de datos y detección de ataques de phishing.

- **Formación Avanzada:** Para personal técnico y equipos de TI, enfocada en ciberseguridad avanzada, gestión de incidentes y análisis forense digital.
- **Simulacros de Ciberataques:** Ejercicios de respuesta ante incidentes para evaluar la preparación de los equipos y mejorar los tiempos de respuesta.

Cultura de Seguridad:
Se promueve una **cultura de ciberseguridad** mediante:

- **Campañas de Concienciación:** Difusión de boletines informativos, alertas de seguridad y materiales educativos.
- **Premios e Incentivos:** Reconocimiento a buenas prácticas en seguridad de la información.
- **Evaluación de la Eficacia:** Medición del impacto de las actividades de formación a través de encuestas, pruebas y análisis de incidentes reportados.

6. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO (NCG 510 - SECCIÓN B)

La **Gestión de la Continuidad del Negocio (BCM, por sus siglas en inglés)** es un proceso fundamental en la estrategia de resiliencia organizacional de FALCOM AGF. Su propósito es garantizar que la organización pueda **responder eficazmente ante incidentes disruptivos**, mantener la operatividad de sus procesos críticos y recuperar rápidamente sus funciones esenciales tras eventos que puedan afectar la continuidad del negocio.

La implementación de un **Sistema de Gestión de Continuidad del Negocio (SGCN)** no solo responde a las exigencias regulatorias establecidas en la **NCG 510 de la Comisión para el Mercado Financiero (CMF)**, sino que también fortalece la confianza de los clientes, socios comerciales y otras partes interesadas.
El enfoque de FALCOM AGF está alineado con estándares internacionales como la **ISO 22301:2019**, la **ISO 27031:2019** para la continuidad de las Tecnologías de la Información, y las mejores prácticas en gestión de riesgos operacionales.

6.1. Política de Continuidad de Negocio

La **Política de Continuidad de Negocio** establece el compromiso de FALCOM AGF con la protección de sus operaciones críticas, asegurando la capacidad de la organización para enfrentar y superar situaciones de crisis. Esta política está aprobada por la Alta Dirección y constituye la base sobre la cual se desarrolla el SGCN.

Objetivos de la Política:

- **Proteger la vida, la salud y la seguridad** de los empleados, clientes y otras partes interesadas en caso de incidentes.
- **Garantizar la continuidad de los procesos críticos** y la disponibilidad de los servicios esenciales durante y después de una interrupción.
- **Minimizar el impacto financiero, operativo y reputacional** de eventos disruptivos.
- **Cumplir con las obligaciones regulatorias y contractuales**, incluyendo los requisitos de la NCG 510 y otras normativas aplicables.
- **Fomentar una cultura de resiliencia organizacional**, integrando la gestión de la continuidad en todos los niveles de la organización.

Alcance de la Política:

La política de continuidad de negocio aplica a:

- **Todas las unidades de negocio** y áreas de soporte de FALCOM AGF.
- **Procesos críticos** identificados en el análisis de impacto en el negocio (BIA).
- **Infraestructura tecnológica** y sistemas de información que soportan operaciones esenciales.
- **Proveedores críticos y socios estratégicos**, cuya interrupción podría afectar la continuidad del negocio.

Responsabilidades:

- **Alta Dirección:** Aprobación de la política, asignación de recursos y supervisión de la implementación del SGCN.
- **Comité de Continuidad del Negocio:** Coordinación de las actividades relacionadas con la continuidad, revisión periódica de planes y supervisión de simulacros.
- **Responsables de Áreas:** Implementación de planes de continuidad en sus respectivas unidades y participación activa en la gestión de crisis.
- **Todos los Empleados:** Conocimiento de los procedimientos de continuidad aplicables a sus funciones y participación en programas de capacitación y ejercicios de simulación.

6.2. Análisis de Impacto en el Negocio (BIA) y Evaluación de Riesgos (RIA)

El **Análisis de Impacto en el Negocio (BIA)** y la **Evaluación de Riesgos de Continuidad (RIA)** son procesos clave para identificar las funciones críticas de la organización, evaluar el impacto potencial de las interrupciones y definir las estrategias de recuperación más adecuadas.

Análisis de Impacto en el Negocio (BIA):

El BIA tiene como objetivo identificar:

- **Procesos Críticos:** Actividades esenciales que, si se interrumpen, podrían afectar significativamente la operatividad, la reputación o el cumplimiento de obligaciones legales de FALCOM AGF.
- **Impacto Potencial:** Evaluación del impacto financiero, legal, operativo y reputacional de la interrupción de cada proceso crítico.
- **Tiempos de Recuperación Aceptables:** Definición de los siguientes parámetros:
    - **RTO (Recovery Time Objective):** Tiempo máximo tolerable para la recuperación de un proceso tras una interrupción.

- **RPO (Recovery Point Objective):** Máxima cantidad de datos que se puede perder sin afectar de manera crítica la operación (define la frecuencia de las copias de seguridad necesarias).

Evaluación de Riesgos de Continuidad (RIA):
El RIA complementa el BIA al identificar y evaluar los riesgos que podrían interrumpir los procesos críticos. Incluye:

- **Identificación de Amenazas:** Fallos tecnológicos, ciberataques, desastres naturales, pandemias, errores humanos, fallos en la cadena de suministro, entre otros.
- **Análisis de Vulnerabilidades:** Factores internos que podrían aumentar la probabilidad o el impacto de una interrupción (por ejemplo, falta de redundancia en infraestructuras críticas).
- **Evaluación del Impacto:** Determinación del nivel de riesgo en función de la probabilidad de ocurrencia y el impacto potencial.
- **Definición de Controles de Mitigación:** Estrategias para reducir la probabilidad de interrupciones o su impacto en la organización.

Estos análisis se revisan de forma periódica y cada vez que haya cambios significativos en el entorno operativo, tecnológico o regulatorio de la organización.

6.3. Planes de Continuidad y Recuperación ante Desastres (BCP/DRP)
FALCOM AGF desarrolla e implementa planes detallados para garantizar la continuidad de sus operaciones críticas y la recuperación de sus sistemas tras un evento disruptivo. Estos planes se dividen en dos categorías principales:

Planes de Continuidad del Negocio (BCP):
El **BCP (Business Continuity Plan)** establece los procedimientos necesarios para mantener la operatividad de la organización durante una interrupción. Incluye:

- **Estrategias de Continuidad:** Definición de soluciones de respaldo para procesos críticos, incluyendo el uso de sedes alternas, trabajo remoto y redundancia de recursos tecnológicos.
- **Planes de Comunicación en Crisis:** Procedimientos para la gestión de la comunicación interna y externa durante una crisis, asegurando la transparencia y la coordinación eficiente.
- **Roles y Responsabilidades:** Definición clara de las funciones de los equipos de gestión de crisis, continuidad del negocio y respuesta a incidentes.

Planes de Recuperación ante Desastres (DRP):
El **DRP (Disaster Recovery Plan)** se centra en la restauración de los sistemas tecnológicos y la infraestructura de TI tras un incidente. Incluye:

- **Procedimientos de Recuperación de Sistemas:** Instrucciones detalladas para la restauración de servidores, bases de datos, redes y aplicaciones críticas.
- **Copias de Seguridad y Recuperación de Datos:** Estrategias de backup que aseguran la integridad y disponibilidad de la información.
- **Sistemas de Alta Disponibilidad y Redundancia:** Implementación de infraestructuras resilientes para minimizar el tiempo de inactividad en caso de fallos tecnológicos.
- **Planes de Recuperación en la Nube:** Procedimientos específicos para entornos de computación en la nube, considerando los acuerdos de nivel de servicio (SLA) con proveedores externos.

Procedimientos de Activación:
Tanto el BCP como el DRP incluyen criterios específicos para la **activación de los planes**, que definen:

- **Escenarios de Activación:** Tipos de incidentes que justifican la activación del plan (por ejemplo, ciberataques, desastres naturales, fallos críticos de infraestructura).
- **Líneas de Comando:** Estructura jerárquica para la toma de decisiones durante la crisis.
- **Protocolos de Escalamiento:** Procedimientos para notificar a la Alta Dirección, autoridades regulatorias y otras partes interesadas.

6.4. Pruebas y Ejercicios de Simulación

La **validación de los planes de continuidad y recuperación** es fundamental para garantizar su eficacia en situaciones reales. FALCOM AGF realiza pruebas y ejercicios de simulación de forma periódica para:

- Evaluar la capacidad de respuesta de la organización ante incidentes disruptivos.
- Identificar oportunidades de mejora en los planes, procedimientos y controles implementados.
- Fortalecer la preparación y concienciación del personal respecto a sus roles y responsabilidades durante una crisis.

Tipos de Pruebas de Continuidad:

- **Revisión de Documentación:** Análisis teórico de los planes para verificar su actualización y coherencia con los procesos actuales.
- **Pruebas de Mesa (Tabletop Exercises):** Simulación de escenarios de crisis en un entorno controlado, donde los equipos discuten y analizan la respuesta sin ejecutar físicamente las acciones.
- **Pruebas Técnicas:** Evaluación práctica de la capacidad para recuperar sistemas tecnológicos, incluyendo pruebas de recuperación de datos, conmutación por error (failover) y restauración de copias de seguridad.
- **Simulacros en Tiempo Real:** Ejercicios integrales que simulan incidentes reales, involucrando a diferentes áreas de la organización y, en algunos casos, a proveedores externos y autoridades regulatorias.

Gestión de Resultados:

Tras la ejecución de cada prueba o simulacro, se realiza un análisis de resultados que incluye:

- **Identificación de Gaps:** Detección de debilidades en la planificación o en la ejecución de los procedimientos.
- **Lecciones Aprendidas:** Documentación de las buenas prácticas y áreas de mejora identificadas durante el ejercicio.
- **Planes de Mejora:** Definición de acciones correctivas para fortalecer la resiliencia de la organización.

La Alta Dirección recibe informes detallados sobre los resultados de las pruebas y el estado de preparación de la organización, lo que permite una mejora continua del SGCN.

7. GESTIÓN DE SERVICIOS EXTERNALIZADOS (NCG 510 - SECCIÓN C)

La **gestión de servicios externalizados** es un componente crítico de la estrategia de seguridad de la información y continuidad del negocio de FALCOM AGF. En un entorno donde la dependencia de proveedores externos, especialmente de servicios tecnológicos y de nube, es cada vez más relevante, la adecuada gestión de terceros se convierte en un factor esencial para mitigar riesgos operacionales, tecnológicos y regulatorios.

De acuerdo con la **Norma de Carácter General N°510 (NCG 510)** de la **Comisión para el Mercado Financiero (CMF)**, las instituciones financieras deben implementar un marco de control que garantice que los riesgos asociados a la externalización de servicios sean identificados, evaluados y gestionados de manera eficaz.
Este enfoque está alineado con estándares internacionales como la **ISO 27001:2022**, la **ISO 27036** (gestión de relaciones con proveedores), y las mejores prácticas del **NIST SP 800-171** para la protección de la información en entornos de terceros.

7.1. Política de Gestión de Terceros

La **Política de Gestión de Terceros** de FALCOM AGF establece los principios y directrices para la evaluación, selección, contratación y supervisión de proveedores de servicios críticos, con el objetivo de:

- **Proteger la confidencialidad, integridad y disponibilidad** de la información procesada o gestionada por terceros.
- **Asegurar la continuidad del negocio**, minimizando el impacto de posibles fallos en los servicios externalizados.
- **Cumplir con las regulaciones vigentes**, incluyendo la NCG 510 y otros marcos regulatorios aplicables.
- **Promover relaciones basadas en la seguridad, la responsabilidad y la transparencia** con los proveedores.

Ámbito de Aplicación:
Esta política aplica a todos los servicios externalizados que puedan tener un impacto significativo en la seguridad de la información, la continuidad del negocio o el cumplimiento normativo. Incluye, entre otros:

- **Proveedores de servicios en la nube (Cloud Services)**
- **Proveedores de infraestructura tecnológica y redes**
- **Servicios de soporte técnico y mantenimiento de sistemas**
- **Consultores de ciberseguridad y servicios de auditoría externa**
- **Proveedores de servicios críticos para la operación financiera**

Principios Rectores:

- **Responsabilidad Compartida:** Aunque un servicio esté externalizado, FALCOM AGF mantiene la responsabilidad final sobre la gestión de riesgos y el cumplimiento de la normativa.
- **Gestión Basada en Riesgos:** La profundidad del control y monitoreo se ajusta al nivel de riesgo asociado al servicio y al proveedor.
- **Evaluación Continua:** Los proveedores críticos están sujetos a revisiones periódicas para garantizar que se mantengan los estándares de seguridad acordados.

7.2. Evaluación de Riesgos Asociados a Proveedores Críticos
La **evaluación de riesgos de terceros** es un proceso clave para identificar y gestionar los riesgos inherentes a la externalización de servicios. Este proceso se lleva a cabo en todas las etapas del ciclo de vida de la relación con el proveedor: selección, contratación, operación y finalización del servicio.

Proceso de Evaluación de Riesgos:

- **Identificación de Proveedores Críticos:** Se consideran críticos aquellos proveedores que:
    - Gestionan información confidencial o sensible de FALCOM AGF o sus clientes.
    - Tienen acceso a sistemas de información o infraestructura tecnológica crítica.
    - Proveen servicios esenciales para la continuidad del negocio.

- **Análisis de Riesgos Inicial:** Evaluación de los riesgos asociados al proveedor antes de formalizar la relación contractual. Incluye:
    - **Revisión de Controles de Seguridad:** Evaluación de las políticas, procedimientos y controles técnicos implementados por el proveedor.
    - **Cumplimiento Normativo:** Verificación del cumplimiento de estándares relevantes, como ISO 27001, SOC 2, PCI DSS, entre otros.
    - **Evaluación de Riesgos de Terceros (TPRM):** Análisis de vulnerabilidades, historial de incidentes de seguridad, estabilidad financiera y riesgos en la cadena de suministro.

- **Reevaluación Periódica:** Los riesgos asociados a proveedores críticos se revisan de forma regular, considerando:
    - Cambios en el entorno de amenazas o en la naturaleza del servicio prestado.
    - Resultados de auditorías internas o externas.
    - Incidentes de seguridad relevantes que puedan afectar la relación comercial.

Herramientas de Evaluación:

- **Cuestionarios de Seguridad para Proveedores:** Recopilación de información detallada sobre los controles de seguridad aplicados.
- **Auditorías de Proveedores:** Evaluaciones presenciales o remotas para verificar el cumplimiento de los requisitos de seguridad establecidos.
- **Monitoreo Continuo:** Herramientas tecnológicas para la supervisión de la seguridad de la infraestructura de terceros, especialmente en entornos de nube.

7.3. Requisitos de Seguridad en Contratos

La gestión de la seguridad de la información en relaciones con terceros se refuerza mediante la inclusión de **cláusulas contractuales específicas** que establecen claramente las responsabilidades del proveedor en materia de ciberseguridad, privacidad de datos y continuidad del negocio.

Elementos Clave en los Contratos:

- **Compromisos de Seguridad de la Información:**
  - Obligación del proveedor de implementar controles de seguridad alineados con los estándares internacionales (ISO 27001, NIST, etc.).
  - Definición de requisitos mínimos de seguridad, incluyendo cifrado de datos, gestión de accesos y monitoreo de seguridad.
- **Protección de Datos Personales:**
  - Cumplimiento con la **Ley de Protección de Datos Personales** y regulaciones internacionales, como el **RGPD** en caso de procesamiento de datos de ciudadanos de la UE.
  - Obligaciones sobre la recolección, almacenamiento, procesamiento y eliminación segura de datos personales.
- **Gestión de Incidentes de Seguridad:**
  - Obligación del proveedor de notificar de forma inmediata cualquier incidente de seguridad que pueda afectar a FALCOM AGF.
  - Establecimiento de plazos para la notificación de incidentes críticos, en línea con la normativa de la CMF.
  - Definición de responsabilidades conjuntas en la respuesta a incidentes y en la comunicación con autoridades regulatorias.
- **Derecho de Auditoría y Monitoreo:**
  - FALCOM AGF se reserva el derecho de auditar o evaluar periódicamente la seguridad del proveedor, directamente o a través de terceros designados.
  - Acceso a reportes de auditoría de seguridad realizados por terceros independientes (por ejemplo, informes SOC 2).
- **Planes de Continuidad del Negocio del Proveedor:**
  - Requisito de que los proveedores críticos cuenten con planes de continuidad del negocio y recuperación ante desastres (BCP/DRP), que sean consistentes con los estándares de FALCOM AGF.
  - Pruebas periódicas de dichos planes, con la participación de FALCOM AGF en simulacros o ejercicios de validación cuando sea necesario.
- **Cláusulas de Terminación y Reversión de Servicios:**
  - Establecimiento de procedimientos para la finalización de la relación contractual, incluyendo la devolución segura o destrucción de la información de FALCOM AGF.
  - Reglas claras para la continuidad de los servicios durante períodos de transición o cambio de proveedor.

7.4. Monitoreo y Evaluación Continua de Proveedores

El hecho de que un proveedor haya sido evaluado y contratado no elimina la necesidad de un **monitoreo continuo** para garantizar que los estándares de seguridad se mantengan durante toda la relación comercial.

Modelo de Monitoreo Continuo:

- **Supervisión de Cumplimiento:**
  - Revisión periódica de los controles de seguridad implementados por el proveedor, en función del nivel de criticidad del servicio.
  - Evaluación de cambios en el entorno del proveedor que puedan afectar la seguridad (por ejemplo, fusiones, adquisiciones, cambios en la infraestructura tecnológica).
- **Revisión de Acuerdos de Nivel de Servicio (SLA):**
  - Verificación del cumplimiento de los SLA relacionados con la disponibilidad del servicio, tiempos de respuesta ante incidentes y niveles de seguridad acordados.
  - Inclusión de métricas específicas de ciberseguridad en los informes de desempeño del proveedor.
- **Auditorías Periódicas:**
  - Ejecución de auditorías internas o externas para evaluar la seguridad de los servicios externalizados.
  - Participación en auditorías conjuntas con otros clientes del proveedor cuando sea posible, para optimizar recursos.
- **Gestión de Incidentes Relacionados con Terceros:**
  - Establecimiento de procedimientos para la **gestión de incidentes de seguridad** que involucren a proveedores, incluyendo la coordinación de la respuesta y la notificación a las autoridades regulatorias cuando corresponda.
  - Evaluación post-incidente para identificar deficiencias en los controles de seguridad del proveedor y definir acciones correctivas.
- **Evaluación de la Resiliencia del Proveedor:**
  - Monitoreo del entorno financiero y operacional del proveedor para identificar riesgos emergentes que puedan afectar la continuidad del servicio.
  - Evaluación de la capacidad del proveedor para adaptarse a cambios regulatorios, tecnológicos o en el panorama de amenazas.

Gestión de Proveedores Críticos y de Alto Riesgo:

Para los proveedores considerados de **alto riesgo** o **estratégicos**, se aplican controles adicionales, como:

- **Reuniones periódicas de revisión de seguridad** con el proveedor.
- **Simulacros conjuntos de gestión de crisis** y pruebas de continuidad del negocio.
- **Evaluación del riesgo de la cadena de suministro**, considerando subcontratistas y dependencias de terceros.

8. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN (NCG 510 - SECCIÓN D)

La **gestión de incidentes de seguridad de la información** es un pilar fundamental en la estrategia de ciberseguridad de FALCOM AGF. En un entorno financiero altamente digitalizado y expuesto a amenazas cibernéticas complejas, la capacidad de detectar, responder y recuperarse rápidamente de incidentes de seguridad es crucial para garantizar la continuidad del negocio, proteger la integridad de la información y mantener la confianza de los clientes y partes interesadas.

La **Norma de Carácter General N°510 (NCG 510)** de la **Comisión para el Mercado Financiero (CMF)** establece requisitos específicos para la gestión de incidentes, enfatizando la necesidad de contar con políticas, procedimientos y estructuras organizativas que permitan una respuesta efectiva ante eventos que puedan afectar la seguridad de la información.

El enfoque de FALCOM AGF está alineado con estándares internacionales como la **ISO/IEC 27035:2016** (gestión de incidentes de seguridad de la información), el **NIST SP 800-61r2** (Computer Security Incident Handling Guide) y las mejores prácticas del **NIST Cybersecurity Framework (CSF)**.

8.1. Política de Gestión de Incidentes

La **Política de Gestión de Incidentes de Seguridad de la Información** define el marco para la identificación, notificación, análisis, respuesta, recuperación y aprendizaje de incidentes de seguridad que puedan comprometer la confidencialidad, integridad o disponibilidad de la información en FALCOM AGF.

Objetivos de la Política:

- **Detectar de manera temprana** incidentes de seguridad que puedan afectar los activos de información críticos.
- **Responder de forma eficaz** para minimizar el impacto de los incidentes en la operación del negocio.
- **Recuperarse rápidamente** para restablecer los servicios afectados con el menor tiempo de inactividad posible.
- **Cumplir con los requisitos regulatorios**, incluyendo los plazos de notificación establecidos por la NCG 510.
- **Promover la mejora continua**, mediante el análisis de causas raíz y la implementación de lecciones aprendidas.

Definición de Incidente de Seguridad:
Se considera **incidente de seguridad de la información** a cualquier evento identificado que pueda:
- Comprometer la **confidencialidad**, **integridad** o **disponibilidad** de la información.
- Afectar la operación de sistemas críticos o servicios esenciales.
- Violar políticas internas de seguridad, procedimientos o regulaciones externas.

Ejemplos de Incidentes Críticos:
- **Ciberataques:** Phishing, ransomware, denegación de servicio (DDoS), explotación de vulnerabilidades, malware avanzado.
- **Violaciones de Datos:** Acceso no autorizado, pérdida o robo de información sensible o datos personales.
- **Fallas Tecnológicas:** Interrupción de servicios críticos, errores en sistemas de control de acceso, fallos en copias de seguridad.
- **Errores Humanos:** Configuraciones incorrectas, envío de información confidencial a destinatarios no autorizados.
- **Incidentes Físicos:** Robo de dispositivos, daños en infraestructura de TI debido a desastres naturales.

Clasificación de Incidentes:
Los incidentes se clasifican en función de su impacto y criticidad:
- **Incidente Crítico:** Afecta la continuidad del negocio, la seguridad de datos sensibles o la reputación de la organización.
- **Incidente Mayor:** Impacto significativo en un área o sistema específico, pero sin comprometer la operación global.
- **Incidente Menor:** Impacto limitado, sin afectación a procesos críticos ni riesgos de seguridad significativos.

La clasificación determina la prioridad en la respuesta y los niveles de escalamiento interno.

8.2. Procedimientos de Respuesta y Recuperación
La **respuesta a incidentes de seguridad de la información** en FALCOM AGF se estructura en un ciclo de vida que abarca desde la detección inicial hasta la recuperación completa y el análisis posterior.

Fases del Ciclo de Vida de Gestión de Incidentes:
- **Detección y Notificación:**
  - **Monitoreo Continuo:** Uso de sistemas de detección de intrusiones (IDS/IPS), herramientas de análisis de seguridad (SIEM), y alertas de ciberseguridad.
  - **Canales de Reporte:** Mecanismos para que empleados, proveedores o clientes reporten incidentes sospechosos de forma rápida y segura.
  - **Evaluación Inicial:** Análisis preliminar para confirmar si el evento reportado constituye un incidente de seguridad.

- **Análisis y Clasificación:**
  - **Determinación del Alcance:** Identificación de los sistemas, datos y usuarios afectados.
  - **Clasificación del Incidente:** Evaluación del nivel de severidad e impacto potencial (crítico, mayor, menor).
  - **Recolección de Evidencia:** Preservación de evidencia digital para análisis forense, si es necesario.
- **Contención:**
  - **Contención Inmediata:** Acciones rápidas para limitar la propagación del incidente y proteger los activos críticos (por ejemplo, desconexión de sistemas comprometidos).
  - **Contención a Largo Plazo:** Implementación de soluciones temporales para mitigar el impacto mientras se desarrolla la remediación definitiva.
- **Erradicación:**
  - **Identificación de la Causa Raíz:** Análisis profundo para determinar cómo ocurrió el incidente.
  - **Eliminación de la Amenaza:** Limpieza de sistemas comprometidos, eliminación de malware, cierre de vulnerabilidades explotadas.
- **Recuperación:**
  - **Restauración de Sistemas:** Reinstalación de sistemas afectados, restauración de datos desde copias de seguridad, validación de la integridad de los sistemas.
  - **Verificación de la Seguridad:** Evaluación post-recuperación para confirmar que no persisten riesgos residuales.
- **Lecciones Aprendidas:**
  - **Análisis Post-Incidente:** Revisión del incidente para identificar oportunidades de mejora en procesos, controles y capacidades de respuesta.
  - **Actualización de Procedimientos:** Revisión de políticas y procedimientos de seguridad en función de las lecciones aprendidas.
  - **Informe Final:** Documentación detallada del incidente, acciones realizadas, impacto, y medidas de mejora implementadas.

8.3. Reporte a la Comisión y Entidades Reguladoras

FALCOM AGF mantiene procedimientos específicos para el **reporte de incidentes de seguridad de la información** a la **Comisión para el Mercado Financiero (CMF)** y otras autoridades regulatorias, en cumplimiento con la **NCG 510**.

Criterios de Notificación:

Se deben notificar aquellos incidentes que:

- Comprometan la seguridad de la información de clientes o terceros.
- Afecten la continuidad de los servicios críticos.
- Implican violaciones significativas a la normativa de ciberseguridad.
- Puedan tener un impacto relevante en la estabilidad del mercado financiero o en la reputación de la organización.

Plazos de Notificación:

- **Incidentes Críticos:** Notificación inmediata (dentro de las primeras 24 horas desde la detección del incidente).
- **Incidentes Menores:** Reporte dentro de los plazos definidos internamente o según lo requiera la autoridad.

Contenido del Reporte:

- **Descripción del Incidente:** Naturaleza del evento, fecha y hora de detección.

- **Impacto Evaluado:** Sistemas y datos afectados, impacto en la operación y en los clientes.
- **Medidas Adoptadas:** Acciones de contención, erradicación y recuperación implementadas.
- **Planes de Mitigación:** Estrategias para prevenir la recurrencia del incidente.
- **Resultados de Análisis Forense:** Si corresponde, información detallada del análisis técnico del incidente.

Canales de Comunicación:
El reporte se realiza a través de los canales oficiales definidos por la CMF, con copia a los organismos internos de cumplimiento y gestión de riesgos de FALCOM AGF.

8.4. Análisis Forense y Mejora Continua
El **análisis forense digital** es una disciplina clave en la gestión de incidentes de seguridad, ya que permite investigar en profundidad los eventos de seguridad para identificar las causas raíz, el alcance del daño y los métodos utilizados por los atacantes.

Objetivos del Análisis Forense:
- **Identificación de la Causa Raíz:** Comprender cómo se originó el incidente y qué vulnerabilidades fueron explotadas.
- **Determinación del Alcance:** Establecer qué sistemas, datos y usuarios se vieron comprometidos.
- **Preservación de Evidencia:** Recolectar, analizar y preservar evidencia digital de manera que sea admisible en procedimientos legales o regulatorios.
- **Apoyo en la Recuperación:** Proporcionar información técnica que facilite la erradicación de la amenaza y la restauración de sistemas afectados.

Metodología de Análisis Forense:
- **Preservación de Evidencias:** Asegurar que los datos críticos no sean alterados durante la investigación.
- **Recolección de Datos:** Extracción de registros de sistemas, archivos de logs, imágenes forenses de dispositivos afectados, etc.
- **Análisis Técnico:** Evaluación detallada de la evidencia para identificar patrones de ataque, rutas de intrusión y técnicas utilizadas por el atacante.
- **Documentación:** Registro de todos los hallazgos, pasos realizados y resultados obtenidos.
- **Informe Forense:** Elaboración de un informe técnico que incluya conclusiones y recomendaciones para prevenir futuros incidentes.

Mejora Continua en la Gestión de Incidentes:
FALCOM AGF promueve un enfoque de **mejora continua** en la gestión de incidentes de seguridad, que incluye:
- **Revisión Post-Incidente (Post-Mortem):** Evaluación de la respuesta al incidente para identificar fortalezas y debilidades en los procesos.
- **Lecciones Aprendidas:** Documentación de las lecciones aprendidas y actualización de procedimientos, políticas y controles de seguridad.
- **Capacitación del Personal:** Formación continua para mejorar las capacidades del equipo de respuesta a incidentes (CSIRT).
- **Simulacros de Incidentes:** Ejercicios periódicos para probar la eficacia de los procedimientos de respuesta y mejorar la preparación de la organización.

9. CUMPLIMIENTO NORMATIVO Y AUDITORÍA

El **cumplimiento normativo y la auditoría** son pilares fundamentales de la gobernanza de la seguridad de la información en FALCOM AGF. Garantizan que la organización opere dentro del marco legal, regulatorio y de mejores prácticas aplicables, además de verificar la eficacia de los controles implementados para proteger la confidencialidad, integridad y disponibilidad de la información.

La gestión de la seguridad de la información no solo se basa en la implementación de controles técnicos, sino también en la capacidad de demostrar que estos controles funcionan de manera efectiva. Por ello, el **cumplimiento continuo** con la normativa vigente, como la **NCG 510 de la CMF**, y con estándares internacionales como **ISO/IEC 27001:2022**, **ISO/IEC 27002:2022**, y el **NIST SP 800-37r2**, es un requisito crítico para la sostenibilidad del negocio.

9.1. Evaluación del Cumplimiento con NCG 510 y Otros Marcos Regulatorios

FALCOM AGF mantiene un enfoque proactivo para garantizar el **cumplimiento de la NCG 510**, así como de otras regulaciones y estándares internacionales relevantes para la seguridad de la información y la gestión de riesgos operacionales.

Regulaciones Nacionales:

- **NCG 510 de la CMF:** Establece directrices para la gestión de riesgos operacionales, continuidad del negocio, ciberseguridad y servicios externalizados.
- **Ley N° 21.663 - Ley Marco de Ciberseguridad:** Define requisitos para la protección de infraestructuras críticas de la información en Chile.
- **Ley de Protección de Datos Personales (Chile) y RGPD (para operaciones internacionales):** Regulan la recolección, uso y protección de datos personales.

Estándares Internacionales:

- **ISO/IEC 27001:2022:** Establece los requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI) efectivo.
- **ISO/IEC 27002:2022:** Proporciona directrices para la implementación de controles de seguridad de la información.
- **NIST SP 800-37r2:** Define un marco de gestión de riesgos que integra seguridad y privacidad en el ciclo de vida de los sistemas.
- **NIST Cybersecurity Framework (CSF):** Proporciona un enfoque basado en riesgos para gestionar y reducir riesgos de ciberseguridad.

Proceso de Evaluación del Cumplimiento:

1. **Identificación de Requisitos:** Análisis de las regulaciones aplicables para determinar las obligaciones de cumplimiento.
2. **Evaluación de Brechas (Gap Analysis):** Comparación entre el estado actual de la organización y los requisitos normativos para identificar áreas de mejora.
3. **Planes de Acción:** Desarrollo de planes de remediación para abordar las brechas identificadas.
4. **Monitoreo Continuo:** Implementación de mecanismos para monitorear el cumplimiento en tiempo real, incluyendo auditorías internas, controles automatizados y revisiones periódicas.

Reportes Regulatorios:

FALCOM AGF mantiene procedimientos establecidos para la **notificación de incidentes de seguridad** y el **reporte de cumplimiento** ante la CMF y otras autoridades regulatorias pertinentes. Esto incluye:

- **Informes periódicos de cumplimiento normativo.**
- **Notificación de incidentes críticos** en plazos definidos por la normativa.
- **Participación en auditorías regulatorias y revisiones de supervisión.**

9.2. Auditorías Internas y Externas de Seguridad de la Información

Las **auditorías de seguridad de la información** son herramientas esenciales para evaluar la eficacia del Sistema de Gestión de Seguridad de la Información (SGSI), identificar debilidades en los controles de seguridad y garantizar el cumplimiento de los requisitos normativos y de la organización.

Auditorías Internas:

Las auditorías internas son realizadas por el equipo de auditoría interna de FALCOM AGF o por profesionales designados que poseen independencia funcional respecto de las áreas auditadas.

Objetivos de las Auditorías Internas:

- Evaluar la eficacia de los controles de seguridad implementados.
- Verificar el cumplimiento de políticas, procedimientos y normativas aplicables.
- Identificar oportunidades de mejora en la gestión de la seguridad de la información.
- Garantizar la adecuada gestión de riesgos de ciberseguridad y continuidad del negocio.

Ciclo de Auditoría Interna:

1. **Planificación:** Definición del alcance, objetivos, criterios y metodología de la auditoría.
2. **Ejecución:** Revisión de documentación, entrevistas con responsables, análisis de procesos y pruebas de controles.
3. **Informe de Resultados:** Documentación de hallazgos, no conformidades y recomendaciones de mejora.
4. **Seguimiento:** Verificación de la implementación de acciones correctivas y preventivas.

Auditorías Externas:

Las auditorías externas son realizadas por entidades independientes, como firmas de auditoría certificadas o autoridades regulatorias.

Objetivos de las Auditorías Externas:

- Validar la conformidad del SGSI con estándares internacionales (ISO 27001, NIST, etc.).
- Evaluar el cumplimiento de regulaciones específicas, como la NCG 510.
- Aportar una perspectiva independiente sobre la eficacia de la gestión de seguridad de la información.

Tipos de Auditorías Técnicas:

- **Pruebas de Penetración (Pentesting):** Simulación de ataques cibernéticos para evaluar la resiliencia de los sistemas.
- **Evaluaciones de Vulnerabilidades:** Identificación de brechas de seguridad en la infraestructura tecnológica.
- **Revisiones de Código Seguro:** Análisis de aplicaciones para detectar vulnerabilidades en el código fuente.

9.3. Gestión de No Conformidades y Planes de Mejora

La **gestión de no conformidades** es un proceso clave para garantizar la mejora continua del SGSI. Permite identificar, analizar y corregir desviaciones respecto a los requisitos establecidos en políticas internas, normativas regulatorias o estándares internacionales.

Definición de No Conformidad:

Se considera no conformidad cualquier incumplimiento de:

- **Requisitos normativos:** Falta de cumplimiento con la NCG 510, ISO 27001, leyes de protección de datos, entre otros.
- **Políticas y procedimientos internos:** Incumplimiento de controles de seguridad definidos por la organización.
- **Controles técnicos de seguridad:** Vulnerabilidades no mitigadas o fallos en la implementación de controles críticos.

Proceso de Gestión de No Conformidades:

1. **Detección:** Identificación de la no conformidad a través de auditorías, evaluaciones de riesgos, incidentes de seguridad o revisiones internas.
2. **Análisis de Causa Raíz:** Evaluación de las causas subyacentes que originaron la no conformidad, utilizando metodologías como el análisis de causa raíz (RCA).
3. **Plan de Acción Correctiva:** Desarrollo e implementación de medidas para corregir la no conformidad y prevenir su recurrencia.
4. **Seguimiento:** Verificación de la efectividad de las acciones correctivas mediante auditorías de seguimiento o revisiones posteriores.
5. **Cierre de No Conformidad:** Documentación formal del cierre de la no conformidad, una vez comprobada la resolución efectiva del problema.

Planes de Mejora Continua:

FALCOM AGF promueve una cultura de mejora continua basada en el ciclo **PDCA (Plan-Do-Check-Act)**. Los planes de mejora se enfocan en:

- Fortalecer los controles de seguridad existentes.
- Adaptar la organización a nuevos riesgos emergentes.
- Mejorar la eficacia de los procesos de seguridad y gestión de incidentes.

- Fomentar la innovación en ciberseguridad, incorporando nuevas tecnologías y mejores prácticas del sector.

Gestión de Hallazgos Críticos:
Las no conformidades o hallazgos de auditoría que representen un riesgo significativo para la organización se escalan de inmediato a la Alta Dirección y al Comité de Tecnología y Ciberseguridad. En estos casos, se definen **planes de acción prioritarios** con seguimiento riguroso hasta su completa resolución.

10. MEJORA CONTINUA

La **mejora continua** es un principio fundamental para la gestión de la seguridad de la información en FALCOM AGF. En un entorno donde las amenazas cibernéticas evolucionan constantemente, la organización debe mantener un enfoque dinámico y proactivo para adaptarse a nuevos desafíos, fortalecer sus capacidades de defensa y optimizar sus procesos de seguridad.

El compromiso con la mejora continua no solo responde a los requisitos de la **Norma de Carácter General N°510 (NCG 510)** de la **Comisión para el Mercado Financiero (CMF)**, sino que también está alineado con estándares internacionales como la **ISO/IEC 27001:2022**, que promueve la gestión sistemática de la seguridad de la información a través del ciclo de mejora continua **PDCA (Plan-Do-Check-Act)**.
Este enfoque garantiza que FALCOM AGF pueda anticiparse a los riesgos emergentes, mejorar su resiliencia organizacional y mantener la confianza de sus clientes y partes interesadas.

10.1. Aplicación del Ciclo PDCA (Plan-Do-Check-Act)

El ciclo **PDCA (Planificar-Hacer-Verificar-Actuar)** es una metodología de gestión ampliamente utilizada para la mejora continua de procesos. En el contexto de la seguridad de la información, el PDCA permite gestionar de forma estructurada los riesgos, optimizar los controles de seguridad y asegurar el cumplimiento de los objetivos organizacionales.

Fases del Ciclo PDCA:

1. **Plan (Planificar):**
    - **Definición de Objetivos:** Establecimiento de metas claras y medibles en materia de seguridad de la información, alineadas con la estrategia de la organización.
    - **Identificación de Riesgos:** Evaluación de amenazas, vulnerabilidades y riesgos para definir prioridades de seguridad.
    - **Desarrollo de Políticas y Procedimientos:** Diseño de controles y procedimientos para mitigar los riesgos identificados.

2. **Do (Hacer):**
    - **Implementación de Controles:** Ejecución de las políticas, procedimientos y controles de seguridad definidos en la fase de planificación.
    - **Concienciación y Formación:** Capacitación del personal en buenas prácticas de ciberseguridad y en la gestión de incidentes.
    - **Gestión de Proveedores:** Aplicación de controles de seguridad en servicios externalizados.
3. **Check (Verificar):**
    - **Monitoreo y Evaluación:** Seguimiento del desempeño de los controles de seguridad mediante auditorías internas, revisiones de cumplimiento y análisis de incidentes.
    - **Análisis de Brechas:** Identificación de desviaciones respecto a los objetivos de seguridad definidos.
    - **Revisión de Indicadores de Desempeño:** Evaluación de la eficacia de los controles mediante métricas e indicadores clave (KPI y KRI).
4. **Act (Actuar):**
    - **Mejora Continua:** Implementación de acciones correctivas y preventivas para abordar las no conformidades detectadas.
    - **Actualización de Políticas:** Revisión y mejora de políticas y procedimientos en función de los resultados obtenidos.
    - **Adaptación a Nuevas Amenazas:** Incorporación de lecciones aprendidas para enfrentar nuevos riesgos emergentes.

Este enfoque iterativo asegura que el Sistema de Gestión de Seguridad de la Información (SGSI) de FALCOM AGF se mantenga actualizado, eficaz y alineado con las necesidades del negocio.

10.2. Indicadores de Desempeño (KPI) en Seguridad de la Información

Los **Indicadores Clave de Desempeño (KPI)** permiten medir la eficacia de los controles de seguridad implementados y evaluar el rendimiento del SGSI. Estos indicadores proporcionan información valiosa para la toma de decisiones estratégicas, la priorización de recursos y la identificación de áreas de mejora.

Características de los KPI Efectivos:

- **Relevantes:** Alineados con los objetivos estratégicos de la organización.
- **Medibles:** Basados en datos cuantificables y verificables.
- **Accionables:** Permiten identificar claramente áreas que requieren mejoras.
- **Comparables:** Facilitan la comparación de resultados a lo largo del tiempo o entre diferentes unidades de la organización.

Ejemplos de KPI en Seguridad de la Información:

1. **Tasa de Incidentes de Seguridad:**
    - Número de incidentes de seguridad reportados en un período determinado.
    - Análisis de tendencias para identificar patrones de riesgo recurrentes.
2. **Tiempos de Respuesta a Incidentes (MTTR):**
    - **MTTR (Mean Time to Respond):** Tiempo medio desde la detección de un incidente hasta su resolución.
    - Indicador clave para evaluar la eficacia de los equipos de respuesta a incidentes (CSIRT).
3. **Nivel de Cumplimiento de Políticas de Seguridad:**
    - Porcentaje de áreas o procesos que cumplen con los requisitos de seguridad establecidos en las políticas internas.
    - Resultados de auditorías internas y externas.
4. **Tasa de Aplicación de Parches de Seguridad:**
    - Proporción de vulnerabilidades críticas corregidas dentro del plazo definido en la política de gestión de parches.

- Evaluación del tiempo de exposición a riesgos conocidos.

5. **Participación en Programas de Concienciación:**
   - Porcentaje de empleados que han completado programas de formación en ciberseguridad en el último año.
   - Resultados de pruebas de simulación de phishing y otros ejercicios de concienciación.
6. **Disponibilidad de Sistemas Críticos:**
   - Porcentaje de tiempo que los sistemas críticos han estado operativos y disponibles.
   - Evaluación de la eficacia de los planes de continuidad del negocio (BCP) y recuperación ante desastres (DRP).
7. **Número de Auditorías de Seguridad Realizadas:**
   - Auditorías internas y externas completadas según el plan anual de auditoría.
   - Seguimiento de acciones correctivas derivadas de auditorías previas.

Uso de KPI en la Toma de Decisiones:
Los resultados de los KPI se presentan periódicamente al **Comité de Tecnología y Ciberseguridad** y a la **Alta Dirección**, para:

- Evaluar el estado de la seguridad de la información en la organización.
- Identificar tendencias emergentes y áreas de alto riesgo.
- Priorizar inversiones en ciberseguridad y recursos tecnológicos.
- Definir acciones correctivas y planes de mejora continua.

10.3. Revisión de la Alta Dirección
La **revisión de la Alta Dirección** es un proceso crítico para garantizar que el SGSI siga siendo adecuado, efectivo y alineado con la estrategia y los objetivos del negocio. Esta revisión se realiza de forma periódica (al menos una vez al año) o cuando se producen cambios significativos en el entorno interno o externo de la organización.

Objetivos de la Revisión de la Alta Dirección:

- Evaluar el desempeño general del SGSI, incluyendo el cumplimiento de los objetivos de seguridad de la información.
- Identificar oportunidades de mejora y áreas que requieren atención prioritaria.
- Revisar los riesgos emergentes, las amenazas cibernéticas y la evolución del panorama regulatorio.
- Asegurar la asignación de recursos adecuados para la gestión de la seguridad de la información.

Elementos de Entrada en la Revisión:

1. **Resultados de Auditorías Internas y Externas:**
   - Hallazgos de auditoría, no conformidades y estado de las acciones correctivas.
2. **Evaluación del Cumplimiento Normativo:**
   - Nivel de cumplimiento con la NCG 510, ISO 27001, Ley de Protección de Datos, entre otros.
3. **Análisis de Incidentes de Seguridad:**
   - Incidentes reportados, análisis forense y lecciones aprendidas.
4. **Riesgos de Seguridad de la Información:**
   - Evaluación actualizada del panorama de riesgos, incluyendo ciberamenazas emergentes.
5. **Resultados de KPI y Métricas de Desempeño:**
   - Desempeño de los controles de seguridad, eficacia de programas de concienciación, etc.
6. **Cambios en el Contexto Organizacional:**
   - Transformaciones tecnológicas, cambios regulatorios, adquisiciones, fusiones o nuevas líneas de negocio.

Resultados Esperados de la Revisión:

- **Decisiones estratégicas:** Actualización de la política de seguridad de la información y aprobación de nuevos objetivos.
- **Mejora continua:** Identificación de oportunidades de mejora y asignación de recursos para iniciativas de ciberseguridad.
- **Evaluación del Apetito por el Riesgo:** Revisión y ajuste de los niveles de tolerancia al riesgo de la organización.
- **Revisión de Recursos:** Evaluación de la necesidad de recursos adicionales (tecnológicos, humanos o financieros) para la gestión de la seguridad.

Seguimiento de la Revisión:
Los acuerdos y decisiones tomadas durante la revisión de la Alta Dirección se documentan en un informe formal, que incluye:

- Resumen de hallazgos y análisis realizados.
- Acciones acordadas y responsables asignados.
- Plazos para la implementación de mejoras.
- Seguimiento de decisiones tomadas en revisiones anteriores.

Este informe es compartido con las áreas responsables de la seguridad de la información y con el Comité de Seguridad, garantizando la implementación efectiva de las mejoras definidas.

11. ANEXOS

La sección de **Anexos** del **Manual de Seguridad de la Información y Ciberseguridad de FALCOM AGF** complementa el contenido principal del documento, proporcionando recursos de apoyo que permiten una mejor comprensión, implementación y seguimiento de las políticas, procedimientos y controles de seguridad descritos en las secciones anteriores.

Estos anexos incluyen un **glosario de términos clave**, **procedimientos específicos**, **referencias normativas y bibliográficas**, y un **registro de cambios del manual**, que garantizan la trazabilidad y la actualización continua del documento.

11.1. Glosario de Términos

El siguiente glosario define los términos técnicos, regulatorios y de gestión utilizados en este manual, facilitando su comprensión para todos los públicos dentro de FALCOM AGF, incluidos directivos, personal técnico y no técnico, auditores, y partes interesadas externas.

Términos Clave:

- **Activo de Información:** Cualquier dato, documento, sistema, infraestructura tecnológica o recurso que tenga valor para la organización.
- **Amenaza:** Evento o circunstancia que puede explotar una vulnerabilidad, causando daño a la organización. Puede ser interna (errores humanos, fraudes) o externa (ciberataques, desastres naturales).
- **Análisis de Impacto en el Negocio (BIA):** Proceso que identifica las funciones críticas del negocio y evalúa el impacto potencial de una interrupción en dichas funciones.
- **Apoyo Crítico:** Servicios, funciones o recursos esenciales para la operación continua del negocio.
- **Autenticación Multifactor (MFA):** Mecanismo de seguridad que requiere más de un factor de verificación para validar la identidad de un usuario.
- **Brecha de Seguridad:** Evento en el que la confidencialidad, integridad o disponibilidad de la información ha sido comprometida.
- **Ciberseguridad:** Conjunto de tecnologías, procesos y prácticas diseñadas para proteger redes, dispositivos, programas y datos contra ataques, daños o accesos no autorizados.
- **Confidencialidad:** Principio que garantiza que la información solo sea accesible por personas autorizadas.
- **Continuidad del Negocio (BCP):** Capacidad de una organización para continuar operando durante y después de un incidente disruptivo.

- **Control de Acceso:** Mecanismos para regular quién puede acceder a los recursos de la organización y bajo qué condiciones.
- **Gestión de Incidentes:** Proceso de identificación, análisis, respuesta y recuperación ante eventos de seguridad de la información.
- **Gestión de Riesgos:** Proceso continuo para identificar, evaluar y mitigar riesgos que puedan afectar la organización.
- **Integridad:** Propiedad que asegura que la información no ha sido alterada de manera no autorizada.
- **Riesgo Residual:** Riesgo que permanece después de que se han aplicado controles de mitigación.
- **Seguridad de la Información:** Protección de la información frente a amenazas que puedan afectar su confidencialidad, integridad y disponibilidad.
- **Vulnerabilidad:** Debilidad en un sistema, proceso o control que puede ser explotada por una amenaza.

Este glosario se actualiza periódicamente para reflejar los cambios en la terminología y las mejores prácticas del sector.

11.2. Procedimientos Específicos y Formularios

Esta sección incluye procedimientos operativos estandarizados y formularios que permiten la aplicación práctica de las políticas y directrices de seguridad establecidas en el manual.

Procedimientos Específicos:

1. **Procedimiento de Gestión de Incidentes de Seguridad de la Información:**
    - Descripción detallada del proceso para identificar, notificar, analizar, contener, erradicar, recuperar y documentar incidentes de seguridad.
    - Incluye flujos de escalamiento, criterios para la clasificación de incidentes y plazos de notificación interna y externa.
2. **Procedimiento de Evaluación de Riesgos de Seguridad de la Información:**
    - Metodología para la identificación, análisis, evaluación y tratamiento de riesgos, incluyendo matrices de riesgos y criterios de aceptación.
    - Definición de roles y responsabilidades en la gestión de riesgos.
3. **Procedimiento de Gestión de Cambios en Sistemas Críticos:**
    - Proceso para la solicitud, evaluación, aprobación, implementación y seguimiento de cambios en la infraestructura tecnológica.
    - Incluye controles de seguridad para minimizar el riesgo de interrupciones o vulnerabilidades.
4. **Procedimiento de Gestión de la Continuidad del Negocio:**
    - Instrucciones para la activación de planes de continuidad del negocio (BCP) y recuperación ante desastres (DRP) en caso de eventos críticos.
    - Incluye criterios de activación, roles del Comité de Gestión de Crisis y planes de comunicación en situaciones de emergencia.
5. **Procedimiento de Gestión de Accesos y Cuentas de Usuario:**
    - Normas para la creación, modificación, revisión y revocación de cuentas de usuario en los sistemas de la organización.
    - Políticas de contraseñas, autenticación multifactor (MFA) y control de accesos privilegiados.
6. **Procedimiento de Evaluación de Proveedores Críticos:**
    - Proceso para la evaluación de riesgos de seguridad en la contratación de terceros y la gestión de servicios externalizados.
    - Incluye criterios para auditorías a proveedores y cláusulas de seguridad en contratos.

Formularios Asociados:

- **Formulario de Registro de Incidentes de Seguridad:** Para documentar incidentes, su análisis y las acciones de mitigación implementadas.
- **Matriz de Evaluación de Riesgos:** Herramienta para registrar, evaluar y hacer seguimiento de los riesgos identificados.
- **Formulario de Solicitud de Acceso a Sistemas Críticos:** Para la gestión de solicitudes de acceso, incluyendo la justificación del acceso y la aprobación correspondiente.
- **Checklist de Auditoría de Seguridad de Proveedores:** Para evaluar el nivel de cumplimiento de seguridad de los proveedores externos.
- **Plan de Respuesta ante Incidentes:** Plantilla para la planificación de la respuesta en caso de incidentes críticos de ciberseguridad.

Estos procedimientos y formularios están disponibles en el repositorio interno de documentación de FALCOM AGF y deben ser utilizados por todas las áreas de la organización según corresponda.

11.3. Referencias Normativas y Bibliográficas

Esta sección recopila las normativas, estándares internacionales, guías y documentos de referencia utilizados para la elaboración del presente manual.

Normativas y Regulaciones:

- **NCG 510 de la Comisión para el Mercado Financiero (CMF)**
- **Ley N° 21.663 - Ley Marco de Ciberseguridad (Chile)**
- **Ley de Protección de Datos Personales (Chile)**
- **Reglamento General de Protección de Datos (RGPD) - Unión Europea**

Estándares Internacionales:

- **ISO/IEC 27001:2022 - Sistemas de Gestión de Seguridad de la Información (SGSI)**
- **ISO/IEC 27002:2022 - Código de Prácticas para Controles de Seguridad de la Información**
- **ISO 22301:2019 - Gestión de la Continuidad del Negocio (BCM)**
- **ISO/IEC 27031:2019 - Directrices para la Continuidad de las Tecnologías de la Información y las Comunicaciones**
- **NIST SP 800-37r2 - Risk Management Framework (RMF)**
- **NIST SP 800-53 - Controles de Seguridad y Privacidad para Sistemas de Información**
- **NIST Cybersecurity Framework (CSF)**

Documentación Interna de FALCOM AGF:

- **Política General de Seguridad de la Información y Ciberseguridad**
- **Política de Seguridad en la Nube**
- **Política de Gestión de Proveedores**
- **Política de Seguridad de Redes**
- **Manual de Continuidad del Negocio (BCP)**
- **Manual de Control Interno y Gestión de Riesgos**

11.4 Incumplimiento

Cualquier incumplimiento de este manual será gestionado de acuerdo con las políticas disciplinarias internas de la organización. Dependiendo de la gravedad del incumplimiento, las sanciones pueden incluir advertencias, suspensión, hasta la terminación del contrato laboral o comercial. En casos graves, que impliquen violaciones legales, la organización podrá tomar acciones legales adicionales contra los infractores.

11.5 Revisión y Actualización

El manual será revisada y actualizada periódicamente, al menos una vez al año, o cuando existan cambios significativos en la tecnología o en el entorno regulatorio que afecten a la organización. Las actualizaciones serán aprobadas formalmente y comunicadas oportunamente a todas las partes interesadas.

11.6 Aprobación

En el caso de que este Manual requiera de modificación, esta debe ser aprobada de acuerdo con el siguiente esquema y orden:

- **Responsable de Seguridad de la Información y Ciberseguridad:** Debe revisar anualmente y presentar a la Alta Gerencia las modificaciones propuestas relacionadas con cambios internos y normativos. En caso de no haber modificaciones a la política, se debe informar que se encuentra vigente hasta ese momento.
- **El Comité de Tecnología y Ciberseguridad:** Debe revisar los cambios propuestos y en caso de que éstos sean consistentes con los lineamientos estratégicos, debe aprobar y escalar al Directorio para su revisión y aprobación.

11.7 Auditoría

La función de auditoría interna considerará este manual como parte del universo o materia auditable sobre el cual se construye el Plan de Auditoría Anual, el cual es sometido al menos anualmente al Comité de Auditoría para su revisión y aprobación.

Si la materia auditable forma parte del plan anual aprobado, se incorporarán en los programas de trabajo la realización de pruebas para evaluar la efectividad de este Manual y el cumplimiento de los puntos específicos detallados en ella.

11.8 Vigencia y Publicación

Este Manual entra en vigencia a contar de su publicación en el portal normativo de FALCOM AGF y debe ser difundida a todos los colaboradores y a terceras partes que deban estar en conocimiento, de acuerdo con lo establecido en la Política.

11.9 Control de Cambios

Elaboración	Revisión	Aprobación
Nombre Cargo dd/mm/aa	Nombre Cargo dd/mm/aa	Nombre Cargo dd/mm/aa

11.10 Historial de Versiones

Versión	Fecha Aprobación	Elaboró	Revisado por	Aprobado Por	Principales cambios
1.0					