Fiduciaria Central

Fiduciaria Central

Manual: Política de Seguridad de la Información y Ciberseguridad

	Fiduciaria Central **Proceso**: Gestión de Riesgos **Manual**: Política de Seguridad de la Información y Ciberseguridad	**Código** PV01-MAN-008 **Fecha** 2025-05-27 **Versión** 12.0

Estratégico	Misional	Apoyo	Evaluación

Responsable

Gerente de Riegos (Gestión de Riesgos)

Contenido

1. INTRODUCCIÓN

El objetivo de este documento es dar a conocer a los funcionarios, clientes, proveedores y demás partes interesadas de La Fiduciaria, la Política de Seguridad de la Información y Ciberseguridad y Ciberseguridad establecida para la protección de la información. Un aspecto fundamental de toda estrategia de seguridad de la información es disponer de unos principios y objetivos claramente identificados y definidos, por ello a través del presente documento se establecen los aspectos de obligatorio cumplimiento por parte de todos los funcionarios para que i) la información sea accedida sólo por los que la requieren para la realización de sus funciones dentro del negocio (Confidencialidad); ii) la información esté protegida contra modificaciones no autorizadas (Integridad); iii) la información esté disponible en todo momento (Disponibilidad); iv) la información sea utilizada para los propósitos que fue obtenida (Privacidad) y v) se tenga acceso al registro de eventos generados al acceder y/o modificar la información (Auditabilidad).

En este documento se detallan las normas, estándares, procedimientos e instrucciones de seguridad de la información y ciberseguridad bajo las cuales operan los sistemas informáticos de la Fiduciaria, los límites que tienen los usuarios y funcionarios que usan los sistemas de información, los lineamientos para aplicar y configurar los servicios de redes y equipos en las diferentes oficinas, los parámetros establecidos que permitan la correcta gestión de los servicios y manejo de información. Asimismo, se establece la Metodología para realizar los Análisis de Riesgos en Seguridad de la Información y Ciberseguridad; esta metodología ha sido planteada tomando como base la medición de la metodología definida por la entidad para el Sistema de Gestión del Riesgo Operacional (GRO).

La construcción de este documento se ha realizado tomando como base el estándar internacional de buenas prácticas en seguridad de la información ISO 27001:2022.

2. ALCANCE

La presente política aplica para los todos los activos de información, ciberactivos y toda la información creada, procesada o utilizada en el desarrollo de las actividades del negocio de La Fiduciaria, sin importar el medio, formato, presentación o lugar en el cual se encuentre.

3. OBJETIVOS

Este documento tiene como objetivo establecer las políticas, responsabilidades y lineamientos generales emitidos por la Junta Directiva y la Alta Gerencia que permitan la gestión y protección de la información, datos personales y ciberactivos de La Fiduciaria.

La Fiduciaria establece la función de Seguridad de la Información y ciberseguridad en la entidad, con el objetivo de:

- Dar cumplimiento a los lineamientos y normatividad aplicable a La Fiduciaria respecto a Seguridad de la Información y Ciberseguridad.

- Mantener la confianza de los clientes y el compromiso de todos los funcionarios, contratistas o terceros de La Fiduciaria, respecto al correcto manejo y protección de la seguridad de información y ciberseguridad.
- Asegurar la identificación y gestión oportuna de los riesgos de seguridad de la información y/o ciberseguridad a los cuales se expone La Fiduciaria.
- Instruir a los funcionarios contratistas y/o terceros sobre el uso adecuado de la información y el ciberespacio garantizando la confidencialidad, la disponibilidad y la integridad de la información de La Fiduciaria y sus clientes.
- Fortalecer la gestión de incidentes en seguridad de la información y ciberseguridad para asegurar la protección de la información de La Fiduciaria y sus clientes y los ciberactivos críticos de La Fiduciaria.

4. DECLARACIÓN DE POLITICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Fiduciaria Central S.A., consciente del valor que tiene la información propia y de sus clientes implementa mecanismos tendientes a su aseguramiento y protección contra las diversas amenazas que puedan afectarla; por ello se han establecido las siguientes políticas de seguridad de la información y ciberseguridad que permitirán gestionar la información con seguridad y calidad, preservando su confidencialidad, integridad y disponibilidad de una manera eficiente y efectiva, con el fin de velar continuamente porque no sea alterada, conocida por terceros no autorizados, ni utilizada para fines diferentes a los pactados con la Fiduciaria.

Esta Política de Seguridad de la Información y Ciberseguridad, especifica las directrices aprobadas por la Junta Directiva que deben ser cumplidas por los funcionarios y partes relacionadas con La Fiduciaria, con el fin de asegurar un adecuado nivel de confidencialidad, integridad y disponibilidad en sus activos de información y ciberactivos.

Con el fin de garantizar la actualización de esta política, la unidad de Seguridad de la Información la revisara por lo menos una vez al año o cuando se presenten cambios importantes en los procesos, productos o sistemas con el fin de identificar mejoras o necesidad de cambios en la misma. Las modificaciones se llevarán al Comité de Riesgo para su revisión y visto bueno para presentación a la Junta Directiva, esta última la revisara y aprobara para su divulgación en La Fiduciaria.

5. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

La política de seguridad de seguridad de la información y ciberseguridad permitirá gestionar con seguridad y calidad los activos de información y ciberactivos de La Fiduciaria, preservando su confidencialidad, integridad y disponibilidad.

6. RESULTADOS IMPORTANTES

La aplicación de la Política de Seguridad de la Información y Ciberseguridad descrita en este documento propende por:

- Reducir la exposición a ataques de seguridad de la información y cibernéticos a La Fiduciaria generadas por diversas fuentes de amenazas Fortalecer la cultura del identificación y gestión continúa de riesgos de seguridad de la información y ciberseguridad en La Fiduciaria por medio de la evaluación continua de la efectividad de los controles.
- Gestionar oportunamente los incidentes de seguridad que pueden afectar a La Fiduciaria, generando acciones de mejoramiento continuo.
- Cumplir con los lineamientos y normatividad aplicable a La Fiduciaria respecto a Seguridad de la información y Ciberseguridad en los tiempos establecidos.

7. CONTEXTO DE APLICACIÓN

7. 1. Personas cubiertas por estas políticas

Esta política está dirigida a todos los funcionarios de La Fiduciaria, al personal temporal, a terceros que prestan servicios (outsourcing) a la fiduciaria en modalidad in-house u out-house, a clientes, proveedores y toda persona natural o jurídica que de alguna manera realice operaciones o transacciones con la fiduciaria.

El monitoreo y la gestión del cumplimiento de las políticas por parte de cada funcionario, proveedor o tercero, corresponde al conocimiento que cada líder de área o responsable por la administración de un servicio tiene sobre el desempeño y cumplimiento de las obligaciones contraídas, realizando las gestiones pertinentes para hacer cumplir las políticas e informando del incumplimiento de estas.

7. 2. Excepciones

Las excepciones a esta Política de Seguridad de la Información y Ciberseguridad establecidas en este documento son la siguientes:

- La copia de información confidencial y el traslado de información interna o confidencial fuera de las instalaciones de la Fiduciaria, solo podrán ser autorizadas por el Jefe Inmediato (Nivel Directivo) mediante el diligenciamiento del formato de Novedad de Usuario (Procedimiento de Administración de usuarios).
- La habilitación de los puertos USB o el uso de correos electrónicos personales en forma temporal, únicamente será autorizada por Presidencia y se deberá solicitar mediante formato de novedad de usuario justificando la necesidad y periodo de uso.

Si el encargado de autorizar considera que una excepción solicitada conlleva riesgos altos para la seguridad de la información puede no autorizarla, o escalarla a su superior según el organigrama de la Fiduciaria.

El Oficial de Seguridad de la Información y Continuidad del Negocio debe solicitar las explicaciones necesarias antes de firmar el formato de Novedad de Usuario para validar si hay algún tipo de afectación a la seguridad de la información.

7. 3. Incumplimiento a las políticas descritas en este documento

En caso de presentarse incumplimiento de la Política de Seguridad de la Información y Ciberseguridad aquí descrita por negligencia o intencionalidad de un funcionario de La Fiduciaria, su superior o el funcionario que lo haya detectado debe realizar el reporte conforme a lo establecido en el procedimiento de gestión de incidentes de seguridad de la información; informar a la Vicepresidencia Administrativa y Financiera con el fin de que sean tomadas las medidas correctivas pertinentes según el caso y se surta el respectivo proceso disciplinario según el reglamento interno de trabajo.

Si el incumplimiento se presenta por parte de un proveedor y/o contratista el supervisor del contrato debe proceder de acuerdo con lo estipulado en el mismo. Si el incumplimiento se presenta por parte de un cliente, se debe analizar el impacto para La Fiduciaria, tomar las medidas necesarias para mitigarlo y decidir la continuación o no de la relación comercial con el cliente.

8. DEFINICIONES

El presente documento cuenta con un glosario de términos que son utilizados en el desarrollo de este.

- **Aceptación de riesgo:** Una decisión informada de asumir las consecuencias y probabilidad de ocurrencia de un riesgo en particular.
- **Active Directory:** Implementación de Microsoft del Protocolo LDAP.
- **Activo de información**: Cualquier bien o ente que crea, usa o trata información, la cual posee un valor y es necesaria para realizar los procesos misionales y de soporte de la Entidad, entre los que se encuentran: información escrita, hablada y digital, infraestructura física y ambientes de trabajo, personas y sistemas de información.
- **Administración de riesgos:** La cultura, procesos y estructuras que están dirigidas hacia la administración efectiva de oportunidades potenciales y efectos adversos.
- **Amenaza:** Todo aquello que puede explotar una vulnerabilidad presente en el activo mediante la cual se pueda ver comprometida la seguridad del activo de información y por ende, la seguridad de la Entidad. Evento inesperado con el potencial para causar daños. Las fuentes comunes de amenazas son las personas, la naturaleza y el ambiente.
- **Análisis de riesgo:** Uso sistemático de la información para identificar las fuentes y estimar el riesgo.
- **Autenticación:** Conjunto de técnicas y procedimientos utilizados para verificar la identidad de un cliente, entidad o usuario. Los factores de autenticación son: algo que se sabe, algo que se tiene, algo que se es.
- **Caracteres alfanuméricos:** Son caracteres combinados entre números y letras ya sean mayúsculas o minúsculas.
- **Ciberespacio:** es el ámbito de información que se encuentra implementado dentro de los ordenadores y de las redes digitales de todo el mundo. Es virtual, inexistente desde el punto de vista físico donde las personas o sujetos, públicas o privadas, desarrollan comunicaciones a distancia, exponen sus competencias, generan interactividad para diversos propósitos.
- **Ciberseguridad:** es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de La Fiduciaria y los usuarios en el ciberentorno. Conjunto de medidas de “Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados”.
- **Cifrado:** Técnicas de codificación que pretenden garantizar el secreto en la comunicación entre dos entidades (personas, organizaciones, etc.). Para proteger dicha información se utilizan algoritmos robustos reconocidos internacionalmente, brindando al menos los niveles de seguridad ofrecidos por 3DES y/o AES, llamados códigos de Cifrado Fuerte utilizados en el intercambio de información digital.
- **Cliente:** Es toda persona natural o jurídica con la cual la entidad establece y mantiene una relación contractual o legal con La Fiduciaria para el suministro de cualquier producto o servicio propio de su actividad.

- **Confidencialidad:** Propiedad que determina que la información sea accesible solo a aquellas personas autorizadas a tener acceso a ella. Los activos de información deben estar debidamente protegidos para evitar la divulgación de la información almacenada, procesada, transmitida o recibida a individuos, organizaciones o procesos no autorizados.
- **Control de riesgos:** Parte de la metodología de riesgos que involucra la implementación controles tales como políticas, estándares, procedimientos y cambios físicos para eliminar o minimizar los riesgos o mantener los riesgos de seguridad de la información por debajo del nivel del riesgo aceptado.
- **Criptografía:** Es la técnica que consiste en cifrar un mensaje, conocido como texto en claro, convirtiéndolo en un mensaje cifrado o criptograma, que resulta ilegible para todo aquel que no conozca el sistema mediante el cual ha sido cifrado.
- **Custodio Técnico:** Es una parte designada de La Fiduciaria, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad (Toma de copias de seguridad, asignación privilegios de: Acceso, Modificaciones, Borrado) que el propietario de la información haya definido, con base en los controles de seguridad y recursos disponibles en La Fiduciaria.
- **DMZ:** Una zona desmilitarizada es una red aislada que se encuentra dentro de la red interna de La Fiduciaria. En ella se encuentran ubicados exclusivamente todos los recursos de la empresa que deben ser accesibles desde Internet, como el servidor web o de correo.
- **Disponibilidad:** Propiedad de que la información sea accesible y utilizable toda vez que los usuarios o procesos autorizados la requieran.
- **Evaluación de riesgos:** El proceso utilizado para comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.
- **Evento de seguridad de la información:** un evento de seguridad de la información es la presencia identificada de un estado que indica un incumplimiento posible de la política de seguridad de la información, una falla de los controles de seguridad, o una situación desconocida que puede ser pertinente para la seguridad de la información.
- **File Server:** Concepto utilizado para una maquina tipo servidor que almacena toda la información en forma organizada de todos los usuarios de un sistema.
- **Frecuencia:** Una medida del coeficiente de ocurrencia de un evento expresado como la cantidad de ocurrencias de un evento en un tiempo dado.
- **Hacker:** Persona que accede a un computador de forma no autorizada e ilegal, con el fin de causar daño o copiar información.
- **Identificación de riesgos:** El proceso de determinar qué puede suceder, por qué y cómo.
- **Impacto:** El producto de un evento expresado cualitativa o cuantitativamente, sea este una pérdida, perjuicio, desventaja o ganancia; como consecuencia de la materialización de una Amenaza.
- **Incidente de seguridad de la información:** un incidente de seguridad de la información está indicado por un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de los activos de información. Los incidentes de seguridad de la información son hechos inevitables sobre cualquier ambiente de información, y estos pueden ser bastante notorios e involucrar un impacto fuerte sobre la información de La Fiduciaria. Cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa.
- **Integridad:** Salvaguardar la exactitud y totalidad de la información y los métodos de procesamiento. Las medidas de validación definidas permitirán detectar las modificaciones inapropiadas, la eliminación o la adulteración de los activos de información.
- **ISO 27001:** Norma que especifica los requisitos para establecer, implementar, operar, hacer seguimiento, revisar, mantener, y mejorar un SGSI documentado dentro del contexto de los riesgos globales del negocio de La Fiduciaria.
- **LDAP:** (Lightweight Directory Access Protocol) Es un protocolo que permite administrar de manera ordenada usuarios y equipos en una red.
- **Operaciones:** Son las acciones a través de las cuales se desarrollan, ejecutan o materializan los productos o servicios que presta La Fiduciaria a sus clientes.
- **Política de Seguridad de la Información y Ciberseguridad:** Es un documento de alto nivel que denota el compromiso de la gerencia con la seguridad de la información. Debe ser enriquecida y compatibilizada con otras políticas dependientes de ésta, objetivos de seguridad, procedimientos, etc.
- **Probabilidad:** Índice que mide la factibilidad de materialización del riesgo en un incidente de seguridad.
- **Proceso de administración de riesgos:** La aplicación sistemática de políticas, procedimientos y prácticas de administración a las tareas de establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar riesgos.
- **Producto:** Son las operaciones legalmente autorizadas que puede promover La Fiduciaria.
- **Propietario de la Información:** El cual es una parte designada de La Fiduciaria, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de definir quienes tienen acceso, que pueden hacer con la información, y de determinar cuáles son los requisitos para que la misma se salvaguarde ante accesos no autorizados, modificación, pérdida de la confidencialidad o destrucción deliberada y al mismo tiempo de definir que se hace con la información una vez ya no sea requerida, así como los tiempos de retención asociados a la misma.
- **Protocolo:** Conjunto de reglas que especifican el intercambio de datos u órdenes durante la comunicación entre sistemas.
- **Proveedores de redes y servicios de telecomunicaciones:** Empresas reguladas por la Comisión de Regulación de Comunicaciones y debidamente habilitadas por el Ministerio de Tecnologías de la Información y las Comunicaciones, responsables de la operación de redes y/o de la provisión de servicios de telecomunicaciones a terceros (de acuerdo a lo establecido en la resolución 202 de 2010 art.1).
- **Riesgo:** Vulnerabilidad o proximidad que se pueda tener ante un posible o potencial perjuicio o daño. El potencial daño o perjuicio normalmente es causado por la exposición a un(os) factor(es) o elemento(s), que de acuerdo con el grado de exposición que se tenga a los mismos se tendrá un mayor o menor grado de daño o perjuicio.
- **Riesgo Puro o Inherente:** Es el nivel de impacto ante el riesgo que existe antes de aplicar cualquier acción de tratamiento.
- **Riesgo residual:** El nivel restante de riesgo luego de implementar el plan de tratamiento de riesgo, medidas o controles de

mitigación del riesgo.

- **Seguridad de la Información:** Es la disciplina que se encarga de garantizar la confidencialidad, integridad y disponibilidad de la información. Medidas y actividades que procuran proteger los activos de información, entendiéndose éstos como los conocimientos o datos que tienen valor para una organización, en sus diferentes formas y estados, a través de la reducción de riesgos a un nivel aceptable, mitigando las amenazas latentes.
- **Seguridad informática:** Conjunto de métodos, procesos o técnicas para la protección de los sistemas informáticos (redes e infraestructura) y la información en formato digital que éstos almacenen.
- **Servicio:** Es toda aquella interacción de las entidades sometidas a inspección y vigilancia de la SFC con sus clientes y usuarios para el desarrollo de su objeto social.
- **Servidor:** Computador de gran capacidad utilizado para realizar grandes procesos o tareas.
- **SGSI:** Es un Sistema de Gestión de la Seguridad de la Información es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.
- **Tratamiento de riesgos:** Proceso de selección e implementación de opciones y controles apropiados para tratar el riesgo.
- **VLAN:** Una red de área virtual o VLAN (acrónimo de Virtual Local Area Network) es una red lógica independiente dentro de una red física de forma que es posible crear diferentes una VLAN que este conectadas físicamente a diferentes segmentos de una red de área local o LAN.
- **VPN:** Una red privada virtual, también conocida por sus siglas VPN (Virtual Private Network) es una tecnología de red que permite una extensión segura de una red local (LAN) sobre una red pública o no controlada como Internet.
- **Vulnerabilidad:** Es una debilidad (vacío) que se puede activar accidentalmente o explotar intencionalmente por medio de una Amenaza, es una falla o debilidad en los procedimientos de seguridad de un sistema, en su diseño, en su implementación o en los controles internos que podrían permitir violar la confidencialidad, integridad o disponibilidad de la información o una violación a las políticas de seguridad.
- **Usuario:** Cualquier persona que genere, obtenga, transforme, conserve o utilice información de La Fiduciaria en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de La Fiduciaria. Son las personas que utilizan la información para propósitos propios de su labor, y que tendrán el derecho manifiesto de su uso dentro del inventario de información. Para cada usuario se debería definir los derechos y niveles de acceso al activo de información (lectura, escritura, borrado, entre otros).

9. MARCO REGULATORIO Y NORMATIVO

A continuación, se relaciona la normatividad aplica al sector financiero y por ende a La Fiduciaria dentro del Modelo de Gestión de la Seguridad de la Información y ciberseguridad.

- Ley 527 de 1999, por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
- Ley estatutaria 1266 de 2008 “Habeas Data”, que regula el manejo de la información de las personas recopiladas y almacenadas en bases de datos de terceros, en especial la información de carácter financiero, crediticio, comercial, de servicios y la proveniente de terceros países.
- Ley 1273 de 2009 por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.
- Ley 1581 de 2012 que fue regulada en el Decreto 1377 de 2013, Ley de protección de datos personales que definen el marco jurídico orientado a garantizar que la debida, recolección, almacenamiento, tratamiento, uso y distribución de los datos personales de los titulares por parte de terceros.
- Circular Básica Jurídica 029 de 2014 Parte I – Título II- Capítulo I de la Superintendencia Financiera de Colombia, por medio de la cual se “establece los requerimientos mínimos se seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios”, y entre otros establece que las entidades vigiladas deben gestionar la seguridad de la información.
- Circular Básica Jurídica 029 Parte I – Título I- Capítulo IV de la Superintendencia Financiera de Colombia, por medio de la cual se determina que las entidades vigiladas deben contar con un adecuado manejo de la gestión de riesgos y controles en la gestión tecnológica y seguridad en los sistemas que garanticen que la información cumpla con los criterios de seguridad relacionados con la confidencialidad, integridad y disponibilidad.
- La Política de Seguridad de la Información y Ciberseguridad se fundamenta y estructura en los 14 dominios de la norma internacional NTC – ISO/IEC 27001:2022 de buenas prácticas de seguridad de la información, para asegurar la confidencialidad, integridad y disponibilidad de la información en La Fiduciaria y en la norma de buenas prácticas ISO 27032:2020, así como en las políticas, recomendaciones y buenas prácticas de Seguridad de la Información y de Ciberseguridad dadas por CISA (Cybersecurity and Infrastructure Security Agency de Estados Unidos), a través de la normativa NIST (National Institute of Standards and Technology) y CSET (Cyber Security Evaluation Tool).

10. COMITÉ DE SEGURIDAD DE LA INFORMACION Y CIBERSEGURIDAD

10. 1. Objetivo

El comité de seguridad de la información y ciberseguridad es el órgano de gobierno corporativo que debe garantizar el apoyo y compromiso de las directivas con estas políticas y monitorear su aplicación y cumplimiento.

10. 2. Conformación

El comité estará conformado por los integrantes del Comité de Presidencia y deberá contar con la participación del Oficial de seguridad de la información como coordinador en temas de seguridad de la información.

A las reuniones del Comité de Seguridad de la información y ciberseguridad podrán ser invitados funcionarios o personal externo a la Fiduciaria, que tengan relación directa o conocimiento de alguno de los temas a tratar en la respectiva reunión.

Nota: Los miembros del comité tienen voz y voto con excepción de los Gerentes de Riesgo y Control Interno que junto con los invitados y organizador solo tienen voz.

10. 3. Funciones

Las funciones del comité son:

- Evaluar el estado general de la seguridad de la información y ciberseguridad
- Revisar y hacer seguimiento a los incidentes de seguridad de la información y ciberseguridad
- Revisar y aprobar los proyectos de seguridad de la información y ciberseguridad.
- Revisar modificaciones o nuevas políticas de seguridad de la información.
- Tomar decisiones relacionadas con el control y protección de la seguridad de la información y ciberseguridad.
- Especificar los objetivos, estrategias y planeación corporativa de seguridad de la información y ciberseguridad de la Fiduciaria.
- Revisar que se cuente con los recursos necesarios para la gestión de seguridad de la información y ciberseguridad.

10. 4. Citación

El Gerente de Riesgos o el Oficial de Seguridad de la Información citará con mínimo tres (3) días de anterioridad a la reunión a través de correo electrónico a todos los integrantes del Comité y a los invitados que se consideren necesarios para el buen desarrollo de este.

10. 5. Periodicidad

El comité se debe reunir al menos una vez cada semestre de forma rutinaria. Se podrán efectuar reuniones extraordinarias en caso de que se presente una situación que lo requiera o que alguno de sus miembros lo considere necesario.

10. 6. Quorum

Habrá quórum deliberatorio y decisorio con la asistencia de la mitad más uno de los miembros permanentes o sus delegados que tengan facultad para votar.

En caso de que alguno de los miembros no pueda asistir a una de las sesiones puede delegar a alguien de su misma área de nivel directivo (Directores o Jefes).

10. 7. Actas

Todas las sesiones, acuerdos y recomendaciones del Comité de Seguridad de la Información y ciberseguridad deberán constar en actas que se llevarán en orden consecutivo, debidamente suscritas y aprobadas por los integrantes presentes en la sesión correspondiente. Las actas serán enviadas por correo electrónico a todos los miembros, dentro de los 5 días hábiles siguientes de haberse efectuado la reunión. Los integrantes del comité tendrán 5 días para hacer cualquier comentario o corrección a las mismas, pasado este plazo se entenderá que están de acuerdo con su contenido.

Estos tendrán únicamente voz.

11. RESPONSABILIDADES EN SEGURIDAD DE LA INFORMACION Y CIBERSEGURIDAD

Los roles y responsabilidades en cuanto a Seguridad de la Información y Ciberseguridad son los siguientes:

11. 1. Junta Directiva

1. Aprobar las políticas de Seguridad de la Información y ciberseguridad y apoyar en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información y ciberseguridad de La Fiduciaria.
2. Aprobar el Manual de Políticas de Seguridad de la Información y Ciberseguridad y sus posteriores actualizaciones.
3. Conocer y hacer seguimiento al perfil de riesgo de seguridad de la información y cibernético de La Fiduciaria.
4. Velar porque se asignen los recursos necesarios que permitan una adecuada gestión de la seguridad de la información y ciberseguridad en la Fiduciaria.
5. Emitir las respectivas recomendaciones o conceptos sobre el informe de seguridad de la información y ciberseguridad presentado semestralmente.

11. 2. Alta Dirección

1. Asistir y participar activamente en el Comité de Seguridad de la Información.
2. Desempeñar las responsabilidades dadas en el Comité de Seguridad de la Información en el cual ellos son miembros.
3. Promover la cultura de seguridad de la información y ciberseguridad en La Fiduciaria.
4. Garantizar que los colaboradores a su cargo conozcan y apliquen las políticas de seguridad de la información y ciberseguridad

11. 3. Unidad de Seguridad de la Información y Ciberseguridad

La unidad de Seguridad de la Información y Ciberseguridad en La Fiduciaria está liderada por el Oficial de Seguridad de la información y Continuidad del Negocio y depende funcionalmente de la Gerencia de Riesgo.

Las funciones de esta unidad comprenden:

- Definir, proponer y mantener las políticas de seguridad de la información.
- Coordinar la implementación de las políticas de seguridad de la información con los diferentes procesos de la Fiduciaria.
- Reportar a la Gerencia de Riesgos semestralmente el estado y gestión de la seguridad de la información y ciberseguridad, el cual realizará presentación a la Junta Directiva y Alta Dirección.
- Coordinar y realizar labores de capacitación, divulgación y concientización de Seguridad de la Información y ciberseguridad para todos los funcionarios y terceros que tengan acceso a los activos de información de la Fiduciaria, así como de posibles ciberamenazas.
- Apoyar en el proceso de medición de la eficiencia de los controles de seguridad implementadas por cada área de La Fiduciaria.
- Hacer una gestión de seguridad de la información que permita mantener la seguridad en niveles razonables, de acuerdo a las vulnerabilidades y amenazas detectadas en la matriz de riesgos.
- Definir y actualizar normas, procedimientos y estándares de la Seguridad de la Información y ciberseguridad.
- Revisar y proponer recomendaciones a la arquitectura de seguridad en la infraestructura tecnológica de La Fiduciaria, a petición de los administradores respectivos.
- Apoyar el análisis de riesgos de seguridad de la información a los procesos que se determinen, de los definidos en La Fiduciaria.
- Evaluar, seleccionar y sugerir la implantación de herramientas que faciliten las labores de seguridad y contingencia.
- Recibir capacitación en seguridad de la información y ciberseguridad.
- Coordinar pruebas de hacking ético, vulnerabilidades y de seguridad en la red de La Fiduciaria.
- Investigar sobre nuevos productos y tecnología de seguridad para la infraestructura de La Fiduciaria.
- Diseñar alarmas, controles destinados a proteger la confidencialidad y/o acceso adecuado a la información.
- Fomentar la coordinación entre los procesos de La Fiduciaria implicados en el logro de un nivel apropiado de seguridad de la información.
- Monitorear cambios significativos en los riesgos que afectan a los recursos de la información de La Fiduciaria frente a posibles amenazas, sean internas o externas.
- Evaluar y apoyar la implementación de controles específicos de Seguridad de la Información y Ciberseguridad para los sistemas o servicios de La Fiduciaria, sean preexistentes o nuevos.
- Mantener a La Fiduciaria al tanto de nuevas leyes y regulaciones aplicables a seguridad de la información y ciberseguridad .
- Monitoreo y verificación del cumplimiento de las políticas y procedimientos que se establezcan en materia de ciberseguridad.

- Asesorar a la Alta gerencia y la Junta Directiva en temas que considere necesarios sobre seguridad de la información y ciberseguridad.
- Sugerir los presupuestos de seguridad de la información y ciberseguridad.
- Asesorar en la aplicación de la metodología para el mantenimiento de los planes de contingencia y continuidad del negocio.
- Asesorar a las áreas que lo requieran en temas de seguridad de la información y ciberseguridad, en proyectos o en la contratación de proveedores.
- Asesorar y coordinar recomendaciones sobre medidas de Seguridad de la Información y Ciberseguridad en la página de La Fiduciaria para los clientes.

11. 4. Dueños de la Información

Toda información utilizada por La Fiduciaria, debe poseer un dueño. Los dueños de la información son los responsables de este activo de información o ciberactivo y deben:

- Definir su clasificación
- Determinar los niveles de acceso a ella
- Autorizar la asignación de permisos de acceso
- Velar porque se apliquen los controles necesarios para su almacenamiento, procesamiento, distribución y uso.

11. 5. Área de tecnología

El área de tecnología de La Fiduciaria es la responsable del conjunto de métodos, procesos, medidas técnicas y herramientas para la protección de los sistemas informáticos(redes, infraestructuras, hardware y software) y de la información en formato digital que soportan la operación de La Fiduciaria, gestiona las implementaciones técnicas de protección de la información, la administración de usuarios de las aplicaciones, el despliegue de las tecnologías antivirus, firewalls, detección de intrusos, detección de anomalías, entre otros, basado en la políticas y directrices de la Fiduciaria para la gestión de seguridad de la información y ciberseguridad.

11. 6. Funcionarios

Todo funcionario de La Fiduciaria es responsable por el cumplimiento de las políticas de seguridad de la información. Adicionalmente cada funcionario está comprometido a reportar cualquier incidente de seguridad del que tenga conocimiento por los procedimientos establecidos. Los funcionarios que posean personal a su cargo son responsables de que ellos conozcan, acepten y cumplan las políticas de seguridad de la información. De igual forma es su deber reportar cualquier incidente de seguridad del que tenga conocimiento, por los medios y formas establecidos para ello.

11. 7. Partes relacionadas

Los contratistas, proveedores y terceros que tengan acceso a los activos de información de La Fiduciaria, están obligados a cumplir esta Política de Seguridad de la Información y Ciberseguridad.

12. METODOLOGÍA DE ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

12. 1. Conceptos Generales

12. 1.1. Introducción

La Administración de Riesgos es una parte fundamental de la gobernabilidad corporativa que busca contribuir eficientemente en la identificación, análisis, tratamiento, comunicación y monitoreo de los riesgos para la seguridad de la información de La Fiduciaria, por ello La Fiduciaria debe enfocarse prioritariamente en la atención de los riesgos, con el propósito de tomar las acciones preventivas necesarias para minimizar la posibilidad de ocurrencia y controlar y minimizar sus impactos.

La administración de Riesgos es parte integral de las buenas prácticas gerenciales, es un proceso iterativo que consta de pasos, los cuales, cuando son ejecutados en secuencia metodológica, posibilitan una mejora continua en la operación de La Fiduciaria y sus procesos misionales provocando una adecuada toma de decisiones enfocadas a mantener la operación de La Fiduciaria de la forma más segura posible.

La Administración de Riesgos en La Fiduciaria se desarrolla en armonía con el enfoque basado en procesos que rige su operación; por lo tanto, los análisis necesarios se realizarán a cada uno de los procesos y se verificará su interacción con los demás elementos del proceso de gestión tales como los objetivos estratégicos y los responsables de la gestión.

12. 1.2. Objetivos

Los objetivos de la gestión de riesgos de seguridad de la información y ciberseguridad son:

Permitir a La Fiduciaria identificar, evaluar, tratar y monitorear los riesgos de la información y definir los criterios de aceptación de riesgos.

Establecer el marco conceptual para la gestión de activos de información y para la gestión de riesgos de seguridad de la información; contemplando criterios para realizar las valoraciones de riesgos, al igual que los impactos, probabilidades, evaluación de riesgos y verificación de los controles existentes a ser tenidos en cuenta en el análisis y evaluación de riesgos.

Integrar las metodologías de valoración de riesgos en La Fiduciaria con el fin de poder tener un panorama general de los riesgos evaluados bajo los mismos criterios para los diversos tipos de sistemas o riesgos en La Fiduciaria.

Incorporar las recomendaciones de buenas prácticas internacionales, como ISO 27001-2022 y NIST, así como de organismos internacionales y proveedores, para la gestión y tratamiento de riesgos emergentes.

12. 1.3. Alcance

Definir la metodología de riesgos de seguridad de la información y ciberseguridad y establecer el contexto y escalas en la valoración de activos y riesgos.

12. 1.4. Periodicidad

Se realizará análisis de riesgos en Seguridad de la Información en La Fiduciaria al menos una vez al año, o cuando se presenten cambios en la infraestructura, los procesos o servicios, que puedan alterar el perfil de riesgo de seguridad de la información de La Fiduciaria. Así mismo el Oficial de Seguridad de la Información debe preparar una vez al año un informe al Comité de Seguridad de la Información con la presentación detallada de los riesgos de seguridad de la información, así como incidentes o eventos de seguridad que se hayan presentado. Es recomendable que la revisión del inventario de activos se lleve a cabo por lo menos una vez al año.

12. 1.5. Responsable

El responsable de gestionar los análisis de riesgos en Seguridad de la Información, la presentación de los resultados y la matriz ante el Comité de Seguridad de la Información es el Oficial de Seguridad de la Información.

12.2. Metodología

La Metodología empleada tiene un enfoque de gestión de riesgos de cara a los activos de información identificados y valorados, así como a los procesos afectados, para poder diseñar, implementar, mantener y mejorar la Seguridad de la Información de La Fiduciaria.

La metodología de valoración de riesgos en seguridad de la información para La Fiduciaria tiene las siguientes fases:

12.2.1. Identificación de activos

Los activos de información son el conjunto de elementos que se utilizan en los diferentes procesos de La Fiduciaria. Los activos de cada proceso deben ser identificados, establecer su sensibilidad en términos de seguridad y finalmente establecer los riesgos de seguridad que pueden afectar el proceso.

12.2.1.1. Información basica de activos de información

La información básica hace referencia a aquellas características del activo que permiten su adecuada documentación e identificación:

- **Identificador:** Número consecutivo único que identifica al activo en el inventario.
- **Proceso:** Nombre del proceso al que pertenece el activo.
- **Nombre Activo:** Nombre de identificación del activo dentro del proceso al que pertenece.
- **Descripción/Observaciones:** Es un espacio para describir el activo de manera que sea claramente identificable por todos los miembros del proceso.
- **Ubicación:** Describe la ubicación tanto física como electrónica del activo de información.
- **Clasificación:** Hace referencia a la protección de información de acuerdo a Confidencialidad, Integridad y Disponibilidad.
- **Criticidad:** Es un cálculo automático que determina el valor general del activo, de acuerdo con la clasificación de la Información.
- **Propietario:** Es un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con el proceso se clasifican adecuadamente. Deben definir y revisar periódicamente las restricciones y clasificaciones del acceso.
- **Custodio:** Es un cargo, proceso, o grupo de trabajo encargado de hacer efectivos las restricciones y clasificaciones de acceso definidos por el propietario. (Para sistemas de información o información consignada o respaldada, generalmente es TI o para información física, los custodios pueden ser los funcionarios o el proceso de archivo o correspondencia, el custodio generalmente se define donde reposa el activo original).

12.2.1.2. Tipología de clasificación para activos de información y ciberactivos

Se debe indicar la tipología de clasificación de activos de información, como se menciona a continuación:

- **Información:** Corresponden a este tipo datos e información almacenada o procesada física o electrónicamente tales como: archivos de datos, contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros.
- **Software:** Software de aplicación, interfaces, software del sistema, herramientas de desarrollo y otras utilidades relacionadas.
- **Aplicación:** Es un programa informático creado para llevar a cabo o facilitar una tarea en un dispositivo informático.
- **Bases de Datos:** Programa capaz de almacenar gran cantidad de datos, relacionados y estructurados, que pueden ser consultados rápidamente de acuerdo con las características selectivas que se deseen.
- **Servicio:** Servicios de computación y comunicaciones, tales como Internet, páginas de consulta, directorios compartidos e Intranet.
- **Hardware:** Equipos de cómputo y de comunicaciones que por su criticidad son considerados activos de información, no sólo activos fijos.
- **Infraestructura Física:** Hace referencia a las locaciones físicas o instalaciones dentro de las cuales se procesa la información (Oficinas, Espacio físico datacenter, centro de datos).
- **Recurso humano:** Aquellas personas que, por su conocimiento, experiencia y criticidad para el proceso, son consideradas activos de información.
- **Otros**: activos de información que no corresponden a ninguno de los tipos descritos anteriormente, pero deben ser valorados para conocer su criticidad al interior del proceso.

12.2.1.3. Tipología de clasificación para los ciberactivos

Todos aquellos ciberactivos deben estar debidamente identificados y clasificados como base en la clasificación dada por la norma ISO 27032:2020: sobre buenas prácticas de ciberseguridad:

Pueden ser:

- Personal: Aquellos que pertenecen al individuo. Ej: dispositivos móviles personales.
- Organización: Aquellos que pertenecen a La Fiduciaria.

Así mismo estos pueden ser:

- Físicos: Cuya forma existe en el mundo real.
- Virtuales: Solo existe en el ciberespacio y no se puede ver o tocar en el mundo real.

12.2.2. Esquema de Valoración de activos de información

Para establecer los activos y su relevancia en el proceso de análisis de riesgos, es necesario identificar y parametrizar las diferentes características y requerimientos de seguridad de los activos de acuerdo a los 3 pilares de seguridad de la información:

a. Confidencialidad: Asegurar que la información sea accesible solo para aquellos autorizados a tener acceso. Se trata básicamente de la propiedad por la que esa información solo resultará accesible con la debida y comprobada autorización. Para calificar los requerimientos de confidencialidad se utilizó la siguiente escala:

Confidencialidad		
Nivel	**Descripción**	**Peso de calificación**
Confidencial	Información de alta sensibilidad que debe ser protegida por su relevancia sobre decisiones estratégicas, impacto financiero, oportunidad de negocio, potencial de fraude o requisitos legales. A este tipo de información sólo podrá tener acceso su propietario o el grupo autorizado al cual pertenece.	33%
Interno	Información que sin ser confidencial, debe mantenerse dentro de la entidad y no debe estar disponible externamente, excepto para terceros involucrados y debidamente autorizados que hayan firmado acuerdos de confidencialidad. Cualquier información no clasificada se considera como interna.	20%
Publico	Es la información cuya divulgación al público no afecte a la Fiduciaria en términos de pérdida de imagen y/o económica. Ésta información ha sido explícitamente aprobada por la entidad para su diseminación pública.	5%

b. Disponibilidad: Asegurar que los usuarios autorizados tengan acceso a la información cuando lo requieran. Para calificar los requerimientos de disponibilidad de la información y los servicios de tecnología se utilizó la siguiente escala:

Disponibilidad		
Nivel	**Descripción**	**Peso de calificación**
Crítica	1 día: Se puede estar sin el activo en funcionamiento máximo 1 día laboral (8 Horas) al cabo de los cuales se comienzan a materializar riesgos financieros y operativos	34%
Alta	2 a 5 días: Se puede estar sin el activo en funcionamiento máximo 5 días al cabo de los cuales se comienzan a materializar riesgos financieros y operativos	20%
Moderada	6 a 15 días: Se puede estar sin el activo en funcionamiento entre 6 a 15 días al cabo de los cuales se comienzan a materializar riesgos financieros y operativos	10%
Baja	15 a 30 días: Se puede estar sin el activo en funcionamiento entre 15 a 30 días al cabo de los cuales se comienzan a materializar riesgos financieros y operativos	5%

c. Integridad: La integridad hace referencia a la cualidad de la información para ser correcta y no haber sido modificada, manteniendo sus datos completitud y exactamente tal cual fueron generados, sin manipulaciones ni alteraciones. Para calificar los requerimientos de integridad (exactitud de la información) se utilizará la siguiente escala:

Integridad		
Nivel	**Descripción**	**Peso de calificación**
Crítica	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad. Adicionalmente no puede volver a obtenerse una calidad semejante a la original.	33%
Alta	Información cuya pérdida de exactitud y completitud puede con llevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen importantes de la entidad. La calidad necesaria se puede reconstruir de forma difícil y costosa.	20%
Moderada	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo moderado de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad. Se identifica si tras el daño se puede reemplazar y ofrecer una calidad semejante con una molestia razonable.	10%
Baja	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos. Si tras el daño se puede reemplazar fácilmente y ofrecer la misma calidad.	5%

NIVEL DE CRITICIDAD:

Cada uno de los factores anteriormente mencionados será calificado por los líderes de cada uno de los procedimientos o dueños de los activos valorados a través del aplicativo y de acuerdo con los resultados obtenidos de la suma de las calificaciones de la Confidencialidad, Disponibilidad e Integridad, se obtiene el nivel de criticad del activo de acuerdo con el seguimiento escala:

Nivel de Criticidad		
Nivel	Descripción	Porcentaje
Crítica	El activo tiene una criticidad y sensibilidad muy alta dada por su clasificación crítica y alta en su Confidencialidad, Integridad o Disponibilidad, por lo que cualquier afectación a este activo puede tener un impacto significativo operacional, económico o de cumplimiento global en la entidad.	81% - 100%
Alta	El activo tiene una criticidad y sensibilidad alta dado por su clasificación alta en su Confidencialidad, Integridad o Disponibilidad, por lo que cualquier afectación a este activo puede tener un impacto operacional, económico o de cumplimiento global o de proceso crítico en la entidad.	61% - 80%
Moderada	El activo tiene un nivel moderado dado por su clasificación en su Confidencialidad, Integridad o Disponibilidad, puede llegar a una afectación moderada a nivel de proceso de la entidad.	31% - 60%
Baja	El activo tiene un nivel bajo dado por su clasificación baja y moderada Confidencialidad, Integridad o Disponibilidad, por lo que su afectación puede tener una afectación mínima en un algún proceso.	0% - 30%

12.2.3. Identificación y análisis del Riesgo

La identificación y clasificación de los riesgos potenciales tienen como objetivo un mejor seguimiento a las posibles debilidades o inadecuaciones que existan en seguridad de la información o ciberseguridad en La Fiduciaria. Para lo anterior, se debe seguir los pasos descritos en el Manual de Administración de Riesgo Operativo SARO en su etapa de “Criterios y procedimiento de identificación de los riesgos potenciales por proceso”, la identificación de riesgos de seguridad de la información seguirá su

identificación por procesos que será realizada por cada uno de los responsables de los procedimientos como está definido en la metodología de riesgo operacional, cuando se considere necesaria la identificación de riesgos se puede realizar basándose en los activos de información y ciberactivos y serán los dueños de estos activos los responsables de esta actividad, las causas para estos últimos pueden basarse en la identificación de vulnerabilidades, amenazas, riesgos emergentes, alertas de entidades del estado Colombiano o Entes Internacionales, recomendaciones de otras entidades financieras o proveedores del SOC o pruebas de ciberseguridad entre otros.

Por medio de este paso se aplica el proceso de identificación de riesgos de la seguridad de la información y ciberseguridad que están asociados con la pérdida de Confidencialidad, de Integridad y de Disponibilidad de información dentro del alcance del sistema de gestión de la seguridad de la información y ciberseguridad. Esos riesgos deben quedar claramente identificados y registrados de acuerdo a la clasificación definida.

Una vez concluida la identificación de riesgos potenciales, debe medirse la probabilidad de ocurrencia de un evento de riesgo de seguridad de la información o ciberseguridad y su impacto en caso de materializarse.

Cada uno de los riesgos identificados deberá ser calificado con base las escalas de probabilidad de ocurrencia y de impacto definidos en el Manual de Administración de Riesgo Operativo en su ítem de “Medición de Riesgo Operacional”.

Para identificar específicamente los ciberriesgos con base en la identificación previa de ciberactivos, se requiere el cambio de ajuste en la valoración de la probabilidad teniendo en cuenta únicamente la materialización del mismo, para lo cual se ajustan la descripción de la escala de valoración como se muestra a continuación:

Materialización del riesgo	Nivel	Porcentaje(%)
Ocurrio mas de una vez al año o ocurrirá con alto nivel de certeza el proximo año.	Muy Alta	81% - 100%
Ocurrio una vez al año y/o es bastante probable que ocurra el proximo año.	Alta	61% - 80%
Ocurrio una vez en dos años y/o ha ocurrido varias veces en el sector financiero en el ultimo año.	Moderada	41% - 60%
Ocurrio alguna vez en mas de tres años y/o ha ocurrido varias veces en el sector financiero.	Baja	21% - 40%
No ha ocurrido nunca	Muy bajo	0% - 20%

Nota: Para realizar la valoración de ciberriesgos se tomarán en cuenta las siguientes fuentes: Ciberincidentes presentados en los últimos años, Informes Ciberseguridad en el Sector Bancario y Financiero, Informes de Ciberseguridad generados por el sector asegurador y sus proyecciones.

La gestión de incidentes de seguridad de la información son fuente fundamental para la posible identificación de riesgos el detalle de este proceso se puede obtener en el anexo de políticas relacionadas sobre la gestión de incidentes de seguridad de la información y su procedimiento.

12.2.4. Evaluación de Riesgo

Durante esta etapa se obtiene el Riesgo Inherente es decir el riesgo sin tener en cuenta los controles por medio del cálculo de la probabilidad e impacto, se idéntica el nivel de riesgo a través de la matriz por medio de la cual se presenta para priorización de tratamiento de los riesgos, como se describe en el Manual de Gestión de Riesgo Operativo Ítem “Perfil de Riesgo Inherente”.

Posteriormente se procede a Calcular el Riesgo Residual es decir el riesgo que queda después de aplicar los controles. La evaluación de los controles identificados se debe analizar con base en las causas (como ayuda a identificación de las causas en riesgos de seguridad se puede realizar sobre las amenazas y vulnerabilidades que pueden afectar el activo) que se hayan identificado para cada uno de los riesgos, es decir que se debe analizar para cada causa el control que aplicaría para su mitigación.

Para establecer el riesgo después de controles es necesario evaluar los mismos teniendo en cuenta su clasificación basada en las condiciones y variables del diseño del control dadas para evaluar las eficiencia o eficacia del mismo dadas en el Manual de Gestión de Riesgo Operativo Ítem “Evaluación de controles”, lo cual permitirá reducir la probabilidad y/o el impacto de los riesgos identificados inicial.

Del resultado de aplicar el efecto de los controles en la probabilidad o el impacto, los riesgos se ubican en una nueva matriz de clasificación llamada matriz de riesgo después de controles o residual, dentro de la cual se observa el movimiento de los riesgos en los diferentes cuadrantes de acuerdo con el efecto que ejercen los controles sobre los mismos. Esta actividad se realiza con base en el Manual de Gestión de Riesgo Operativo SARO Ítem “Perfil de Riesgo Residual”

12.2.5. Plan de Tratamiento de Riesgo

Los criterios o políticas para la aceptación de los riesgos seguirán los niveles de tolerancia del Riesgo Operacional a continuación se informa las zonas de riesgo que están en el mapa de calor de La Fiduciaria con las respectivas opciones de tratamiento.

NIVELES DE RIESGO POR ZONAS:

Riesgo Extremo	Se deberá tomar acciones inmediatas a nivel gerencial, sus opciones de tratamiento pueden ser Mitigar o Gestionar el riesgo, evitar, compartir o transferir.
Riesgo Alto	Las medidas a implementar deben ser lideradas a nivel directivo o por el líder del procedimiento, sus opciones de tratamiento pueden ser : Mitigar o gestionar el riesgo, evitar, compartir o transferir
Riesgo Moderado	Estos riesgos deben con especificación de responsabilidad a nivel directivo o responsables de los procedimientos sus opciones de tratamiento pueden ser: asumir el riesgo o mitigar el riesgo
Riesgo Inferior	Estos riesgos deben ser administrados mediante proceso de rutina a nivel del responsable del procedimiento sus opciones de tratamiento pueden ser: asumir el riesgo o mitigar el riesgo.

TIPOS DE TRATAMIENTO:

TIPO DE TRATAMIENTO DEL RIESGO	DESCRIPCIÓN
Mitigar o Gestionar	Reducir la probabilidad o impacto de que se materialice el riesgo mediante medidas de seguridad y control. Establecer medidas y controles que permitan el riesgo a un nivel aceptable.
Transferir	Pasar el costo que representarían las pérdidas por la ocurrencia del riesgo a otro bien u otra organización, como trasferencia del riesgo por medio de pólizas de seguros, mediante el proveedor o mediante el cliente.
Asumir el Riesgo	Se aceptar las consecuencias y pérdidas que pueda ocasionar la ocurrencia del riesgo dentro de su nivel normal de operación.
Evitar o Eliminar	Utilizar procedimientos o activos diferentes a los que están generando el riesgo. Si la prestación de in servicio supone un gran riesgo el servicio se deja de prestar.

Las zonas y opciones de tratamiento anteriormente indicados son tomados de los niveles de tolerancia de riesgo operacional de La Fiduciaria. De igual forma, se distribuyen los riesgos (inherentes y residuales) en las zonas de riesgo de acuerdo con el mapa de calor de La Fiduciaria.

Una vez identificado el nivel de riesgo, se formulan una serie de recomendaciones orientadas a la implementación de medidas de control para mitigar los riesgos a niveles aceptables para la Fiduciaria. La oficial de seguridad de la información podrá proponer nuevos controles o mejoras a los ya existentes como apoyo en la implementación de planes de tratamiento por el responsable del riesgo o procedimiento.

En esta etapa de se diseña e implementa un plan de tratamiento al riesgo, con el cual se busca mejorar la postura en ciberseguridad, mitigando la probabilidad de los riesgos o el impacto que pueden ocasionarse a partir de fallas en los controles y en los activos.

Para los planes de tratamiento y si la decisión de tratamiento es gestionarlo, eliminar y trasferir se sigue el procedimiento que se utiliza actualmente para el tratamiento de riesgo. En cualquier caso, si el tratamiento seleccionado para un riesgo es asumirlo, esto

debe ser aceptado y aprobado por la Alta Dirección si se encuentra dentro del apetito de La Fiduciaria, o será llevado para dicho procedimiento a la Junta Directiva si sobrepasa el nivel de apetito aprobado.

Es posible que no todos los controles recomendados se implementen, esto depende del resultado del análisis costo/beneficio, el cual debe demostrar que la implementación se justifica porque hay una reducción en el nivel de riesgo. Adicionalmente es necesario evaluar cuidadosamente el impacto operacional causado por la introducción de las recomendaciones durante el proceso de mitigación.

Considerando que eliminar todos los riesgos es algo imposible de llevar a cabo, es responsabilidad de la Alta Dirección y de los administradores funcionales y de la Fiduciaria implementar los controles más apropiados para reducir la exposición a riesgos a un nivel aceptable, con un mínimo impacto adverso sobre los recursos y la misión de La Fiduciaria.

12.2.6. Consolidación de Riesgo

La responsabilidad de la consolidación de riesgos de seguridad de la información es del Oficial de Seguridad de la Información. Los riesgos de seguridad de la información están contenidos dentro de matriz de riesgo operacional los cuales están claramente identificados y en caso que se requiera en La Fiduciaria se podrá obtener una matriz de riesgos con base en los activos de información o ciberactivos que ya estén valorados.

13. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

En los capítulos anteriores del documento se han mencionado las Políticas de Alto Nivel de Seguridad de la información y ciberseguridad en La Fiduciaria, así como los elementos fundamentales para el adecuado gobierno y gestión del modelo de seguridad de la información y ciberseguridad en La Fiduciaria; adicional a ello existen las políticas específicas de seguridad de la información que se describen y detallan en el Anexo 1. POLITICAS ESPECIFICAS DE SEGURIDAD DE LA INFORMACIÓN y CIBERSEGURIDAD, estas son parte integral de este documento y deben ser conocidas y aceptadas por todos los funcionarios de La Fiduciaria.

Este anexo está estructurado con base en las buenas prácticas de seguridad de la información de la norma ISO 27001:2022 y contiene las siguientes políticas:

1. **SEGURIDAD DEL RECURSO HUMANO:** Se establecen las responsabilidades de seguridad de la información antes, durante y después de la contratación laboral, así como los procesos disciplinarios del incumplimiento de esta política.
2. **SEGURIDAD EN GESTIÓN DE ACTIVOS DE INFORMACIÓN:** se dan directrices y esquema de clasificación de información en La Fiduciaria, así como uso aceptable de activos y servicios como:
    - **Uso general**
    - **Uso de computadores personales**
    - **Utilización de Internet**
    - **Utilización de correo electrónico y mensajería instantánea**
    - **Uso de telefonía y Grabación de llamadas**
    - **Uso de Impresoras y multifuncionales**
    - **Utilización de servicios de red**
    - **Utilización de las aplicaciones corporativas**
    - **Utilización de la red inalámbrica**
    - **Uso de dispositivos móviles**
    - **Trabajo remoto**
    - **Devolución de activos**
    - **Uso seguro de la información**
    - **Uso datos personales**
    - **Manejo de medios**
    - **Gestión de medio Removibles**
    - **Disposición de Medios**
    - **Trasferencia de medios físicos**
3. **CONTROL DE ACCESO:** La Fiduciaria cuenta con un modelo para la gestión de accesos que permite limitar el acceso a información y a instalaciones de procesamiento de información, gestionar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios. Se informa las directrices para el registro o cancelación de usuarios, retiro o ajuste de los derechos de acceso, Administración de Contraseñas de Usuarios Finales, Recomendaciones para el uso de la contraseña.
4. **CRIPTOGRAFIA:** Dentro de esta política encontrara los lineamientos para gestión cifrado en La Fiduciaria y las claves respectivas que se utilizan en el proceso, con el fin de asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.
5. **SEGURIDAD FÍSICA Y AMBIENTAL:** Esta política tiene las directrices necesarias con el objetivo de prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de La

Fiduciaria. Encontrará directrices para:
    - Seguridad del perímetro y control de acceso físico a zonas restringidas
    - Seguridad en las oficinas y salas
    - Áreas públicas y de entrega de correspondencia.
    - Seguridad de los Equipos Fuera de las Instalaciones de la Fiduciaria
    - Ingreso y Retiro de Activos de Información de Terceros
    - Traslado de Activos de Información
    - Equipo de usuario desatendido
    - Política de escritorio y pantalla despejados
6. **SEGURIDAD DE LAS OPERACIONES:** Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra posibles amenazas que las puedan afectar y evitar las pérdidas de Confidencialidad, Integridad o Disponibilidad de la información.
    - Procedimientos operacionales y responsabilidades
    - Gestión del Cambio
    - Protección contra código malicioso y código móvil
    - Copias de respaldo
    - Registro y seguimiento
    - Control de software operacional
    - Gestión de la vulnerabilidad técnica
7. **SEGURIDAD DE LAS COMUNICACIONES:** Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte, Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa pueden identificar las directrices para la Gestión de seguridad de las redes y Transferencia de información.
8. **ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN:** Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes públicas, Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información: Requisitos de seguridad de los sistemas de información, Seguridad en los procesos de desarrollo y soporte, datos de prueba
9. **RELACIONES CON LOS PROVEEDORES:** Asegurar la protección de los activos de La Fiduciaria que sean accesibles a los proveedores, Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores: Identificación de los riesgos relacionados con partes externas, Seguridad con las partes externas
10. **INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD:** Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades, Todos los funcionarios tienen la obligación de reportar cualquier incidente de seguridad de la información por medio de las directrices y procedimientos establecidos para este reporte.
11. **SEGURIDAD EN LA CONTINUIDAD DEL NEGOCIO:** La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de La Fiduciaria.
12. **CUMPLIMIENTO:** Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad, asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales: Derechos de propiedad intelectual.

Archivos adjuntos

- ANEXO_1.PolticasEspecficasdeSeguridaddelaInformacin 30042024.pdf