1. OBJETIVO GENERAL

Establecer la Política General para la Gestión de la Seguridad de la Información y la Ciberseguridad en FIDUCOLDEX y sus patrimonios administrados, la cual hace parte del Sistema de Gestión de Seguridad de la Información (SGSI) implementado en la Fiduciaria y que está alineado al estándar ISO 27001:2013 y al Modelo de Seguridad y Privacidad de la Información, con el propósito de proteger y preservar los activos de información y mitigar los riesgos que pueden afectar su confidencialidad, privacidad y disponibilidad.

1.1 OBJETIVOS ESPECÍFICOS:

a) Definir e implementar políticas, lineamientos, estrategias y controles que propendan por la adecuada gestión de la seguridad de la información, Ciberseguridad en información en FIDUCOLDEX y sus patrimonios administrados, la cual soporte el cumplimiento de los objetivos estratégicos y la satisfacción de los clientes y partes interesadas de la Entidad.

b) Realizar una efectiva y oportuna identificación, medición, control y monitoreo de los riesgos de seguridad y ciberseguridad a fin de establecer medidas y tratamientos para mitigar posibles impactos económicos o reputacionales que puedan afectar la Fiduciaria y sus Patrimonios administrados.

c) Fortalecer la capacidad institucional para identificar, detectar, responder y recuperarse ante un incidente de seguridad o de ciberseguridad.

d) Preservar la confidencialidad, integridad, disponibilidad de los activos de información.

e) Fortalecer el Sistema de Gestión de Seguridad de la Información, (SGSI), promoviendo la mejora continua de los procesos y realizando un seguimiento y monitoreo periódico.

f) Proteger los activos de información, tecnológicos y de seguridad digital.

g) Fortalecer la cultura de seguridad de la información y ciberseguridad en los Funcionarios de la Fiduciaria y los patrimonios administrados, mediante la ejecución de planes de sensibilización y capacitación.

h) Asegurar el cumplimiento de la normatividad aplicable y de los requerimientos legales y contractuales en materia de seguridad, de la información y ciberseguridad.

2 ALCANCE

El alcance del Sistema de Gestión de Seguridad de la Información comprende los procesos de FIDUCOLDEX, acorde con el mapa de procesos del Sistema de Gestión Calidad, así como los procesos misionales de los patrimonios autónomos.
La presente Política, junto con el manual, Procedimientos, Planes y demás documentos asociados debe ser aplicada por todos los Funcionarios de FIDUCOLDEX y sus Patrimonios Administrados, así como por los terceros, empresas o entidades que tengan un vínculo contractual con FIDUCOLDEX y accedan, gestionen, manipulen, transporten o almacene información de la entidad.

3 GLOSARIO

- Acuerdo de Confidencialidad: Contrato suscrito entre las partes con el fin de compartir material confidencial o conocimiento para ciertos propósitos, pero restringiendo su uso público.
- Activo de información: Conocimiento o datos que tienen valor para la entidad o el individuo.
- *Backup:* En tecnologías de la información e informática es una copia de los datos originales que se realiza con el fin de disponer de un medio de recuperación en caso de su pérdida.
- Ciberseguridad: Es el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de la entidad.
- Confidencialidad: Propiedad de la información que la hace no disponible o que no sea divulgada a individuos, entidades o procesos no autorizados.
- Disponibilidad: Propiedad de la información de ser accesible y utilizable a demanda por una parte interesada.
- Firewall: Dispositivo tecnológico que tiene como función proteger la red interna de una FIDUCOLDEX de accesos no autorizados del exterior vía Internet.
- Incidente de Seguridad: Ocurrencia de una situación que pone en peligro la confidencialidad, integridad o disponibilidad de un sistema de información o la información que el sistema procesa, almacena o transmite; o que constituye una violación a las políticas de seguridad, procedimientos de seguridad o políticas de uso aceptable.

- Integridad: Propiedad de la información que busca preservar su exactitud y completitud.

- LAN: Local área network o red de área local, es la interconexión de una o varias computadoras y periféricos.
- Seguridad de la Información: Es el conjunto de políticas, estrategias, metodologías, recursos, soluciones informáticas, prácticas y competencias para proteger, asegurar y preservar la confidencialidad, integridad y disponibilidad de la información que se almacene, reproduzca o procese en los sistemas informáticos de la entidad.

- Seguridad Informática: Se encarga del aseguramiento de la infraestructura tecnológica mediante herramientas o elementos físicos, para evitar que se materialización las amenazas que se propagan por la red.

- Sistema de Gestión de Seguridad de la Información (SGSI): Es el conjunto de manuales, procedimientos, controles y técnicas utilizadas para controlar y salvaguardar todos los activos que se manejan dentro de una entidad.

- SPAM: Se llama spam, correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido (correo anónimo), habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming.

- Tercero(s): Cualquier persona natural o jurídica en calidad de proveedor, outsourcing o consultor.

- TIC: Tecnologías de la información y comunicaciones.

- Usuario: Este concepto cobija a todos los clientes internos, Funcionarios y contratistas que utilicen la red de la entidad.

- VPN: Una red privada virtual, RPV, o VPN de las siglas en inglés de Virtual Private Network, es una tecnología de red que permite una extensión segura de la red local sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada.

4 NORMATIVIDAD APLICABLE

- Parte I, Titulo IV, Capítulo V, de la Circular Básica Jurídica. SUPERINTENDENCIA FINANCIERA DE COLOMBIA. Requerimientos Mínimos para la Gestión de la Seguridad de la Información y la Ciberseguridad.
- Parte I, Titulo II, Capítulo I, de la Circular Básica Jurídica. SUPERINTENDENCIA FINANCIERA DE COLOMBIA. Canales, Medios, Seguridad y Calidad en el Manejo de Información en la Prestación de Servicios Financieros.
- Parte I, Título I Capítulo VI, de la Circular Básica Jurídica. SUPERINTENDENCIA FINANCIERA DE COLOMBIA. Reglas Relativas al Uso de Servicios de Computación en la Nube.
- Parte I – Título I – Capítulo IV, de la Circular Básica Jurídica. SUPERINTENDENCIA FINANCIERA DE COLOMBIA. Sistema de Control Interno.

• Ley 603 de 2000 (27/07/2000): Por la cual se modifica el artículo 47 de la Ley 222 de 1995.

- Ley 1266 de 2008 (31/12/2008): Por la cual se dictan las disposiciones generales del Habeas Data y se regula el manejo de la información contenida en bases de datos personales.
- Ley 1273 de 2009 (5/01/2009): Por medio de la cual se modifica el Código Penal, se crea un nuevo bien tutelado denominado "de la protección de la información y los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- Ley 1341 de 2009 (30/07/2009): Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
- Ley 1712 de 2014 (06/03/2014). CONGRESO DE LA REPÚBLICA. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- Decreto 1377 de 2013 /27/06/2013): Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Derogado Parcialmente por el Decreto 1081 de 2015.
- Decreto 2573 de 2014 (12/12/2014): Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
- Decreto 1078 de 2015 (26/05/2015): Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Resolución 2710 de 2017 (03/10/2017). Ministerio de Tecnologías de la Información y las Comunicaciones. Por la cual se establecen lineamientos para la adopción del protocolo IPv6.

- Resolución 1519 de 2020 (24/08/2020). Ministerio de Tecnologías de la Información y las Comunicaciones. Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
- Resolución 500 de 2021 (10/03/2021). Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.

5. DESARROLLO DE LA POLÍTICA

5.1 COMPROMISO DE LA ALTA DIRECCION

La Alta Dirección FIDUCOLDEX con el apoyo de la Dirección de Seguridad de la Información y PCN se comprometen a apoyar y liderar el establecimiento, implementación, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información (SGSI); así mismo, se comprometen a revisar el avance de la implementación del SGSI de manera periódica y también a garantizar los recursos suficientes (tecnológicos y talento humano calificado) para implementar y mantener el sistema, así mismo, incluirá dentro de las decisiones estratégicas, la seguridad de la información y la ciberseguridad.

5.2 POLITICA GENERAL

El presente documento establece y define las siguientes directrices que deben cumplir los Funcionarios, proveedores y entidades que tengan relación con FIDUCOLDEX y sus Patrimonios Administrados, con respecto a la Seguridad de la Información y Ciberseguridad:

- En FIDUCOLDEX se establece, implementa, monitorea y mantiene un Sistema de Gestión de Seguridad de la Información (SGSI), consistente con su tamaño y naturaleza, así como con la complejidad de sus operaciones, que permita preservar la confidencialidad, integridad y disponibilidad de la información de la entidad y sus Patrimonios Autónomos, siguiendo el Modelo de seguridad y Privacidad de la Información establecido por el Gobierno nacional y el Estándar ISO 27001: 2013, con el propósito de garantizar la protección de sus activos de información, la operatividad de los procesos del negocio, el cumplimiento de las obligaciones legales y contractuales y preservar la imagen y reputación de la Fiduciaria..

- En el marco del SGSI, se debe realizar la Identificación, medición, control y monitoreo permanentemente de los posibles riesgos de seguridad de la información y ciberseguridad a los que pueda exponerse FIDUCOLDEX y sus patrimonios administrados.

- Se deben establecer las medidas de seguridad de la información y ciberseguridad necesarias para el cumplimiento regulatorio de las leyes, reglamentos, políticas, normativas de la SFC y los acuerdos con terceros vigentes relacionados a la seguridad de la información y ciberseguridad.

- Se debe preparar, detectar, informar y gestionar los incidentes de seguridad de la información y ciberseguridad que puedan afectar o atenten contra la confidencialidad, disponibilidad e integridad de la información.

- Se debe motivar, capacitar y concientizar permanentemente a los Funcionarios sobre la responsabilidad de hacer uso adecuado de la información que pertenezca a la FIDUCOLDEX y sus Patrimonios Administrados.

- El incumplimiento total o parcial por parte de los Funcionarios de FIDUCOLDEX S.A o de sus Patrimonios administrados de las políticas, lineamientos y obligaciones establecidas en el SGSI se considerará como falta, en los términos del Código de Ética y Conducta y del Reglamento Interno.

- El incumplimiento a la Política de Seguridad de la Información y ciberseguridad o de sus lineamientos derivados, como procedimientos, manuales entre otros por parte de terceros traerá consigo, las consecuencias legales que estén definidos en los negocios jurídicos.

- Esta política será efectiva desde su aprobación por la Junta Directiva de FIUDOLDEX. Su revisión y actualización se hará en las siguientes condiciones: ○ De forma anual, donde se deberá revisar la efectividad de la política y sus objetivos.
- Si se presentan cambios estructurales en la entidad (restructuración de áreas o procesos), en el objeto misional o plan de negocio.
- Incidentes de seguridad de la información que requieran que la política requiera cambios. ○ Se deben realizar revisiones y seguimiento periódico al SGSI con el fin de asegurar la efectividad del sistema frente a los objetivos planteados. Dichas revisiones estarán apoyadas en los siguientes aspectos:
- Informes semestrales sobre la gestión de seguridad y ciberseguridad de la información que realice el Oficial de Seguridad de la Información y presente a la Junta Directiva y Comité de Riesgo Operacional.

Esta política se encuentra alineada al estándar internacional ISO 27001:2013, el cual indica los lineamientos necesarios para poder establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de la Seguridad de la Información (SGSI).