TABLA DE CONTENIDO

1. OBJETIVO GENERAL 2
1.1 OBJETIVOS ESPECÍFICOS: 2
2 ALCANCE 2
3 GLOSARIO 3
4 NORMATIVIDAD APLICABLE 4
5 DESARROLLO DE LA POLÍTICA 6
5.1 ROLES Y RESPONSABILIDADES 6
5.2 COMPROMISO DE LA ALTA DIRECCION 8
5.3 POLITICA GENERAL 8
5.4 LINEAMIENTOS A NIVEL DEL TALENTO HUMANO 10
5.5 POLITICAS ESPECIFICAS 11
6 DOCUMENTOS ASOCIADOS 14
7 CONTROL DE DOCUMENTOS 16

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 ROLES Y RESPONSABILIDADES

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES RESPECTO A LA SEGURIDAD DE LA INFORMACIÓN)
Junta Directiva	• Aprobar la política de Seguridad de la Información y Ciberseguridad y sus actualizaciones. • Proporcionar los recursos necesarios para la implementación y mantenimiento del SGSI. • Realizar seguimiento a la gestión del SGSI, a través de los informes que presente el oficial de seguridad de la información y los resultados de las auditorías y verificaciones que adelante la Gerencia de Auditoría Interna y la Revisoría fiscal.
Alta Dirección (Comité de Estrategia)	• Revisar la propuesta de política de Seguridad de la Información y Ciberseguridad y sus actualizaciones y proponer ajustes, mejoras o actualizaciones.

Comité de Riesgo Operacional	• Servir como instancia de apoyo de la Alta Dirección para:
	  • La revisión y aprobación del plan anual de seguridad de la información.
	  • Seguimiento al estado de implementación y mantenimiento del SGSI y adopción de medidas para su fortalecimiento.
	  • Revisión y seguimiento al perfil de riesgos de seguridad de la información.
	  • Análisis y seguimiento de incidentes de seguridad y ciberseguridad de la información y de los planes de tratamiento y medidas adoptadas.

Director de Seguridad de la Información y PCN (Oficial de Seguridad de la Información)	• Proponer el plan anual de seguridad y ciberseguridad de la información y el presupuesto requerido para la implementación y mantenimiento del SGSI. • Adelantar los análisis de riesgos en coordinación con los procesos y proponer las estrategias y medidas que permitan gestionar la seguridad de la información. • Formular la política de seguridad de la información y sus actualizaciones y generar la propuesta de los lineamientos (Manuales, procedimientos, instrumentos y formatos) que permitan el establecimiento y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información en la Entidad.

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES RESPECTO A LA SEGURIDAD DE LA INFORMACIÓN)
	• Monitorear y verificar el cumplimiento de las políticas, procedimientos y controles que se establezcan en materia de seguridad de la información y ciberseguridad y realizar la medición de indicadores para evaluar el SGSI. • Reportar a la Junta Directiva y a la Alta Dirección, los resultados de su gestión, respecto a la evaluación que haga de la confidencialidad, integridad y disponibilidad de la información, la identificación de ciberamenazas, los resultados de la evaluación de efectividad de los programas y propuestas de mejora en materia de ciberseguridad y gestión de incidentes de seguridad y ciberseguridad que afectaron la entidad.
Gerencia de Informática y Tecnología	• Implementar los controles de tipo tecnológico que ayuden a mitigar los riesgos de seguridad de la información.
Dirección de Talento Humano	• Apoyar la ejecución de los programas de sensibilización y capacitación para promover en los Funcionarios de la Sociedad Fiduciaria y los Patrimonios Administrados la toma de conciencia de sus responsabilidades en seguridad de la información, el cumplimiento de las políticas y procedimientos establecidos. • Adelantar los análisis correspondientes frente al incumplimiento por parte de los Funcionarios, respecto a la política, los lineamientos y responsabilidades del SGSI definidos y aprobados en la entidad.
Gerencia de Auditoría	• Incluir en los planes de auditoría institucionales, la verificación de la efectividad del Sistema de Gestión de Seguridad de la Información mediante la validación de cumplimiento de la política, lineamientos, procedimientos, controles y planes, acorde con los roles y responsabilidades establecidos en la presente política. • Apoyar en situaciones de posibles violaciones a las políticas de seguridad de la información.
Oficina de Comunicaciones	• Apoyar en las labores de comunicación y sensibilización en seguridad de la información, para difundir la información en todos los niveles de la entidad.
Gerencia Jurídica	• Establecer implementar las medidas de seguridad de la información en la gestión con los proveedores y contratistas de la entidad. • Procurar la protección de la seguridad de la información de todos los activos de la información que puedan verse involucrados en procesos o contratos.

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES RESPECTO A LA SEGURIDAD DE LA INFORMACIÓN)
Líderes de Proceso y Funcionarios	• Implementar las políticas y procedimientos que se definan como parte del SGSI (Por ejemplo: gestión de activos, gestión de riesgos, entre otros). • Promover la asistencia a las capacitaciones y actividades de sensibilización del SGSI que se desarrollen en la Fiduciaria y los patrimonios administrados • Reportar los incidentes de seguridad de la información y ciberseguridad y brindar apoyo en la atención e investigación de los mismos y en la formulación y ejecución de planes de tratamiento • Apoyar la identificación y clasificación de activos de información y participar en los análisis de riesgo de seguridad y ciberseguridad de la información.

5.2 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.

5.3 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:

- Revisión del cumplimiento de los siguientes indicadores definidos para el Sistema de Gestión de Seguridad de la Información:
  - Gestión de incidentes de seguridad de la información
  - Gestión de vulnerabilidades de seguridad de la información
  - Cobertura de programas de inducción y capacitación.
  - Nivel de riesgo residual de seguridad y ciberseguridad de la información.
- Revisión de avance en la implementación y/o mantenimiento del Modelo de Seguridad y Privacidad de la Información (MSPI).
- 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).

5.4 LINEAMIENTOS A NIVEL DEL TALENTO HUMANO

- Todo nuevo Funcionario o tercero debe aceptar y firmar, antes de iniciar cualquier relación con la entidad, las obligaciones y políticas a cumplir en la Fiduciaria con respecto a la seguridad de la información y Ciberseguridad.

- Todo nuevo Funcionario debe realizar la inducción de Seguridad de la información, ciberseguridad protección de datos y Plan de continuidad de negocio.

- Todo Funcionario o tercero debe encontrarse capacitado para cumplir con las políticas de seguridad de la información y ciberseguridad, de acuerdo con las funciones y responsabilidades que desempeñe.

- La entidad podrá suspender los accesos a la información de un Funcionario, en caso de que un incumplimiento a estas políticas ponga en riesgo la seguridad de la información y ciberseguridad de la entidad. La duración de la suspensión de los accesos será hasta que se evidencie que el riesgo no existe o haya sido mitigado.

- Todo Funcionario debe cumplir con el proceso disciplinario y de descargos ante algún incumplimiento de las políticas de seguridad de la información y ciberseguridad establecidas por la entidad.

- Los análisis correspondientes frente a algún incumplimiento a las politicas de seguridad de la información y ciberseguridad serán realizados por la Dirección de Gestión humana, con acompañamiento del área Gerencia Jurídica y la Dirección de Seguridad de la Información y PCN.
- Todo Funcionario, tercero o entidad que tenga relación con FIDUCOLDEX, y que vaya a terminar su relación con la entidad, debe comunicar y delegar oportunamente, sus responsabilidades sobre seguridad de la información y ciberseguridad. De manera que siempre exista un dueño o propietario de la información o activo de información.

- La culminación de las labores o la relación contractual con FIDUCOLDEX implica el retiro de los derechos de acceso a la información o activos de información.

  Por ello, es deber del Funcionario, informar oportunamente a la Dirección de Seguridad de la Información y PCN de FIDUCOLDEX y a las áreas pertinentes el término de la relación con la Entidad. A su vez los terceros o entidades que tenga relación contractual con la entidad deberán gestionar con el supervisor del contrato para que este adelante lo correspondiente

- En caso de que el Funcionario, tercero o empresa, cambie de posición, roles o funciones, los derechos de acceso a la información o activos de información deben ser revisados por la Dirección de Seguridad de la Información y PCN para que sean retirados o modificados.

- Todos los Funcionarios que administran, leen, modifican o generen información en FIDUCOLDEX deben firmar un acuerdo de confidencialidad o de no divulgación como parte de sus términos y condiciones iníciales de empleo. Esta directriz también aplica al personal temporal y a los usuarios externos y proveedores no contemplados en un contrato de trabajo.

5.5 POLITICAS ESPECIFICAS

A continuación, se presenta el alcance de las políticas específica de seguridad de la información y ciberseguridad que complementan la Política General:

Política de navegación en internet

- Establece los perfiles de navegación de Internet.
- Crea filtros de navegación que permita tener control sobre páginas maliciosas y que de esta manera los Funcionarios, terceros y empresas que tienen vinculo contractual con FIDUCOLDEX o los Patrimonios Administrados, no les permita ingresar.

- Crea grupos de navegación que permitan a los Funcionarios, terceros y empresas con vinculo contractual con FIDUCOLDEX ejercer sus labores y se conecten únicamente a las páginas que están autorizados.

Política de tratamiento y manejo de datos personales.

- Establece los lineamientos para el manejo y tratamiento de los datos personales de acuerdo con la ley 1581 de 2012 de la Superintendencia de Industria y Comercio (SIC).
- Indica que todo Colaborador, tercero o empresa que cuente con vinculo contractual con FIDUCOLDEX, es responsable de proteger los datos personales y respetar cada uno de los principios de protección de los mismos establecidos por la legislación local y la política de seguridad de datos personales de la entidad.

Política de Control de Acceso

- Se deben identificar los privilegios asociados a sistemas operativos, bases de datos, aplicaciones, servicios de red y cualquier otro componente tecnológico, para lo cual la Dirección de Seguridad de la Información deberá consolidar una matriz de roles y perfiles, a partir de las aprobaciones realizadas por los lideres de proceso. Esta matriz debe revisarse y actualizarse (si se requiere) como mínimo con periodicidad anual.
- Se debe garantizar que el nivel de acceso otorgado es adecuado para el propósito de la función del usuario y coherente con las necesidades de la Entidad y el alcance de los procesos.
- Se debe definir un procedimiento donde establezcan las responsabilidades en cuanto a las solicitudes de acceso por parte de los líderes de proceso, la revisión de las mismas acorde con la matriz de roles y perfiles y su ejecución.

Política del escritorio limpio y bloqueo de pantalla.

- Establece los lineamientos para proteger los documentos ubicados en los escritorios y el bloqueo de los equipos de cómputo cuando el usuario no se encuentre en su puesto de trabajo. Así mismo aquellos documentos que un usuario gestione y que sean confidenciales, deben mantenerse bajo llave.

Política de responsabilidades operacionales y control de cambios

- Establece los lineamientos para cuando se requieren hacer cambios importantes en la infraestructura tecnológica o sistemas de información que pueden afectar la continuidad de la operación.

Política de protección contra software nocivo y software autorizado

- Establece los lineamientos para evitar la descarga, instalación y propagación de software nocivo (virus y sus variantes.
- Los Funcionarios, terceros o empresas con relación contractual en la entidad, que tenga equipos informáticos de FIDUCOLDEX, solo deben hacer uso del software autorizado por la entidad.
- Estipula que la desinstalación del software del equipo informático es responsabilidad de la Gerencia de IT y se rige por el procedimiento establecido.
- La instalación de software nuevo o adicional se dará exclusivamente al usuario que por motivos laborales necesite debe ser autorizada por la Dirección de Seguridad de la Información y PCN, siempre y cuando se solicite por medio de la herramienta de gestión de servicios de IT y se justifique con VoBo por el líder de área. El nuevo software autorizado debe contar con las licencias de uso correspondientes y en caso de ser una aplicación free, esta debe ser evaluada por la Dirección de Seguridad de la Información y PCN.

Política para el buen uso del correo electrónico institucional (mensajería electrónica)

- Establece los lineamientos para el uso eficiente y seguro del correo electrónico de la entidad.
- La asignación de correo electrónico, mensajería instantánea y redes sociales se dan en función al rol desempeñado por el Funcionario y deben respetar las políticas establecidas por la entidad.
- Para la activación de redes sociales se debe justificar y aprobar desde el Líder de área, y autorizado por medio de una solicitud mediante la herramienta de gestión de servicios de IT desde la Dirección de Seguridad de la Información y PCN.
- El uso de correo electrónico, mensajería instantánea y redes sociales asignados a un Funcionario o tercero está restringido a los propósitos del negocio y las funciones que desempeñen.

Política de Gestión de Incidentes de Seguridad de la Información y Ciberseguridad.

- Los Funcionarios, terceros o empresas que tengan vinculo contractual con FIDUCOLDEX, son responsables de reportar oportunamente al Equipo de soporte de la Gerencia de IT, bajo los medios establecidos, los eventos, debilidades o amenazas relativos a la seguridad de la información y ciberseguridad.
- Todo Funcionario, tercero o empresa que tenga vinculo contractual con FIDUCOLDEX, debe proporcionar las evidencias requeridas por la Dirección de Seguridad de la Información y PCN ante la detección de un incidente que comprometa la seguridad de la información y ciberseguridad de la entidad.

- La Fiduciaria debe definir e implementar un procedimiento mediante el cual se identifiquen, reporten, gestionen y monitoreen los incidentes de seguridad de la información y ciberseguridad.

Política de gestión de vulnerabilidades, ethical hacking y parches de seguridad.

- Toda Infraestructura en FIDUCOLDEX, y que tenga servicios críticos, debe ser evaluada frente a análisis de vulnerabilidades, y por parte de la Gerencia de IT y/o el personal de tecnología o los responsables de la infraestructura de los Patrimonios Administrados, deben realizar un plan y realizar su respectiva mitigación, todo lo anterior con seguimiento por parte de la Dirección de Seguridad de la Información y PCN.
- La Gerencia de IT debe realizar la revisión de actualización de parches de seguridad, actividad que debe ser supervisada por la Dirección de Seguridad de la Información y PCN.
- Las conexiones y/o aplicaciones expuestas a internet, y que sean CORE del negocio para FIDUCOLDEX o sus Patrimonios Autónomos, deben someterse a pruebas de Ethical Hacking, y este plan de mitigación debe ser mitigado, por cada uno de los responsables de esta infraestructura.
- Todo usuario debe aceptar en sus equipos informáticos todas las actualizaciones que sean autorizadas por la Dirección de SGSI y PCN y liberadas por la Gerencia de IT.

Política de Continuidad de Negocio

- Todo Colaborador o tercero, ante cualquier evento de crisis, debe seguir cumpliendo con las políticas de seguridad de la información establecidas por la Compañía.
- Todo Colaborador que es designado para participar en tareas de continuidad de negocios es responsable de la recuperación de la operatividad y seguridad en los activos de información y del negocio y debe asistir a los entrenamientos para la ejecución de los procedimientos de recuperación y contingencia definidos.

6 DOCUMENTOS ASOCIADOS

Se enumeran los documentos que tienen relación con el documento en el que están referenciados.

- CA-GRI-001 GESTIÓN DE RIESGOS
- MA-GRI-011 GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
- MA-GRI-012 MANUAL CONTINUIDAD DEL NEGOCIO
- PL-GRI-004 ORGANIZACIÓN SEGURIDAD DE LA INFORMACIÓN
- PL-GRI-005 SEGURIDAD DEL RECURSO HUMANO

- PL-GRI-006 GESTIÓN DE LOS ACTIVOS
- PL-GRI-007 CONTROL DE ACCESO
- PL-GRI-008 CRIPTOGRAFÍA
- PL-GRI-009 SEGURIDAD DE LAS OPERACIONES
- PL-GRI-010 SEGURIDAD DE LAS COMUNICACIONES
- PL-GRI-011 RELACIONES CON LOS PROVEEDORES
- PL-GRI-012 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN
- PL-GRI-013 SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO
- PL-GRI-014 CUMPLIMIENTO
- PL-GRI-015 SEGURIDAD FÍSICA Y DEL ENTORNO
- PR-GRI-004 GESTIÓN DE INCIDENTES SEGURIDAD DE LA INFORMACION
- PR-GRI-020 PROCEDIMIENTO OPERACIÓN REMOTA EN CONTINGENCIA
- IT-GRI-001 ADMINISTRACIÓN DE USUARIOS
- IT-GRI-002 GESTIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN
- IT-GRI-005 ANÁLISIS DE IMPACTO EN EL NEGOCIO
- IT-GRI-012 ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO
- IT-GRI-013 CUMPLIMIENTO
- IT-GRI-014 REQUERIMIENTOS DE SEGURIDAD EN DESARROLLO DE SISTEMAS DE INFORMACION
- PN-GRI-001 PLAN DE CONTINUIDAD FRENTE A EVENTOS DE INTERRUPCIÓN POR NO DISPONIBILIDAD O DISPONIBILIDAD PARCIAL DE INSTALACIONES E INFRAESTRUCTURA FÍSICA
- PN-GRI-002 MANEJO DE CRISIS
- PN-GRI-003 PLAN DE CONTINUIDAD FRENTE A EVENTOS DE INTERRUPCIÓN POR EVENTO DE INTERRUPCIÓN POR NO DISPONIBILIDAD O DISPONIBILIDAD PARCIAL EN LA INFRAESTRUCTURA TECNOLOGICA Y LAS TELECOMUNICACIONES
- PN-GRI-004 CONTINUIDAD FRENTE A EVENTOS DE INTERRUPCIÓN POR NO DISPONIBILIDAD RECURSO HUMANO
- PN-GRI-005 CONTINUIDAD FRENTE A EVENTOS DE INTERRUPCIÓN POR EVENTOS DE FALLA O INTERRUPCIÓN DE LOS PROVEEDORES
- PN-GRI-006 CONTINUIDAD FRENTE A EVENTOS DE INTERRUPCIÓN POR INFORMACIÓN NO DISPONIBLE
- PN-GRI-007 CONTINUIDAD FRENTE A EVENTOS DE INTERRUPCIÓN POR DESORDEN CIVIL
- PN-GRI-008 CONTINUIDAD FRENTE A EVENTOS DE INTERRUPCIÓN POR EPIDEMIA O PANDEMIA
- FT-GRI-007 MATRIZ DE INVENTARIO Y VALORACIÓN DE ACTIVOS DE INFORMACIÓN GESTIÓN DOCUMENTAL
- FT-GRI-008 MATRIZ DE INVENTARIO Y VALORACIÓN DE OTROS ACTIVOS DE INFORMACIÓN

- FT-GRI-017 ANÁLISIS DE IMPACTO EN EL NEGOCIO BIA
- FT-GRI-019 CERTIFICACIÓN DE PERFILES
- FT-GRI-020 LLAVES Y CLAVES
- FT-GRI-023 LISTA DE VERIFICACIÓN DE CUMPLIMIENTO EN SEGURIDAD DE LA INFORMACIÓN Y CONTINUIDAD DEL NEGOCIO PARA PROPONENTES Y TERCEROS PROVEEDORES
- Norma Técnica Colombiana NTC-ISO-IEC 27002:2015: Norma técnica de seguridad. Código de practica para controles de seguridad de la información.
- Norma Técnica Colombiana NTC-ISO-IEC 27001:2013: Norma técnica de sistemas de gestión de la seguridad de la información. Requisitos.
- Norma Técnica Colombiana NTC-ISO-IEC 31000:2018: Norma técnica de gestión del riesgo. Principios directrices.

7 CONTROL DE DOCUMENTOS

NRO. VERSIÓN	FECHA	OBSERVACIONES
1	16/05/2024	Primera versión, aprobada por Junta Directiva # 461, en sesión del 16 de mayo de 2024

ELABORÓ	REVISÓ	APROBÓ
Nombre: Jeison Medina Valdez Cargo: Director Seguridad de la Información y PCN Fecha: 10/05/2024	Nombre: Mary Yazmin Vergel Cardozo Cargo: Gerente de Riesgos Fecha: 16/05/2024	Nombre: Mary Yazmin Vergel Cardozo Cargo: Gerente de Riesgos Fecha: 16/05/2024