POLÍTICA CIBERNÉTICA Y DE INFORMÁTICA

FCI ADMINISTRADORA, S.C.

TABLA DE CONTENIDO

1 SEGUIMIENTO 3

1.1 SEGUIMIENTO A LAS VERSIONES DEL DOCUMENTO 3

2 INTRODUCCIÓN 3

4 RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN 4

5 PROTECCIÓN Y TRATAMIENTO DE LOS DATOS 4

6 MEDIDAS DE SEGURIDAD DE LA INFORMACIÓN 5

7 RESPUESTAS A INCIDENTES 5

8 CONTROL DE ACCESO Y AUTENTICACIÓN 6

9 SEGURIDAD DE TERCEROS 6

10 SEGURIDAD PARA ACCESOS REMOTOS 6

11 CUMPLIMIENTO Y SEGUIMIENTO 7

12 MEDIDAS DISCIPLINARIAS 7

13 REVISIONES Y ACTUALIZACIONES 8

14 APROBACIÓN DE LA POLÍTICA 8

15 DEFINICIONES 9

1 SEGUIMIENTO

1.1 SEGUIMIENTO A LAS VERSIONES DEL DOCUMENTO

Versión del Documento	Fecha de aprobación	Modificación incluida
1.0	25/06/2025	Desarrollo y aprobación de la primera versión

2 INTRODUCCIÓN

La presente Política Cibernética y de Informática tiene como objetivo establecer los lineamientos, controles y procedimientos necesarios para garantizar la seguridad, confidencialidad, integridad y disponibilidad de la información, así como el uso adecuado de los sistemas tecnológicos y activos digitales de Fondo Capital Infraestructura (FCI). Esta política responde a la creciente necesidad de proteger los entornos digitales ante amenazas cibernéticas, accesos no autorizados, pérdida de datos y demás riesgos asociados al uso de tecnologías de la información.

FCI reconoce que los sistemas informáticos, redes, dispositivos y plataformas digitales constituyen activos estratégicos fundamentales para el cumplimiento de sus funciones y objetivos institucionales. Por ello, se reafirma el compromiso de implementar prácticas responsables, éticas y seguras en la gestión tecnológica, en línea con su visión, misión y valores: honestidad, respeto, compromiso y eficiencia.

Esta política complementa y refuerza lo establecido en el Código de Ética, conformando un marco integral de gobernanza tecnológica. Todo Colaborador tiene la responsabilidad de conocer, comprender y cumplir con las disposiciones aquí descritas, así como de reportar cualquier actividad o comportamiento que represente una posible vulnerabilidad, incidente o incumplimiento en materia de ciberseguridad.

La protección del entorno digital institucional no solo constituye un imperativo técnico y legal, sino también un compromiso ético con la confianza depositada en FCI por sus Colaboradores, Tenedores y demás partes interesadas.

3 ALCANCE

Esta política aplica a todos los Colaboradores de FCI, así como a inversionistas, proveedores, clientes, consultores tecnológicos, prestadores de servicios externos y cualquier tercero que, por la naturaleza de su relación con FCI, tenga acceso a sistemas, redes, equipos, aplicaciones o información tecnológica relacionada directa o indirectamente con FCI.

El alcance de esta política incluye tanto a FCI como Administrador de fondos de inversión, como a los activos gestionados directa o indirectamente por FCI, incluyendo vehículos de inversión, sociedades operativas y cualquier otra entidad bajo su administración o influencia, en la medida en que utilicen o interactúen con los sistemas tecnológicos de FCI o compartan infraestructura digital.

4 RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN

La gestión y supervisión de la seguridad de la información en FCI será responsabilidad directa del área corporativa de sistemas y del Director Ejecutivo de Administración de Inversiones y Finanzas, quienes deberán asegurar que esta se integre como un componente esencial en todas las actividades operativas de la organización.

El titular del área corporativa de sistemas asumirá adicionalmente el rol de Oficial de Seguridad de la Información, siendo el encargado de liderar la implementación, monitoreo y mejora continua de las políticas, lineamientos y controles relacionados con la protección de los activos informáticos y la información institucional.

Por su parte, todos los colaboradores de FCI tienen la obligación de cumplir con los procedimientos establecidos en materia de seguridad de la información y actuar de manera diligente para salvaguardar la confidencialidad, integridad y disponibilidad de los datos y sistemas bajo su responsabilidad.

5 PROTECCIÓN Y TRATAMIENTO DE LOS DATOS

FCI establecerá lineamientos claros para la protección y tratamiento adecuado de los datos, con base en su clasificación, sensibilidad e importancia para la organización. Los datos serán categorizados en distintos niveles de sensibilidad, y los titulares de la información deberán aplicar las medidas de seguridad correspondientes a cada categoría, asegurando su manejo adecuado y conforme a las políticas institucionales.

El acceso a datos y sistemas sensibles estará restringido exclusivamente al personal autorizado, y los permisos serán revisados y ajustados de forma periódica para mantener un control actualizado y minimizar riesgos de acceso no autorizado.

Para garantizar la confidencialidad e integridad de la información, los datos clasificados como confidenciales serán cifrados tanto en tránsito como en almacenamiento, utilizando protocolos criptográficos reconocidos por la industria.

Asimismo, se establecerán procedimientos específicos para la eliminación segura de datos confidenciales, lo que incluirá la destrucción adecuada de soportes físicos y electrónicos, a fin de prevenir su recuperación o uso indebido.

6 MEDIDAS DE SEGURIDAD DE LA INFORMACIÓN

Con el objetivo de proteger la integridad, confidencialidad y disponibilidad de la información, FCI implementará un conjunto de medidas técnicas y organizacionales orientadas a la prevención, detección y respuesta ante incidentes de seguridad.

Se utilizarán firewalls y sistemas de detección de intrusiones (IDS) para monitorear el tráfico de red y prevenir accesos no autorizados o actividades maliciosas.

Adicionalmente, se desplegarán soluciones antimalware actualizadas que permitan detectar, bloquear y eliminar software malicioso en los equipos y sistemas institucionales.

Como parte de una estrategia de defensa proactiva, todos los sistemas operativos, aplicaciones y demás componentes de software serán actualizados de forma periódica, con el fin de corregir vulnerabilidades y fortalecer la postura de seguridad de la infraestructura tecnológica.

Finalmente, se impartirá capacitación continua a empleados y funcionarios sobre prácticas seguras de manejo de la información, enfocándose en la identificación de amenazas comunes como ataques de phishing, ingeniería social y otras tácticas utilizadas para comprometer la seguridad organizacional.

7 RESPUESTAS A INCIDENTES

FCI establecerá un enfoque estructurado y ágil para la gestión de incidentes de seguridad de la información, con el fin de minimizar su impacto y restablecer la operación normal en el menor tiempo posible.

Todos los incidentes de seguridad, incluyendo infracciones, accesos no autorizados, pérdida de datos o cualquier actividad sospechosa, deberán ser reportados de forma inmediata a los Directores Ejecutivos y al Oficial de Seguridad de la Información, quienes coordinarán las acciones de respuesta correspondientes.

Además, FCI contará con un Plan de Recuperación ante Desastres (DRP, por sus siglas en inglés), el cual definirá los procedimientos específicos para la contención, análisis, mitigación y recuperación frente a incidentes cibernéticos.

Este plan será revisado y actualizado periódicamente para garantizar su efectividad, y será probado mediante simulacros que permitan evaluar la preparación del personal y la capacidad de respuesta ante distintos escenarios de riesgo.

8 CONTROL DE ACCESO Y AUTENTICACIÓN

Para proteger los sistemas y la información institucional, FCI implementará controles estrictos de acceso y mecanismos de autenticación robustos.

Todos los empleados y funcionarios deberán utilizar contraseñas seguras, únicas y complejas para cada sistema al que accedan, y estas deberán ser actualizadas de manera periódica conforme a las políticas internas de seguridad.

Con el fin de fortalecer aún más la protección del acceso a sistemas críticos, se adoptará la autenticación multifactorial (AMF), la cual requerirá al menos dos métodos de verificación independientes (como contraseñas, tokens o datos biométricos) antes de permitir el ingreso.

Estas medidas buscan reducir significativamente el riesgo de accesos no autorizados y garantizar que solo personal debidamente autorizado pueda interactuar con la información y los recursos tecnológicos de FCI.

9 SEGURIDAD DE TERCEROS

Se reconoce la importancia de garantizar que los terceros con acceso a su información cumplan con los mismos estándares de seguridad exigidos internamente. Por ello, todos los proveedores externos que procesen, almacenen o tengan acceso a datos del Administrador serán objeto de una evaluación previa a su contratación, con el fin de verificar la solidez de sus controles de seguridad y su alineación con los lineamientos establecidos en la presente Política. Esta evaluación incluirá, entre otros aspectos, la revisión de sus políticas de Cibernética y de Informática, certificaciones relevantes y prácticas de gestión de riesgos.

10 SEGURIDAD PARA ACCESOS REMOTOS

FCI establecerá medidas específicas para garantizar que el acceso remoto a sus sistemas y datos se realice de manera segura, minimizando los riesgos asociados a conexiones externas.

Todo acceso remoto deberá realizarse a través de canales protegidos, utilizando redes privadas virtuales (VPN) u otros mecanismos equivalentes que aseguren la confidencialidad y la integridad de la información transmitida.

Además, los dispositivos utilizados para acceder remotamente —ya sean institucionales o personales autorizados— deberán cumplir con los estándares de seguridad definidos por FCI, incluyendo la instalación de software actualizado, soluciones antimalware y configuraciones de seguridad adecuadas.

Estos dispositivos estarán sujetos a controles periódicos para verificar su conformidad y garantizar que no representen una vulnerabilidad para la infraestructura tecnológica del Administrador.

11 CUMPLIMIENTO Y SEGUIMIENTO

FCI adoptará un enfoque proactivo para asegurar el cumplimiento de la presente Política de Cibernética y de Informática, mediante la ejecución regular de evaluaciones de seguridad, auditorías internas y controles de cumplimiento.

Estas actividades se realizarán al menos una vez al año, con el propósito de identificar posibles brechas, verificar la efectividad de las medidas implementadas y asegurar la alineación con las mejores prácticas del sector.

Asimismo, se mantendrán registros actualizados de las acciones de capacitación en seguridad de la información, incluyendo el porcentaje de empleados capacitados anualmente.

Este seguimiento permitirá medir la cobertura y efectividad de las actividades formativas, asegurando que todo el personal esté debidamente informado y comprometido con el cumplimiento de esta Política.

12 MEDIDAS DISCIPLINARIAS

Los Colaboradores que violen los Principios del Manejo de Información Confidencial estarán sujetos a las sanciones y/o medidas disciplinarias que el Comité de Ética dicte.

De manera enunciativa más no limitativa, y dependiendo de la gravedad de la falta cometida, el Comité de Ética podrá aplicar una o más de las siguientes sanciones:

(i) Amonestación por escrito.

(ii) Amonestación económica o pecuniaria.

(iii) Revocación de nombramiento.

(iv) Rescisión del contrato de trabajo.

(v) Denuncia de hechos ante las autoridades competentes.

13 REVISIONES Y ACTUALIZACIONES

Esta Política será revisada anualmente y actualizada cuando sea necesario para asegurar su alineación con los cambios en las normativas y regulaciones en materia de ciberseguridad, las mejores prácticas en tecnología informática, y la evolución de los riesgos asociados con amenazas cibernéticas y vulnerabilidades tecnológicas.

El área de Administración de Inversiones y Finanzas, en conjunto con el titular del área corporativa de sistemas, serán los encargados de liderar el proceso de revisión, formulando propuestas de ajuste que deberán ser aprobadas por el Vicepresidente Corporativo o el órgano que corresponda, conforme a los procedimientos internos establecidos.

Toda modificación significativa a esta política será comunicada oportunamente a los colaboradores, acompañada de la capacitación necesaria para asegurar su adecuada implementación.

14 APROBACIÓN DE LA POLÍTICA

Esta política ha sido revisada y aprobada por las direcciones ejecutivas, garantizando su conformidad con los lineamientos institucionales y su alineación con los objetivos estratégicos de la organización. La aprobación entra en vigor a partir de la fecha indicada a continuación y permanecerá vigente hasta que se emita una revisión o actualización formal.

Revisado por	Fecha de Actualización	Nombre y Firma
Director de Administración de Inversiones y Finanzas	Junio 2025	Elías Antonio Amione Gorches
Director de Inversiones	Junio 2025	José Antonio Estrada Pérez

15 DEFINICIONES

Administrador: FCI Administradora, S.C, actuando en su carácter de administrador conforme al Contrato de Administración y al Contrato de Fideicomiso, o cualquier otra Persona que sustituya a dicho Administrador en términos del Contrato de Fideicomiso y del Contrato de Administración.

Buzón de Ética: Canal para la transmisión de denuncias hechas, ya sea como sospechas o como hechos comprobables.

Código/Código de Ética: El presente documento Política de Integridad, Código de Ética y Manejo de Conflictos de Interés de FCI.

Colaborador/Colaboradores: Toda persona que trabaje directa o indirectamente de manera sustantiva para FCI o, que tenga voz y voto en cualquier órgano de gobierno de FCI.

Comité/Comité de Ética: Órgano colegiado de carácter consultivo para la atención y seguimiento del cumplimiento de la normatividad y los aspectos éticos y de conflictos de interés, así como de la sanción a faltas o violaciones a lo preceptuado por el presente Código, la demás normatividad aplicable (interna o externa) y el marco legal.

FCI: FCI Administradora, S.C., entidad responsable de la administración del Fondo y del Fideicomiso, conforme a los términos y condiciones del contrato respectivo.

Fideicomiso: Significa el Contrato de Fideicomiso Irrevocable número F/2504 de fecha 28 de julio de 2016, celebrado entre FCI Administradora, S.C. como administrador, Estrategia en Finanzas & Infraestructura, S.A. de C.V., como asesor, Banco Invex, S.A. Institución de Banca Múltiple, Invex Grupo Financiero, como fiduciario y Monex Casa de Bolsa, S.A. de C.V., Monex Grupo Financiero, como representante común de los Tenedores, según el mismo sea modificado, total o parcialmente, adicionado, renovado o de cualquier otra forma reformado en cualquier momento.

Información Confidencial: Cualquier dato, documento, conocimiento o comunicación, en cualquier formato (ya sea verbal, escrito, digital, etc.), relacionado con las actividades, operaciones, estrategias comerciales, financieros o técnicos de FCI, que no sea de dominio público.

Información Privilegiada: Toda aquella información que por restricción presuponga una ventaja para la toma de decisiones que pudiera derivar en una ganancia patrimonial indebida para beneficio propio o para un tercero, o una afectación al patrimonio de un tercero.

Política: Hace referencia a la Política Cibernética y de Informática.

Tenedor: Significa cada titular de los certificados bursátiles fiduciarios de desarrollo, sin expresión de valor nominal, no amortizables que sean emitidos por el Fiduciario de conformidad con los términos del Contrato de Fideicomiso, el Acta de Emisión, los Títulos, y las disposiciones de conformidad con la Ley Aplicable.