

**PLAN DE CONTINUIDAD DEL  
NEGOCIO (BCP) Y DE  
RECUPERACIÓN ANTE  
DESASTRES (DRP)**

**FCI ADMINISTRADORA, S.C.**

## TABLA DE CONTENIDO

<b>1</b>	<b>SEGUIMIENTO</b>	<b>3</b>
1.1	SEGUIMIENTO A LAS VERSIONES DEL DOCUMENTO	3
<b>2</b>	<b>INTRODUCCIÓN</b>	<b>3</b>
<b>3</b>	<b>OBJETIVOS DEL DOCUMENTO</b>	<b>3</b>
<b>4</b>	<b>ALCANCE</b>	<b>4</b>
<b>5</b>	<b>ESTRATEGIA DE ADMINISTRACIÓN DE RIESGOS DE CONTINUIDAD</b>	<b>4</b>
	PROCESOS CRÍTICOS	4
	RECURSOS Y DOCUMENTOS INDISPENSABLES	5
	AMENAZAS POSIBLES	5
	ANÁLISIS DE FRECUENCIA DEL RIESGO E IMPACTO AL NEGOCIO	6
	ROLES ESTABLECIDOS PARA LA ATENCIÓN DEL BCP Y DRP	7
	<b>MITIGANTES</b>	<b>9</b>
	ESTRUCTURA ORGANIZACIONAL	9
	REPLAZO/SUPLENTE PARA LAS ÁREAS QUE REALIZAN LAS ACTIVIDADES CRÍTICAS	10
	PLAN DE RETENCIÓN DE PERSONAL CLAVE	11
	RECURSOS SUFICIENTES PARA CONTINUAR CON LA OPERACIÓN DE LA ORGANIZACIÓN	11
	FLEXIBILIDAD TECNOLÓGICA PARA OPERAR DESDE UBICACIONES REMOTAS	11
	REVISIONES DE CONTROL A EQUIPOS PORTÁTILES	12
	ALMACENAMIENTO DE DOCUMENTOS FÍSICOS EN BODEGA	12
	DIGITALIZACIÓN DE LOS DOCUMENTOS QUE ESTÁN EN FÍSICOS EN BODEGA	12
	OFICINA SEGURA	12
	CIBERSEGURIDAD, PROTECCIÓN DE INFORMACIÓN Y SISTEMAS	12
	PROTECCIÓN DE DOCUMENTOS (INFORMACIÓN) INDISPENSABLES	13
	PROTECCIÓN DE INFORMACIÓN EN LOS EQUIPOS PORTÁTILES	13
	ACCESOS RESTRINGIDOS A LOS SISTEMAS INSTITUCIONALES	13
	MONITOREO Y VIGILANCIA	13
	SERVICIOS DE TIA TRAVÉS DE UN PROVEEDOR EXTERNO	13
	<b>TIEMPOS ESTIMADOS DE RECUPERACIÓN</b>	<b>14</b>
<b>6</b>	<b>PLAN DE RECUPERACIÓN ANTE DESASTRES (DRP)</b>	<b>15</b>
<b>7</b>	<b>MEDIDAS DISCIPLINARIAS</b>	<b>16</b>
<b>8</b>	<b>REVISIONES Y ACTUALIZACIONES</b>	<b>16</b>
<b>9</b>	<b>APROBACIÓN DEL PLAN</b>	<b>17</b>
<b>10</b>	<b>DEFINICIONES</b>	<b>18</b>

## 1 SEGUIMIENTO

### 1.1 SEGUIMIENTO A LAS VERSIONES DEL DOCUMENTO

<i>Versión del Documento</i>	<b>Fecha de aprobación en Comité Ética</b>	<b>Modificación incluida</b>
<i>1.0</i>	25/06/2025	Desarrollo y aprobación de la primera versión

## 2 INTRODUCCIÓN

Con el incremento de las amenazas externas e internas, diversas organizaciones han comenzado a implementar planes, procedimientos y estructuras que garanticen la continuidad de los procesos críticos para el negocio. En este contexto, Fondo Capital Infraestructura (FCI) ha desarrollado el presente Plan para establecer mecanismos para gestionar los riesgos a la continuidad operativa y poder mantener el cumplimiento del Fideicomiso y del Contrato de Administración existente.

FCI además determina, a través del presente documento, la manera en que va a priorizar las actividades en diversos escenarios de disminución parcial o total de su operación. Lo anterior, para definir las actividades y los roles que deben atender los Colaboradores ante una eventualidad de ese tipo y reducir el tiempo de respuesta para restablecer la normalidad.

Para constituir este documento se tomaron en consideración los requisitos establecidos en la norma internacional ISO 22301 Sistemas de Gestión de la Continuidad del Negocio.

## 3 OBJETIVOS DEL DOCUMENTO

Las finalidades principales del documento son establecer:

- (1) El marco de actuación a seguir para mitigar los riesgos de continuidad y sostener la operación de los procesos críticos;
- (2) Los procedimientos para restaurar la operación a su normalidad después de una interrupción parcial o total; y
- (3) El compromiso de capacitar periódicamente a los Colaboradores en procedimientos de emergencia y de operación alternativa y de revisarlos para una restauración fluida y rápida de los servicios.

#### **4 ALCANCE**

Los criterios, estrategias, procedimientos y demás información aquí descrita es de observancia obligatoria para todo los Colaboradores; principalmente, para aquellas personas en las que recaen los procesos críticos y que tienen asignados roles, responsabilidades y facultades especificados en el presente documento.

Los Directores Ejecutivos muestran su compromiso con la continuidad de negocios al establecer este documento y garantizar su respaldo directivo y financiero para promover la mejora continua de las operaciones de FCI. Asimismo, el alcance de este plan incluye tanto a FCI como Administrador de fondos de inversión, como a los activos gestionados directa o indirectamente por FCI, tales como vehículos de inversión, sociedades operativas, filiales y cualquier otra entidad bajo su administración o influencia.

#### **5 ESTRATEGIA DE ADMINISTRACIÓN DE RIESGOS DE CONTINUIDAD**

El ejercicio realizado para la administración de riesgos es:

- (1) Definir los procesos críticos que deben mantenerse en operación;
- (2) Identificar los recursos y documentos necesarios para la operación de dichos procesos;
- (3) Visualizar las Amenazas que podrían afectar a los recursos operativos;
- (4) Reconocer cuáles de éstas tienen tanto frecuencias como impactos relevantes sobre los procesos críticos;
- (5) Enumerar los controles que tiene FCI para mitigarlos, al reducir las frecuencias de las fallas y/o su impacto; y
- (6) Identificar los tiempos requeridos para restaurar y verificar los recursos necesarios para operar.

##### **Procesos críticos**

Para FCI, los procesos considerados como críticos son:

1. Originación y promoción de las inversiones
2. Proceso de disposición y/o aportación
3. Seguimiento a inversiones
4. Pagos
5. Compras
6. Contratación de asesores
7. Reportes

Los procesos críticos son ejecutados, fundamentalmente, por los Colaboradores adscritos a la Dirección Ejecutiva de Administración de Inversiones y Finanzas y a la Dirección Ejecutiva de Inversiones.

## Recursos y documentos indispensables

Los recursos indispensables para la operación de los procesos críticos son:

1. Recursos Humanos: Personal capacitado
2. Información: La requerida para operar
3. Recursos Tecnológicos: tecnología para comunicación, almacenamiento, computadoras, teléfonos, etc.
4. Infraestructura: oficinas y almacén
5. Proveedores: el soporte externo requerido

Los documentos (información) indispensables para la operación de los procesos críticos son, entre otros:

1. Archivos y bases de datos: de seguimiento, de gestión financiera y presentaciones a diversos órganos colegiados.
2. Autorizaciones y confirmaciones de todas las transacciones financieras
3. Comprobantes y facturas de todo tipo de pagos y transferencias
4. Contratos: con Inversionistas, empresas promovidas y proveedores de servicios
5. Documentación de la relación con proveedores (cotizaciones, alta y decisión de compra).
6. Instrucciones realizadas al Fideicomiso o de cualquier pago con soportes.
7. Opiniones y acuerdos de órganos colegiados: Comité de Inversiones y otros comités y grupos de trabajo internos de FCI, así como los del Fideicomiso.
8. Reportes y entregables de evaluaciones: de Due Diligence y de asesores en general.
9. Revisiones y aprobaciones de contratos y montos
10. Solicitudes de disposiciones: con soportes (facturas, pagarés y/o reconocimiento de adeudos y opiniones de especialistas), así como de disposición y reconocimiento de adeudo

## Amenazas posibles

Los recursos indispensables para la operación de los procesos críticos están sujetos a diversas amenazas y que, en caso de materializarse, pueden afectar la disponibilidad y/o operación de éstos.

<b>Recurso indispensable</b>	<b>Amenazas</b>
Recursos Humanos	Pérdida de personal: Rotación, despido, incapacidad por enfermedad o accidente
Información	Indisponibilidad por pérdida, extravío o robo de información, ya sea física o digital
Recursos Tecnológicos	Falla o falta de disponibilidad de los activos o recursos tecnológicos: ciberataques, intermitencias o fallas, y pérdida o robo
Infraestructura	Imposibilidad de acceder a las instalaciones por eventos naturales, pandemias o inseguridad
Proveedores	Pérdida de proveedores por incumplimiento de contrato

### Análisis de frecuencia del riesgo e impacto al negocio

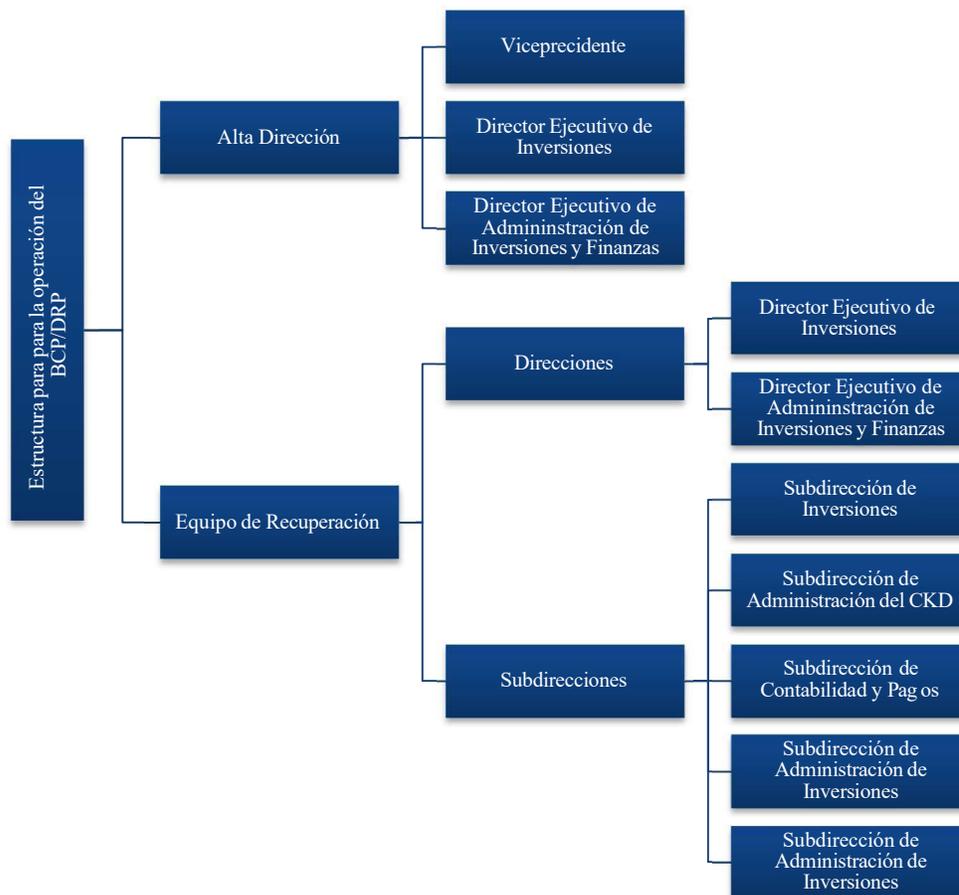
Para cada uno de los procesos críticos, se visualiza la magnitud de pérdida por falta de continuidad, tomando en consideración la frecuencia del riesgo y su impacto financiero y reputacional.

Procesos	Riesgos asociados	Frecuencia	Impacto al Negocio	
			Financiero	Reputacional
1. Seguimiento de las inversiones	Falla o falta de disponibilidad de los recursos tecnológicos	Alto		
	Pérdida o robo de información	Medio	Alto	Alto
	Pérdida de personal Falta de oficina / almacén	Bajo		
2. Originación y promoción de las inversiones	Falla o falta de disponibilidad de los recursos tecnológicos	Alto		
	Pérdida o robo de información		Alto	Alto
	Pérdida de proveedores	Bajo		
	Pérdida de personal Falta de oficina / almacén			
3. Proceso de disposición y/o aportación	Falla o falta de disponibilidad de los recursos tecnológicos	Alto		
	Pérdida o robo de información	Medio	Alto	Alto
	Pérdida de personal Falta de oficina / almacén	Bajo		
4. Pagos	Falla o falta de disponibilidad de los recursos tecnológicos	Alto	Alto	Medio

	Pérdida o robo de información	Medio		
	Pérdida de personal	Bajo		
	Falta de oficina / almacén			
<b>5. Compras</b>	Falla o falta de disponibilidad de los recursos tecnológicos	Alto		
	Pérdida o robo de información	Medio		
	Pérdida de proveedores		Bajo	Medio
	Pérdida de personal	Bajo		
	Falta de oficina / almacén			
<b>6. Contratación y pago de asesores</b>	Falla o falta de disponibilidad de los recursos tecnológicos	Alto		
	Pérdida o robo de información	Medio	Bajo	Alto
	Pérdida de personal	Bajo		
	Falta de oficina / almacén			

### **Roles establecidos para la atención del BCP Y DRP**

Respecto a la toma de decisiones y seguimiento a las actividades del BCP y DRP se establecen los siguientes roles:



La Alta Dirección es el más alto nivel de toma de decisiones de FCI, su función principal es decidir sobre las acciones a tomar durante y después de un escenario de no disponibilidad.

En caso de que se interrumpa parcial o totalmente la operación, los Directores Ejecutivos deberán tomar las decisiones sobre la aplicación de las diferentes estrategias a ejecutar acompañados por el Vicepresidente Corporativo.

A su vez, se establece como miembros del Equipo de Recuperación ante Desastres a las siguientes personas que serán responsables de coordinar las actividades en FCI:

### Equipo de Recuperación de Desastres

Área	Persona designada
Director Ejecutivo de Inversiones	José Antonio Estrada Pérez
Director Ejecutivo de Administración de Inversiones y Finanzas	Elías Antonio Amione Gorchés
Subdirector de Administración Fiduciaria del CKD	América Florián González Ayala
Subdirector Junior de Inversiones	Alejandro Guerrero

A continuación, un desglose de los roles y responsabilidades establecidos:

<b>Rol</b>	<b>Responsabilidad durante el desastre</b>	<b>Responsabilidad después del desastre</b>
<b>Equipo de Recuperación ante Desastres.</b>	<p>Coordinar las actividades del DRP.</p> <p>Dar inicio a las actividades de las estrategias operativas del DRP y coordinar la comunicación con los integrantes de FCI para garantizar su seguridad y la continuidad de las operaciones.</p> <p>Coordinar con los proveedores de tecnología e infraestructura, la recuperación y funcionamiento de los sistemas o infraestructura de la organización.</p>	<p>Coordinar las actividades necesarias para el restablecimiento de las operaciones y, en su caso, realizar adecuaciones o mejoras al BCP y DRP.</p> <p>Mantener, restaurar y garantizar la operación de los sistemas de la organización, a través de los proveedores de cada servicio requerido para la operación.</p> <p>Atender las incidencias que surjan en la operación diaria.</p> <p>Reportar el estado de los respaldos de cada área.</p>
<b>Alta Dirección</b>	<p>Persona o grupo de personas que decide las estrategias operativas a seguir durante un escenario de no disponibilidad.</p>	<p>Asegurar que los sistemas y procesos funcionen correctamente dentro de la organización.</p> <p>Comunicar cualquier tema necesario con los integrantes del equipo, Inversionistas y proveedores.</p>
<b>Responsables de cada área</b>	<p>Los responsables de las áreas deberán atender las indicaciones del Equipo de Recuperación ante Desastres sobre la implementación de las actividades de las estrategias operativas y, en su caso, comunicar cualquier eventualidad adicional.</p>	<p>Coordinar las actividades respectivas para que los integrantes de FCI puedan restaurar y/o recuperar sus actividades de forma segura y eficiente.</p>

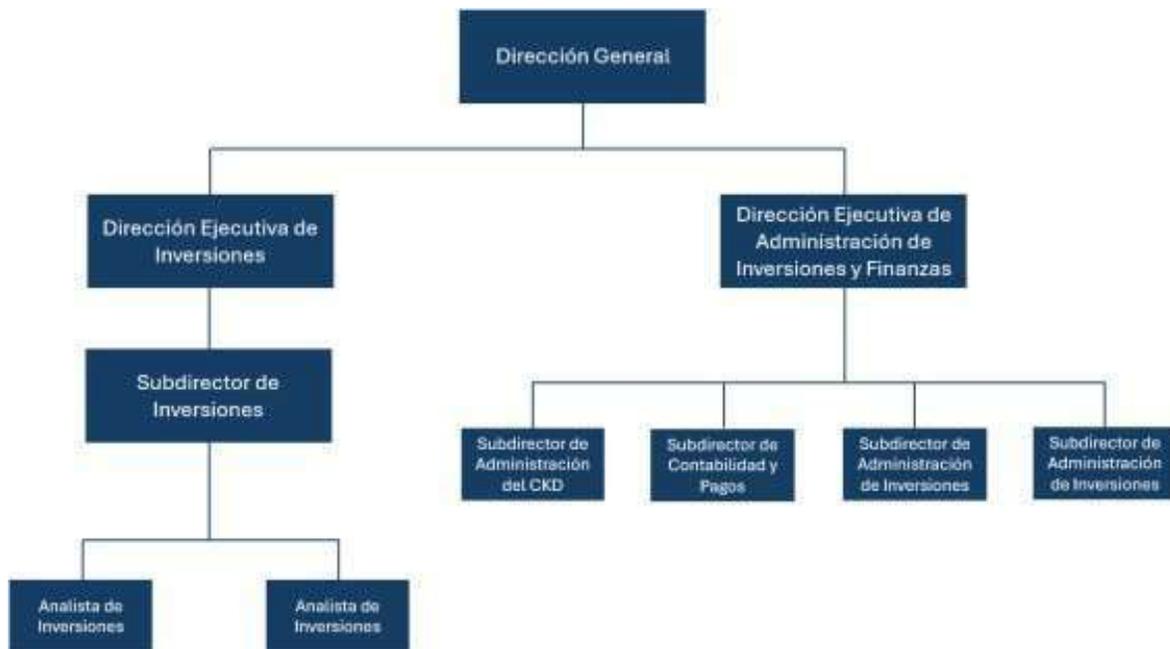
## Mitigantes

### Estructura Organizacional

El Administrador cuenta con distintas áreas en su estructura con puestos y responsabilidades definidas que permiten la continuidad de los procesos críticos. Además, se busca que no sea una única persona quien tenga el conocimiento absoluto sobre una actividad, sino que este conocimiento sea compartido entre varios integrantes del equipo.

De esta manera, en caso de ausencias, las actividades de un puesto no quedan pausadas, sino que pueden retomarse por algún otro miembro del equipo y el desempeño de la operación no se vea afectado de manera significativa.

**Estructura del Administrador**



**Remplazo/suplente para las áreas que realizan las actividades críticas**

Las áreas de FCI que ejecutan procesos críticos cuentan con un responsable clave y uno o varios suplentes por cada responsable clave, todos ellos con experiencia y conocimiento para mantener la operación.

RESPONSABLE	PUESTO	REEMPLAZO /SUPLENTE
Alberto Bitar Hank	Vicepresidenste	1. José Antonio Estrada 2. Elías Antonio Amione Gorches
José Antonio Estrada	Director Ejecutivo de Inversiones	1. Alejandro Guerrero
Elías Antonio Amione Gorches	Director Ejecutivo de Administración de Inversiones y Finanzas	1. América Florián González Ayala

En el caso de ausencia del Director General y/o Vicepresidente Corporativo uno de los Directores Ejecutivos actúa como suplente y realiza reuniones con el resto de los Directores Ejecutivos de forma semanal para tomar decisiones. En los casos de ausencia de uno de los Directores Ejecutivos de Inversiones o de Administración de Inversiones y Finanzas el Vicepresidente Corporativo actúa como reemplazo de inmediato y éste realiza reuniones semanales con el equipo que quedó sin Director Ejecutivo.

En cualquiera de los casos, la suplencia se anuncia a todos los Colaboradores de manera inmediata para mantener la operación de manera continua.

### **Plan de retención de personal clave**

FCI ha adoptado una política de *Bonos anuales* que busca recompensar el desempeño de sus colaboradores, así como el cumplimiento de la normatividad y las políticas internas. La filosofía de FCI en este tema *se fundamenta en la idea de que la remuneración de los miembros de su equipo debe estar alineada con los intereses de nuestros Inversionistas, por lo que se vincula la remuneración con el desempeño de FCI*. En este sentido, el personal de FCI recibe un salario mensual, con prestaciones establecidas en la Ley Federal del Trabajo y, en su caso, un bono anual por desempeño.

### **Recursos suficientes para continuar con la operación de la organización**

El Vicepresidente Corporativo tiene la capacidad de aprobar los gastos necesarios para implementar las alternativas y medidas de remediación que aporten a la continuidad del negocio. La Administradora tiene fondos suficientes en sus activos líquidos y capacidad de acceder a fondos adicionales en caso de que sus activos líquidos sean insuficientes. Adicionalmente, se cuentan con seguros para proteger a FCI de gastos legales y responsabilidades de sus funcionarios.

### **Flexibilidad tecnológica para operar desde ubicaciones remotas**

FCI cuenta con un esquema de funcionalidad que reduce los eventos de discontinuidad de negocio. Actualmente tiene la capacidad de operar de forma remota gracias a una combinación de los siguientes elementos de equipamiento de cómputo portátil, almacenamiento en servidores con respaldo y comunicaciones ágiles vía telefonía celular. En particular:

1. Todo el personal cuenta con equipos portátiles para trabajar de manera indistinta desde la oficina o desde casa o desde cualquier otra ubicación que les permita la continuidad de sus actividades.
2. La información de los usuarios se guarda en un servidor en la nube, hay una conexión vía VPN (OpenVPN) entre los equipos y este servidor.
3. La información de trabajo en las computadoras portátiles se respalda de manera periódica por un contrato de servicio con un proveedor de servicios de TI.
4. La comunicación de trabajo se realiza a través de correo electrónico institucional al cual todos los empleados tienen acceso en equipos portátiles y en sus equipos de telefonía celular.
5. La comunicación vía voz entre los empleados se realiza a través de telefonía fija y un servicio de conmutador de telefonía fija con extensiones por persona, que se enlaza con los números celulares.
6. La comunicación vía mensajes se realiza a través de herramientas como WhatsApp por medio de las cuales el personal puede contactar y gestionar chats con las diferentes partes interesadas del FCI.

7. Las reuniones entre varias personas se realizan con herramientas como Zoom.

El uso conjunto de todo lo anterior permite que la comunicación remota y constante del equipo sea eficiente, inmediata y transparente.

### **Revisiones de control a equipos portátiles**

Todos los equipos de cómputo, institucionales y personales que se usen para realizar el trabajo se someten a la revisión y control de accesos que el proveedor de servicios de tecnología establezca, para asegurar seguridad de accesos y protección a virus, así como la confidencialidad y seguridad de la información. Dichas revisiones mantienen actualizados los aplicativos para evitar ataques de virus.

### **Almacenamiento de documentos físicos en bodega**

Se cuenta con un espacio de almacenamiento (bodega) donde se realiza el resguardo de la documentación física de manera periódica. El acceso a la bodega es controlado.

### **Digitalización de los documentos que están en físicos en bodega**

Cada área se encarga de digitalizar y resguardar en el servidor con acceso FortiClient todos sus documentos de forma previa a enviar los a su resguardo correspondiente.

### **Oficina segura**

El mantenimiento de la infraestructura de FCI (instalaciones) se encuentra a cargo de un equipo dedicado del edificio en dónde se encuentran las oficinas de FCI, quien revisa, mantiene y mejora las instalaciones.

La oficina cumple con todos los requerimientos estipulados por Protección Civil (Programa de Protección Civil) y, en su momento, en el caso de la pandemia por COVID - 19 con los requerimientos estipulados por la Secretaría de Salud.

Parte de la seguridad física ofrecida por las instalaciones (oficina) consta de los siguientes mecanismos de monitoreo:

- Vigilancia 24/7 por parte del edificio,
- Acceso de visitantes o proveedores a las instalaciones es previa autorización,
- Acceso a las instalaciones a través de la recepción del edificio,
- Acceso del personal a través de la asignación de tarjetas de radio frecuencia,

### **Ciberseguridad, protección de información y sistemas**

FCI ha definido los lineamientos, procedimientos y responsabilidades que permiten dar soporte tecnológico oportuno a las operaciones en caso de ocurrencia de un evento de riesgo tecnológico y poder restablecer los procesos críticos en el menor tiempo y costo posible.

### **Protección de documentos (información) indispensables**

FCI cuenta con un servidor con acceso FortiClient para almacenar los documentos (información) indispensables y tiene la política de respaldarlo de forma diaria en el servicio de One Drive. Con lo anterior se protege la información ante cualquier eventualidad.

Cada Colaborador cuenta con una guía rápida para acceder a la base de datos con la información necesaria para que pueda tener los documentos (información) indispensables para la operación de los procesos críticos.

Los documentos (información) indispensables para la operación de los procesos críticos están digitalizados, una copia física en resguardo del Director Ejecutivo de Administración de Inversiones y Finanzas y otra en la Bodega.

### **Protección de información en los equipos portátiles**

Adicionalmente, para asegurar la disponibilidad de la información contenida en los equipos cómputo portátiles se realizan respaldos periódicos e incrementales en el servidor, en el servicio de One Drive o en el NAS.

### **Accesos restringidos a los sistemas institucionales**

Todos los sistemas de operación para la administración y acceso de forma remota cuentan con candados de seguridad y, en su caso, se solicita la activación de la autenticación en dos pasos.

### **Monitoreo y vigilancia**

El monitoreo y vigilancia de los recursos tecnológicos como los equipos de cómputo, teléfonos móviles, infraestructura de redes o servicios propiedad de FCI cuentan con lo siguiente:

- ESET Antivirus Internet Security, activado en los equipos propiedad de FCI,
- Mantenimiento de equipos de cómputo y servidores (Calendarización de mantenimiento preventivo),
- Acceso a las cámaras de seguridad de las oficinas (a través de proveedor de oficina),
- Actualización de inventario de licencias (Administrado por el área corporativa de servicios informáticos),
- Actualización de inventario de equipos de cómputo y teléfonos móviles (Administrado por el área corporativa de servicios informáticos),
- Actualización de inventario de credenciales asignadas a cada colaborador (Administrado por el área corporativa de servicios informáticos),
- Servicio de soporte tecnológico a través del área corporativa de servicios informáticos (sistema de tickets y reportes de servicios correctivos)

### **Servicios de TI a través de un proveedor externo**

Todos los recursos tecnológicos son monitoreados a través del área corporativa de servicios informáticos quienes dan soporte y mantenimiento a los recursos de la organización y realiza recomendaciones a los controles de seguridad existentes. El servicio tiene un alcance global y mantiene la atención de usuarios de forma remota y, en su caso, incluye el mantenimiento y soporte presencial donde FCI le indique.

De igual forma se encarga de la revisión de controles y mecanismos adicionales para la protección y mantenimiento de los servidores o equipos que se encuentren en las instalaciones de la organización.

Las actividades desempeñadas por el área corporativa de servicios informáticos incluyen el soporte en caso de un ataque cibernético, realizando la identificación, reporte, remediación y monitoreo de Amenazas y, en su caso, recuperación del incidente. De forma adicional y bajo una calendarización el proveedor apoya a FCI con el envío de información relevante en materia de seguridad informática.

### **Tiempos estimados de recuperación**

Considerando los mitigantes y controles que se han puesto en práctica, los siguientes son los tiempos en los cuales se estima se restaura la operación normal ante la materialización de una amenaza.

<b>Recursos de FCI asociados al escenario</b>	<b>Escenarios de no operabilidad</b>	<b>Tiempo de restauración ante la materialización del escenario</b>
<b>Recursos Tecnológicos</b>	1.-Falla o Falta de disponibilidad en los Recursos Tecnológicos de comunicación.	34 horas
	2.-Falla o Falta de disponibilidad de los Recursos Tecnológicos para el desarrollo de información.	34 horas
	3.-Perdida, Extravío o Robo de Recursos Tecnológicos Físicos para el desarrollo/procesamiento de información crítica de FCI.	34 horas
	4.-Falla en los Recursos Tecnológicos de gestión interna.	34 horas
	5.-Falla o Falta de disponibilidad de los en los Recursos Tecnológicos de resguardo de documentos.	34 horas
<b>Recursos Humanos</b>	6.-Falta de Personal con capacitación especializada.	6 semanas
	7.-Falta de Personal clave por enfermedad.	6 semanas
	8.-Falta de Personal clave por rotación.	6 semanas
	9.-Falta de Personal clave por accidentes o por contingencias ambientales, sociales o sanitarias.	5 semanas
<b>Infraestructura</b>	10.-Falla de los Recursos de resguardo de información física y atención personal.	1 semana y 10 horas
	11.-Desastre físico en las oficinas principales de FCI.	3 semanas
<b>Proveedores</b>	12.-Falla o Falta de disponibilidad de los Proveedores de servicios tecnológicos.	4 semanas

	13.-Falla o Falta de disponibilidad del Proveedor de las instalaciones (oficina).	4 semanas
<b>Información</b>	14.-Perdida, Extravío o Robo de información (Física y Digital) crítica de las operaciones.	58 horas

## 6 PLAN DE RECUPERACIÓN ANTE DESASTRES (DRP)

El DRP es parte integral de este Plan e indica a todos los Colabores:

- (1) Qué hacer en caso de que se presente un escenario de desastre que impida parcial o totalmente la operación;
- (2) Quién lo hace;
- (3) Cómo se hace; y
- (4) La manera en la que se comunica lo que está sucediendo.

Las instrucciones del DRP se aplican hasta que los Directores Ejecutivos indiquen que se ha normalizado la operación.

En caso de que se materialice un escenario de desastre:

- **Todos los Colaboradores** deben notificar de inmediato el escenario que se percibe al a los Directores Ejecutivos:
  - o La notificación debe hacerse de manera inmediata y repetida, hasta obtener confirmación de que se ha recibido el mensaje.
  - o La notificación se debe hacer a través de todos los medios de comunicación que el colaborador tenga disponibles: de manera presencial, vía telefónica o mensaje de voz, vía aplicaciones de mensaje, y/o vía correo electrónico.
- **Los Directores Ejecutivos** deben analizar la información proporcionada de manera expedita para determinar el grado del desastre/evento/incidente. Con base en su deliberación deberá determinar la estrategia operativa a seguir y, en su caso, comunicar a los colaboradores las actividades a implementar a través de todos los medios de comunicación que el colaborador tenga disponibles hasta obtener confirmación de que recibió la instrucción.
- **El Equipo de Recuperación ante Desastres** será el área corporativa de servicios informáticos, quien deberá dar seguimiento a las acciones implementadas, y notificar a las partes interesadas el avance en permanente coordinación con los Directores Ejecutivos hasta que éste declare el restablecimiento normal de las operaciones.

FCI de forma anual realiza ejercicios y pruebas a los procedimientos de continuidad de negocio establecidos en el DRP y produce un reporte con los resultados, recomendaciones y acciones para implementar mejoras. Estos ejercicios pueden incluir auditorías internas para identificar el nivel de eficacia obtenido en los ejercicios de prueba y/o durante la activación ante un incidente y ejercicios de prueba a cada escenario identificado en dicho documento.

## ■ 7 MEDIDAS DISCIPLINARIAS

Los Colaboradores que violen los Principios establecidos en la siguiente política 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.

## ■ 8 REVISIONES Y ACTUALIZACIONES

Este plan será revisado anualmente y actualizado según sea necesario para asegurar su alineación con cambios en las leyes, regulaciones y mejores prácticas aplicables. Las revisiones considerarán también la evolución de los riesgos legales, regulatorios y éticos, con el fin de mantener un marco de cumplimiento robusto.

Las actualizaciones garantizarán que el plan se mantenga relevante frente a nuevos desafíos, cambios normativos y mejores prácticas en las áreas de cumplimiento legal, conducta ética y transparencia. Asimismo, se evaluarán los procedimientos internos y los mecanismos de monitoreo para asegurar su efectividad y adaptabilidad frente a las nuevas condiciones regulatorias y de mercado.

La revisión periódica buscará fortalecer la implementación del plan, asegurando que se sigan los más altos estándares de cumplimiento y se protejan los intereses de los inversionistas y demás partes interesadas.

■ **9 APROBACIÓN DEL PLAN**

Este plan ha sido revisado y aprobado por la alta dirección, 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.

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

## 10 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.

**Alta Dirección:** Grupo de funcionarios de mayor jerarquía en FCI responsables de la toma de decisiones estratégicas y del cumplimiento de los objetivos institucionales.

**Amenaza / Amenazas:** Incidente no deseado que provoca la no disponibilidad de la operación de los procesos críticos de la organización.

**BCP:** Business Continuity Plan o Plan de Continuidad de Negocio, mismo que describe cómo FCI seguirá funcionando durante una interrupción no planificada de sus actividades.

**BMV:** Bolsa Mexicana de Valores.

**CNBV:** Comisión Nacional Bancaria y de Valores.

**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 Técnico:** El comité técnico establecido de conformidad con el Artículo 80 de la LIC y conforme a los términos del Contrato de Fideicomiso.

**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.

**Contrato de Administración:** Significa el contrato de administración celebrado entre el fiduciario y el administrador, según se establece en el Contrato de Fideicomiso, según el mismo sea modificado, total o parcialmente, adicionado, renovado o de cualquier otra forma reformado en cualquier momento.

**Contrato de 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.

**DRP:** Disaster Recovery Plan o Plan de Recuperación ante Desastres, mismo que describe las estrategias operativas o instrucciones detalladas para gestionar las interrupciones, incidentes, desastres o eventos no planificados que afecten a algún activo o proceso crítico para la operación de FCI.

**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 / CKD:** 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.

**Frecuencia del Riesgo:** Es el número de veces que se espera se materialice una amenaza en un periodo de tiempo determinado.

**Impacto del Riesgo:** Es la afectación financiera o reputacional esperada en caso de que se materialice una Amenaza.

**LMV:** Ley del Mercado de Valores.

**Plan:** Es el Plan de Continuidad de Negocio y de Recuperación ante Desastres.

**Recuperación:** Actividades y tiempos en los que se realizan acciones definidas para volver a la normalidad de las operaciones.

**Recursos críticos:** Cualquier información o elemento relacionado con la operación de FCI (pudiendo ser sistemas, información, edificios, personas, etc.) que sea indispensable para su operación.

**Representante Común:** Es Monex Casa de Bolsa, S.A. de C.V., Monex Grupo Financiero en su carácter de representante común de los Tenedores.

**Restauración:** La normalidad de las operaciones.

**Riesgo:** Pérdida financiera o reputacional que resulta de una falla de procesos, personas, sistemas o causa externa.

**TI:** Tecnologías de Información.

**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.