

The background is a solid teal color. It is decorated with several white, abstract, hand-drawn style lines that form various shapes, including circles, ovals, and irregular polygons, scattered across the page.

# éxes

Procedimento de BCM -  
Continuidade de Negócios

**MARÇO DE 2025**

# Sumário

<b>SUMÁRIO</b>	<b>2</b>
<b>1) ESCOPO</b>	<b>3</b>
<b>2) NORMAS RELACIONADAS</b>	<b>3</b>
<b>3) PÚBLICO-ALVO</b>	<b>3</b>
<b>4) RESPONSABILIDADE</b>	<b>3</b>
<b>5) PREMISSAS PARA O GERENCIAMENTO DE CONTINUIDADE DE NEGÓCIOS</b>	<b>3</b>
<b>6) PRAZO PARA O RETORNO DAS ATIVIDADES</b>	<b>4</b>
<b>6.1 GESTÃO DE FII, FIDC E FUNDOS FINANCEIROS DE CRÉDITO PRIVADO</b>	<b>4</b>
<b>7) CENÁRIOS</b>	<b>4</b>
<b>7.1 IMPOSSIBILIDADE DE ACESSO AO EDIFÍCIO</b>	<b>4</b>
<b>7.2 ADICIONALMENTE, PARA FINS DAS COMUNICAÇÕES COM OS CLIENTES E PARCEIROS, ESTAS PODERÃO SER REALIZADAS POR MEIO DOS TELEFONES CELULARES PESSOAIS DOS PRÓPRIOS COLABORADORES.</b>	
<b>INDISPONIBILIDADE DE MAIS DA METADE DOS COLABORADORES</b>	<b>5</b>
<b>7.3 INDISPONIBILIDADE DE SISTEMAS, DADOS, ESTRUTURA TECNOLÓGICA E ATAQUE CIBERNÉTICO</b>	<b>5</b>
<b>8) DECLARAÇÃO DE CONTINGÊNCIA</b>	<b>5</b>
<b>9) TESTES E AVALIAÇÃO</b>	<b>6</b>
<b>10) DEVER DE REPORTE À ALTA ADMINISTRAÇÃO E AO REGULADOR</b>	<b>6</b>
<b>11) MANUTENÇÃO E PRAZO DE GUARDA</b>	<b>6</b>
<b>12) VIGÊNCIA E ATUALIZAÇÃO</b>	<b>6</b>
<b>13) SANÇÕES</b>	<b>6</b>
<b>14) EXCEÇÕES</b>	<b>6</b>

## 1) Escopo

Este documento detalha o fluxo para o gerenciamento de continuidade de negócios, ou, na sigla em inglês, BCM – *Business Continuity Management* (“Procedimento”).

## 2) Normas Relacionadas

- Resolução CVM nº 21/2021 (“RCVM 21”).
- Resolução CVM nº 35/2021 (“RCVM 35”).
- Código ANBIMA de Administração e Gestão de Recursos de Terceiros (“Código ANBIMA”).
- Guia de Cibersegurança ANBIMA - Versão Junho de 2021.
- P02 – Política de Compliance e Controles Internos.
- P07 – Política de Segurança da Informação ou Segurança Cibernética.

## 3) Público-alvo

Todos os funcionários, terceiros, estagiários e sócios com funções internas (“Colaboradores”) estão sujeitos a este Procedimento.

## 4) Responsabilidade

A responsabilidade pela estrutura de continuidade de negócios está a cargo do Diretor do Compliance e Risco.

Tal profissional manterá uma via impressa deste documento, bem como uma cópia eletrônica em seus dispositivos eletrônicos pessoais.

## 5) Premissas para o Gerenciamento de Continuidade de Negócios

O plano de continuidade de negócios da ÉXES tem as seguintes premissas:

- Atuação como gestora de fundos ilíquidos (FIDCs e FIIs), com ativos de crédito privado a serem mantidos até o vencimento, bem como em fundos líquidos majoritariamente compostos por ativos de renda fixa permitidos, conforme a política de investimento de cada veículo.
- Avaliação e definição de criticidade dos processos, subprocessos e atividades críticas da instituição (“Processos Críticos”).
- Definição de planos de ação em caso de impossibilidade de se realizar Processo Crítico por conta da situação de contingência (“Planos de Ação”).
- Definição e teste de cenários de contingência.
- Estabelecimento de prazo para o retorno das atividades ÉXES, caso necessário.

## Uso Interno

Processos Críticos e Planos de Ação são especificados em planilha de Excel (“Planilha de Controles – TI e BCM”), sob responsabilidade do Diretor de Compliance e Risco.

O acionamento parcial ou integral do plano será necessariamente proporcional à extensão do dano, fato ou ato que demande o acionamento do plano de contingência e norteado pelo conceito jurídico de força maior.

## 6) Prazo para o Retorno das Atividades

Os prazos aqui previstos consideram eventos máximos e hipotéticos que determinem o acionamento completo do plano de contingência da ÉXES, tal como ataque cibernético que afete toda a estrutura tecnológica da ÉXES e, também, a particular de seus profissionais.

### 6.1 Gestão de FII, FIDC e Fundos Financeiros de Crédito Privado

Pelo tipo e pela composição dos veículos geridos, o prazo para o retorno das atividades da ÉXES em caso de cenário de extrema contingência admite certa tolerância na maioria das atividades, vez que: **(a)** não há, como regra, atuação diária em mercados de ações, futuros e derivativos, que demandam definições e decisões de investimento (compra ou venda) imediatas a depender da oscilação de preços de negociação em determinado dia; e **(b)** os fundos estruturados tendem a ser constituídos sob a forma de condomínio fechado e os fundos financeiros serão majoritariamente compostos por ativos de renda fixa (conforme permitido pela política de investimento de cada veículo), o que praticamente elimina diversas das rotinas diárias comuns a fundos líquidos de gerenciamento de liquidez para se fazer frente a resgates.

Assim, com exceção de estar em andamento ofertas de distribuição pública pendentes de subscrição ou liquidação – caso em que, a restauração tecnológica precisa ser o mais breve possível, ainda que com a ativação de plano de provedores ou de contrapartes –, a ÉXES entende que é tolerável suspender totalmente suas atividades por até 2 (dois) dias.

## 7) Cenários

Os cenários analisados para a continuidade de negócios são:

- Impossibilidade de acesso ao edifício sede da Éxes Gestora.
- Indisponibilidade de mais de 50% (cinquenta por cento) do quadro de Colaboradores.
- Indisponibilidade de acesso a sistemas, dados ou toda a estrutura tecnológica da ÉXES, inclusive em caso de ataque cibernético.

### 7.1 Impossibilidade de Acesso ao Edifício

Em caso de edifício inacessível – exemplo, pane elétrica que demande revisão total do prédio – o plano de contingência é o trabalho remoto.

## Uso Interno

Todos os Colaboradores estão autorizados a trabalhar de modo remoto, conforme cadastro feito na Planilha de Controles – TI e BCM. Todos os processos podem ser performados, com priorização dos Processos Críticos.

Dado que a Éxes possui como política o trabalho de forma híbrida, desde que tenham acesso à internet, os colaboradores podem executar suas funções de forma remota, por meio da tecnologia, incluindo sistemas, e-mails, comunicações internas e externas etc., todos os sistemas utilizados possuirão a possibilidade de serem acessados de maneira remota.

**7.2 Adicionalmente, para fins das comunicações com os clientes e parceiros, estas poderão ser realizadas por meio dos telefones celulares pessoais dos próprios colaboradores. Indisponibilidade de mais da metade dos Colaboradores**

Na hipótese de indisponibilidade, ainda que remota, de mais de 50% (cinquenta por cento) dos Colaboradores (e.g., por motivo de doença) e de haver determinado Processo Crítico a ser performado, a ÉXES entende que haverá ao menos um Colaborador remanescente com condições de, em situação de urgência, realizar determinada atividade.

### **7.3 Indisponibilidade de Sistemas, Dados, Estrutura Tecnológica e Ataque Cibernético**

Em caso de indisponibilidade de acesso a sistemas ou dados, inclusive em caso de ataque cibernético, há duas medidas: **(a)** início do plano de recuperação de desastres dos fornecedores de estrutura tecnológica; e **(b)** implementação dos Planos de Ação da ÉXES, desenhados para o desenvolvimento dos Processos Críticos, os únicos a serem performados em contingência.

Para iniciar o plano de recuperação de desastres, a ÉXES mantém lista de todos os provedores de serviços em controle interno, sob responsabilidade do Diretor de Compliance e Risco.

Os Planos de Ação constam na Planilha de Controles – TI e BCM.

Especificamente no que se refere ao risco de ataque cibernético – com eventual perda ou vazamento de dados – a ÉXES: **(a)** implantou, por meio da P07-Segurança da Informação e Cibernética, formas de mitigar esta possibilidade e regras de conduta para vazamento de dados; e **(b)** conta com o “*back up*” de terceiros no caso de informações que devam ser também armazenadas por intermediários de ordens, administradores fiduciários de fundos geridos, custodiantes, escrituradores e, especificamente no caso de garantias e transações relacionadas a imóveis, com os registros oficiais mantidos em tabelionatos e registros públicos.

A ÉXES utiliza, ainda, o armazenamento em nuvens, com o backup de dados a cargo do provedor de serviços contratado.

## **8) Declaração de Contingência**

A declaração de contingência fica a cargo do Diretor de Compliance e Risco, que também deve informar os demais Colaboradores a respeito.

Na ausência do Diretor de Compliance e Risco, esta definição fica a cargo do Diretor de Administração de Carteiras.

## 9) Testes e Avaliação

A ÉXES avaliará, ao menos uma vez por ano, o plano de continuidade de negócios formalizado por este Procedimento.

Esta avaliação se dará da seguinte maneira: (a) atuação remota e simultânea de todos os Colaboradores listados em Planilha de Controles –TI e BCM como autorizados a atuar off-site em caso de contingência; e (b) realização de Processos Críticos listados por meio do método alternativo definido como plano de ação.

Os testes acima poderão ser efetuados em dias e períodos distintos ou, ainda, de modo fracionado – isto é, testar a realização de um Processo Crítico por vez em contingência, via método proposto no Plano de Ação.

Haverá documentação de tais testes por meio de prints de telas e registro de logs de acesso remoto.

## 10) Dever de Reporte à Alta Administração e ao Regulador

Na forma da RCVN 35, artigo 38, eventos que gerem a ativação completa do plano de contingência devem ser informados à alta administração da ÉXES, aos competentes administradores fiduciários, à Comissão de Valores Mobiliários e, se cabível, a clientes afetados.

## 11) Manutenção e Prazo de Guarda

Os documentos relacionados a testes de contingência ou a este Procedimento serão armazenados por ao menos 5 (cinco) anos.

## 12) Vigência e Atualização

Este Procedimento será revisado anualmente, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo, sobretudo em caso de alterações na atividade de ÉXES ou em sua localização. Poderá, ainda, ser alterado a qualquer tempo em razão de circunstâncias que demandem tal providência.

## 13) Sanções

O descumprimento deste Procedimento, como de qualquer regra ÉXES, pode gerar sanções internas, incluindo desligamento

## 14) Exceções

Exceções a este Procedimento devem ser aprovadas pela Diretor de Compliance e Risco.