Procedimento de BCM – Continuidade de Negócios

Junho de 2022.

éxes

Sumário

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

- Instrução CVM nº 558/2015 ("ICVM 558").
- Instrução CVM nº 505/2011 ("ICVM 505").
- Código ANBIMA de Melhores Práticas de Administração de Recursos ("Código ANBIMA").
- Manual de Segurança Cibernética ANBIMA – Versão Dezembro de 2017.
- 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 EXES 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 títulos públicos.
- 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 EXES, caso necessário.

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 EXES, tal como ataque cibernético que afete toda a estrutura tecnológica da EXES e, também, a particular de seus profissionais.

6.1. Gestão de FII, FIDC e Fundos ICVM 555 de Crédito Privado

Pelo tipo e pela composição dos veículos geridos, o prazo para o retorno das atividades da EXES 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 ICVM 555 serão majoritariamente compostos por títulos públicos, 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 EXES 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.
- Indisponibilidade de mais de 50% (cinquenta por cento) do quadro de Colaboradores.
- Indisponibilidade de acesso a sistemas, dados ou toda a estrutura tecnológica da EXES, 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.

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.

Apesar de todos os Colaboradores possuírem acesso remoto, não é recomendado para se trabalhar senão em casos de contingência, com exceção de Colaboradores cuja senioridade transpassa a necessidade de trabalho presencial. Isto se dá porque o acesso é fornecido com base na criticidade da função desenvolvida ou na senioridade. Assim, é possível que profissional que tenha acesso remoto por sua senioridade não tenha sob sua responsabilidade Processo Crítico a ser executado em contingência.

7.2. 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 EXES 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 tecnológico; e **(b)** implementação dos Planos de Ação da EXES, desenhados para o desenvolvimento dos Processos Críticos, os únicos a serem performados em contingência.

Para iniciar o plano de recuperação de desastres, a EXES 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 EXES: **(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 EXES 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.

Enquanto o número de Colaboradores for inferior a 10 (dez) profissionais, não haverá o desdobramento de *call chain,* cabendo ao diretor que decretar contingência informar os demais a respeito.

9. Testes e Avaliação

A EXES 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 ICVM 505, artigo 35-A, eventos que gerem a ativação completa do plano de contingência devem ser informados à alta administração da EXES, 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 EXES 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 EXES, pode gerar sanções internas, incluindo desligamento

14. Exceções

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