Política de Contingenciamento e Continuidade

Data: Fevereiro de 2022

infinity

(11) 3049-0770
www.infinityasset.com.br
contato@infinityasset.com.br

Rua Funchal, 418, 23º andar
Ed. e-Tower - Vila Olímpia
CEP 04551-060 - São Paulo - SP

SUMÁRIO

1. Objetivo

A Infinity estabeleceu um plano de continuidade de negócios a fim de evitar a descontinuidade de suas atividades em caso de qualquer sinistro que impeça o acesso de dos Colaboradores ao seu escritório em São Paulo, bem como nos casos de eventos que causem um impacto em suas rotinas operacionais que impeçam a continuidade das atividades prestadas no dia-a-dia ("Eventos de Contingência").

Neste sentido, o plano de continuidade de negócios contempla quatro tópicos principais que devem ser observados no caso de sua efetivação:

(i) Local designado como site de contingência, ao qual os Colaboradores designados deverão se dirigir quando da ocorrência de um Evento de Contingência;
(ii) Colaboradores designados para atuar no site de contingência; e
(iii) Principais procedimentos a serem observados na hipótese de um Evento de Contingência.
(iv) Validação ou testes, no mínimo, a cada doze meses, ou em prazo inferior se exigido pela Regulação em vigor.

O **Plano de Contingência** prevê ações que durem até o retorno à situação normal de funcionamento da Infinity Asset dentro do contexto de seu negócio. O Plano de Contingência identifica duas variáveis para o funcionamento adequado da empresa: Infraestrutura e Processos.

A Infraestrutura engloba todas as variáveis utilizadas para realização dos processos: energia, telecomunicações, informática e sistemas internos. Para cada um dos itens que compõem a infraestrutura existe uma ação a ser tomada.

Já os processos são as atividades realizadas para operar os negócios da Infinity. Os processos dependem da infraestrutura toda ou de parte da estrutura em funcionamento. Somente com os processos em andamento pode-se definir que o plano de ação foi bem executado.

Back-up: Os backups são realizados da seguinte forma:

(v) Diária: para as informações críticas e/ou estratégicas, cujos dados não são recuperados facilmente;

(vi) Semanal: para as informações não críticas ao negócio da Instituição, cujos dados são recuperados com menor grau de dificuldade;
(vii) Mensal ou outra periodicidade: para os dados históricos.
(viii) Periodicamente são feitas avaliações e análises para poder detectar eventuais novas necessidades no processo, levando-se em conta as necessidades de contingência de infraestrutura, de TI, de fornecedores externos, de sistemas, bem como de contingência pessoal ou de estrutura física.

As informações do portfólio além de estarem nos sistemas internos da infinity Asset são disponibilizadas diariamente pelo administrador, que também informará qualquer movimentação no passivo dos fundos para adequação do caixa dos fundos. Em caso de falha de fornecimento de energia, a Infinity possui nobreak para suportar o funcionamento de seus servidores, rede corporativa, telefonia e estações de trabalho (desktops) para a efetiva continuidade dos negócios.

Em caso de efetiva necessidade de utilização da estrutura de contingência, o plano de ação está descrito abaixo.

1.1. Site de Contingência

Na hipótese de ocorrência de um Evento de Contingência, os Colaboradores designados nos termos do item abaixo deverão manter contato por telefone no intuito de se adequarem quanto a seriedade do processo e decidirem pelo acesso VPN para a realização via home office, das atividades diárias, recebendo todo apoio necessário, de forma a evitar uma interrupção nos serviços prestados pela Infinity.

1.2. Colaboradores Designados

Conforme detalhando acima, os seguintes colaboradores deverão se deslocar para o site de contingência:

(i) O Presidente da Infinity;
(ii) 3 (três) membros da equipe de gestão, designado previamente;
(iii) 2 (dois) membros da equipe de tecnologia da informação.

Os demais Colaboradores deverão permanecer em São Paulo e deverão atuar, dentro do possível,

para a manutenção das atividades da Infinity diante do referido Evento de Contingência, fazendo uso da infraestrutura da Infinity disponível, via VPN, que serão disponibilizadas com base nos backups e registros externos

Adicionalmente ao disposto acima, os seguintes Colaboradores deverão atuar em São Paulo com foco na restauração das atividades em seu curso ordinário:

(ix) o Diretor de Compliance e Riscos;
(x) 1 (um) membro da equipe administrativa, previamente designado;
(xi) 1 (um) um membro da equipe de BackOffice, previamente designado; e
(xii) 1 (um) membro da equipe de tecnologia da informação

1.3. Procedimentos a Serem Observados

Na hipótese de ocorrência de um Evento de Contingência, os principais procedimentos deverão ser observados:

1.3.1. Comunicação

Os Colaboradores possuem em seus celulares os telefones das pessoas chave da Infinity. Uma vez que qualquer Colaborador tenha ciência da ocorrência de um Evento de Contingência, este deverá entrar em contato com qualquer das pessoas chave, a qual será responsável por notificar os demais colaboradores (em especial os designados nos termos do item acima), bem como por dar início aos demais procedimentos de contingência abaixo descritos.

1.3.2. Mobilização

Os Colaboradores designados nos termos do item 1.2, assim que forem notificados da ocorrência de um Evento de Contingência, se reunir nas proximidades da sede da Infinity e atuar nas instruções, sejam por telefone/celular/ internet com os profissionais acima listados.

A equipe responsável pela normalização das atividades, será responsável por avaliar o problema, estabelecer um prazo para a regularização das atividades e tomar as providências cabíveis junto aos

diretores da Infinity para liberar o acesso ao escritório e aos recursos, ou providenciar novas instalações o mais rápido possível.

Demais Colaboradores deverão permanecer em suas residências, aguardando o contato dos responsáveis pela normalização das atividades, a fim de estabelecer quais providências a serem adotadas no caso específico.

A equipe responsável pela normalização das atividades, será responsável por avaliar o problema, estabelecer um prazo para a regularização das atividades e tomar as providências cabíveis junto aos diretores da Infinity para liberar o acesso ao escritório e aos recursos, ou providenciar novas instalações o mais rápido possível.

1.3.3. Processamento em Nuvem

A Resolução 4658/2018, dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

Neste sentido, o risco na Infinity CCTVM é mitigado, considerando que sua atuação consistiu somente na distribuição de fundos de investimentos e que os procedimentos descritos nesta política buscam estar de acordo com:

- O porte, o perfil de risco e o modelo de negócio da Infinity;
- A natureza das operações e a complexidade dos produtos, serviços, atividades e processos, e
- A sensibilidade dos dados e das informações sob responsabilidade.

A Infinity não possui histórico de incidentes ou de interrupções de serviços relevantes, porém, caso venha a ocorrer ocorram situações que configurem situação de crise, o Diretor de Compliance e Riscos da Infinity atuará na comunicação tempestiva ao Banco Central do Brasil, bem como dará andamento nas providências quanto ao reinício das suas atividades e relatos formais de como a implementação será realizada.

Em seguida, deverá formalizar a suspeita por e-mail à área de Tecnologia da empresa terceirizada, responsável pelo sistema tecnológico contratado. Paralelamente, os profissionais de tecnologia da

Infinity investigarão visando documentar cada etapa, bem como determinar a criticidade do incidente, da utilização do software e hardware e trilha de auditoria, mantendo a confidencialidade e segurança física dos demais ambientes de operação e processamento.

Ainda, a Infinity visa assegurar que qualquer contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem será previamente comunicada ao Banco Central do Brasil pelo Diretor de Riscos e Compliance.

Inclusive, qualquer novo contrato com empresa de tecnologia somente poderá ser assinado após a confirmação da existência de clausula específica e plano contingencial, ambos à luz da Resolução Cibernética, aliado aos procedimentos de contratação da Política de Contratação de Terceiros e com consecutiva aprovação do Diretor de Risco e Compliance.

No caso de interrupção de serviço relevante de processamento e armazenamento de computação em nuvem, de empresa contratada que não respeite o prazo de restauração informado em seu plano contingencial, a Infinity poderá atuar na substituição da mesma, firmando contrato com empresa que preste a mesma atividade, aliado aos procedimentos de contratação constantes na Política de contratação de terceiros.

O prazo interno estipulado para reinício das atividades poderá sofrer alterações de acordo com a gravidade do incidente ocorrido, porém os históricos dos testes já realizados pela Infinity demonstraram resultados satisfatórios, já que as atividades são salvas através de arquivos, sistemas e servidores virtualizados, assegurados por diversos níveis dos procedimentos de backups.

Para restauração de arquivos o procedimento não excederá o prazo de duas horas para restauração total, sendo que no decorrer da restauração alguns arquivos já poderão ser acessados dando assim a possibilidade de continuidade das atividades dos negócios.

Na restauração de servidores virtuais o processo não excederá seis horas para total recuperação. Sendo que sempre serão priorizados os serviços e sistemas mais críticos.

Buscando reduzir a vulnerabilidade da Infinity em caso de incidentes e atender os objetivos de segurança cibernética a Política de Segurança da Informação e cibernética estabelece as medidas de segurança obtidas pela utilização de Firewall, Antivírus e Serviços de E-mail seguros.

2. Controle de revisões

Revisão da Política	Data	Motivo
Diretoria Compliance	25/08/2016	Atualização
Diretoria Compliance	26/12/2017	Revisão
Gerência de Compliance	05/02/2018	Inclusão no item 1.2
Gerência de Riscos	05/02/2019	Revisão Geral
Compliance	31/07/2020	Revisão Geral
Compliance	09/2020	Alteração logotipo e tipografia
Compliance	12/2020	Inclusão Cibernética
Compliance	02/2020	Não ocorreram alterações