Política de Contingenciamento e Continuidade

Data: maio de 2023

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 ao escritório, 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").

O **Plano de Contingência** prevê ações que durem até o retorno à situação normal de funcionamento da Infinity Asset, identificando as 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 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:

(i) Diária: para as informações críticas e/ou estratégicas, cujos dados não são recuperados facilmente;
(ii) Semanal: para as informações não críticas ao negócio da Instituição, cujos dados são recuperados com menor grau de dificuldade;
(iii) Mensal ou outra periodicidade: para os dados históricos.
(iv) 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 do fundo para adequação do caixa. 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.

Na hipótese de ocorrência de um Evento de Contingência, os diretores/Sócios deverão manter contato por telefone no intuito de se adequarem quanto a seriedade do processo, mantendo o acesso pelo acesso VPN, para a realização via home office, das atividades diárias.

2. Designações

Um profissional de tecnologia deverá atuar, em parceria com o Diretor Administrativo, na demanda de restauração.

Os demais sócios/diretores deverão fazer uso da infraestrutura da Infinity disponível, via VPN, disponibilizada com base nos backups e registros.

3. Procedimentos

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

3.1 Comunicação

A Infinity mantém os números dos celulares das pessoas chave da Infinity. Tendo ciência de qualquer Evento de Contingência, pelo profissional de Tecnologia, este deverá informar ao Diretor de Compliance, Riscos e PLD/FTP, que deverá dar ciência aos demais sócios/diretores para dar início nos demais procedimentos de contingência.

3.2 Mobilização

Assim que ocorrer a identificação de um Evento de Contingência, todos deverão permanecer em suas residências, aguardando o contato dos responsáveis e normalização das atividades.

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.

4. Processamento em Nuvem

Considerando a Resolução CVM 35/2021 que dispõe sobre a política de segurança cibernética e a Resolução 4.658/2018 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, entendemos que o risco na Infinity Asset Management é mitigado, já que sua atuação consiste somente na gestão e distribuição de apenas um fundo restrito. Ainda, a Infinity não possui histórico de incidentes ou de interrupções de serviços relevantes, no entanto, caso venha a ocorrer situações que configurem situação de crise, o Diretor de Compliance e Riscos da Infinity atuará nos procedimentos regulamentares.

Caso ocorra algum incidente, o Diretor de Compliance e Riscos da Infinity deverá formalizar a suspeita à empresa terceirizada e ao responsável pelo sistema tecnológico contratado que, em parceria com o profissional de tecnologia da Infinity investigará, documentando cada etapa para 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.

Qualquer novo contrato com empresa de tecnologia somente poderá ser assinado após a confirmação da existência de cláusula 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 Compliance, Riscos e PLD/FTP.

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, 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.

5. 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
Compliance e TI	Maio/2023	Revisão Geral. Infinity passou a atuar na gestão de um só fundo