Plano de Contingência, Continuidade de Negócios e Recuperação de Desastres

Documento confidencial - Circulação restrita

ÍNDICE

1. INTRODUÇÃO

1.1 – Pelo presente documento, a INFRA ASSET MANAGEMENT LTDA. ("INFRA ASSET"), vem, nos termos da Instrução Normativa nº 558 da Comissão de Valores Mobiliários, de 26 de março de 2015 ("ICVM 558"), e do Código de Regulação e Melhores Práticas para Fundos de Investimento da ANBIMA – Associação Brasileira de Entidades dos Mercados Financeiros e de Capitais ("ANBIMA") e das diretrizes baixadas pelo Conselho de Regulação e Melhores Práticas da ANBIMA, definir seu Plano de Continuidade do Negócio ("PCN") que estabelece estratégias e procedimentos a serem observados na eventualidade de incidentes ou situações de emergência que envolvam a INFRA ASSET e/ou seus sócios, dirigentes, empregados, consultores, funcionários, trainees, estagiários ("Colaboradores").

2. OBJETIVO

2.1 – O objetivo principal deste PCN é minimizar os efeitos de acontecimentos de natureza variada, que possam prejudicar parcial ou totalmente o desenvolvimento dos negócios da INFRA ASSET. Em outras palavras, objetiva a manutenção das atividades consideradas essenciais, em caso de contingência.

3. ASPECTOS GERAIS

3.1 – GESTÃO, ABRANGÊNCIA

3.1.1 – A gestão do PCN é realizada pela Diretor de Gestão de Risco, Compliance e Prevenção à Lavagem de Dinheiro, Sr. Paulo André Gil Boschiero ("Diretor de Risco e Compliance") e pelo responsável pela área de Controles Internos, Sr. Cristiano Otoni.

O time de Compliance é responsável pela gestão dos participantes por meio de convites/comunicação aos Colaboradores para o devido planejamento e execução dos treinamentos.

3.2 – ABRANGÊNCIA

3.1.2 – Este PCN aplica-se a todos os níveis hierárquicos da INFRA ASSET, ou seja, se estende a todos os seus Colaboradores.

3.3 – ATUALIZAÇÃO E DIVULGAÇÃO

3.3.1 – A atualização e divulgação do PCN serão realizadas pelo Diretor de Gestão de Risco e Compliance.

A atualização do PCN será realizada a qualquer momento, desde que sejam identificadas melhorias ou alterações nos procedimentos que compõem o PCN.

A divulgação do PCN será feita na página da rede mundial de computadores da INFRA ASSET (www.infraasset.com) e em material impresso, sendo que cabe ao Diretor de Risco e Compliance assegurar o *upload* da versão mais atualizada do PCN.

3.4 – MANUTENÇÃO

3.4.1 – O Diretor de Compliance e Riscos analisará anualmente eventuais riscos que possam impactar a continuidade dos negócios da INFRA ASSET, como também, se entender necessário, decidirá pela manutenção dos termos deste PCN.

4. DESCRIÇÃO DA INFRAESTRUTURA

4.1 – DISTRIBUIÇÃO FÍSICA

4.1.1 – A INFRA ASSET tem sede e foro na cidade de São Paulo, Estado de São Paulo, na Rua Padre João Manuel, nº 923, 11º andar, conjunto, CEP 01411-000.

4.2 – INFRAESTRUTURA DE TELECOMUNICAÇÕES

4.2.1 – A infraestrutura de telecomunicações da INFRA ASSET dispõe de um servidor com capacidade de 2TB de armazenamento e de um *no-break* para manutenção do servidor, caso tenha queda no fornecimento de energia elétrica.

Tem disponível filtro de *e-mail* provido pela *Microsoft*, além de soluções de segurança como antivírus e *firewall software* do sistema operacional (*Windows*).

O *backup* é realizado diariamente através do servidor programado, para a nuvem *Microsoft Azure Backup*, mantidas cópias dos últimos 10 (dez) dias e cópias mensais por 5 (cinco) anos.

O acesso à rede contém controle por meio de *login* e senha por usuário. Além do acesso local, a rede pode ser acessada por meio de acesso remoto (via VPN) para usuários que necessitam acessar externamente.

O acesso à internet é feito por *link* da Net, com redundância de *link backup* (Tim), caso ocorra queda de sinal com um deles.

A telefonia dispõe de uma central PABX INTELBRAS misto analógico e digital interno com ramais integrados.

Os equipamentos estão localizados em sala própria, fechada e climatizada.

5. TESTES DE SEGURANÇA E TREINAMENTOS

5.1 – TESTES DE SEGURANÇA

5.1.1 – O Diretor de Riscos e Compliance da INFRA ASSET coordenará a realização testes de segurança para assegurar-se de que os procedimentos previstos do PCN são viáveis e eficazes. São eles:

(i) anualmente, testes dos aparelhos de telefonia e atualização dos contatos telefônicos para confirmar se as informações de contato de emergência estão precisas e atualizadas;

(ii) anualmente, testes dos equipamentos operacionais, como *softwares* de gestão e controles instalados e *hardwares* compatíveis com as exigências operacionais dos *softwares* e redes;

(iii) anualmente, testes para aferir bom funcionamento dos computadores, *desktops* e, se for o caso, *notebooks* utilizados pelos Colaboradores;

(iv) mensalmente, testes de segurança, integridade e acessibilidade dos dados capturados e arquivados pelo sistema de *backup* do procedimento de *restore* de *backups* (sistema de informações);

(v) anualmente, testes de acesso ao e-mail corporativo (*Office 365*) e à internet;

(vi) conforme necessidade, testes para apurar a eficácia e/ou eventual necessidade de atualização dos sistemas operacionais adotados (*Office 365*, *Windows*, antivírus etc.).

5.1.2 – Ao final, será possível verificar se há necessidade da implementação de melhorias nos procedimentos adotados, bem como a incorporação de novas tecnologias disponíveis.

5.2 – TREINAMENTOS

5.2.1 – Além disso, todos os Colaboradores sujeitam-se a realização de treinamentos, a fim de averiguar a adesão dos mesmos aos procedimentos deste PCN na eventualidade de um desastre.

Assim, todos os Colaboradores da INFRA ASSET deverão conhecer os procedimentos de *backup*, salvaguarda de informações relacionadas às suas atividades e melhores práticas de saúde e segurança no ambiente de trabalho.

5.2.2 – A implementação dos resultados obtidos nos treinamentos/testes será realizada pelo Diretor de Riscos e Compliance.

6. ANÁLISE DE RISCOS

6.1. – Os cenários de riscos e o potencial impacto na operação da INFRA ASSET são avaliados de acordo com o impacto e com as frequências dos eventos associados aos fatores de riscos. O resultado da avaliação de riscos auxilia na tomada de decisões sobre quais riscos necessitam de tratamento e a prioridade para a implementação do tratamento. Segue abaixo fluxograma para análise de riscos:

FREQUÊNCIA	IMPACTO
ALTA	ALTO
MÉDIA	MÉDIO
BAIXA	BAIXO

Com base no impacto que pode ser causado pelo evento, é possível classificar os riscos por prioridade orientada pelos critérios de aceitabilidade. Assim, tem-se o seguinte:

Aceitável – quando o impacto é baixo. Neste caso, não é necessário acionar o plano de contingência nem adotar medidas mitigatórias, a menos que se possa reduzir mais o risco com pouco custo ou esforço.

Tolerável – quando o impacto é médio. A gestora está preparada para suportar o risco, não havendo necessidade de instalar o plano de contingência, mas medidas mitigatórias são recomendadas.

Intolerável – quando o impacto é alto. Tratam-se de condições que implicam na paralisação das operações até que o risco se reduza ao nível pelo menos tolerável. Aqui, o plano de contingência deverá ser acionado.

7. IDENTIFICAÇÃO DO EVENTO

7.1 – Na análise dos eventos possíveis, foram levados em consideração aqueles que possam comprometer dados e informações dos clientes sob gestão (ativo), corpo técnico (Colaboradores), equipamentos de informática e de comunicação e, ainda, as instalações físicas.

Seguem abaixo os fatores de continuidade dos negócios da INFRA ASSET, que são considerados como imprescindíveis à sociedade:

(i) Inacessibilidade às instalações físicas:

- Exemplos: Desastres internos: incêndios, explosões, acidentes, inundações (vazamento, rupturas de tubulação).
  Desastres externos: distúrbios civis (greves, passeatas), incêndios, explosões, acidentes, inundações (chuvas, enchentes), paralisação de transporte público, catástrofes naturais.
- Frequência: baixa
- Impacto: alto

(ii) Corpo técnico:

- Exemplos: distúrbios civis (greves, paralisação), mortes múltiplas.
- Frequência: baixa
- Impacto: alto

(iii) Segurança, integridade, qualidade e acessibilidade aos dados e informações dos clientes:

- Exemplos: entrada de dados; vazamento de dados; falhas de configuração; erros de manutenção; sabotagem; roubo, furto ou desvio de informação; ataques internos e externos (vírus, *hackers*).
- Frequência: baixa
- Impacto: alto

(iv) Falhas de equipamentos de informática – *softwares* de gestão e controles, *hardwares*:

- Exemplos: falhas de configuração; erros de manutenção; sabotagem; ataques internos e externos (vírus, *hackers*).
- Frequência: baixa
- Impacto: alto

(v) Falhas de equipamentos de comunicação:

- Exemplos: falhas de configuração; erros de manutenção; sabotagem; ataques internos e externos (vírus, hackers); sobrecarga no tráfego da rede; perda de performance; indisponibilidade do *firewall*.
- Frequência: baixa
- Impacto: alto

(vi) Interrupção do fornecimento de itens primários:

- Exemplos: energia (*black out*, local, por longa/curta duração, por tempo indeterminado); variação extrema da temperatura (falha em sistema de refrigeração); água (concessionária, bomba inoperante).
- Frequência: baixa
- Impacto: médio

(vii) Falhas humanas:

- Exemplos: erros e acidentes técnicos; funcionários despreparados; fraudes.
- Frequência: baixa
- Impacto: médio

8. PROCEDIMENTO DE ATIVAÇÃO DO PLANO DE CONTINUIDADE DE NEGÓCIOS ("PLANO DE CONTINGÊNCIA")

8.1 – Diante de um cenário definido como **alto**, será acionado o Plano de Contingência pelo Diretor de Riscos e Compliance da INFRA ASSET, que deverá, também, ser responsável pela comunicação aos clientes e mercado da impossibilidade da INFRA ASSET de operar em condições normais, informando que a gestora se encontra em contingência, mas, que, ao mesmo tempo, está buscando manter as suas atividades, ainda que com capacidade reduzida de recursos.

8.2 – O responsável pela área de Controles Internos será responsável por verificar e validar a segurança, integridade e acessibilidade dos dados capturados e arquivados pelo sistema de *backup* de dados diário e ativar os serviços de TI contratados previamente, assim como os técnicos responsáveis por manutenção e funcionalidade dos *hardwares* e *softwares*.

8.3 – Em caso de problemas na locomoção das pessoas envolvidas no Plano de Contingência, a INFRA ASSET será responsável pelo transporte e custos envolvidos.

8.4 – A INFRA ASSET celebra contratos relacionados à sistemas de informática, domínio da internet, domínio de e-mail, número e registro/licenças (como *Windows*, *Office 365*, por exemplo) para realizar o *backup* de dados e armazenamento de todas as suas informações em nuvem.

O monitoramento e armazenamento das cópias de segurança do servidos de arquivos é feita por empresa especializada contratada especificamente para tal função. O monitoramento, administração e suporte dos servidores é feito no formato 24/7 (24 horas por dia nos 7 dias da semana), sendo guardadas cópias mensais e anuais pelo período de 5 (cinco) anos. A INFRA ASSET também mantém cópias digitalizadas e físicas de seus documentos.

Na hipótese de ocorrência de problemas com a nuvem, a empresa contratada pela INFRA ASSET para gerenciar *backups* de dados e do procedimento de *restore* de *backups* também possui formas de recuperação dos dados no caso supramencionado. Tal dispositivo é obrigatório e previsto no contrato de prestação de serviços firmado com a INFRA.

A estrutura de e-mails utilizada pela INFRA também é armazenada em nuvem, utilizando-se do sistema do programa *Office 365*.

8.5 – Em caso de um evento que interrompa o uso da infraestrutura (de informações, de comunicação e/ou do espaço físico) da INFRA ASSET, de forma temporária ou permanente, devem ser tomadas as seguintes medidas dependendo das circunstâncias específicas:

(i) Acionar a empresa contratada para gerenciar o *backup* dos dados armazenados nos servidores remotos e o *restore* de *backups*, caso seja necessária a reposição emergencial e temporária dos servidores da INFRA ASSET;

(ii) Disponibilizar computadores, *desktops* e/ou *notebooks* autorizados aos Colaboradores, de modo a restaurar o quanto antes as comunicações via rede dentro e fora da empresa;

(iii) Na impossibilidade de se utilizar o espaço físico do escritório, a INFRA ASSET poderá fazer uso de um local remoto como escritório temporário para contornar problemas específicos que venham a ocorrer na sede da empresa. As operações serão automaticamente migradas para a sede principal da INFRA ASSET tão logo as instalações estiverem aptas para o desenvolvimento normal dos negócios. Tal local deverá ser determinado pelos administradores da INFRA ASSET. Ainda, neste caso, a INFRA ASSET poderá continuar a funcionar através de *Home Office*, utilizando-se de *notebooks* autorizados, internet banda larga e telefone, acessando seus dados por meio da rede mundial de computadores.

8.6 – Todos os telefones pessoais da equipe são disponibilizados pelos Colaboradores aos seus clientes, na eventualidade dos telefones comerciais não funcionarem, comprometendo-se a agendar reuniões e *conference calls* sempre que se fizer necessário.

8.7 – Os Administradores Fiduciários dos fundos de investimentos contam com procedimentos próprios e sólidos de continuidade de negócios, fortalecendo a preservação dos ativos e direitos dos cotistas.

Todos os documentos possuem tanto cópias digitalizadas quanto físicas, as quais poderão ser acessadas pela INFRA ASSET se e quando necessário. A responsabilidade pela guarda da documentação dos fundos de investimentos geridos pela INFRA ASSET é de responsabilidade dos respectivos administradores, o que reduz ainda mais o risco de segurança aos dados e às informações dos fundos sob gestão no caso de contingências.

8.8 – Para a retomada célere e eficaz das operações após uma contingência, o Diretor de Riscos e Compliance da INFRA ASSET deve adotar as seguintes medidas, conforme o caso:

(i) Monitorar continuamente o escritório na sua reocupação;

(ii) Verificar a ausência de efeitos pós-desastre e de possíveis ameaças;

(iii) Garantir que todos os serviços de infraestrutura como, energia, água, telecomunicação, segurança, estão operacionais;

(iv) Instalar novos *softwares* e *hardwares*;

(v) Garantir bom funcionamento dos equipamentos de informática e comunicação, como também dos sistemas operacionais para assegurar completa funcionalidade;

(vi) Finalizar o Plano de Contingência;

(vii) Coordenar o retorno dos integrantes da equipe para o escritório original.

9. CONTATOS

Contatos:

Ricardo Kassardjian
Diretor-Presidente
ricardo@infraasset.com
(11) 3165-8100

Paulo Boschiero
Diretor de Compliance, Gestão de Riscos e PLD
paulo@infrasset.com
(11) 3165-8100

Cristiano Otoni
Gerente Controles Internos
cristiano@infrasset.com
(11) 3165-8100