



POLÍTICA DE CONTINGÊNCIA E CONTINUIDADE DE NEGÓCIOS

NORMA INTERNA	IDENTIFICAÇÃO	PÁG.
CONTINGÊNCIA E CONTINUIDADE DE NEGÓCIOS	NI-REIT-09.01	2 de 8

1. OBJETIVO

O Plano de Contingência e Continuidade de Negócios (“**PCN**”) da Reit Securitizadora S.A. (“**REIT**”) é um conjunto de definições, ações e estratégias que deverá ser seguido na ocorrência de incidentes ou emergências que causem a interrupção ou indisponibilidade dos processos de negócio ou dos recursos da REIT.

O plano visa assegurar que, em caso de emergência, os processos de negócios críticos possam ser reestabelecidos antes de causar prejuízos sensíveis à REIT e, consequentemente, aos seus clientes.

Este documento apresenta o planejamento de recuperação da REIT e as principais técnicas para casos de indisponibilidade dos ativos visando à manutenção e continuidade plena dos negócios com custo proporcional ao da possível perda operacional.

O plano de continuidade será atualizado no mínimo anualmente para garantir a eficácia da recuperação dos negócios. Devem ser avaliadas as alterações em relação aos ativos mínimos dos processos, aos avanços tecnológicos, bem como mudanças na estrutura e estratégia do plano.

Outra atividade essencial para assegurar o sucesso do plano é a realização de testes ou ações que permitam avaliar a capacidade de resposta da REIT à situação de contingência, bem como identificar se os parâmetros e estratégias estão alinhados e apropriados.

A forma de divulgação do plano de continuidade de negócios é por meio de conscientização dos colaboradores da REIT na utilização dos recursos alternativos de contingência.

2. DEFINIÇÕES

2.1. Contingência – é uma eventualidade, um acaso, um acontecimento que tem como fundamento a incerteza de que pode ou não acontecer. Contingência é a característica daquilo que é contingente, ou seja, que é duvidoso, possível, mas incerto, que pode ocorrer, mas não necessariamente.

2.2. Continuidade de Negócios – mais conhecido como PCN, refere-se a um conjunto de estratégias e planos de ação preventivos que garantem o pleno funcionamento dos serviços essenciais de uma empresa durante quaisquer tipos de falhas, até que a situação seja normalizada. As organizações com visão de futuro, que possuem um Plano de Continuidade de Negócios bem elaborado e estruturado, garantem sua perenidade e sobrevivência diante de circunstâncias inesperadas, além de terem uma visão integral e abrangente de seus processos de negócio.

NORMA INTERNA	IDENTIFICAÇÃO	PÁG.
CONTINGÊNCIA E CONTINUIDADE DE NEGÓCIOS	NI-REIT-09.01	3 de 8

3. RESPONSABILIDADES E COMPETÊNCIAS

3.1. Da Diretoria de Compliance:

3.1.1. Manter atualizada esta Política de Contingência e Continuidade de Negócios e garantir a execução do plano em caso de necessidades;

3.1.2. Providenciar a realização do treinamento anual, sem que haja aviso prévio para tal, conforme itens **11.1** e **11.2**;

3.1.3. Cuidar da atualização dos personagens envolvidos no PCN, conforme quadros demonstrados nos itens **9.1**, **10.1** e **12.1**.

3.2. Da Divisão de Tecnologia da Informação:

3.2.1. Manter atualizada esta Política de Contingência e Continuidade de Negócios no que diz respeito aos requisitos técnicos;

3.2.2 Garantir que a estrutura tecnológica necessária esteja apta a ser utilizada quando necessário;

3.1.3. Comunicar ao Diretor de Compliance quaisquer situações que possam impedir a realização do plano de contingência.

3.2. De todas as áreas e colaboradores:

3.2.1. Ter ciência dessa política e do papel de cada um no caso de ocorrência de contingência.

4. PREMISSAS

4.1. A correta ativação do PCN se baseará nas seguintes premissas:

4.1.1. A existência de pessoas chaves, que garantirão que os procedimentos de emergência serão imediatamente colocados em prática após a ocorrência de uma interrupção/desastre;

4.1.2. A guarda e a manutenção deste PCN ou qualquer outro material associado à continuidade fora das dependências da REIT, facilitando o acesso em caso de desastre ou indisponibilidade de acessos as suas instalações.

5. CONTINUIDADE DOS PROCESSOS VITAIS – PRIORIZAÇÃO DE RECUPERAÇÃO DAS ATIVIDADES

5.1. Uma vez que a REIT dispõe de um número reduzido de funcionários e para continuidade de suas atividades basta qualquer computador ou tablet, desde que tenha internet segura e telefone, o prazo para adoção das medidas do planejamento da recuperação e o momento de ativação das estratégias de continuidade dos processos são **imediatos** (até 2 horas).

NORMA INTERNA	IDENTIFICAÇÃO	PÁG.
CONTINGÊNCIA E CONTINUIDADE DE NEGÓCIOS	NI-REIT-09.01	4 de 8

6. SERVIDORES

6.1. As áreas operacionais da REIT, para realizar suas atividades, utilizam 03 (03) sistemas, sendo:

- Akruai
- Alterdata
- Risk3

7. SERVIDORES

7.1. A REIT dispõe de 3 (três) servidores, sendo um para dados, outro para domínio/sistema contábil (folhamatic) e outro na nuvem para sistema backoffice (espelhamento interno HD's segregados dentro do próprio servidor);

7.2. Além dos servidores citados, em sua estrutura a REIT possui:

7.2.1. Um Nobreak com capacidade de 4 horas;

7.2.2. Dois "links" de dados, multivox 16 M e MLSWire 10 M;

7.2.3. SOS Backup (backup para NAS, incremental diário e completo mensal na nuvem Mandik);

7.2.4. Antivírus;

7.2.5. E-mail institucional google (webmail+outlook local);

7.2.6. Loadbalance (função de equilíbrio dos links existentes);

7.2.7. HJ TA sem firewall;

7.2.8. Uma central telefônica SN500.

7. INSTALAÇÕES E RECURSOS ADICIONAIS

7.1. Sede:

7.1.1. A sede da REIT está situada à Rua Visconde de Pirajá, nº 152, Sala 301, Ipanema, Rio de Janeiro, CEP 22410-000, em imóvel alugado junto a REAL E BENEMÉRITA SOCIEDADE PORTUGUESA CAIXA DE SOCORROS D. PEDRO V, inscrita no CNPJ/MF sob o nº 33.601.048/0001-04.

7.1.2. As instalações possuem seguro de edificação e conteúdo (mobiliário e equipamentos), o qual é renovado anualmente.

7.2. Endereço de Contingência:

7.2.1. O Site de contingência está situado à Rua Visconde de Pirajá, nº 152, sala 301, Ipanema, Rio de Janeiro/RJ.

NORMA INTERNA	IDENTIFICAÇÃO	PÁG.
CONTINGÊNCIA E CONTINUIDADE DE NEGÓCIOS	NI-REIT-09.01	5 de 8

8. PLANO DE CONTINGÊNCIA

Uma vez classificado os tipos de riscos, bem como definida a “Equipe de Contingência”, a REIT detalha abaixo o Plano de Contingência considerando cada tipo de intercorrência:

8.1. Falta de energia elétrica

Estabelecimento de trabalho remoto (home office), uma vez que todo o servidor da REIT possui sistema de No-Break e pode ser acessado remotamente via VPN, o qual cada Colaborador possui seu login individual de usuário. Caso seja necessária, por qualquer motivo, a execução de trabalho em conjunto presencial, os Colaboradores da REIT irão se reunir em espaços de coworking que possuam ambiente e infraestrutura para tanto, até a normalização da situação.

8.2. Falta do abastecimento de água

Estabelecimento de trabalho remoto (home office), uma vez que todo o servidor da REIT possui sistema de No-Break e pode ser acessado remotamente via VPN, o qual cada Colaborador possui seu login individual de usuário. Caso seja necessário por qualquer motivo a execução de trabalho em conjunto presencial, os Colaboradores da REIT irão se reunir em espaços de coworking que possuam ambiente e infraestrutura para tanto, até a normalização da situação;

8.3. Paralisação de transporte público

Estabelecimento de trabalho remoto (home office), uma vez que todo o servidor da REIT possui sistema de No-Break e pode ser acessado remotamente via VPN, o qual cada Colaborador possui seu login individual de usuário;

8.4. Interdições pelas autoridades do prédio ou do entorno dos escritórios da REIT

Estabelecimento de trabalho remoto (home office), uma vez que todo o servidor da REIT possui sistema de No-Break e pode ser acessado remotamente via VPN, o qual cada Colaborador possui seu login individual de usuário. Caso seja necessário por qualquer motivo a execução de trabalho em conjunto presencial, os Colaboradores da REIT irão se reunir em espaços de coworking que possuam ambiente e infraestrutura para tanto, até a normalização da situação;

8.5. Pandemias

Estabelecimento de trabalho remoto (home office), uma vez que todo o servidor da REIT possui sistema de No-Break e pode ser acessado remotamente via VPN, o qual cada Colaborador possui seu login individual de usuário;

8.6. Greves e/ou situações extremas de contingência em que reduzam drasticamente o número de Colaboradores

NORMA INTERNA	IDENTIFICAÇÃO	PÁG.
CONTINGÊNCIA E CONTINUIDADE DE NEGÓCIOS	NI-REIT-09.01	6 de 8

Estruturação e garantia de manutenção mínima de Colaboradores suficientes para a execução funcional das atividades desenvolvidas pela REIT, nos termos definidos da cláusula 8.1 retro.

8.7. Falha nas conexões de rede e/ou falha nos links de internet

A REIT possui 2 (dois) provedores de internet, que em caso de falha de um deles, o outro entra em funcionamento automaticamente. Além disso, a REIT possui uma internet dedicada que possui um prazo reduzido de reestabelecimento de internet. Em caso de períodos longos sem internet, estabelecimento de trabalho remoto (home office), uma vez que todo o servidor da REIT possui sistema de No-Break e pode ser acessado remotamente via VPN, o qual cada Colaborador possui seu login individual de usuário. Caso seja necessário por qualquer motivo a execução de trabalho em conjunto presencial, os Colaboradores da REIT irão se reunir em espaços de coworking que possuam ambiente e infraestrutura para tanto, até a normalização da situação;

8.8. Falha nas linhas telefônicas

Estabelecimento das comunicações via celulares da empresa, e nos casos possíveis, o uso do e-mail para essas, até a normalização da situação;

8.9. Perda de documentos importantes

Possuímos uma política de digitalização de todos os documentos – adicional a guarda física desses se necessário – e um modelo de backup. Esse sistema de proteção digital consiste no servidor fisicamente instalado na REIT, um HD dentro desse servidor físico, e um backup em nuvem desses arquivos. Dessa forma, o plano de contingência é estabelecer procedimento de backup.

8.10. Falhas nos sites das empresas que fornecem sistemas de uso da REIT para realizar operações

Estabelecimento de contato por meio de ligações telefônicas, Skype, WhatsApp, com as casas em que operamos;

8.11. Incêndio

Estabelecimento de trabalho remoto (home office), uma vez que todo o servidor da REIT possui sistema de Back-Up em “nuvem” e pode ser acessado remotamente via VPN, o qual cada Colaborador possui seu login individual de usuário. Caso seja necessário por qualquer motivo a execução de trabalho em conjunto presencial, os Colaboradores da REIT irão se reunir em espaços de coworking que possuam ambiente e infraestrutura para tanto, até a normalização da situação;

8.12. Alagamento

Estabelecimento de trabalho remoto (home office), uma vez que todo o servidor da REIT possui sistema de Back-Up em “nuvem” e pode ser acessado remotamente via VPN, o qual cada Colaborador possui seu login individual de usuário. Caso seja necessário por qualquer motivo a execução de trabalho em conjunto

NORMA INTERNA	IDENTIFICAÇÃO	PÁG.
CONTINGÊNCIA E CONTINUIDADE DE NEGÓCIOS	NI-REIT-09.01	7 de 8

presencial, os Colaboradores da REIT irão se reunir em espaços de coworking que possuam ambiente e infraestrutura para tanto, até a normalização da situação;

8.13. Ataques virtuais/hacker

A princípio, cabe ressaltar que não ficaríamos sem operar mesmo que nossos sistemas e computadores fossem atacados, uma vez que as operações feitas pela REIT nas carteiras dos clientes são realizadas via sistemas das Instituições Financeiras com as quais trabalhamos. Sendo estas sempre monitoradas por meio de nosso processo de KYP, descrito em política própria, que garante que os colaboradores com quem trabalhamos tenham estrutura e meios de funcionamento em caso de ocorrências de contingências. Em caso de perda dos arquivos, conforme já adiantado, temos backup do servidor e backup em nuvem. Qualquer outro acontecimento que gere impacto no desempenho das atividades necessárias para a continuidade do negócio será objeto de determinação de ativação Plano de Contingência e deliberação de plano de ação imediato pela Equipe de Contingência já estabelecida nessa política.

9. TESTES DE CONTINGÊNCIA

9.1. A REIT dispõe de um cronograma anual de testes de contingência. Referidos testes são realizados em julho, sendo:

9.1.1. Testes de acesso remoto aos sistemas e arquivos.

9.1.2. Simulação de queda de energia ou indisponibilidade total de acesso ao endereço sede com as pessoas chaves acessando e executando as atividades críticas do endereço de contingência.

9.2. Os Testes de Contingência devem ser realizados pela Diretoria de Administração e Compliance, em comum acordo com o Diretor Superintendente e de Investimentos, sem prévio aviso aos demais colaboradores, que devem ser surpreendidos pelo teste para que haja simulação real de ocorrência.

10. ATIVIDADES CRÍTICAS

10.1. As atividades críticas abaixo são as que estão inseridas no escopo deste plano de continuidade, a saber:

ATIVIDADE CRÍTICA	PRINCIPAL RESPONSÁVEL	BREVE RESUMO DA ATIVIDADE
Aplicações diárias	Diretoria Administrativa Operacional	Realizar as operações de aplicações diárias nos patrimônios separados nas emissões, de forma a cumprir a liquidação dos mesmos.

NORMA INTERNA	IDENTIFICAÇÃO	PÁG.
CONTINGÊNCIA E CONTINUIDADE DE NEGÓCIOS	NI-REIT-09.01	8 de 8

10. DISPOSIÇÕES GERAIS

11.1. Este Manual será atualizado ordinariamente a cada 24 meses e extraordinariamente quando houver alterações relacionadas à contingência e continuidade de negócios, seguindo o mesmo fluxo de aprovação e divulgação.