POLÍTICA

PCN – PLANO DE CONTINUIDADE DE NEGÓCIOS

REVISÃO		PÁGINAS ALTERADAS	ÁREA RESPONSÁVEL	DESCRIÇÃO DA ALTERAÇÃO
Nº	DATA			
01	01/03/16	-	TI e Gerenciamento de Riscos	Publicação
02	24/10/17	Todas	TI e Gerenciamento de Riscos	Alterações Técnicas
03	15/01/19	Todas	TI e Gerenciamento de Riscos	Alterações Técnicas
04	21/01/20	4	TI e Gerenciamento de Riscos	Complemento das responsabilidades da área de Gerenciamento de Riscos
05	07/01/22	Todas	Governança de TI	Atualização de normativos revogados e revisão periódica.
06	06/10/23	-	Governança de TI	Revisão periódica
07	13/09/24	3 e 4	Governança de TI	Inclusão de cenário de interrupção

Esta Política será revisada a cada 12 (doze) meses ou sempre que houver alguma alteração na diretriz descrita.

1. OBJETIVO

Esta Política descreve os planos de contingência implantados nas empresas do Grupo StoneX no Brasil, com o objetivo de evitar que suas atividades sejam interrompidas em caso de falhas ou desastres significativos, minimizando seus impactos e atendendo as regulamentações vigentes.

2. ABRANGÊNCIA

Todas as empresas do Grupo StoneX no Brasil.

3. LEGISLAÇÃO RELACIONADA

- Resolução CVM 35/2021;
- Resolução CMN 4.557/2017;
- Resolução CMN 4.968/2021;
- Ofício Circular 053/2012-DP, Itens 2.5.6 e 2.5.7;
- Decreto nº 63.911 de 10/12/2018;
- Lei Federal 6.514/1977 NR 23.

4. DEFINIÇÕES

4.1. SIGLAS & TERMINOLOGIA

4.1.1. Alta Administração – Corpo formado pelos diretores estatutários das empresas do Grupo StoneX no Brasil.

4.1.2. Call Tree - é a forma de comunicação utilizada pelo Grupo StoneX em casos de emergência ou situações que demandem a comunicação entre os funcionários.

4.1.3. CVM - Comissão de Valores Mobiliários;

4.1.4. GRC - Sigla em inglês que remete à área subordinada ao time global de "*Governance, Risk and Compliance"*.

4.1.5. PCN – Plano de Continuidade de Negócios

4.1.6. T.I. - Tecnologia da informação

4.2. ÁREAS ENVOLVIDAS NO PROCESSO

4.2.1. Área Responsável

- Governança de TI, Risco, Conformidade e Resiliência de Negócios

4.2.2. Áreas Suporte

- Alta Administração
- Área de Marketing
- Áreas gestoras de processos críticos

5. DISPOSIÇÕES

5.1. DIRETRIZES

5.1.1. O PCN deve abranger minimamente os 7 (sete) principais cenários de interrupção, sendo eles:

a. Perda de TI / Aplicativos - Incidentes de infra-estrutura podem incluir a perda de sistemas e aplicativos importantes, acesso à Internet ou qualquer outro problema relacionado a TI;

b. Perda de Telefones / Comunicações - Incidentes de infra-estrutura relacionados à perda repentina de capacidade de usar telefones ou sistemas / dispositivos de comunicação;

c. Perda de Equipe - Incidentes de pessoal significa uma perda repentina de pessoal que torna os membros-chave indisponíveis ou causa uma falta significativa de pessoal;

d. Interrupção de energia elétrica - Incidentes de infra-estrutura, como corte de energia, que causa perda de energia em nosso escritório;

e. Perda de instalações - Incidentes nas instalações podem incluir inundação, incêndio, restrição de acesso ou qualquer outro desastre que torne nosso escritório inacessível.

f. Perda de terceiros críticos - Perda de um fornecedor crítico ou terceiro que fornece um serviço ou produto essencial. A perda pode ser serviço do fornecedor, suporte ou relacionado a aplicativos/TI.

g. Pandemia - Interrupções nas operações resultantes da exposição da(s) região/funcionário(s) a um incidente de doença pandêmica.

5.1.2. Os PCNs devem preparar previamente as empresas do Grupo StoneX no Brasil de maneira a manter ativo seus processos e atividades essenciais e recursos críticos após a ocorrência de um evento até o retorno das operações a um nível aceitável dentro de um prazo desejável.

5.1.3. A StoneX deve revisar anualmente ou quando necessário sua matriz de PCN, assegurando a identificação, classificação e documentação dos processos críticos de negócio, bem como avaliar os potenciais efeitos da interrupção destes processos;

5.1.4. Anualmente deve ser formalizada e aprovada, junto à Alta Administração, sua matriz PCN, contendo as estratégias para manter o funcionamento parcial dos processos críticos, detalhando os prazos aceitáveis e as ações que serão adotadas até seu o restabelecimento pleno, bem como as comunicações que se fizerem necessárias;

5.1.5. Deve ser registrado em relatório os testes referentes aos planos de continuidade, com periodicidade anual, incluindo avaliação do resultado dos testes e as ações promovidas para aprimoramento do PCN;

5.1.6. O PCN deve considerar inclusive os processos críticos suportados ou executados por intermédio de serviços de terceiros;

5.1.7. A StoneX utiliza uma a plataforma externa para realizar o Call Tree;

5.1.8. Os documentos referentes ao PCN devem estar disponibilizados na plataforma global de políticas e procedimentos para todos os colaboradores;

5.1.9. O não cumprimento de quaisquer políticas, padrões de controle ou procedimentos associados pode resultar em ações disciplinares, incluindo a rescisão do contrato de trabalho para funcionários ou rescisão do contrato para contratados, parceiros,

consultores ou outras entidades. Ações legais também podem ser tomadas por violações das leis e regulamentos aplicáveis;

5.1.10. Os pedidos de isenções a esta política e quaisquer políticas, padrões ou procedimentos associados devem ser submetidos ao departamento de Governança de TI para processamento e revisão. Exceções só serão permitidas após o recebimento da aprovação por escrito tanto da empresa quanto do proprietário do aplicativo ou tecnologia.

5.2. RESPONSABILIDADES

5.2.1. Área de Gestão de Crise (Governança de TI) deve:

- Entender as necessidades sistêmicas básicas para suportar os processos críticos e providenciar mecanismos de contingência, contemplando infraestrutura e sistemas;
- Atender, na medida do possível, os requisitos de Segurança da Informação regulados para o setor correspondente ao processo crítico;
- Efetuar os procedimentos de contingência, conforme prioridade definida pela Alta Administração, suportar as necessidades sistêmicas dos gestores de processos críticos no momento da crise e efetuar os procedimentos de restabelecimento do sistema principal.

5.2.2. Àrea de TI Sistema e Infra deve:

- Providenciar os backups periódicos para assegurar a disponibilidade das informações;

5.2.3. A Alta Administração deve:

- Orientar os colaboradores em relação as diretrizes estratégicas no momento de crise;
- Aprovar os estudos de Impacto, Planos de Continuidade de Negócios, Planos de Comunicação e orientar os gestores para a correta aplicação das diretrizes definidas;
- Aprovar os investimentos necessários para atender os PCNs;

- Declarar o momento do ingresso ao Plano de Continuidade de Negócios, no caso de crise, bem como declarar a retomada dos procedimentos padrão;

- Aprovar os relatórios referentes aos PCNs.

5.2.4. Área de Gerenciamento de Riscos deve:

- Suportar a área de tecnologia da informação no aculturamento dos colaboradores da instituição referente a correta adoção dos procedimentos de Continuidade de Negócios;

- Suportar a ára de tecnologia da informação na execução do plano de contingência.

5.2.5. Área de Marketing deve:

- Assegurar a existência de Planos de Comunicação contemplando: imprensa, colaboradores, fornecedores, clientes, reguladores e auditorias;

- Manter atualizada a lista oficial de Porta Vozes, inclusive em momento de crise.

5.2.6. Áreas gestoras de processos críticos devem:

- Avaliar e definir quais são os processos críticos sob sua gestão através da metodologia definida previamente definida;

- Manter-se cientes de suas responsabilidades no caso de um incidente e participar, conforme necessidade, como parte de uma equipe de resposta ou recuperação em uma situação de teste ou exercício;

- Descrever detalhadamente os procedimentos que devem ser adotados para realização dos processos críticos no momento de crise, mantendo-os devidamente atualizados;

- Participar dos testes periódicos e avaliar o atingimento dos resultados esperados;

- Acionar os colaboradores sob sua responsabilidade através da Call Tree;

- Respeitar as diretrizes definidas no PCN.