POLÍTICA

GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

REVISÃO		PÁGINAS ALTERADAS	ÁREA RESPONSÁVEL	DESCRIÇÃO DA ALTERAÇÃO
Nº	DATA			
01	28/04/19	-	Governança de TI	Criação e Publicação
02	02/06/20	-	Governança de TI	Revisão Periódica
03	24/08/22	-	Governança de TI	Revisão Periódica
04	06/10/23	-	Governança de TI	Revisão Periódica
05	10/10/24	-	Governança de TI	Revisão Periódica e atualização de Regulamentação
06	05/09/25	4, 5, 6 e 7	Compliance	Adoção de recomendações regulatórias

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

1. OBJETIVO

Estabelecer diretrizes para o gerenciamento de resposta a incidentes de segurança documentada e formalizada, onde a conformidade com a política e com os procedimentos de suporte colaboram para garantir a segurança dos recursos de sistema da Empresa.

2. ABRANGÊNCIA

Esta política abrange todos os recursos de sistema pertencentes, operados, mantidos e controlados pela Empresa e todos os outros recursos, internos e externos, que interagem com tais sistemas, quando utilizados pelas empresas do grupo StoneX sediadas no Brasil.

3. LEGISLAÇÃO RELACIONADA

- Resolução CMN 4.893/21;
- Política de PCN – Plano de Continuidade de Negócios (POL-045);
- Cadeia de Valor;
- Política de Contratação de Serviços Terceirizados (POL-009);
- Norma de Aprovação ou Alteração de Produtos (NOP-031);
- Plano de Gestão de Incidentes de Segurança da Informação;
- Resolução CVM 35/2021;
- Roteiro PQO (Programa de Qualificação Operacional).

4. DEFINIÇÕES

4.1. SIGLAS & TERMINOLOGIA

4.1.1. Agentes afetados - clientes internos ou externos e entidades administradoras de mercado organizado que tenham suas atividades afetadas pela instabilidade/indisponibilidade de um sistema;

4.1.2. CMN – Conselho Monetário Nacional

4.1.3. IRR – Relatório de Respostas a Incidentes

4.1.4. SFN – Sistema Financeiro Nacional

4.1.5. PCN – Plano de Continuidade de Negócio

4.1.6. Dispositivos de Rede - firewalls, roteadores, comutadores, balanceadores de carga e outros dispositivos de rede.

4.1.7. Incidente de segurança - um incidente, evento ou atividade real ou suspeita que comprometa a segurança dos sistemas de TI da Empresa ou de seus dados.

4.1.8. Servidores – hardware e os sistemas operacionais e aplicativos neles contidos, incluindo servidores físicos e virtuais.

4.1.9. Resposta a incidentes - Medidas tomadas para a preparação, detecção, resposta, contenção e recuperação de um incidente de segurança, além de todas as atividades pós-incidente e de conscientização.

4.1.10. Usuários - qualquer indivíduo com direitos de acesso remoto aprovado pela Empresa e que tenha passado por todas as etapas necessárias de provisionamento. Os usuários geralmente incluem, mas não estão limitados a usuários, consultores, fornecedores e contratados.

4.2. ÁREAS ENVOLVIDAS NO PROCESSO

4.2.1. Área Responsável

- Governança de TI

4.2.2. Áreas Suporte

- Riscos
- Controles Internos
- Compliance
- Jurídico

5. DISPOSIÇÕES

O plano de resposta a incidentes deve ser visto como um conjunto de procedimentos para avaliação de um incidente de segurança, que inclui preparação, detecção, resposta, contenção, recuperação, comunicação, atividades pós-incidente necessárias, incluindo treinamentos e testes.

5.1. DIRETRIZES

5.1.1. A Política do plano de continuidade de negócios (POL-045) determina a realização de análise de impacto (BIA) para identificar as atividades críticas para o negócio, bem determina sua atualização periódica. Nos detalhamentos de cada atividade crítica são estabelecidos os responsáveis, procedimentos de contingência, critérios, impactos, comunicações relevantes e prazos para recuperação e reinício de cada atividade, em específico.

5.1.2. Devem ser implementados sistemas de salvaguarda e mecanismos de controle para proteção dos recursos de sistema em toda a empresa, reforçando os sistemas críticos quanto à segurança da informação.

5.1.3. Os usuários autorizados devem adotar as devidas diligências para detectar um incidente ou anormalidades no sistema.

5.1.4. O plano de de ação e resposta a incidentes, estabelecido pela Empresa, deve ser seguido para minimizar o impacto do incidente na infraestrutura crítica de rede e sistema da Empresa, devendo ser testado anualmente.

5.1.5. Uma vez que o sistema afetado é restabelecido, deve ser realizada uma análise técnica para examinar detalhadamente a integridade dos dados.

5.1.6. Deve ser atribuído o nível de impacto causado pelo incidente de acordo com parâmetros definidos internamente, onde os graus de risco são por definição:

i. Alto (Impacto Grave) – Incidente que afeta sistemas relevantes ou informações críticas, com potencial para gerar impacto negativo sobre a receita ou clientes.

ii. Médio (Impacto Significativo) – Incidente que afeta sistemas ou informações não críticas, sem impacto negativo à receita ou clientes; investigações de colaboradores com validade limitada devem ser tipicamente classificadas neste nível.

iii. Baixo (Impacto Mínimo) – Possível incidente, sistemas não críticos; investigações de incidentes ou de colaboradores; investigações de longo prazo envolvendo pesquisa extensa e/ou trabalho forense detalhado.

5.1.7. Apenas incidentes que afetem serviços considerados relevantes, de acordo com a cadeia de valor estabelecida em estudo interno, são abrangidos pela Resolução CMN 4.893/21.

5.1.8. Para os incidentes de risco médio ou alto, a área de gestão de crise deve ser comunicada, em até 4h da identificação do incidente, reportando a indisponibilidade

ou instabilidade do sistema, contendo informações tais como: (i) sistema afetado; (ii) público impactado; (iii) estimativa inicial de impactos; (iv) estimativa de prazo para resolução – se houver; (v) minuta de comunicado aos clientes impactados, autoridades competentes, reguladores e ou supervisores, autorreguladores e/ou entidades administradoras de mercado, bem como mídia e/ou imprensa – se for o caso.

5.1.9. A Área de Gestão de Crise, em conjunto com a Alta Administração, apoiadas pelas áreas de suporte, deliberarão as providências e orientações que serão adotadas, bem como o tipo e periodicidade de acompanhamento até a regularização da situação de crise.

5.1.10. Após a resolução do incidente, um Relatório de Resposta a Incidentes (IRR) deverá ser elaborado, arquivado pelo prazo regulatório e disponibilizado para eventual gerenciamento.

5.1.11. Devem ser estabelecidos processos, testes, métricas, indicadores, identificação, avaliação e correção de eventuais deficiências, com base no Procedimento de Contratação de Fornecedores, para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

5.1.12. A comunicação de novos fornecedores, em atendimento a Resolução CMN 4.893/21, ao BACEN, deve ocorrer em até 10 (dez) dias após sua contratação ou da alteração contratual relevante.

5.2. RESPONSABILIDADES

5.2.1. Área de Governança de TI

a) Provisão de orientação, liderança e suporte para o programa de resposta a incidentes da Empresa;

b) estabelecimento e aprimoramento contínuo de programas e sistemas para prevenção de incidentes de Segurança da Informação;

c) acompanhamento e reporte do monitoramento ativo e contínuo dos sistemas de segurança;

d) desenvolvimento e atualização do programa de gestão de incidentes;

e) elaboração de treinamentos e programas de capacitação, contemplando avaliação periódica de aprendizagem;

f) aplicar o programa de gerenciamento de crises, caso ocorram incidentes;

g) elaboração do relatório anual sobre programa de gestão de incidentes de segurança da informação e relatórios sobre incidentes classificados como risco alto;

h) Acompanhar e reportar os relatórios de PEN Test (teste de invasão), quando aplicável.

5.2.2. Área de Gerenciamento de Riscos

a) Monitoramento da matriz de risco, dados os sistemas expostos a riscos cibernético;

b) incluir a avaliação de risco cibernético na matriz de PCN;

c) fomentar a criação de plano de resposta a incidentes, junto aos responsáveis;

d) aprovação da classificação de incidentes, quando classificados como relevantes.

5.2.3. Área de Controles Internos

a) Mapeamento de controles internos para os sistemas expostos a risco cibernético.

5.2.4. Área de Compliance

i) Reporte dos incidentes relevantes junto às autoridades competentes, regulador, supervisor, autorregulador e/ou entidade administradora de mercado, conforme deliberação da área de gerenciamento de crises ou para o cumprimento de obrigações regulatórias.

5.2.5. Departamento Jurídico

a) Revisões contratuais de provedores dos sistemas utilizados, associados aos serviços relevantes, assegurando a formalização de SLAs (nível de resposta a incidentes).

5.2.6. Área de TI

a) Monitorar a disponibilidade dos sistemas críticos, reportando aos responsáveis incidentes ou detalhes técnicos para aprimorar o ambiente debilitado;

b) Municiar à área de gerenciamento de crise com informações técnicas sobre os incidentes relevantes, bem como os esforços necessários e prazos para recuperação das atividades;

c) Priorizar as atividades e sistemas deliberados pela área de gerenciamento de crises.

5.2.7. Área de Marketing

a) Comunicar aos agentes afetados sobre a indisponibilidade ou instabilidade dos sistemas críticos, conforme deliberado pela Gestão de Crise.