

StoneX [®]	POLÍTICA	Código: POL-052/05
	Gestão de Incidentes de Segurança da Informação	Vigor em: 14/12/2024
		Pág.: 1 / 5

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

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

StoneX®	POLÍTICA	Código: POL-052/05
	Gestão de Incidentes de Segurança da Informação	Vigor em: 14/12/2024
		Pág.: 2 / 5

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

4. DEFINIÇÕES

4.1. SIGLAS & TERMINOLOGIA

4.1.1. CMN – Conselho Monetário Nacional

4.1.2. IRR – Relatório de Respostas a Incidentes

4.1.3. SFN – Sistema Financeiro Nacional

4.1.4. PCN – Plano de Continuidade de Negócio

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

4.1.6. 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.

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

StoneX®	POLÍTICA	Código: POL-052/05
	Gestão de Incidentes de Segurança da Informação	Vigor em: 14/12/2024
		Pág.: 3 / 5

4.1.8. 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.

4.1.9. 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. 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.

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

StoneX®	POLÍTICA	Código: POL-052/05
	Gestão de Incidentes de Segurança da Informação	Vigor em: 14/12/2024
		Pág.: 4 / 5

- 5.1.3. 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.
- 5.1.4. Uma vez que o sistema afetado é restabelecido, deve ser realizada uma análise técnica para examinar detalhadamente a integridade dos dados.
- 5.1.5. 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.
- 5.1.6. 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.
- 5.1.7. O incidente classificado como de “risco alto” deve ser comunicado de acordo com procedimentos internos, podendo envolver instituições do SFN e reguladores externos de acordo com a categorização do incidente.
- 5.1.8. Após a resolução do incidente, um Relatório de Resposta a Incidentes (IRR) deverá ser elaborado e disponibilizado para gerenciamento.
- 5.1.9. 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. A comunicação de novos fornecedores ao BACEN deve ocorrer, no mínimo, sessenta dias antes da contratação do serviço.

StoneX [®]	POLÍTICA	Código: POL-052/05
	Gestão de Incidentes de Segurança da Informação	Vigor em: 14/12/2024
		Pág.: 5 / 5

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) 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 e avaliação periódica de pessoal;
- f) aplicar o programa de gestão 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.

5.2.2. Área 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) criação de plano de resposta a incidentes;
- 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

- a) Reporte dos incidentes relevantes junto ao regulador.

5.2.5. Departamento Jurídico

- a) Revisões contratuais de provedores dos sistemas utilizados, associados aos serviços relevantes.