POLÍTICA DE SEGURANÇA CIBERNÉTICA

RESUMO

Esta Política aborda as diretrizes, atribuições e responsabilidades no processo de Segurança Cibernética da Stone Pagamentos S.A. “Stone”.

ÍNDICE

1. TERMOS E DEFINIÇÕES

Ameaça: Fonte potencial de dano; elemento ou atividade que possui potencial de causar uma consequência.

Colaborador: empregado em regime CLT ou estagiário (aquele que possui um termo de compromisso firmado entre a empresa e a instituição de ensino).

ETIR - Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais: Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança da informação.

Evento de segurança da informação: Ocorrência identificada em um sistema, serviço ou rede que indica uma possível violação da Política de segurança da informação ou falha de controles de segurança da informação, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.

Evidência: Dados que apoiam a existência ou a veracidade de alguma coisa.

Incidente: Qualquer ocorrência que não é parte padrão da operação de um serviço e que pode causar uma indisponibilidade, redução na qualidade do mesmo, perda de integridade ou confidencialidade das informações.

Risco Cibernético: Ameaça à confidencialidade, integridade e disponibilidade das informações no Espaço Cibernético.

Terceiros: Pessoas que não possuam vínculo empregatício com a Stone e que não sejam estagiários. Por Terceiros entende-se tanto a entidade, quanto seu representante legal e/ou preposto que prestem ou estejam prestando serviços para a Stone, como os prestadores de serviço em si, parceiros, franquias, fornecedores, auditores ou qualquer outro que se enquadre como trabalhador contratado por outra companhia que não a Stone.

Vulnerabilidade: Brecha sistêmica que permite ataque de exploração ou violação à segurança da informação de uma aplicação/rede.

2. OBJETIVO

Estabelecer as diretrizes para compor um programa de Segurança Cibernética na Stone.

3. ABRANGÊNCIA

Esta Política abrange todas as ferramentas, aplicações, processos e monitoramento de Segurança da Informação e Segurança Cibernética no ambiente da Stone Pagamentos S.A, independente da sua localização física.

4. ATRIBUIÇÕES E RESPONSABILIDADES

4.1. Área de Segurança da Informação

- Realizar a Gestão de Incidentes de Segurança da Informação na Stone.
- Verificar a conformidade desta Política.
- Implantar controles de Segurança da Informação de acordo com as instruções deste regulamento.
- Desenvolver e atualizar, sempre que necessário, as diretrizes gerais para a Gestão de Riscos de Segurança da Informação e Segurança Cibernética.
- Elaborar diretrizes para coleta e preservação de evidências de incidentes de segurança da informação.
- Elaborar diretrizes para comunicação sobre incidentes de segurança da informação.
- Elaborar/aprovar procedimentos técnicos de tratamento de incidentes de segurança da informação, com apoio das áreas da TI da Stone.
- Implementar melhorias no tratamento de incidentes de segurança da informação;
- Proteger o valor e a reputação da Stone.
- Identificar violações de Segurança Cibernética, estabelecendo ações sistemáticas de detecção, tratamento e prevenção de incidentes, ameaças e vulnerabilidades nos ambientes físicos e lógicos, objetivando a mitigação dos riscos cibernéticos, dentre outros.
- Garantir a continuidade de seus negócios, protegendo os processos críticos de interrupções inaceitáveis causadas por falhas ou desastres significativos.
- Atender aos requisitos legais, regulamentares e às obrigações contratuais pertinentes a atividade da empresa.

- Conscientizar, educar e treinar os colaboradores nas suas atividades diárias com foco na Segurança Cibernética.
- Estabelecer e melhorar continuamente um processo de Gestão de Riscos de Segurança Cibernética.

4.2. Gestor de Segurança da Informação

- Atuar como proprietário do Processo de Gestão de Tratamento e Resposta a Incidentes de Segurança da Informação.

4.3. Colaboradores

- Conhecer e cumprir as diretrizes estabelecidas nesta Política.
- Reportar qualquer incidente de Segurança da Informação, mesmo que suposto, o mais rapidamente possível, por meio do canal apropriado.

5. DIRETRIZES

Os incidentes de segurança da informação podem ser notificados por qualquer usuário da Stone ou identificados por áreas da Tecnologia da Informação “TI”.

5.1. Plano de Segurança Cibernética

- Proteger as informações contra acesso, modificações, destruição ou divulgação não autorizada.
- Prover a adequada classificação da informação, sob os critérios de confidencialidade, disponibilidade e integridade.
- Assegurar que os recursos utilizados para o desempenho de sua função sejam utilizados apenas para as finalidades aprovadas pela Stone.
- Garantir que os sistemas e as informações sob responsabilidade da Stone estejam adequadamente protegidos.
- Garantir a continuidade do processamento das informações críticas de negócios.
- Selecionar os mecanismos de segurança da informação, balanceando fatores de riscos, tecnologia e custo.
- Comunicar imediatamente à área de Segurança da Informação, quaisquer descumprimentos da Política Corporativa de Segurança Cibernética.

5.2. Proteção do Ambiente

Devem ser constituídos controles e responsabilidades pela gestão e operação dos recursos de processamento das informações que garantem a segurança na infraestrutura tecnológica de redes locais e internet, através de um gerenciamento efetivo no monitoramento, tratamento e respostas aos incidentes, para minimizar o risco de falhas e a administração segura de redes de comunicações, incluindo a gestão de serviços contratados de processamento e armazenamento de dados e informações em nuvem.

5.3. Segurança Física e Lógica

Os equipamentos e instalações de processamento de informação críticas ou sensíveis devem ser mantidos em áreas seguras, com níveis e controles de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais.

Os requisitos de segurança de sistemas de informação devem ser identificados e acordados antes do seu desenvolvimento e/ou de sua implementação, para que assim possam ser protegidos visando a manutenção de sua confidencialidade, integridade e disponibilidade.

Os colaboradores e terceiros da Stone devem ser treinados periodicamente sobre os conceitos de Segurança da Informação, através de um programa de conscientização.

5.4. Gestão de Acesso

Os acessos às informações devem ser controlados, monitorados, restringidos à menor permissão e privilégios possíveis, revistos periodicamente com a aprovação do gestor do responsável e o da informação, e cancelados tempestivamente ao término do contrato de trabalho do colaborador ou do prestador de serviço.

5.5. Processamento, Armazenamento de Dados e Computação em Nuvem

Conforme a Resolução 3.909/2018 do Banco Central do Brasil, para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, a Stone deve possuir procedimentos efetivos para a aderência às regras previstas na regulamentação em vigor.

5.6. Continuidade de Negócios

O processo de gestão de continuidade de negócios relativo a segurança da informação, deve ser implementado para minimizar os impactos e recuperar perdas de ativos da informação, após um incidente crítico, a um nível aceitável, através da combinação de requisitos como operações, funcionários chaves, mapeamento de processos críticos, análise de impacto nos negócios e testes

periódicos de recuperação de desastres. Incluem-se nesse processo, a continuidade de negócios relativos aos serviços contratados de nuvem e os testes previstos para os cenários de ataques cibernéticos.

6. CONSIDERAÇÕES FINAIS

6.1. **Treinamento**

Um programa de conscientização em Segurança Cibernética à garantia dos objetivos e diretrizes definidos nesta Política é realizado adequando-se às necessidades e responsabilidades específicas de cada colaborador e, onde pertinente, terceiros da Companhia.