Política de Segurança Cibernética

moneycorp
Banco de câmbio

Sumário

1. OBJETIVO

Este documento tem como objetivo informar as principais diretrizes da Política de Segurança da Informação. Esta política suporta a metodologia de riscos da Moneycorp, estabelecendo os fundamentos para um programa de segurança da informação para proteger a instituição, permitindo a implementação de medidas preventivas e detectivas para combater os riscos de segurança cibernética e das informações. Para efeitos desta política, o termo 'segurança da informação' inclui riscos de segurança cibernética.

A política estabelece os requisitos para a conformidade com regulamentações e padrões da indústria, suportando as áreas de negócio, áreas de controle e auditoria corporativa para atingir objetivos estratégicos. A política é suportada pelos requisitos ("normas") e fundamentos que fornecem requisitos adicionais ou orientação para a realização do programa da Moneycorp.

O time executivo da Moneycorp está comprometido com a Política de Segurança da Informação e com a melhoria contínua dos processos associados, tendo designado um diretor estatutário responsável pela política e pela execução do plano de ação e respostas a incidentes cibernéticos.

2. CONCEITOS

A Segurança Cibernética, constitui-se da preservação das propriedades da informação, notadamente sua confidencialidade, integridade e disponibilidade, permitindo o uso e o compartilhamento da informação de forma controlada, bem como do monitoramento e tratamento de incidentes provenientes de ataques cibernéticos.

Confidencialidade: garantia de que a informação é acessível somente as pessoas autorizadas.

Integridade: salvaguarda da exatidão e completeza da informação e dos métodos de processamento.

Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Riscos Cibernéticos: Riscos de ataques cibernéticos, oriundos de malware, técnicas de engenharia social, invasões, ataques de rede (DDoS e Botnets), fraudes externas, desprotegendo dados, redes e sistemas da empresa causando danos financeiros e de reputação consideráveis.

Malwares:

- Vírus: software que causa danos a máquina, rede, softwares e banco de dados;
- Cavalo de Troia: aparece dentro de outro software e cria uma porta para a invasão do computador;

- Spyware: software malicioso para coletar e monitorar o uso de informações;

- Ransomware: software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.

Engenharia Social:

- Pharming: direciona o usuário para um site fraudulento, sem o seu conhecimento;

- Phishing: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;

- Vishing: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;

- Smishing: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais;

- Acesso pessoal: pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.

Fraudes Externas e invasões: Realização de operações por fraudadores, utilizando-se de ataques em contas bancárias, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Ataques DDoS e Botnets: Ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos Botnets, o ataque vem de um grande número de computadores infectados utilizados para criar e enviar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.

3. FUNDAMENTOS E APLICABILIDADE

A política está estruturada para fornecer os requisitos necessários para que a Moneycorp se prepare, previna, detecte, responda e recupere-se das ameaças. O programa fornece soluções e utiliza técnicas avançadas para prevenir que ameaças de segurança da informação abalem a confiança do cliente e interrompam as operações de negócios.

Como parte da infraestrutura, a Moneycorp atualiza sua política, controles e processos em toda a instituição. Esta política aplica-se aos sistemas de informação e ativos gerenciados internamente ou como parte de relações de terceiros, quando da contratação e uso de serviços de processamento e/ou armazenamento de dados dos nossos serviços relevantes.

4. REQUISITOS

As leis aplicáveis, regras e regulamentos são alinhados com a política em normas e fundamentos, conforme necessário para garantir a conformidade. Estes requisitos abrangem medidas preventivas, detectivas/de rastreabilidade e corretivas, voltadas à gestão do ambiente cibernético, para mitigação de potenciais ameaças / incidentes de segurança cibernética e redução de pontos de vulnerabilidades.

Apresenta-se abaixo a lista dos principais domínios, que visam garantir a confidencialidade, integridade e disponibilidade das informações e dos sistemas que suportam os serviços relevantes:

- Segurança da Aplicação;
- Criptografia;
- Proteção dos Dados;
- Segurança do Usuário Final;
- Gestão de Identidades e Acessos;
- Gerenciamento do Programa de Segurança da Informação;
- Infraestrutura;
- Monitoramento, Resposta e Forense;
- Segurança de Terceiros; e

Para isso, resumem-se os seguintes requisitos e controles que permeiam este objetivo:

- Autenticação, criptografia, controles de acesso e de segmentação da rede de computadores; segregação dos dados dos clientes da instituição por meio de controles físicos ou lógicos
- Classificação da Informação;
- Prevenção e detecção de invasão e vazamento de informações;
- Realização periódica de testes e varreduras para detecção de vulnerabilidades;
- Proteção contra softwares maliciosos;
- Mecanismos de rastreabilidade da informação;

- Manutenção de cópias de segurança (back-up);

- Secure by Design - desenvolvimento seguro de sistemas e para implementação de tecnologias;

- Gestão de incidentes, plano de ação e de respostas a incidentes cibernéticos;

- Conscientização de usuários, clientes e fornecedores, contemplando-se iniciativas de conscientização da cultura de segurança cibernética, incluindo a implementação de programas de treinamento e de avaliação periódica da conscientização de colaboradores, bem como iniciativas de conscientização sobre segurança cibernética para clientes, empresas terceiras e prestadores de serviços relevantes; e

- Continuidade de Negócio.

- Iniciativas para compartilhamento de informações sobre os incidentes relevantes com outras instituições financeiras autorizadas pelo Banco Central do Brasil ocorridos na Moneycorp e/ou comunicados por terceiros que prestam serviços relevantes de processamento de dados a Moneycorp.

- Elaboração de cenários de incidentes cibernéticos para a realização de testes de continuidade de negócio.

5. Contato

Através dos canais de atendimento ao cliente disponíveis no site da Moneycorp podem ser comunicados eventuais incidentes que forem identificados.

***Declaramos que a presente é parte da Política de Segurança Cibernética, que foi atualizada e aprovada pela Diretoria em 08/03/2021.**