Política de Segurança Cibernética

SUMÁRIO

INTRODUÇÃO 3

OBJETIVO 3

ABRANGÊNCIA 4

DOCUMENTOS DE REFERÊNCIA 4

PROCEDIMENTOS E CONTROLES PARA REDUÇÃO DE VULNERABILIDADES 4

CONTROLE DE INCIDENTES RELEVANTES 5

DIRETRIZES 5

Elaboração de cenários de incidentes considerados no PCN 5

Definição de procedimentos e controles voltados à prevenção e ao tratamento de incidentes a serem adotados por empresas prestadoras de serviços 5

Classificação de dados e informações 5

MECANISMOS PARA DISSEMINAÇÃO DA CULTURA DE SEGURANÇA CIBERNÉTICA 6

Programas de capacitação e avaliação periódica 6

Melhoria contínua 6

Compartilhamento de informações sobre os incidentes relevantes 6

GESTÃO DE RISCOS CIBERNÉTICOS 6

CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM 7

DISPOSIÇÕES GERAIS 7

INTRODUÇÃO

Este documento visa descrever diretrizes sobre a Política de Segurança Cibernética da **CREDIFIT SOCIEDADE DE CRÉDITO DIRETO S.A. ("CREDIFIT")** e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem. Tais diretrizes orientam o uso aceitável dos ativos de informação e/ou tecnológicos da instituição, baseado nos princípios de confidencialidade, integridade e disponibilidade, garantindo esses três pilares:

- Confidencialidade: condição em que apenas usuários autorizados têm permissão para acessar a informação;
- Integridade: condição em que apenas alterações autorizadas podem ser realizadas na informação;
- Disponibilidade: condição em que a informação deve ser disponível para usuários autorizados quando solicitado.

OBJETIVO

(i) Estabelecer diretrizes e normas de Segurança da Cibernética que permitam aos colaboradores da **CREDIFIT** adotar padrões de comportamentos seguros, adequados às suas metas e necessidades;

(ii) Prevenir possíveis causas de incidentes de segurança cibernética;

(iii) Capacitar os colaboradores no que se refere à prevenção, detecção e resposta a incidentes de segurança cibernética;

(iv) Orientar os colaboradores quanto a adoção de controles e processos para atendimento dos requisitos de segurança cibernética;

(v) Resguardar ativos de informação e / ou tecnológicos da **CREDIFIT**, garantindo requisitos de confidencialidade, integridade e disponibilidade;

(vi) Minimizar os riscos de perdas financeiras, da confiança de clientes ou de qualquer outro impacto negativo no negócio da **CREDIFIT** como resultado de falhas de segurança.

ABRANGÊNCIA

Esta política é aplicável a todos os colaboradores da **CREDIFIT**, no exercício de suas funções, inclusive prestadores de serviços, fornecedores e parceiros de negócios que se vinculam à instituição.

DOCUMENTOS DE REFERÊNCIA

- RESOLUÇÃO CMN Nº 4.893/21
- RESOLUÇÃO BCB Nº 85/21

PROCEDIMENTOS E CONTROLES PARA REDUÇÃO DE VULNERABILIDADES

A **CREDIFIT** é responsável pela confiabilidade, pela integridade, pela disponibilidade, pela segurança e pelo sigilo em relação aos serviços contratados, bem como pelo cumprimento da legislação e da regulamentação em vigor.

Para reduzir a vulnerabilidade do cliente a incidentes cibernéticos e atender aos demais objetivos de segurança cibernética, são adotados procedimentos e controles, conforme porte e perfil de risco, considerando:

A. Regras para controlar complexidade e qualidade das credenciais utilizadas para acesso aos sistemas e aos dados sob responsabilidade do cliente;
B. Recursos criptográficos adequados para garantir a privacidade, integridade e não-repúdio dos dados mantidos;
C. Solução de proteção contra ameaças avançadas em e-mail e no acesso a sites na internet, solução de proteção de dispositivos, antivírus de borda;
D. Manutenção de cópias de segurança dos dados e das informações.
E. Implantação e manutenção de firewall para proteção a ataques cibernéticos;
F. Gestão de acesso.

Os procedimentos e controles são aplicados para sistemas de informação desenvolvidos internamente ou adquiridos de terceiros. As diretrizes destacadas contemplam procedimentos e controles em níveis de complexidade, abrangência e precisão compatíveis com os utilizados pelo próprio cliente.

CONTROLE DE INCIDENTES RELEVANTES

A **CREDIFIT** realiza o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as suas atividades.

DIRETRIZES

Elaboração de cenários de incidentes considerados no PCN

Os cenários de incidentes considerados no PCN são elaborados com equipe multidisciplinar.

Definição de procedimentos e controles voltados à prevenção e ao tratamento de incidentes a serem adotados por empresas prestadoras de serviços

Existem procedimentos e controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da **CREDIFIT**;

Classificação de dados e informações

Classificar dados de acordo com sua criticidade e sensibilidade para o negócio e seus clientes, de forma que a segurança adequada seja aplicada a fim de reduzir vulnerabilidades, conforme os níveis abaixo:

a. Confidencial;
b. Restrito ou de Uso Interno;
c. Público.

MECANISMOS PARA DISSEMINAÇÃO DA CULTURA DE SEGURANÇA CIBERNÉTICA

Programas de capacitação e avaliação periódica

Segurança Cibernética é parte da cultura empresarial da **CREDIFIT**. Com isto em consideração, o assunto é abordado em diversos ciclos:

a. Onboarding de todos os colaboradores diretos;
b. Anualmente, em evento específico de treinamento sobre a política;
c. Vídeos disponíveis nos canais compartilhados;
d. Reuniões periódicas.

Melhoria contínua

Melhoria contínua é parte da cultura empresarial da **CREDIFIT**. Com isto em consideração, qualquer desvio ou sugestão de melhoria relacionado ao assunto de segurança cibernética é registrado na ferramenta de gestão de atividades, e priorizada para sua realização. A alta direção está comprometida com o assunto.

Compartilhamento de informações sobre os incidentes relevantes

A **CREDIFIT** pratica o compartilhamento de informações sobre os incidentes relevantes com as instituições de pagamento e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

GESTÃO DE RISCOS CIBERNÉTICOS

A gestão de riscos cibernéticos é uma responsabilidade de todos os envolvidos com a **CREDIFIT**, sob coordenação da área de Tecnologia. Este processo identifica os requisitos de segurança relacionados às necessidades da instituição. A gestão de riscos cibernéticos é contínua e define contextos internos e externos para avaliação, além de tratar dos riscos identificados de modo que sejam reduzidos a níveis aceitáveis.

CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM

A **CREDIFIT**, em seu fluxo de contratação de serviços de terceiros, considera cláusulas específicas para aqueles que prestam serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, no País ou no exterior, para assegurar o cumprimento da legislação e da regulamentação em vigor.

DISPOSIÇÕES GERAIS

As políticas da **CREDIFIT** sobre de gerenciamento de riscos dispõe, no tocante à continuidade dos serviços de pagamento prestados, sobre:

I. O tratamento dos incidentes relevantes relacionados com o ambiente cibernético;
II. Procedimentos a serem seguidos no caso da interrupção de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem contratados, abrangendo cenários que considerem a substituição da empresa contratada e o reestabelecimento da operação normal da instituição;
III. Cenários de incidentes considerados nos testes de continuidade de serviços de pagamento prestados.

Os procedimentos da **CREDIFIT** para gerenciamento de riscos, no tocante à continuidade dos serviços de pagamento prestados, especificam:

I. O tratamento previsto para mitigar os efeitos dos incidentes relevantes e da interrupção dos serviços relevantes de processamento, armazenamento de dados e de computação em nuvem contratados;
II. O prazo estipulado para reinício ou normalização das atividades ou dos serviços relevantes interrompidos; e

III. A comunicação tempestiva ao Banco Central do Brasil das ocorrências de incidentes relevantes e das interrupções dos serviços relevantes, que configurem situação de crise, bem como das providências para o reinício das suas atividades.

A **CREDIFIT** utiliza mecanismos de acompanhamento e de controle com vistas a assegurar a implementação e a efetividade da política de segurança cibernética, do plano de ação e de resposta a incidentes e dos requisitos para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, incluindo:

I. A definição de processos, testes e trilhas de auditoria;
II. A definição de métricas e indicadores adequados; e
III. A identificação e a correção de eventuais deficiências.