CredFederal

Cooperativa de Crédito Mútuo dos Policiais Federais e Servidores da União no Espírito Santo

POLÍTICA DE SEGURANÇA CIBERNÉTICA

Resolução 4.658/18

CredFederal
Cooperativa de Crédito Mútuo dos Policiais Federais e Servidores da União no Espírito Santo

POLÍTICA DE SEGURANÇA CIBERNÉTICA

01. OBJETIVO

Esta Política de Segurança Cibernética da Cooperativa, bem como os requisitos para a contratação, avaliação e gestão de serviços de processamento e armazenamento de dados e de computação em nuvem visando observância e adequação ao exigido na Resolução nº 4.658/18 do Banco Central do Brasil.

O principal objetivo desta Política é assegurar a proteção dos ativos de informação da Cooperativa contra ameaças, internas ou externas, reduzir a exposição a perdas ou danos decorrentes nas falhas de segurança cibernética e garantir que os recursos adequados estarão disponíveis, mantendo um processo de segurança para garantir os negócios e suas continuidades.

02. DEFINIÇÕES

Como uma definição usa palavras para definir ou esclarecer uma palavra, uma dificuldade comum nessa prática é ter de escolher termos cuja compreensão seja mais acessível que a daquele que se quer definir. Para devida compreensão e aplicabilidade de termos usados no ambiente cooperativo e cibernético, são definidas as definições a seguir:

2.1 **Clientes ou Cooperados ou Associados**: Pessoas físicas e/ou jurídicas que utilizam os serviços prestados pela Cooperativa.

2.2 **Colaboradores**: São os administradores, corpo diretivo, funcionários, jovens aprendizes, estagiários, auxiliares ou quaisquer outros colaboradores da Cooperativa.

2.3 **Dado(s) e/ou informação (ões)**: São todos os dados referentes às atividades desenvolvidas pela Cooperativa na execução de seu objetivo social, incluindo dados de clientes, pessoais ou não, e classificados de acordo com o item 03 desta Política.

2.4 **Incidentes**: Qualquer ocorrência que realmente ou potencialmente comprometa a confidencialidade, integridade ou disponibilidade de um sistema de informação ou a informação que o sistema processa, armazena ou transmite ou que constitui uma violação ou ameaça de violação de políticas de segurança, procedimentos de segurança ou políticas de uso aceitáveis. São considerados incidentes, mas não se limitando a esses:

a) acesso indevido a contas e/ou sistemas da Cooperativa;
b) acessos não autorizado a base de Dados ou Informações de uso interno ou confidencial da Cooperativa;

c) alteração ou perda de Dados ou Informações, ou de acesso a sistemas ou ambientes lógicos, como da integridade destes;
d) vulnerabilidades existentes nos sistemas, como situações de indisponibilidades dos sistemas e/ou das informações ou;
e) demais falhas de segurança que acarretem em acesso não autorizados a sistemas ou ambientes tecnológicos da Cooperativa, por meio de técnicas, conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

2.5 **Prestador de Serviço**: Pessoa física ou jurídica, devidamente contratada pela Cooperativa para prestação:

a) de tecnologia;
b) de armazenamento ou qualquer forma de tratamento de Dados e Informações; ou
c) que venha a ter acesso, por conta do escopo de sua contratação, a Dados confidenciais, como classificados nesta Política.

2.6 **Riscos Cibernéticos**: São os riscos de ataques cibernéticos, oriundo de malware, técnicas de engenharia social, invasões, ataques de rede (DDoS e Botnets), fraudes externas, entre outros, que possam expor Dados, redes e sistemas da Cooperativa, causando danos financeiros e/ou de reputação consideráveis, podendo em algumas circunstâncias, prejudicar a continuidade das atividades da Cooperativa, conforme destacamos abaixo:

a) **malware**, softwares desenvolvidos para corromper computadores e redes;
b) **engenharia social**, métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito;
c) **vírus**, software que causa danos a máquina, rede, softwares e banco de dados;
d) **cavalo de tróia**, aparece dentro de outro software e cria uma porta para a invasão de computador;
e) **spyware**, software malicioso para coletar e monitorar o uso de informações;
f) **ransomware**, software malicioso que bloqueia o acesso a sistemas e base de dados, solicitando um resgate para que o acesso seja restabelecido;
g) **pharming**, direciona o usuário para um site fraudulento, sem o seu conhecimento;
h) **phishing**, links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação oficial para obter informações confidenciais;

i) **vishing**, simula ser um pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;

j) **smishing**, simula ser um pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais;

k) **ataque de DDoS (distribute denial of services) e Botnets**, ataques visando negar ou atrasar o acesso aos serviços ou sistemas da Cooperativa, no caso do Botnets, o ataque vem de um grande número de computadores infectados utilizados para criar e mandar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços;

l) **acesso pessoal**, pessoas localizadas em lugares públicos com bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque;

m) **invasões (advanced persistent threats)**, ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidade específicas em um ambiente tecnológico.

2.7 **Serviços Relevantes**: Serviços prestados por prestadores de serviço à Cooperativa cuja indisponibilidade, vulnerabilidade ou inconsistência possa prejudicar a continuidade de seus negócios:

a) afetando o atendimento ofertado ao Cliente;
b) paralisando a operação da Cooperativa, podendo causar perdas financeiras; ou
c) impedindo o fornecimento de informações pela Cooperativa aos entes reguladores e/ou o cumprimento de direitos e garantias dos Clientes.

03. CLASSIFICAÇÃO DE DADOS

Os dados objetos da presente Política serão classificados de acordo com as categorias abaixo indicadas, considerando a relevância das informações na Cooperativa:

3.1 **Classe 01 – Documentos Públicos**, informações aprovadas pelo Conselho de Administração ou pela Diretoria para uso público (interno ou externo), ou se solicitado pelo Banco Central do Brasil, por exemplo: Art. 5º da Resolução 4.658/18 "**As instituições devem divulgar ao público resumo contendo as linhas gerais da política de segurança cibernética**";

3.2 **Classe 02 – Somente Uso Interno**, informação não aprovada para circulação fora da Cooperativa como, por exemplo: memorandos

internos, minutas ou atas de reuniões, procedimentos, rotinas operacionais ou de controles internos;

3.3 **Classe 03 – Confidencial**, informações cuja circulação interna é controlada, por questões estratégicas e de gestão, e cuja a circulação externa é vedada, pois se tornadas públicas ou compartilhadas causarão impactos e prejuízos aos negócios, podendo ser: planos de negócios, especificações que definem a forma que a Cooperativa opera, informações contábeis, informações sobre Clientes ou outros. Esta Classe envolve todas as informações e Dados referentes aos Clientes da Cooperativa, inclusive Dados pessoais.

3.4 **Classe 04 – Informações Sensíveis** – informações internas ou confidenciais críticas ao desenvolvimento das atividades da Cooperativa, que:

a) são acobertadas por sigilo bancário, nos termos da legislação aplicável; e/ou
b) cuja perda ou indisponibilidade pode prejudicar ou impedir a adequada prestação de serviços pela Cooperativa ao Cliente, a realização de operações da Cooperativa e/ou o cumprimento de suas obrigações legais e/ou normativas.

A Cooperativa manterá um programa de revisão e de classificação contínua das informações.

04. DIRETRIZES

A presente Política deverá ser cumprida e respeitada por todos os Colaboradores e Prestadores de Serviços da Cooperativa. Neste sentido, deverão ser respeitadas as seguintes diretrizes gerais:

4.1 **Assegurar a confidencialidade** dos ativos de informações (garantia de que o acesso à informação seja obtido somente por pessoas autorizadas) observadas as regras de sigilo e confidencialidade.

4.2 **Assegurar a integridade** (garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais).

4.3 **Assegurar a disponibilidade** dos dados e sistemas de informação utilizados na Cooperativa (garantia de que os usuários autorizados obtenham o acesso à informação e aos ativos correspondentes sempre que necessário).

4.4 **Implementação** desta Política considera as seguintes compatibilidades da Cooperativa:

a) o porte, perfil de risco e o modelo de negócios;
b) a natureza das operações e a complexidade dos produtos, serviços, atividades e processos atuais;
c) a sensibilidade dos dados e das informações sob responsabilidade da instituição.

05. MECANISMOS DE SEGURANÇA DA INFORMAÇÃO

Para assegurar que as informações tratadas estejam adequadamente protegidas, a Cooperativa adota os seguintes mecanismos:

5.1 **Controles físicos** – são barreiras que limitam o contato ou acesso direto a informação ou a estrutura (que garante a existência da informação) que a suporta. Exemplos de mecanismos de segurança que apoiam os controles físicos: portas, trancas, paredes entre outros; e

5.2 **Controles lógicos** - são barreiras que impedem ou limitam o acesso a informação, que está em ambiente controlado, geralmente eletrônico, e que, de outro modo, ficaria exposta a alteração não autorizada. Exemplos de mecanismos de segurança que apoiam os controles lógicos: autenticação de acesso (senhas), criptografia de Dados, prevenção e detecção de acesso, entre outros.

06. INCIDENTES DE SEGURANÇA

Os incidentes de segurança serão classificados conforme sua relevância e de acordo com a classificação dos Dados e Informações envolvidos; e o impacto na continuidade dos negócios da Cooperativa nas seguintes categorias:

6.1 **Baixo** – causa lentidão ou indisponibilidade no acesso a sistemas e/ou Dados, sem, entretanto, afetar o atendimento ao Cliente ou a realizações de transações.

6.2 **Médio** – causa lentidão no atendimento ao Cliente, podendo, ainda, impedir o acesso a alguns serviços não essenciais; e

6.3 **Alto** – impede o atendimento ao Cliente e/ou a realização de transações.

07. AÇÕES DE PREVENÇÃO

Devem ser criados mecanismos de monitoramento de todas as ações de proteção implementadas para garantir o bom funcionamento e efetividade da segurança cibernética da Cooperativa através das seguintes ações:

7.1 Manter inventários atualizados de hardware e software, bom como verificá-los com frequência para identificar elementos estranhos à cooperativa. Por exemplo, computadores não autorizados ou software não licenciado.

7.2 Manter os sistemas operacionais e softwares de aplicação sempre atualizados, instalando as atualizações sempre que forem disponibilizadas.

7.3 Monitorar diariamente as rotinas de backup, executando testes regulares de restauração dos dados.

7.4 Realizar análises de vulnerabilidades na estrutura tecnológica, periodicamente ou sempre que houver mudança significativa em tal estrutura.

7.5 Periodicamente testar os procedimentos de resposta a incidentes, simulando os cenários.

08. TRATAMENTO DE INCIDENTES

8.1 Incidentes são interrupções de sistema não planejadas que ocorrem de várias naturezas e que afetam os negócios da Cooperativa, como por exemplo:

- Queda de energia elétrica;
- Falha de um elemento de conexão (cabeamento);
- Servidor fora do ar;
- Ausência de conexão com internet;
- Sabotagem (interna);
- Indisponibilidade de acesso à Cooperativa;
- Ataques de hacker.

8.2 Qualquer Colaborador que detectar um incidente deverá comunicar imediatamente as demais áreas sobre o fato para que o mesmo seja levado ao conhecimento do Diretor responsável pela Política de Segurança Cibernética.

8.3 O Diretor responsável pela Política de Segurança Cibernética deverá avaliar o impacto do incidente nos diversos riscos envolvidos.

8.4 Recuperação, essa fase começa após o incidente ter sido contornado, já tendo sido a contingência acionada.

8.5 Retomada tal fase refere-se ao período de transição do retorno ao modo normal de operação e pode incluir a análise de projetos, como voltar à operação normal, reconstrução de eventuais sistemas, eventuais mudanças e medidas de prevenção.

8.6 A área de TI ou os responsáveis pelos Dados/Informações na cooperativa devem supervisionar e monitorar com o objetivo de verificar sua efetividade e detectar as ameaças em tempo hábil, reforçando os controles, caso necessário, e identificar possíveis anomalias no ambiente tecnológico, incluindo a presença de usuários, componentes ou dispositivos não autorizados.

09. PROCESSAMENTO, ARMAZENAMENTO DE DADOS E COMPUTAÇÃO EM NUVEM

A contratação, pela Cooperativa de serviços de processamento e armazenamento de dados e de computação em nuvem considerados relevantes nos termos dessa política, se dá de acordo com o disposto na Resolução 4.658/2018 do Conselho Monetário Nacional, conforme cláusulas inseridas em referidos contratos, devendo estes ser devidamente validados pelo Conselho de Administração ou pela Diretoria.

A decisão de contratação de Serviços Relevantes junto a Prestadores de Serviços externos deverá ser amparada nos seguintes critérios:

- Confirmação da capacidade técnica do Prestador de Serviço de cumprir o disposto nesta Política e na legislação aplicável à segurança cibernética;
- Dificuldade ou impossibilidade técnica ou custo elevado para a execução do Serviço Relevante pela Cooperativa em sua própria infra estrutura; e
- A criticidade e relevância do serviços a ser contratado.

10. CONTINUIDADE DE NEGÓCIOS

O processo de gestão de continuidade de negócios relativo à segurança da informação, é implementado para minimizar os impactos e recuperar perdas de ativos da informação, após um incidente crítico, retornando a operação 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.

Referido processo deverá considerar, ao menos, os seguintes cenários para a realização de testes de continuidade de negócios:

a) Exploração de possíveis vulnerabilidades que permitam o acesso, a cópia e /ou a extração de Informações e Dados internos e/ou confidenciais do ambiente lógico da Cooperativa;
b) Realização de testes de intrusão a base de dados contendo Informações Sensíveis da Cooperativa;
c) Tempo de recuperação de acesso a informações de backup em caso de perda de Informações Sensíveis;
d) Estratégias para a recuperação de Informações Sensíveis e Serviços Relevantes.

11. DOCUMENTOS À DISPOSIÇÃO DO BANCO CENTRAL

Os seguintes documentos devem ficar à disposição do Banco Central do Brasil pelo prazo de cinco anos:

- Política de Segurança Cibernética;
- Ata de Reunião do Conselho de Administração ou Diretoria da Cooperativa implementado a Política de Segurança Cibernética;
- Documento relativo ao Plano de Ação e de resposta a incidentes relativos a implementação da Política de Segurança Cibernética;
- Relatório anual sobre a implementação do Plano de ação e de resposta e incidente;
- Documentação sobre os procedimentos relativos à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem;
- Contratos de Prestação de serviços relevantes de processamento, armazenamento de dados e computação na nuvem.

12. ABRANGÊNCIA, APROVAÇÃO, DIVULGAÇÃO E REVISÃO DA POLÍTICA

O conteúdo desta Política de Segurança Cibernética Política aplica-se a todos os Colaboradores e Prestadores de Serviços Relevantes da Cooperativa, no âmbito de suas atividades, atribuições e responsabilidades.

Está sendo comunicada para todos os Colaboradores e Prestadores de Serviços Relevantes para o necessário cumprimento.

Um resumo da Política de Segurança Cibernética estará sendo divulgado aos Clientes e público da Cooperativa.

É obrigação de todo Colaborador conhecer e praticar os dispositivos desta Política e assegurar que, quando necessário, prestadores de serviços sejam informados sobre as regras estabelecidas.

Será implementado o plano de ações e respostas a incidentes para atender as diretrizes desta Política.

Esta Política será revisada anualmente ou quando mudanças significativas ocorrerem assegurando a sua contínua pertinência, adequação e eficácia.

13. DISPOSIÇÕES FINAIS

A Política de Segurança Cibernética foi aprovada na Reunião Extraordinária do Conselho de Administração realizada no dia 07 de janeiro de 2021, conforme Ata nº 02/2021.

Roberto Silveira
Diretor-Presidente

Rubens Antônio dos Santos
Diretor Operacional

Sérgio dos santos Calazans
Diretor Administrativo

Antônio Honório Vieira
Conselheiro de Administração