



POLÍTICA DE SEGURANÇA CIBERNÉTICA E SEGURANÇA DA INFORMAÇÃO

POLÍTICA DE SEGURANÇA CIBERNÉTICA E DA SEGURANÇA DA INFORMAÇÃO

OBJETIVOS E FINALIDADES

A **Cooperativa de Economia e Crédito Mútuo dos Eletricitários e dos Trabalhadores das Empresas do Setor de Energia-COOPCRECE**, inscrita no CNPJ/MF sob nº 92.825.397/0001-79, vem por meio desta política estabelecer critérios a serem observados, no que diz respeito ao assunto “Política de Segurança Cibernética e Segurança da Informação”, atendendo a Resolução nº 4.893/21, adequados ao porte, a complexidade, a estrutura, o perfil de risco e seu modelo de negócio.

RESPONSABILIDADES DAS ÁREAS ENVOLVIDAS

Os serviços de tecnologia da informação utilizados pela COOPCRECE são terceirizados pelo Grupo NGX, composto pelas empresas NGXit e Cloud2GO, pela empresa CashWay e pela empresa Sinqia. Os contratos de prestação de serviços são geridos pela Diretoria Executiva e monitorados pelo Gerente Executivo.

Conselho de Administração

Responsável por:

- Aprovar a Política de Segurança Cibernética e Segurança da Informação;
- Monitorar a aplicação dos procedimentos que atendam a legislação;
- Aprovar as revisões e atualizações.

Diretoria Executiva

Responsável por:

- Elaborar a política em conjunto com os demais responsáveis;
- Propor aprovação da política;
- Divulgar e manter a política atualizada;
- Acompanhar a aplicação da política;
- Elaborar relatório anual e plano de ação e de resposta a incidentes;
- Dar ciência aos colaboradores e prestadores de serviços sobre a política.

CONCEITOS / CRITÉRIOS GERAIS

1 - PÚBLICO-ALVO

Esta política destina-se:

- ✓ A todos os colaboradores da COOPCRECE. Para os fins do disposto nesta política o termo "Colaboradores" abrange todos os empregados, menores aprendizes e estagiários;
- ✓ Aos prestadores de serviços, pessoas físicas ou jurídicas, que manuseiem dados ou informações sensíveis à condução das atividades operacionais da COOPCRECE.

2 - OBJETIVO

Estabelecer os princípios, conceitos, valores e práticas de proteção das informações e da propriedade intelectual da COOPCRECE, dos associados e usuários, do público em geral que devem ser adotados pelos Colaboradores e prestadores de serviço da COOPCRECE, visando:

- ✓ Proteger o valor, a reputação e integridade da COOPCRECE;
- ✓ Garantir a confidencialidade, integridade e disponibilidade das informações da COOPCRECE, e de informações de terceiros por ela custodiadas, contra acessos indevidos e modificações não autorizadas, assegurando ainda que as informações estarão disponíveis a todas as partes autorizadas, quando necessário;
- ✓ 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;
- ✓ Garantir a continuidade de seus negócios, protegendo os processos críticos de interrupções causadas por falhas ou desastres significativos;
- ✓ Atender aos requisitos legais, regulamentares e às obrigações contratuais pertinentes a atividade da COOPCRECE;
- ✓ Conscientizar, educar e treinar os colaboradores por meio da Política de Segurança Cibernética e Segurança da Informação, sobre normas e procedimentos internos aplicáveis as suas atividades diárias;
- ✓ Estabelecer e melhorar continuamente um processo de Gestão de Riscos de Segurança Cibernética.

3 - 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 às 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 Tróia:** 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 restabelecido.
- ✓ 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 muitos computadores infectados utilizados para criar e enviar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.

4 - PRINCÍPIOS

A proteção e privacidade de dados dos associados e usuários refletem os valores da COOPCRECE e reafirmam o seu compromisso com a melhoria contínua da eficácia do processo de Proteção de Dados.

Quanto às informações de nossos clientes, são obedecidas as seguintes determinações:

- ✓ São coletadas de forma ética e legal, para propósitos específicos e devidamente informados;
- ✓ Somente serão acessadas por pessoas autorizadas e capacitadas para o seu uso adequado;
- ✓ Poderão ser disponibilizadas a empresas contratadas para prestação de serviços, sendo exigido de tais organizações o cumprimento de nossas diretrizes de segurança e privacidade de dados;
- ✓ As informações constantes de nossos cadastros, bem como outras solicitações que venham garantir direitos legais ou contratuais, somente serão fornecidas aos próprios interessados, mediante a solicitação formal, seguindo os requisitos legais vigentes.

5 - DIRETRIZES

O cumprimento da Política de Segurança Cibernética e Segurança da Informação é de responsabilidade de todos os Colaboradores e dos prestadores de serviços, os quais devem obedecer às seguintes diretrizes:

- ✓ As informações da COOPCRECE, dos associados e do público em geral devem ser tratadas de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, evitando-se mau uso e exposição indevida;
- ✓ 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 COOPCRECE;
- ✓ Garantir que os sistemas e as informações sob sua responsabilidade estejam adequadamente protegidos;
- ✓ Garantir a continuidade do processamento das informações críticas de negócios;
- ✓ Atender às leis que regulamentam as atividades da COOPCRECE e sua área de atuação;
- ✓ Selecionar os mecanismos de segurança da informação, balanceando fatores de riscos, tecnologia e custo;
- ✓ Comunicar imediatamente à Diretoria Executiva e área de Segurança Cibernética, quaisquer descumprimentos da Política de Segurança Cibernética e Segurança da Informação;
- ✓ O acesso às informações e recursos só deve ser feito se devidamente autorizado;
- ✓ A identificação de qualquer Colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas;
- ✓ A senha é utilizada como assinatura eletrônica através de verificação através de Multifator e deve ser mantida secreta, sendo proibido seu compartilhamento;
- ✓ As responsabilidades quanto à Segurança da Informação devem ser amplamente divulgadas aos Colaboradores, que devem entender e assegurar estas diretrizes.

6 - ESTRUTURA DE GERENCIAMENTO

O gerenciamento de procedimentos e controles de Segurança Cibernética objetivam assegurar que os procedimentos operacionais de segurança sejam desenvolvidos, implementados e mantidos ou modificados de acordo com os objetivos estabelecidos pela Política de Segurança Cibernética e Segurança da Informação.

6.1. Gestão de acessos às informações

Os acessos às informações são controlados, monitorados, restringidos à menor permissão e privilégios possíveis, revistos periodicamente com a aprovação da Diretoria Executiva, responsáveis pelos quesitos de segurança da informação, e cancelados tempestivamente ao término do contrato de trabalho do Colaborador ou do prestador de serviço.

6.2. Gestão de Riscos

Os riscos devem ser identificados por meio de processo estabelecido para análise de vulnerabilidades, ameaças e impactos sobre os ativos de informação da COOPCRECE, para que sejam recomendadas as proteções adequadas.

6.3. Proteção do ambiente

São 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.

6.4. Segurança Física e Lógica

Os equipamentos e instalações de processamento de informação críticas ou sensíveis são 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 são 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.

6.5. 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, 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.

6.6. Processamento, Armazenamento de dados e Computação em nuvens

Conforme a Resolução nº 4.893/21, para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, a COOPCRECE deve assegurar-se de um procedimento efetivo para a aderência às regras previstas na regulamentação em vigor.

6.7. Governança com as Áreas de Negócio e Tecnologia

As iniciativas e projetos das áreas de negócio e tecnologia devem estar alinhadas com as diretrizes e arquiteturas de segurança da informação, garantindo a confidencialidade, integridade e disponibilidade das informações.

6.8. Segurança no Desenvolvimento de Sistemas de Aplicação

O processo de desenvolvimento de sistemas de aplicação deve garantir a aderência às políticas de segurança da COOPCRECE e às boas práticas de segurança.

7 - RESPONSABILIDADE

O Diretor Responsável pela área de Segurança Cibernética se compromete com a melhoria contínua dos procedimentos e controles relacionados nesta Política, os quais devem ser objetos de pautas em reuniões de conselhos da COOPCRECE, quando necessário.



8 - COMPARTILHAMENTO DE INFORMAÇÕES

O Diretor Responsável pela área de atuação da Segurança Cibernética e Segurança da Informação se compromete a comunicar tempestivamente ao Banco Central do Brasil as ocorrências de incidentes relevantes e as interrupções dos serviços relevantes, que configurem uma situação de crise, bem como as providências para o reinício das suas atividades.

Sem prejuízo do dever de sigilo e da livre concorrência, a COOPCRECE deverá comunicar-se com NGXit, Cloud2GO, CASHWAY, SINQIA e demais prestadores de serviços, para compartilhamento de informações sobre os incidentes relevantes.

9 - COMUNICAÇÃO

Quaisquer indícios de irregularidades no cumprimento das determinações desta política serão alvo de investigação interna e devem ser comunicadas imediatamente para o endereço de e-mail ouvidoria@crece.com.br ou podem ser informadas no Canal de Denúncias:

<https://www.crece.com.br/comunicacao/registro-de-denuncias-e-reclamacoes>

Esta Política de Segurança Cibernética e Segurança da Informação entrará em vigor a partir de sua aprovação, pelo Conselho de Administração.

Porto Alegre, 12 de janeiro de 2023.

Antônio Carlos Oleques da Rocha

Presidente

Paulo Roberto Gonçalves Fernandes

Vice-Presidente