POLÍTICA DE SEGURANÇA CIBERNÉTICA DA CREDIBELGO

1ª edição aprovada em 10/12/2020

2ª edição atualizada em 10/02/2023

Política de Segurança Cibernética da Credibelgo

1. Esta Política de Segurança Cibernética da Credibelgo:

a) é aprovada pelo Conselho de Administração;

b) a Cooperativa deve indicar diretor responsável pelo gerenciamento da segurança cibernética. O diretor indicado poderá exercer outras funções, desde que não haja conflito de interesse;

c) é divulgada a todos os usuários que compõem as estruturas organizacionais (dirigentes, empregados e estagiários) da Credibelgo e às demais pessoas com acesso autorizado às informações da Cooperativa, incluindo cooperados, parceiros, empresas prestadoras de serviço e ao público;

d) reforça o comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados com a segurança cibernética.

2. São objetivos desta Política:

a) a definição de diretrizes para a segurança do espaço cibernético, relacionadas à capacidade da Credibelgo de prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético;

b) a proteção das informações sob responsabilidade da Cooperativa preservando sua confidencialidade, integridade, disponibilidade e autenticidade;

c) a prevenção de eventual interrupção, total ou parcial, dos serviços de TI acessados pela Cooperativa e pelos cooperados e, no caso de sua ocorrência, a redução dos impactos dela resultantes;

d) o tratamento e a prevenção de incidentes de segurança cibernética;

e) a formação e a qualificação dos recursos humanos necessários à área de segurança cibernética;

f) a promoção do intercâmbio de conhecimentos entre as demais instituições financeiras, órgãos e entidades públicas a respeito da segurança cibernética.

3. Das responsabilidades:

3.1. Do Conselho de Administração:

a) revisar e aprovar anualmente as políticas e estratégias de gerenciamento de segurança cibernética;

b) assegurar a aderência da Cooperativa às políticas e estratégias de gestão da segurança cibernética;

c) assegurar a correção tempestiva das deficiências das estruturas de gerenciamento de segurança cibernética;

d) promover a disseminação da cultura de gerenciamento de segurança cibernética.

3.2. Do diretor responsável pela segurança cibernética na Crebibelgo:

a) supervisionar o desenvolvimento, a implementação e o desempenho da estrutura de gerenciamento de segurança cibernética, incluindo seu aperfeiçoamento;

b) subsidiar e participar do processo de tomada de decisões estratégicas relacionadas ao gerenciamento de segurança cibernética, auxiliando o Conselho de Administração;

c) responsabilizar-se pela capacitação adequada dos empregados que compõem a estrutura de gerenciamento de segurança cibernética, acerca das políticas, dos planos e dos controles.

d) definir políticas, planos, manuais e controles para o gerenciamento de segurança cibernética;

e) definir e acompanhar indicadores de gestão da segurança cibernética;

f) providenciar o relacionamento com as áreas internas de supervisão, responsáveis pelo relacionamento com os órgãos de supervisão externos;

g) informar ao Comitê da Estrutura Simplificada de Gerenciamento Contínuo de Riscos e de Capital e Agente de Controles Internos e Conformidade sobre os incidentes cibernéticos relevantes;

h) reportar ao Conselho de Administração e à Diretoria Executiva as informações relativas à gestão centralizada de segurança cibernética;

i) compartilhar informações sobre incidentes cibernéticos relevantes com as instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

j) fazer recomendações de aperfeiçoamento da política, dos planos, manuais, controles e procedimentos relacionados à segurança cibernética;

k) implementar e executar os procedimentos descritos nas políticas, planos e manuais relativos ao tema;

4. Dos procedimentos e controles:

4.1 Para reduzir a vulnerabilidade da instituição a incidentes cibernéticos, prevenir o vazamento de informações e atender aos demais objetivos de segurança cibernética, a Cooperativa deve adotar procedimentos e controles, conforme porte e perfil de risco da entidade, tais como:

a) regras para controlar complexidade e qualidade das credenciais utilizadas para acesso aos sistemas e aos dados sob responsabilidade da Credibelgo;

b) duplo fator de autenticação nos ambientes em que o recurso está disponível;

c) solução de prevenção e detecção de intrusão, solução de proteção de dispositivos, procedimentos de hardening, monitoramento de tráfego na rede,

monitoramento de atividades em bancos de dados, monitoramento de atividade de usuários privilegiados;

d) testes de invasão realizados por equipe interna da entidade ou por empresa contratada quando a entidade possuir serviços de TI sob sua responsabilidade;

e) processo de gestão de vulnerabilidades de ativos de TI;

f) solução de proteção contra ameaças avançadas em e-mail e no acesso a sites na internet, solução de proteção de dispositivos, antivírus de borda;

g) gerenciador de eventos e incidentes em segurança que mantém registro dos eventos do ambiente, permitindo a rastreabilidade de vários tipos de ocorrências;

h) solução de prevenção de vazamento de dados;

i) segmentação de rede, com isolamento de ambientes (como produção e homologação) e áreas;

j) manutenção de cópias de segurança dos dados e das informações;

k) critérios de decisão quanto à terceirização de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem.

4.2 Os procedimentos e controles são aplicados para sistemas de informação desenvolvidos internamente ou adquiridos de terceiros.

4.3 As empresas terceirizadas que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da entidade deverão estabelecer procedimentos e controles com complexidade, abrangência e precisão compatíveis com os utilizados pela Credibelgo.

4.4 É estabelecido plano de ação e de resposta a incidentes, revisado anualmente.

5. As informações de propriedade ou sob custódia da Credibelgo, mantidas em meio eletrônico ou físico, são classificadas de acordo com os requisitos de proteção esperados em termos de sigilo, valor, requisitos legais, sensibilidade e necessidades do negócio, de modo que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados, conforme manual de classificação da informação específico.

6. São adotados mecanismos para disseminação da cultura de segurança cibernética na instituição, incluindo:

a) implementação de programas de capacitação e de avaliação periódica de pessoal;

b) prestação de informações a clientes e usuários sobre precauções na utilização de produtos e serviços financeiros.

7. Complementam esta política e a ela se subordinam todas as normas e procedimentos operacionais que regulam a segurança cibernética.