01. APRESENTAÇÃO

1.1. A Política Institucional de Segurança Cibernética da COOPERATIVA DE CRÉDITO DOS EMPREGADOS DA COMPANHIA INDUSTRIAL CATAGUASES E DA BAUMINAS LTDA. - COOPECIC objetiva:

a) definir as diretrizes para a segurança cibernética, relacionadas à capacidade da Cooperativa de prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados ao ambiente cibernético;

b) reforçar o comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados com a segurança cibernética;

c) proteger as informações sob responsabilidade da Cooperativa preservando sua confidencialidade, integridade, disponibilidade e autenticidade;

d) prevenir eventual interrupção, total ou parcial, dos serviços de TI da Cooperativa e, no caso de sua ocorrência, a redução dos impactos dela resultantes;

e) prevenir e tratar incidentes de segurança cibernética;

f) formar e qualificar os recursos humanos necessários à área de segurança cibernética, ou contratar mão de obra especializada para desenvolver as atividades relacionadas a tal área.

1.2. Esta Política deve ser observada por todos os componentes da estrutura organizacional da Cooperativa, bem como pelas demais pessoas com acesso autorizado às informações da instituição.

02. DA POLÍTICA

2.1. São atribuições da Diretoria Executiva da Cooperativa:

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

cibernética;

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

c) promover a disseminação da cultura de gerenciamento de segurança cibernética;

d) definir o diretor responsável pela gestão de segurança cibernética.

2.2. São atribuições do diretor responsável pela gestão de segurança cibernética:

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

b) definir políticas, planos, manuais e controles para o gerenciamento de segurança cibernética da Cooperativa;

c) definir e acompanhar indicadores de gestão da segurança cibernética na Cooperativa;

d) reportar à Diretoria Executiva as informações relativas à gestão de segurança cibernética;

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

f) subsidiar e participar do processo de tomada de decisões estratégicas relacionadas ao gerenciamento de segurança cibernética, auxiliando a Diretoria Executiva;

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

h) informar à Diretoria Executiva sobre os incidentes cibernéticos relevantes.

2.4. São atribuições de todos os componentes da estrutura organizacional notificar sobre incidentes de segurança cibernética à Diretoria Executiva.

2.5. Para reduzir a vulnerabilidade da Cooperativa a incidentes cibernéticos, prevenir o vazamento de informações e atender aos demais objetivos de segurança cibernética, deverão ser adotados procedimentos e controles, tais como:

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

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

c) recursos criptográficos adequados para garantir a privacidade, integridade e não-repúdio dos dados mantidos pela Cooperativa;

d) 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;

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

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

g) solução de prevenção de vazamento de dados;

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

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

2.6. Os procedimentos e controles devem ser aplicados para sistemas de informação

desenvolvidos internamente ou adquiridos de terceiros, devendo as empresas terceirizadas que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da Cooperativa estabelecer tais condutas.

2.7. Deve ser estabelecido plano de ação e de resposta a incidentes.

2.8. As informações de propriedade ou sob custódia da Cooperativa, 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.

2.9. Devem ser adotados mecanismos para disseminação da cultura de segurança cibernética na Cooperativa, tais como implementação de programas de capacitação e de avaliação periódica de pessoal e prestação de informações a clientes e usuários sobre precauções na utilização de produtos e serviços da Cooperativa.

2.10. Complementam a presente Política e a ela se subordinam todas as normas e procedimentos operacionais que regulam a Segurança Cibernética na Cooperativa.

03. DISPOSIÇÕES FINAIS

3.1. Esta Política deve ser aprovada e avaliada anualmente pela Diretoria Executiva da Cooperativa.

3.2. Na revisão desta Política devem ser considerados os resultados das auditorias externas, as legislações e as normas aplicáveis vigentes.

3.3. As normas legais prevalecem sobre esta Política, sempre que houver divergência ou conflito.

3.4. A presente Política Institucional entra em vigor na data de sua aprovação.