POLÍTICA DE SEGURANÇA CIBERNÉTICA

O propósito desta Política é orientar a Cooperativa, seus colaboradores e seus prestadores de serviço no que diz respeito à gestão de riscos e ao tratamento de incidentes de Segurança da Informação Cibernética, em conformidade com as disposições constitucionais, legais e regimentais vigentes, a fim de garantir a aplicação dos princípios e diretrizes de proteção das informações e da propriedade intelectual da cooperativa, dos cooperados e envolvidos.

O Conselho de Administração da C.E.C.M.S FED. COMÉRCIO, SESC E SENAC DE SP, é o responsável pelas informações contidas nesta política, em cumprimento às exigências da Resolução nº 4.658/18 do Banco Central do Brasil, bem como a sua divulgação pública.

1. OBJETIVOS

- Assegurar, de forma conjunta, o uso efetivo do espaço cibernético (preparo e emprego operacional) da Cooperativa;
- Impedir e dificultar sua utilização contra os interesses da mesma;
- Capacitar e gerir talentos humanos necessários à conduta ética e segura das atividades no âmbito tecnológico;
- Prover uma base comum para as práticas efetivas de gestão de segurança cibernética;
- Viabilizar a confiança nos relacionamentos entre a cooperativa e seus colaboradores.

2. CONCEITO – ESPAÇO CIBERNÉTICO

O Espaço Cibernético é um ambiente resultante da interação de pessoas, software e serviços na Internet, suportado por instrumentos físicos de tecnologia da informação e comunicação e redes conectadas e distribuídas e que interagem diretamente com o ambiente de negócios da Cooperativa.

3. APLICAÇÃO

Esta política aplica-se aos funcionários da Cooperativa e às empresas prestadoras de serviços de acordo com as funções desempenhadas e com a sensibilidade das informações tratadas.

4. AMEAÇAS

4.1 Ameaças aos Ativos Pessoais

Ameaças aos ativos pessoais referem-se a questões de identidade, representadas pelo vazamento ou roubo de informações pessoais.

4.2 Ameaças aos Ativos Organizacionais

Ameaças aos negócios referem-se a transações realizadas pela instituição e informações de funcionários, clientes, parceiros ou fornecedores, registros financeiros e a infraestrutura que suporta a internet e o espaço cibernético.

5. PROCESSO DE SEGURANÇA DA INFORMAÇÃO

Para assegurar que as informações tratadas estejam adequadamente protegidas, a cooperativa adota os seguintes processos:

a) Gestão de ativos da informação, devem ser identificados de forma individual, inventariado e protegido de acesso indevido, fisicamente e logicamente, ter documentos e planos de manutenção;
b) Classificação da informação, devem ser de acordo com a confidencialidade e as proteções necessárias;
c) Gestão de acesso, devem utilizar as ferramentas e os processos da cooperativa, sendo rastreáveis, para garantir todas as ações passíveis de auditoria;
d) Gestão de riscos, são escalonados nos setores apropriados, para decisão;
e) Tratamento de incidentes de segurança da informação e Cyber Security, os incidentes devem ser reportados ao Conselho de Administração, bem como suas

informações serem registradas e armazenadas em arquivo eletrônico e/ou físico por um período mínimo de 5 (cinco) anos;

f) Conscientização em segurança da informação e Cyber Security, a disseminação dos princípios e diretrizes de segurança da informação são promovidos pela cooperativa, através de conscientização e capacitação;

g) Segurança física do ambiente, que visa estabelecer o controle ao acesso físico do ambiente;

h) Programa de Cyber Security, é norteado por regulamentações vigentes, melhores práticas e cenário mundial.

4. GERENCIAMENTO DE INCIDENTES

Tem o objetivo de assegurar que os eventos de segurança da informação sejam tratados de forma efetiva, permitindo o adequado registro, investigação e tomada de ação corretiva em tempo hábil, para mitigar o impacto negativo sobre os sistemas de informação da cooperativa.

I – Recepção da denúncia ou alteração interna de atividade suspeita;
II – Medidas de contenção imediata do incidente;
III – Coleta de informações e evidências;
IV – Análise das informações e evidências;
V – Notificação dos envolvidos.

5. CONTRATAÇÃO DE CLOUD SERVICES E PROCESSAMENTO / ARMAZENAMENTO DE DADOS

Por se tratar de uma cooperativa onde toda a operação é via Cloud Service, não há necessidade de contratação de novos serviços e processamento de dados neste ambiente. Qualquer alteração deverá constar na política.

6. PLANO DE AÇÃO A CENÁRIOS DE INCIDENTES

A Diretoria da Cooperativa conforme diretrizes do Banco Central do Brasil e políticas internas, estabeleceu mecanismos de tratamento de incidentes, de procedimentos a serem seguidos em caso de interrupção de serviços relevantes, de processamento e armazenamento de dados e de computação em nuvem contratado e, cenários de incidentes, considerados nos testes de continuidade de negócios.

7. PLANO DE RESPOSTA A INCIDENTES

O plano de resposta a incidentes identifica e descreve as funções e responsabilidades da equipe de resposta a incidentes, para que o plano de ação seja efetivado.

- ✓ Time de resposta a incidentes, responsável por evitar a perda de lucros, confiança do cliente ou ativos de informação e está autorizado a tomar medidas apropriadas para conter, mitigar ou resolver um incidente de segurança de computadores;
- ✓ Responsabilidade dos usuários da informação, todos os funcionários devem relatar qualquer violação suspeita ou confirmada de informações pessoas;
- ✓ Classificação/identificação de um potencial incidente: severidade alta, média ou baixa;
- ✓ Resposta a incidentes, todas as informações necessárias serão coletadas pelo suporte técnico.

8. COMUNICAÇÂO AO BANCO CENTRAL

Todo incidente de segurança cibernético considerado relevantes será avaliado e comunicado ao Banco Central do Brasil.

A Comunicação ao Banco Central deve incluir:

- ✓ A descrição do incidente, indicando dado ou informação sensível afetada e de que forma os clientes foram afetados;
- ✓ Avaliação sobre o número de clientes potencialmente afetados;
- ✓ Medidas já adotadas pelo Cooperativa ou as que pretende adotar;
- ✓ Tempo consumido na solução do evento ou prazo esperado para que isso ocorra; e

- ✓ Qualquer outra considerada importante.

10. DIVULGAÇÃO DA POLÍTICA

Esta política está aprovada pela Diretoria e está publicada e comunicada para todos os colaboradores, empresas contratadas de serviços, clientes e partes externas relevantes, para o necessário cumprimento.

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