Política de Segurança Cibernética do SICOOB:

Conforme consta na Política Institucional de Segurança Cibernética do Sicoob atualizada em 09/06/2020 sobre procedimentos utilizados para redução da vulnerabilidade descrito abaixo:

5. Dos procedimentos e controles:

5.1 Para reduzir a vulnerabilidade da instituição a incidentes cibernéticos, prevenir o vazamento de informações e atender aos demais objetivos de segurança cibernética, as entidades devem adotam 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 do Sicoob;

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 pelo Sicoob;

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

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

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

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

i) solução de prevenção de vazamento de dados;

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

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

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

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

5.3 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 pelo Sicoob.

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

6. As informações de propriedade ou sob custódia das entidades do Sicoob, 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.

7. 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.

8. Complementam esta política e a ela se subordinam todas as normas e procedimentos operacionais que regulam a segurança cibernética no âmbito das entidades do Sicoob.

1ª edição em 10/4/2019 - Resolução Sicoob Confederação 283 / Atualizada em 9/6/2020 - Resolução Sicoob Confederação 356