COPERURA

POLÍTICA DE SEGURANÇA CIBERNÉTICA

COPERURA

1. DEFINIÇÃO

O presente documento visa atender à resolução 4.658, de 26 de abril de 2018, do Banco Central do Brasil, que estabelece a implementação da Política de Segurança Cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados de computação em nuvem, bem como assegurar princípios e diretrizes básicas que garantem a integridade, confidencialidade, disponibilidade e autenticidade dos dados, observando o porte, o perfil de risco e os negócios desenvolvidos, a natureza das operações, a complexidade dos produtos, serviços, atividades e processos, assim como a sensibilidade dos dados e das informações sob responsabilidade da cooperativa.

2. OBJETIVO

2.1 – Garantir a integridade, confidencialidade, disponibilidade e autenticidade dos dados armazenados nos diversos sistemas utilizados pela cooperativa;

2.2 – Estabelecer ações para prevenir e detectar Softwares maliciosos, tentativas de invasão e fraudes no sistema;

2.3 – Estabelecer procedimentos para manutenção de cópias de segurança dos dados, considerando a rede interna e o ambiente em nuvem;

2.4 – Estabelecer procedimentos específicos para o controle de acesso à informação, por parte dos colaboradores.

2.5 – Registrar e analisar a causa do impacto e o controle dos efeitos de incidentes relevantes para as atividades da instituição.

3. RESPONSABILIDADES

3.1 – CONSELHO DE ADMINISTRAÇÃO E DIRETORIA

3.1.1 - Aprovar, supervisionar e revisar, sempre que necessário, a presente política, garantindo a gestão de toda segurança cibernética da cooperativa.

3.1.2 – Designar diretor responsável pela política de segurança cibernética e pela execução do plano de ação e de resposta a incidentes.

3.2 – GERÊNCIA

3.2.1 – Definir as permissões de acesso ao sistema, restringindo e controlando o acesso dos usuários;

3.2.2 – Definir em conjunto com a empresa responsável pela infra estrutura de rede, os softwares de detecção de vírus, mantendo suas versões, sempre, atualizadas;

3.2.3 – Elaborar o relatório anual referente a implementação do plano de ação e de resposta a incidentes;

3.2.4 – Dar publicidade a presente política, divulgando aos colaboradores, fornecedores e cooperados, as linhas gerais da política de segurança cibernética da Coperura.

4 – DO ARMAZENAMENTO E HOSPEDAGEM EM NUVEM

A Cooperativa através de contrato firmado com a empresa Rezek Ferreira Informática Ltda – Fácil Informática, terá todo o sistema Faccred – e os dados operacionalizados por ele – hospedados em DataCenter com disponibilidade de tempo (99,97%), em nuvem, utilizando a estrutura da empesa AMAZON.

5. NORMAS GERAIS

A hospedagem em nuvem seguirá os seguintes disciplinamentos:

5.1 - A hospedagem em nuvem dispensa a aquisição de licenças dos softwares de banco de dados, sistema operacional e antivírus, necessários aos servidores em nuvem;

5.2 – A empresa contratada realizará o backup em nuvem, totalmente automatizado, em ambiente de alta disponibilidade e durabilidade, com garantia da integridade dos dados por meio de restaurações periódicas em ambiente de homologação e confidencialidade das informações;

5.3 – A empresa contratada monitorará o banco de dados, incluindo o dimensionamento, instalação e configuração até tuning, backup/recover, monitoramento e aplicação de patches;

5.4 – A empresa contratada realizará o monitoramento de servidores e serviços, notificando em caso de falhas, mantendo características proativas (ações para antecipação de falhas), reativas (ações de respostas a eventuais falhas) e preventivas (ações para minimizar probabilidade de falhas);

5.5 – A empresa contratada deverá implementar e manter controles de segurança incluindo, sem limitação, segurança de hardware e software, firewalls, filtros e outras ferramentas de segurança;

5.6 – A empresa contratada se responsabilizará por armazenar e transmitir as credenciais de acesso e demais informações confidenciais de maneira criptografada;

5.7 – A empresa contratada deverá garantir a segregação de acesso entre os ambientes de seus diferentes clientes, impedindo o acesso não autorizado às informações;

5.8 – Caberá à empresa contratada disponibilizar informações para auditorias (internas e externas) e investigações judiciais quando solicitadas;

5.9 – O Backup citado no item 5.2 deverá ser realizado de acordo com a periodicidade abaixo descrita, mantendo cada um dos backups efetuados sob a política cíclica de armazenamento, que garante a disponibilidade de restauração de backup dos 7 (sete) últimos dias, com as seguintes características:

5.9.1 – backup diário de todo o Banco de Dados, utilizando ambiente redundante (replicado) e de alta disponibilidade (99,9999999% de durabilidade e de 99,97% de disponibilidade), inclusive nos sábados, domingos e feriados nacionais; e

5.9.2 – para garantir a sua integridade, os backups serão testados semanalmente;

5.10 – Será disponibilizado, diariamente, a critério da cooperativa, um arquivo contendo o backup lógico do banco de dados da Coperura.

A presente política de segurança cibernética deverá ser divulgada a todos os colaboradores da cooperativa, bem como às empresas prestadoras de serviços terceirizados.

Política de Segurança Cibernética Revisada pela Diretoria em 18 / 09 / 2019