**MODELO Nº 008/2020**

***(Observação:*** *Este modelo apresenta sugestões que devem ser avaliadas e adaptadas de acordo com as particularidades da Cooperativa.)*

**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**

1. **APRESENTAÇAO**

A presente Política de Segurança da Informação visa garantir a aplicação dos princípios e diretrizes de proteção das informações e da propriedade intelectual da \_\_\_\_\_\_\_\_\_\_\_\_\_(denominação da cooperativa), dos clientes e do público em geral.

1. **APLICABILIDADES**

Aplica-se a \_\_\_\_\_\_\_\_\_(órgão de administração da cooperativa), colaboradores, estagiários e prestadores de serviços da \_\_\_\_\_\_\_\_\_\_\_\_\_(denominação da cooperativa).

1. **CONCEITOS**

Para esta política são definidos:

1. segurança da informação: refere-se à proteção do conjunto de informações, no sentido de preservar o valor que possuem para a cooperativa.
2. backup: é uma cópia de segurança dos seus dados (física ou em nuvem) de um dispositivo de armazenamento ou sistema.

São propriedades básicas da segurança da informação: confidencialidade, integridade, disponibilidade, autenticidade e legalidade

1. **REGULAMENTAÇÃO**

Para esta política estão associadas a Resolução 4.658/2018 publicado pelo Conselho Monetário Nacional (CMN) e a Política de Segurança de Cibernética.

1. **RESPONSABILIDADES**

É de responsabilidade dos conselheiros, diretores, colaboradores, estagiário, prestador de serviços, parceiro ou visitante, observar e seguir a as diretrizes, padrões, procedimentos e orientações estabelecidas para o cumprimento da presente Política de Segurança da Informação.

É imprescindível que cada pessoa compreenda o papel da segurança da informação em suas atividades diárias.

Todas as atividades executadas pelos colaboradores, estagiários, prestadores de serviços devem observar a legislação vigente e a normatização de órgãos e entidades reguladoras, com relação à segurança da informação.

As diretrizes estabelecidas nesta política são extensíveis aos prestadores de serviços da cooperativa.

1. **SEGURANÇA DA INFORMAÇÃO**

A informação é um dos principais patrimônios da cooperativa, refere-se a um ativo com constantes ameaças e quando não gerenciados adequadamente, esses riscos e ameaças podem causar consideráveis danos a ***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(denominação da cooperativa).***

Assim, a Política de Segurança da Informação torna-se alicerce dos esforços de proteção à informação da cooperativa.

A Segurança da Informação são esforços contínuos para a proteção dos ativos de informação e para tanto, visa atingir os seguintes objetivos:

1. confidencialidade: garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas;
2. integridade: garantir que as informações sejam mantidas íntegras, sem modificações indevidas – acidentais ou propositais;
3. disponibilidade: garantir que as informações estejam disponíveis a todas as pessoas autorizadas a tratá-las.

* 1. **Proteção da Informação**

A informação é um importante ativo para a operação das atividades comerciais da cooperativa e deve ser adequadamente manuseada e protegida e pode estar presente em diversas formas, tais como:

1. sistemas de informação;
2. diretórios de rede;
3. bancos de dados;
4. mídia impressa;
5. magnética ou ótica;
6. dispositivos eletrônicos;
7. equipamentos portáteis;
8. microfilmes; e
9. meio da comunicação oral.

Toda a informação gerada ou desenvolvida nas dependências da cooperativa constitui ativo essencial à condução de negócios, e em última análise, à sua existência e deve ser utilizada unicamente para a finalidade para a qual foi autorizada, independente da forma ou por meio pelo qual é compartilhada.

Assim, é diretriz que toda informação de propriedade da cooperativa seja protegida de riscos e ameaças que possam comprometer a confidencialidade, integridade ou disponibilidade.

* 1. **correio eletrõnico**

Com objetivo de garantir a integridade dos sistemas de informação a área responsável pela segurança da informação na ***\_\_\_\_\_\_\_\_\_\_(denominação da cooperativa)*** poderá monitorar, investigar, ler ou verificar toda a atividade dos colaboradores e prestadores de serviços, abrangendo:

1. sem limites as informações;
2. dados;
3. conteúdo e mensagens ou arquivos enviados, recebidos ou armazenados;
4. acesso e as atividades aos sites da internet visitados.
   1. **ACESSO A INTERNET**

O acesso à internet deve ser utilizado para fins corporativos visando buscar informações que possam contribuir para o desenvolvimento das atividades relacionadas a cooperativa e ***\_\_\_\_\_\_\_\_\_\_(descrever área responsável pela tecnologia da informação)*** poderá monitorar ou bloquear o acesso à internet em caso de risco ao funcionamento do ambiente.

São permitidas o acesso à *internet* para fins pessoais ( *home banking,* lojas virtuais e afins) desde que o colaborador tenha bom senso e respeitando os direcionamentos de segurança estabelecidos.

É vedado o uso da internet para acesso a sites de relacionamento qualquer tipo de *download* e *upload*, uso de softwares *“peer-to-peer”(*P2P) e acesso a computadores e acesso a site com conteúdo impróprios.

O acesso externo à rede interna, para fins de manutenção de infraestrutura ou sistemas somente poderão ser realizados por ***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(descrever como são realizados os processos na cooperativa, empresas terceirizadas).***

.

* 1. **CONTROLE DE ACESSO**

A***\_\_\_\_\_\_\_\_(denominação da cooperativa)*** deverá manter restrito, o acesso as áreas onde serão processadas ou armazenadas informações pertinentes à operação da cooperativa, mantendo lista de acesso a estes ambientes.

O colaborador é responsável por todos os atos executados com suas credenciais de acesso, portanto deverá:

1. manter a confidencialidade, registrando as senhas em ambientes seguros;
2. alterar a senha sempre que existir qualquer suspeita de comprometimento de sua confidencialidade;
3. selecionar senhas de qualidades, cuidando para não usar datas de aniversários, entre outros;
4. evitar o uso dos equipamentos por outros colaboradores enquanto este estiver conectado com suas credenciais;
5. bloquear o equipamento ao se ausentar da estação de trabalho;
6. é proibido compartilhar a senha e o uso de logins automáticos e recursos de memorização de senhas são proibidos.

* *Descrever procedimentos para logins e senhas utilizados na cooperativa (tamanho mínimo de caracteres utilizados, proibição das últimas senhas utilizadas, regras em caso de expiração da senha, regras para bloqueio e desbloqueio de senhas, armazenamento em banco de forma criptografada, outras utilizadas na cooperativa)*

Os fornecedores, temporários (pessoas físicas ou jurídica), visitantes devem ter seus “Logins” diferentes dos colaboradores da cooperativa.

A***\_\_\_\_\_\_\_\_\_\_(descrever a área responsável pela segurança da informação)*** estabeleceu um fluxo de criação e bloqueio através de chamado técnico ***\_\_\_\_\_\_\_\_\_(descrever o fluxo na cooperativa, e-mail, sistemas etc.)*** que abrange as seguintes etapas:

1. admissão e demissão de colaboradores;
2. fornecedores, temporários (pessoas físicas ou jurídica), visitantes;
3. ativação ou bloqueio do login do colaborador para acesso a rede, e-mail, outros;
4. definição de acessos e permissão do colaborador pelo gestor.
   1. **BACKUP**

* *(Descrever os procedimentos de Backup realizados na cooperativa)*
  1. **SOFTWARES**

As instalações de softwares serão permitidas somente para os homologados.

A área de segurança da informação deverá realizar um inventário anual em todas as estações de trabalho e caso seja identificados softwares não homologados, poderá ser desinstalado sem aviso prévio ao colaborador e comunicado ao responsável da área.

* 1. **antivirus**

Todos os equipamentos da ***\_\_\_\_\_\_\_\_\_\_(denominação da cooperativa)*** devem possuir antivírus instalados.

* 1. **classificação de dados**

Os dados poderão ser classificados em:

1. público: quando o conteúdo puder ser distribuído a qualquer pessoa interna ou externa e for de conhecimento geral;
2. somente interno: conteúdo produzido pela cooperativa para conhecimento exclusivos dos colaboradores, terceiros e fornecedores;
3. confidencial: conteúdo sensível e de acesso apenas a pessoas que devem conhecer o conteúdo.

O acesso aos dados somente será autorizado aos usuários que tiver necessidade de conhecer a respectiva informação.

* 1. **CRIPTOGRAFIAS E CERTIFICADOS DIGITAIS**

A guarda das chaves de criptografia para acessos aos recursos computacionais devem ser mantidas de forma segura, bem como o registro de todas as chaves de criptografia e certificados digitais existentes.

Devem ter controles e documentar o processo de guarda, renovação, revogação e inutilização de certificados digitais.

* 1. **TESTES DE INVASÃO**

*a* ***\_\_\_\_\_\_\_\_\_(área de segurança da informação)*** executa periodicamente rotinas de testes de defesa contra possíveis ataques aos sistemas de informação. *(Descrever como o processo é realizado na cooperativa)*

* 1. **comunicação**

As informações sobre potenciais ameaças à integridade dos sistemas de informação são repassadas periodicamente a todos os colaboradores.

* 1. **armazenamento e descarte de informação**

Nenhuma informação confidencial deve ser deixada à vista, seja em papel ou em quaisquer dispositivos, eletrônicos ou não.

Ao usar uma impressora coletiva, recolher o documento impresso imediatamente.

Os colaboradores ou prestadores de serviços não discutir ou comentar assuntos confidenciais em locais públicos.

* 1. **Equipamentos particulares/privados**

Os equipamentos particulares/privados, como computadores ou qualquer dispositivo portátil que possa armazenar e/ou processar dados, não devem ser usados para armazenar ou processar informações relacionadas com o negócio, nem devem ser conectados às redes da cooperativa.

1. **PERIODOCIDADE DE REVISÃO**

Esta Política de Segurança da Informação (PSI) é de responsabilidade da ***\_\_\_\_\_\_\_(descrever área responsável pelo processo na cooperativa).***

A fim de assegurar a constante adequação e eficácia da segurança da informação da cooperativa esta política deverá ser revisada a cada 2 (dois) anos pela ***\_\_\_\_\_\_\_\_\_\_\_(descrever área responsável pelo processo na cooperativa)*** ou quando necessário decorrentes de mudanças na legislação ou ainda atualizações de processos internos.

1. **CONSIDERAÇÕES FINAIS**

Esta PSI após aprovação do órgão de administração deverá ser divulgada para todos os colaboradores e prestadores de serviços.

O descumprimento das diretrizes desta política sujeitará ao infrator aplicação de advertência verbal ou escrita, demissão por justa causa ou rescisão contratual, bem como demais penalidades administrativas, cíveis e penais previstas na legislação.

Esta política foi aprovada pelo ***\_\_\_\_\_\_\_\_\_\_\_\_(órgão de administração da cooperativa)*** realizada em \_\_\_\_/\_\_\_\_\_/\_\_\_.