# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

## 1. OBJETIVO

A informação é um dos principais bens de qualquer Instituição. Para a devida proteção desse bem, a Cooperativa de Crédito Rural Coopavel – Credicoopavel, com base na Resolução CMN nº 4893 de 26/02/2021 estabelece a presente Política de Segurança da Informação e Segurança Cibernética, visando assegurar a confidencialidade, integridade, disponibilidade e proteger as informações da instituição, dos cooperados, colaboradores e do público em geral para garantir a continuidade dos negócios minimizando os Riscos.

A segurança da informação é aqui caracterizada pela preservação dos seguintes conceitos:

- **Confidencialidade:** Garante que a informação seja acessível somente pelas pessoas autorizadas e devidamente credenciadas, pelo período necessário;
- **Disponibilidade:** Garante que a informação esteja disponível para as pessoas autorizadas sempre que se fizer necessária;
- **Integridade:** Garante que a informação esteja completa, exata e íntegra e que não tenha sido modificada ou destruída de maneira não autorizada ou acidental durante o seu ciclo de vida.

## 2. DEFINIÇÕES

- **Ativos de Informação:** conjunto de informações, armazenado de modo que possa ser identificado e reconhecido como valioso para a instituição.

- **Informação:** resultado do processamento e organização de dados (eletrônicos ou físicos) ou registros de um sistema. É composta por dados, mas um conjunto de dados não necessariamente é considerado uma informação.

- **Sistemas de informação:** de maneira geral, são sistemas computacionais utilizados pela instituição para suportar suas operações.

## 3. ABRANGÊNCIA

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, estagiários, prestadores de serviços, consultores, auditores, temporários, fornecedores, parceiros e associados da Cooperativa de Crédito Rural Coopavel – Credicoopavel.

Esta Política informa que os ambientes, sistemas, computadores e redes da instituição poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

É também obrigação de cada colaborador e estagiário se manter atualizado em relação a esta Política e aos Procedimentos e Normas relacionadas, buscando orientação do seu gestor ou da Gerência de Tecnologia da Informação sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

Toda informação produzida ou recebida pelos colaboradores, estagiários, prestadores de serviços, consultores, auditores, temporários, fornecedores e parceiros como resultado da atividade profissional contratada pela Credicoopavel pertence à mesma.

Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores, estagiários, consultores, auditores e temporários para a

realização das atividades profissionais. O uso pessoal dos recursos somente será permitido com autorização expressa da direção.

## 4. ESTRUTURA NORMATIVA

A estrutura normativa da Segurança da Informação da Credicoopavel é composta por um conjunto de documentos, relacionados a seguir.

- **Política:** define a estrutura, as diretrizes e os papéis referentes à segurança da informação;
- **Normas:** estabelecem regras, definidas de acordo com as diretrizes da Política, a serem seguidas em diversas situações em que a informação é tratada;
- **Procedimentos:** instrumentam as regras dispostas nas Normas, permitindo a direta aplicação nas atividades da Credicoopavel.

## 5. DIRETRIZES

A seguir, são apresentadas as diretrizes da Política de Segurança da Informação da Credicoopavel. Tais diretrizes norteiam as Normas e Procedimentos:

### 5.1. Aspectos gerais

As informações (em formato físico ou arquivos eletrônicos digitais) e os ambientes tecnológicos utilizados pelos usuários são de exclusiva propriedade da Credicoopavel, não podendo ser interpretados como de uso pessoal;

As informações da Credicoopavel, dos associados e do público em geral devem ser tratadas de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, evitando-se mau uso e exposição indevida.

Todos os colaboradores, estagiários, prestadores de serviços e demais devem ter ciência de que o uso das informações e dos sistemas de informação podem ser monitorados, e que os registros assim obtidos poderão ser utilizados para detecção de violações da Política e das Normas de Segurança da Informação, podendo estas servir de evidência para a aplicação de medidas disciplinares, processos administrativos e/ou legais;

A responsabilidade em relação à segurança da informação é comunicada na fase de contratação dos colaboradores. Todos os colaboradores são instruídos e orientados sobre os procedimentos de segurança, bem como do uso correto dos ativos de informação, a fim de reduzir possíveis riscos. Para tanto o aspecto "responsabilidade" e "confidencialidade" tratado nesta Política será exigindo, dos colaboradores, a assinatura do termo de confidencialidade e proteção de dados.

## 5.2. Tratamento da informação

Para assegurar a proteção adequada às informações, deve existir um método de classificação da informação de acordo com o grau de confidencialidade e criticidade para o negócio da Credicoopavel, se enquadrando nos seguintes níveis: Restrita, Confidencial, Interna e Pública

As informações devem ser atribuídas a um proprietário, formalmente designado como responsável pela autorização de acesso às informações sob a sua responsabilidade;

Todas as informações devem estar adequadamente protegidas em observância às diretrizes de segurança da informação da Credicoopavel em todo o seu ciclo de vida, que compreende: geração, manuseio, armazenamento, transporte e descarte;

A informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada.

Para assegurar os três itens mencionados no item 1 desta Política, a informação deve ser adequadamente gerenciada e protegida contra roubo, fraude, espionagem, perda não-intencional, acidentes e outras ameaças.

É fundamental para a proteção e salvaguarda das informações que os usuários adotem a ação de Comportamento Seguro e consistente com o objetivo de proteção das informações, devendo assumir atitudes proativas e engajadas no que diz respeito à proteção das informações.

Campanhas contínuas de conscientização de Segurança da Informação serão utilizadas para monitoração e controle destas diretrizes.

### 5.3. Gestão de acessos e identidades

O acesso às informações e aos ambientes tecnológicos da Credicoopavel deve ser controlado de acordo com sua classificação, de forma a garantir acesso apenas às pessoas autorizadas, mediante aprovação formal;

Os acessos aos colaboradores, estagiários e prestadores de serviços devem ser solicitados e aprovados somente às informações necessárias ao desempenho de suas atividades.

### 5.4. Gestão e tratamento de incidentes de segurança da informação e Cibernética.

Em casos de violação e incidentes desta Política e Normas de Segurança da Informação e Cibernética, o ocorrido deve ser informado de imediato a Diretoria

Executiva da Credicoopavel, que realizará deliberações somente nos incidentes classificados com alta criticidade, os demais casos terão tratamentos pelo fluxo normal de resposta a incidentes. Após deliberações, a Diretoria Executiva poderá tomar uma ação de segurança ou disciplinar quanto a violação ou incidente ocorrido.

Um plano de contingência e a continuidade dos principais sistemas e serviços deverão ser implantados e testados no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

Todos os requisitos de segurança da informação, incluindo a necessidade de planos de contingência, devem ser identificados na fase de levantamento de escopo de um projeto ou sistema, e justificados, acordados, documentados, implantados e testados durante a fase de execução.

### 5.5. Partes Externas

Quando necessário e, para atender demandas e necessidades pontuais da com suas contrapartes (instituição e pessoas externas), deverá constar nos contratos, uma Cláusula de Confidencialidade ou a formalização (assinatura) de um Termo de Confidencialidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela instituição.

## 6. RESPONSABILIDADES

Esta Política é implementada na Credicoopavel por meio de procedimentos específicos, obrigatórios para todos os colaboradores, independentemente do nível hierárquico ou função na instituição, bem como de vínculo empregatício ou prestação de serviço.

O não cumprimento dos requisitos previstos nesta Política e das Normas de Segurança da Informação acarretará violação às regras internas da instituição e sujeitará o usuário às medidas administrativas e legais cabíveis.

De forma geral, cabe a todos os colaboradores, estagiários e prestadores de serviços:

- Cumprir fielmente a Política, as Normas e os Procedimentos de Segurança da Informação da Credicoopavel, buscar orientação do gestor imediato em caso de dúvidas relacionadas à segurança da informação;

- Proteger as informações contra acessos, modificação, destruição ou divulgação não autorizados pela Credicoopavel;

- Assegurar que os recursos tecnológicos, as informações e sistemas a sua disposição sejam utilizados apenas para as finalidades aprovadas pela Credicoopavel;

- Cumprir as leis e as normas que regulamentam a propriedade intelectual;

- Não compartilhar informações confidenciais de qualquer tipo;

- Comunicar imediatamente à área de Gestão de Segurança da Informação qualquer descumprimento ou violação desta Política e/ou de suas Normas e Procedimentos.

### 6.1. Área de gestão de segurança da informação

Cabe à área de Gestão de Segurança da Informação:

- Prover todas as informações de gestão de Segurança da Informação solicitadas pela Diretoria Executiva;

- Prover divulgação da Política e das Normas de Segurança da Informação para todos os colaboradores, estagiários e prestadores de serviços;

- Promover ações de conscientização sobre Segurança da Informação para os colaboradores, estagiários e prestadores de serviços;

- Propor projetos e iniciativas relacionados ao aperfeiçoamento da segurança da informação da Credicoopavel;

- Estabelecer procedimentos relacionados à instrumentação da segurança da informação da Credicoopavel.

## 6.2. Conscientização em Segurança da Informação e Segurança Cibernética

A Credicoopavel deve promover a disseminação dos princípios e diretrizes de Segurança da Informação por meio de programas de conscientização e capacitação interna bem como a divulgação no site da instituição uma área com informações e dicas pertinentes para os cooperados, com o objetivo de fortalecer a cultura de Segurança da Informação.

## 6.3. Governança com as Áreas de Negócio e Tecnologia

As iniciativas e projetos das áreas de negócio e tecnologia devem estar alinhadas com as diretrizes e arquiteturas de segurança da informação, garantindo a confidencialidade, integridade e disponibilidade das informações.

## 6.4. Segurança no Desenvolvimento de Sistemas de Aplicação

O processo de desenvolvimento de sistemas de aplicação e às boas práticas de segurança, deve garantir a aderência nesta Política de Segurança da Credicoopavel.

Deverá ter controle de acesso, log de alterações de dados, controle de permissões, criptografia no tráfego das informações, adequadas aos dados armazenados.

A Credicoopavel conta com o Sistema homologado pelo BCB o qual constitui boas práticas de programação, a iniciar pelos levantamentos dos dados, análise, programação, homologação e finalmente a implantação dos programas que fazem parte do sistema. De forma a garantir que o sistema cumpra com os objetivos aos quais foi concebido, mantendo a integridade e segurança necessária para o cumprimento dos objetivos propostos.

## 6.5. Requisitos de Segurança do ambiente físico

As máquinas (servidores) que armazenam sistemas da Credicoopavel deverão estar em áreas protegidas com acesso devidamente controlado e monitorado.

A entrada nestas áreas ou partes dedicadas, por pessoas não autorizadas (visitantes, prestadores de serviço, terceiros e até mesmo colaboradores, sem acesso liberado), que necessitarem ter acesso físico ao local, sempre o farão acompanhados de pessoas autorizadas.

## 6.6. Sistema de Gestão

Os sistemas devem possuir controle de acesso lógico de modo a assegurar o uso apenas por usuários autorizados. O responsável pela autorização deve ser claramente definido e ter registrado a aprovação concedida.

## 6.7. Backup

Todos os backups devem ser automatizados por sistemas de agendamento para que seja realizado um Backup Completo diariamente dos arquivos/pastas dos usuários bem como do Banco de Dados e poderá ser realizado Backup Incremental diário do Banco de Dados.

Os colaboradores responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros.

Testes de restauração (*restore*) de backup devem ser executados por seus responsáveis, nos termos dos procedimentos específicos.

## 6.8. A Instalação de *Softwares*

A instituição respeita os direitos autorais dos *softwares* que usa e reconhece que deve pagar o justo valor por eles, não recomendando o uso de programas não licenciados nos computadores da instituição. É terminantemente proibido o uso de *softwares* ilegais (sem licenciamento).

A Infraestrutura de TI poderá valer-se deste instrumento para desinstalar, sem aviso prévio, todo e qualquer *software* sem licença de uso, em atendimento à Lei 9.609/98 (Lei do *Software*).

## 6.9. Controle de Acesso Lógico

Todo usuário deve ter uma identificação única, pessoal e intransferível, qualificando-o como responsável por qualquer atividade desenvolvida sob esta identificação. O titular assume a responsabilidade quanto ao sigilo da sua senha pessoal.

## 6.10. Rastreabilidade das informações

A Credicoopavel dispõe em seu sistema legado ferramentas para identificação de todas as solicitações e transações efetuadas pelo sistema legado e Internet Banking (Web e Mobile) sendo registrado o tipo da solicitação/transação, data e hora, informações da operação, IP do equipamento, marca e sistema operacional, sendo este acesso restrito a usuários devidamente nomeados.

É mantido e analisado Log de todas as aplicações Web e Mobile para identificar e mitigar qualquer eventual brecha ou ataque externo a aplicação e seu sistema de gerenciamento. Estes logs são mantidos por 5 anos e armazenados no local de geração bem como uma cópia é realizada e transferida para o sistema interno da Cooperativa para realização do devido backup.

São realizados testes periódicos através de ferramentas específicas para validação da segurança e criptografia aplicada aos serviços disponibilizados aos cooperados.

### 6.11. Autenticação e Criptografia

Toda solicitação realizada via Web e Mobile deve transitar em ambiente seguro com aplicação de certificados de segurança e criptografia nas duas pontas para assegurar que a informação não possa ser interceptada e decodificada.

### 6.12. Serviços em nuvem

Os serviços em nuvem deverão se comprometer com a segurança, proteção e privacidade das informações que são armazenadas ou que trafegadas por suas plataformas bem como deverão respeitar as leis de proteção de dados inerentes as suas funções.

## 7. AÇÕES EM CASO DE NÃO CONFORMIDADE

As regras que estabelecem o controle e o tratamento de situações de não conformidade relativas à Política e às Normas de Segurança da Informação da Credicoopavel devem ser tratadas conforme as Normativas internas.

Na ocorrência de violação desta Política ou das Normas de Segurança da Informação, a Diretoria Executiva poderá adotar, com o apoio da Assessoria Jurídica e de Recursos Humanos, sanções administrativas e/ou legais, que poderão culminar com o desligamento e eventuais processos criminais, se aplicáveis.

Cascavel, 25 de fevereiro de 2022

Mario José Zambiazi
Diretor Administrativo

Paulo Aparecido Arantes
Diretor Financeiro