POLÍTICA SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO

SULCREDI ÂMPLEA

2025

Sulcredi Amplea

SUMÁRIO

1. OBJETIVO

1.1 A política apresenta diretrizes e responsabilidades relacionadas à prevenção de incidentes e controle do fluxo de informações centralizadas pela Cooperativa e ameaças cibernéticas, assegurando a confidencialidade, integridade e disponibilidade das informações e a continuidade dos negócios.

2. REGULAMENTAÇÕES

Resolução CMN nº 4.557/2017: Dispõe sobre a estrutura de gerenciamento de riscos, a estrutura de gerenciamento de capital e a política de divulgação de informações;
Resolução CMN nº 4.893/2021: Dispõe sobre a política de segurança cibernética e requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil.

3. CONCEITOS

Ativo de informação: Qualquer informação, dado ou equipamento de processamento de informação que tenha valor para a Cooperativa e que necessite de proteção (ex: dados de cooperados, sistemas, servidores, notebooks).
Ameaça cibernética: Qualquer circunstância ou evento com potencial para causar dano a um sistema ou à informação no espaço cibernético, por meio de acesso não autorizado, destruição, divulgação, modificação de dados ou negação de serviço.
BCB: Banco Central do Brasil.
Canal de atendimento: meio disponibilizado pela instituição para utilização dos serviços disponíveis por seus clientes.
CMN: Conselho Monetário Nacional.
Computação em nuvem: Disponibilidade sob demanda de recursos de sistema de computador, especialmente armazenamento de dados e capacidade de computação (incluindo modelos como IaaS, PaaS e SaaS), sem o gerenciamento ativo direto pelo usuário.
Controles de segurança: Medidas (administrativas, técnicas, físicas ou

organizacionais) implementadas para prevenir, detectar, corrigir ou reduzir o risco de um incidente de segurança.

Incidente cibernético: Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança cibernética que comprometa a confidencialidade, a integridade ou a disponibilidade de um ativo de informação ou sistema.

KYC (Know Your Customer): sigla em inglês que significa “Conheça seu Cliente”, e representa o processo utilizado para obter informações integrais sobre os clientes com a finalidade de, mediante diligência prévia, conferir sua reputação, idoneidade e atestar a veracidade dos dados cadastrais informados para mitigar riscos e evitar a prática de Lavagem de Dinheiro e Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa.

LGPD: Lei Geral de Proteção de Dados, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Monitoramento: É o acompanhamento, avaliação e reporte de processos avaliados, sob a luz das diretrizes para análise de risco, por meio de indicadores e/ou processos definidos.

PCN: Plano de Continuidade dos Negócios

Perda Operacional: Valor quantificável associado aos eventos de risco operacional.

PLD/FT: Prevenção a Lavagem de Dinheiro e ao Financiamento ao Terrorismo.

PGRO: Política de Gerenciamento de Riscos Operacionais

PRI: Plano de Resposta à Incidentes

Risco Operacional: possibilidade da ocorrência de perdas resultantes de eventos externos ou de falha, deficiência ou inadequação de processos internos, pessoas ou sistemas, incluído o risco legal associado à inadequação ou deficiência em contratos firmados pela instituição, às sanções em razão de descumprimento de dispositivos legais e às indenizações por danos a terceiros decorrentes das atividades desenvolvidas pela instituição.

Segurança Cibernética: São ações voltadas para a segurança de operações, de forma a garantir que os sistemas de informação sejam capazes de resistir a eventos

no espaço cibernético capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis.

Vulnerabilidade: Uma fraqueza em um ativo, sistema ou controle que pode ser explorada por uma ou mais ameaças.

4. DIRETRIZES DE SEGURANÇA CIBERNÉTICA

4.1 GOVERNANÇA E RESPONSABILIDADES

4.1.1 A Cooperativa mantém governança e processos de segurança cibernética pautados nas boas práticas de mercado.

4.1.2 O gerenciamento de segurança cibernética é parte integrante e fundamental nas atividades da Cooperativa sendo que são medidas de segurança para a proteção e uso seguro da rede tecnológica, das soluções e dos dispositivos corporativos.

4.1.3 Adota padrões e critérios de segurança tecnológica para gestão do acesso lógico aos recursos computacionais e protege as informações corporativas de acessos, alterações e compartilhamentos indevidos.

4.1.4 A Cooperativa mantém mecanismos de proteção e gerenciamento da identidade lógica dos usuários internos e externos.

4.1.5 O ciclo de desenvolvimento de sistemas e serviços segue princípios estabelecidos de segurança cibernética, assegurando a aplicação de práticas de proteção em todas as etapas do processo.

4.1.6 Os sistemas dispõem de trilhas de auditoria que permitem a rastreabilidade de ações e a identificação de eventuais irregularidades ocorridas nos sistemas de informação ou exigidas por norma legal, preservando o sigilo e a confidencialidade das informações.

4.1.7 Estabelece procedimentos e controles preventivos destinados à detecção e mitigação de ameaças, à avaliação de seus impactos e à definição de ações para monitoramento, análise e geração de relatórios internos.

4.1.8 Realizam-se periodicamente avaliações e testes de segurança no ambiente

cibernético, com a finalidade de identificar e tratar vulnerabilidades, priorizando aquelas que possam acarretar maior risco cibernético ou efeitos relevantes sobre os negócios.

4.1.9 A gestão de incidentes de segurança cibernética abrange a detecção, análise, contenção, eliminação e recuperação dos ativos de tecnologia da informação.

4.1.10 Mantém procedimentos estruturados e elevado nível de preparação para assegurar respostas eficazes a incidentes de segurança cibernética, atuando de forma contínua no monitoramento e avaliação dos controles de proteção da infraestrutura tecnológica.

4.1.11 Implementar ações voltadas ao compartilhamento de informações relativas a incidentes de segurança cibernética relevantes com outras instituições financeiras e/ou parceiros externos.

4.1.12 São estruturados cenários de incidentes de segurança cibernética para aplicação nos testes dos planos de continuidade operacional de Tecnologia da Informação e Comunicação.

4.1.13 As decisões sobre a terceirização de serviços de segurança cibernética são orientadas pelas estratégias da organização e pelo gerenciamento de riscos.

4.2 DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

4.2.1 A Cooperativa contempla em seu planejamento estratégico a gestão da segurança da informação.

4.2.2 A Cooperativa mantém processos de governança associados à segurança da informação adequadas à natureza e complexidade de suas operações e produtos, e à dimensão de sua exposição a esse tipo de risco.

4.2.3 Os dados e as informações são ativos essenciais para a Instituição e são protegidos com soluções de segurança, visando seu uso de forma adequada, promovendo sua disponibilidade, integridade, confidencialidade e autenticidade.

4.2.4 As informações da Instituição, dos clientes/associados, dos fornecedores e dos empregados são tratadas de acordo com boas práticas de mercado, sendo adotadas medidas técnicas e administrativas de Segurança da Informação.

4.2.5 A Cooperativa comunica a ocorrência de incidentes relevantes de segurança

de acordo com sua criticidade e seus impactos nos negócios e atividades da Cooperativa.

4.2.6 Todos os ativos e serviços de informação, recursos computacionais da Instituição, bem como toda informação trafegada ou armazenada nos mesmos, são de uso exclusivo para o desempenho das atividades laborais e estão sujeitos à monitoramento.

4.2.7 O uso dos recursos computacionais, o acesso remoto à internet, à computação em nuvem, às redes sociais e comunicadores instantâneos são realizados por meio de soluções tecnológicas advindas dos prestadores de serviço contratados pela Cooperativa, previamente homologadas e parametrizadas para a devida proteção das informações.

4.2.8 O tratamento de informações corporativas e de clientes por meio de comunicadores instantâneos é efetuado por meio de comunicadores aprovados pelas áreas de tecnologia e segurança.

4.2.9 Os contratos, convênios e acordos operacionais que impliquem manuseio de informações da Cooperativa possuem cláusula de confidencialidade.

4.2.10 Os ambientes físicos e lógicos são criados e geridos de forma compatível com a confidencialidade das informações neles tratadas, inclusive com segregação de ambiente e controles de acesso adequados.

4.2.11 A Cooperativa dissemina e mantém cultura de segurança e de uso correto da informação para seus usuários, inclusive, por ações corporativas educacionais e de treinamento.

4.2.12 O Diretor de Riscos é o responsável pela Política de Segurança Cibernética, nos termos do Art. 7º da Resolução CMN nº 4.893/2021.

5. ASPECTOS GERAIS

5.1 ESTRUTURA DE GERENCIAMENTO DE RISCOS

5.1.1 A estrutura de gerenciamento dos riscos associadas à Segurança Cibernética deve prever:

a) Os procedimentos e os controles adotados para reduzir a vulnerabilidade da Cooperativa a incidentes e atender aos demais objetivos de segurança

cibernética;

b) Os mecanismos de controle, inclusive os direcionados ao acompanhamento e registro do fluxo das informações, voltados a preservar a proteção, o sigilo e a confiabilidade de dados sensíveis;
c) O registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da instituição;
d) Os cenários de incidentes considerados nos testes de continuidade dos serviços;
e) O estabelecimento de diretrizes e mecanismos de controle destinados à prevenção e à gestão de incidentes, a serem observados por prestadores de serviços que tratem dados ou informações confidenciais, ou que desempenhem funções essenciais às operações da Cooperativa;
f) A classificação dos dados e das informações quanto à relevância;
g) O estabelecimento de critérios e métricas para a avaliação da gravidade e da importância dos incidentes;
h) A capacidade de prevenir, monitorar e atenuar eventos adversos relacionados à segurança cibernética.

5.1.2 Os métodos adotados para promover a conscientização sobre segurança cibernética dentro da cooperativa, abrangendo:

- Desenvolvimento de programas de avaliação periódica de pessoal;
- Prestação de informações aos usuários finais sobre cuidados e boas práticas na utilização dos produtos e serviços disponibilizados; e
- Comprometimento da alta administração na promoção e no aprimoramento contínuo dos processos e procedimentos relacionados à segurança cibernética.

5.2 CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM

5.2.1 A Cooperativa deve assegurar que suas políticas, estratégias e estruturas para gerenciamento de riscos, especificamente no tocante aos critérios de decisão quanto à terceirização de serviços, contemplem a contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, no País

ou no exterior.

5.2.2 Antes da contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, são aplicados, em conformidade com a Política Interna de Contratação de Serviços Terceirizados, os seguintes procedimentos:

- A adoção de práticas de governança corporativa e de gestão proporcionais à relevância do serviço a ser contratado e aos riscos a que estejam expostas; e
- A verificação das qualificações técnicas e profissionais esperadas, que correspondem com o nível de complexidade do serviço a ser contratado, assegurando, o cumprimento da legislação e da regulamentação em vigor.

5.2.3 Devem ser observados, ainda, aspectos relacionados ao acesso da instituição aos dados e informações processados ou armazenados pelo prestador de serviços, à garantia da confidencialidade, integridade, disponibilidade e recuperação desses dados, à conformidade com as certificações exigidas, o fornecimento de informações e recursos necessários para o monitoramento dos serviços, bem como à adequada identificação e segregação dos dados dos usuários finais por meio de controles físicos ou lógicos.

5.2.4 A contratação de serviços relevantes de processamento e armazenamento de dados, bem como de computação em nuvem, deve ser comunicada pela instituição ao Banco Central do Brasil no prazo máximo de dez dias após sua efetivação, contendo as seguintes informações:

- A denominação da empresa contratada.
- Os serviços relevantes contratados; e
- Indicação dos países e das regiões onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados, no caso de contratação no exterior.

5.2.5 A contratação de serviços no exterior, além da comunicação prevista no item 5.2.4, está condicionada à observância dos requisitos do Art. 23 da Resolução CMN nº 4.893/2021, que inclui, entre outros:

a) A existência de convênio entre o Banco Central do Brasil e a autoridade supervisora do país onde os serviços serão prestados;
b) O prestador de serviços deve garantir o pleno acesso da Cooperativa e do Banco Central do Brasil aos dados e informações;
c) O prestador de serviços não deve criar restrições ou impedimentos à atuação do Banco Central do Brasil.

5.3 CLASSIFICAÇÃO DA INFORMAÇÃO

5.3.1 A Cooperativa classifica seus dados e informações quanto à sensibilidade, visando aplicar os controles de proteção adequados para preservar sua confidencialidade, integridade e disponibilidade.

5.3.2 A classificação deve, no mínimo, contemplar os seguintes níveis:

- **Pública**: Informações que podem ser divulgadas externamente sem restrições, para o público em geral.
- **Interna**: Informações de uso exclusivo e disponível para todos os colaboradores e terceiros autorizados.
- **Confidencial**: Informações sensíveis cujo acesso é restrito a grupos específicos e cuja divulgação não autorizada pode causar impacto financeiro, legal ou de reputação à Cooperativa ou seus cooperados.

5.3.3 Procedimentos e normas internas específicas estabelecerão os requisitos de manuseio, armazenamento, tráfego, descarte e proteção para cada nível de classificação.

6. CANAIS DE ATENDIMENTO AO CLIENTE

Dúvidas, sugestões, elogios ou reclamações: sac@amplea.coop.br
Canal de Denúncia: https://contato.amplea.coop.br/canal-de-etica
Ouvidoria: 0800 761 6196 – das 8h às 17h, de segunda a sexta-feira.
Redes Sociais: @Sulcrediamplea

7. VIGÊNCIA

7.1 Esta política entra em vigor na data de sua publicação e será revisada

sempre que o conselho de administração entender necessário ou anualmente, conforme estabelecido pela Regulamentação vigente.

Histórico de atualizações			
Versão	**Data de aprovação**	**Área(s) responsável(eis) pelo desenvolvimento**	**Aprovado por**
V3	14/10/2025	Suporte/TI Compliance	Conselho de Administração
Abrangência da norma: Equipe funcional, terceiros contratados e terceiros interessados			
Classificação da informação: *Uso público*			