COOPERATIVA DE CRÉDITO CRED VALE DOCE

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)
PSI-2025

Cred Vale Doce

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)	
	Data de Publicação: 29-11-2025	Versão: 001-PSI-2025
	Classificação: Interna 🟡	Revisão: Luana Souza, 26-11-2025

Índice

1. INTRODUÇÃO

A Política de Segurança da Informação (PSI) da Cred Vale Doce estabelece o conjunto estruturado de diretrizes que regula a forma como a informação é concebida, tratada, armazenada, manipulada, transmitida e descartada dentro da cooperativa. Em uma instituição financeira cooperativa, a informação constitui um ativo estratégico cuja proteção se torna essencial não apenas para a operação segura dos serviços de crédito, mas também para a preservação da confiança dos cooperados, da integridade do sistema financeiro e da conformidade com normas regulatórias rigorosas.

A Cred Vale Doce opera em um ambiente caracterizado por intensa digitalização de processos, integrações sistêmicas com instituições financeiras, uso de plataformas eletrônicas e tratamentos contínuos de dados sensíveis. Nesse cenário, a segurança da informação representa um pilar de sustentação da estabilidade operacional, mitigando riscos cibernéticos, prevenindo atos de engenharia social, evitando vazamentos e assegurando que cada sistema desempenhe sua função de forma segura e controlada.

Esta PSI busca consolidar de maneira analítica e normativa os princípios fundamentais da segurança da informação dentro da cooperativa, oferecendo um documento orientador que sustenta auditorias, ações preventivas, investigações de anomalias, análises de risco e gestão de incidentes. É um instrumento vivo, em constante aprimoramento, alinhado às exigências legais, ao avanço tecnológico e às melhores práticas nacionais e internacionais.

1.1. OBJETIVO

O objetivo desta política é definir a estrutura normativa que orienta o tratamento seguro das informações na Cred Vale Doce, assegurando que todos os dados institucionais, financeiros, operacionais e pessoais sejam protegidos de acordo com seu valor, criticidade e sensibilidade. A PSI promove uma visão holística da segurança da informação, articulando conceitos, regras e responsabilidades que sustentam o modelo de governança da cooperativa.

A política também objetiva promover uma cultura organizacional baseada em responsabilidade, vigilância e conformidade, garantindo que colaboradores, parceiros e fornecedores compreendam o papel que desempenham na proteção dos ativos informacionais. Não apenas estabelece controles, mas orienta comportamentos, determina limites de uso e fortalece a capacidade institucional de detectar, responder e aprender com incidentes.

1.2. ESCOPO

Esta política é aplicável a todas as pessoas e entidades que acessam, manipulam ou armazenam informações pertencentes à Cred Vale Doce. Engloba colaboradores, estagiários, prestadores de serviço, consultores externos, parceiros tecnológicos, fornecedores, equipes terceirizadas e qualquer indivíduo que, por sua função ou atividade, tenha contato com sistemas da cooperativa.

O escopo abrange ainda todos os ambientes tecnológicos e físicos que suportam os processos da organização, incluindo data centers, ambientes em nuvem, estações de trabalho, redes internas, dispositivos móveis corporativos, documentos físicos, repositórios digitais, aplicações internas e sistemas de terceiros integrados por meio de APIs ou convênios.

Esta PSI está vinculada às demais políticas internas relativas a segurança, tecnologia, continuidade de negócios, privacidade e controles operacionais. Seu cumprimento é obrigatório e sua aplicação se estende a todo o ciclo de vida da informação.

2. PRINCÍPIOS DE SEGURANÇA

A Cred Vale Doce adota princípios estruturantes que fundamentam toda a sua governança de segurança da informação. Esses princípios orientam decisões estratégicas, implementação de controles e o comportamento esperado dos usuários que interagem com os sistemas corporativos.

2.1. CONFIDENCIALIDADE

O princípio da confidencialidade estabelece que a informação deve ser acessada exclusivamente por pessoas ou sistemas que possuam autorização formal. Em um ambiente onde dados financeiros, pessoais e estratégicos circulam continuamente, a proteção contra acessos indevidos é vital para a preservação da confiança e para o cumprimento de exigências legais.

A cooperativa financeira implementa mecanismos que asseguram que a informação não seja visualizada, transferida ou divulgada sem permissão. Esses mecanismos incluem processos formais de classificação da informação, autenticação reforçada, gestão de identidades, criptografia e controles de monitoramento. A preservação da confidencialidade é tratada como obrigação institucional e individual.

2.2. INTEGRIDADE

A integridade garante que a informação permaneça completa, precisa e confiável ao longo de todo seu ciclo de vida. Alterações não autorizadas, sejam acidentais ou maliciosas, podem comprometer transações financeiras, relatórios contábeis, decisões de crédito e registros regulatórios. Por isso, a cooperativa adota mecanismos de validação, trilhas de auditoria, controles de versões, reconciliações e verificações sistemáticas.

A integridade não se limita ao aspecto técnico: envolve também processos administrativos que asseguram que cada dado seja tratado de forma correta desde sua origem. Preservar a integridade é fundamental para garantir transparência, confiança e conformidade.

2.3. DISPONIBILIDADE

Garantir a disponibilidade significa assegurar que sistemas, informações e serviços essenciais estejam acessíveis sempre que necessários. A cooperativa depende de plataformas contínuas para atendimento ao cooperado, concessão de

crédito, integrações bancárias e comunicação interna. Qualquer interrupção pode gerar impactos operacionais, financeiros e reputacionais.

Para promover a disponibilidade, a Cred Vale Doce utiliza mecanismos de redundância, políticas de backup estruturadas, enlaces de comunicação alternativos, monitoramento contínuo e planos formais de continuidade de negócios. Esses mecanismos permitem que a organização opere mesmo diante de falhas, incidentes ou adversidades externas.

2.4. CLASSIFICAÇÃO DA INFORMAÇÃO

A Cred Vale Doce classifica todas as informações sob seu controle de acordo com seu valor, criticidade e sensibilidade, assegurando que sejam tratadas, armazenadas, transmitidas e descartadas de forma adequada. A classificação da informação orienta os controles de acesso, a aplicação de criptografia, o armazenamento seguro, a transmissão confiável e o descarte responsável, garantindo conformidade com a LGPD, normas do Banco Central e melhores práticas de segurança da informação.

As informações da cooperativa são categorizadas em quatro níveis principais:

- **Público:** São informações que podem ser divulgadas externamente sem riscos à cooperativa ou aos cooperados. Incluem, por exemplo, comunicados institucionais, materiais de marketing e informações gerais de caráter não sensível.

- **Interno:** São informações destinadas exclusivamente ao uso interno da cooperativa e não devem ser compartilhadas com o público externo. Exemplos incluem procedimentos internos, organogramas e comunicados internos.

- **Confidencial:** São informações sensíveis, cujo acesso deve ser restrito a pessoas autorizadas. O vazamento ou acesso indevido pode gerar impactos legais, financeiros ou reputacionais. Entre elas estão os dados de

cooperados, relatórios financeiros internos e contratos estratégicos.

- **Secreto ou Restrito:** São informações críticas, cujo acesso deve ser estritamente controlado, devido ao potencial de causar prejuízos significativos à cooperativa em caso de divulgação indevida. Incluem credenciais de sistemas críticos, chaves criptográficas, relatórios de auditoria interna e investigações de incidentes.

A classificação deve ser aplicada a todas as informações geradas, armazenadas, transmitidas ou descartadas, considerando todo o seu ciclo de vida: desde a criação, passando pelo armazenamento e uso, até a transmissão e o descarte final. O acesso a informações classificadas como Confidenciais ou Restritas será sempre controlado de acordo com o modelo de **Controle de Acesso Baseado em Função (RBAC)**, garantindo que apenas colaboradores devidamente autorizados tenham acesso.

Além disso, a Cred Vale Doce assegura que todos os colaboradores recebam orientação e treinamento contínuo sobre a aplicação correta da classificação da informação, tanto na integração quanto em reciclagens periódicas, fortalecendo a cultura de proteção e responsabilidade no tratamento dos dados da cooperativa. A correta aplicação da classificação é uma responsabilidade compartilhada por todos, e quaisquer situações suspeitas devem ser reportadas à equipe de Segurança da Informação.

Informações classificadas como Confidenciais ou Restritas devem ser armazenadas e transmitidas utilizando mecanismos de criptografia, incluindo AES, e, quando aplicável, proteção via HSM, garantindo confidencialidade e integridade.

3. GERENCIAMENTO DE ACESSO

O gerenciamento de acesso regula formalmente como as permissões são concedidas, monitoradas, modificadas e revogadas dentro da cooperativa. Este processo é estruturado de forma a garantir que somente usuários devidamente autorizados possam acessar informações compatíveis com suas funções.

As permissões de acesso a sistemas e informações também considerarão a classificação da informação, garantindo que dados Confidenciais ou Restritos sejam acessados apenas por usuários autorizados de acordo com suas funções.

3.1. CONTROLE DE ACESSO

Para isso, a Cred Vale Doce adota o modelo de Controle de Acesso Baseado em Função (RBAC), no qual as permissões são concedidas a partir de perfis definidos previamente de acordo com responsabilidades funcionais. Atribuições de acesso são sempre individuais e nunca compartilhadas, reforçando o princípio de rastreabilidade.

3.2. AUTENTICAÇÃO

O processo de autenticação é conduzido de forma rigorosa, utilizando senhas fortes, verificação de duas etapas e mecanismos adicionais aplicados a sistemas sensíveis. Alterações de função, desligamentos ou movimentações internas são imediatamente refletidas na revisão de acessos, evitando que permissões desnecessárias permaneçam ativas e garantindo rastreabilidade. Para reforçar a segurança, todos os usuários que manipulam informações sensíveis devem utilizar Autenticação Multifator (MFA) ou Two-Factor Authentication (2FA).

3.3. AUTORIZAÇÃO

A autorização será baseada em perfis de acesso definidos também por função (RBAC). Funcionários, Gerentes de Departamentos e equipe de staff terão permissões distintas, limitando o acesso à informações e sistemas conforme suas necessidades. O acesso a dados administrativos e sensíveis será restrito apenas a pessoas autorizadas.

4. SEGURANÇA FÍSICA E AMBIENTAL

A segurança física e ambiental da Cred Vale Doce constitui um pilar fundamental para a proteção dos ativos de informação, complementando os

controles lógicos e organizacionais estabelecidos nas demais seções desta política. Assim como ameaças digitais, riscos físicos, como acesso não autorizado, desastres ambientais, falhas estruturais ou danos acidentais, podem comprometer a confidencialidade, a integridade e a disponibilidade das informações, especialmente em ambientes que abrigam infraestrutura crítica de TI e arquivos sensíveis.

As diretrizes a seguir estabelecem requisitos mínimos para proteção das instalações, controle de acesso físico e mitigação de riscos ambientais, garantindo um ambiente seguro, monitorado e em conformidade com práticas reconhecidas no setor financeiro.

4.1. PROTEÇÃO DE INSTALAÇÕES

A Cred Vale Doce adota medidas de proteção destinadas a assegurar que áreas operacionais e administrativas — incluindo salas técnicas, infraestrutura de comunicação, espaços de atendimento ao cooperado e arquivos físicos — sejam resguardadas contra ameaças internas e externas.

A proteção das instalações inclui:

- utilização de barreiras físicas (portas reforçadas, trancas, fechaduras eletrônicas e divisórias seguras);
- vigilância permanente por meio de sistemas de monitoramento eletrônico;
- adoção de rotinas de inspeção periódica das áreas críticas;
- manutenção preventiva de equipamentos e estruturas que suportam os serviços essenciais;
- garantia de que áreas sensíveis permaneçam isoladas de ambientes públicos ou de livre circulação.

Esses mecanismos minimizam riscos de sabotagem, danos intencionais, furtos, acidentes e interrupções operacionais.

4.2. CONTROLE DE ACESSO FÍSICO

O acesso físico às instalações da cooperativa é regulamentado, monitorado e concedido conforme critérios de necessidade e função. A Cred Vale Doce implementa controles que asseguram que somente pessoas devidamente autorizadas possam ingressar em ambientes classificados como críticos, incluindo salas de servidores, áreas de telecomunicações, setores administrativos sensíveis e depósitos de documentação.

Os controles de acesso físico compreendem:

- identificação individual por crachá, biometria ou outros mecanismos de autenticação;
- registro obrigatório de entrada e saída de colaboradores, visitantes e prestadores de serviço;
- acompanhamento presencial de visitantes por colaboradores da área responsável;
- revisão periódica da lista de acessos autorizados, com revogação imediata em caso de desligamento ou alteração de funções;
- monitoramento contínuo por circuito fechado de TV (CFTV) com retenção segura das gravações;
- alarmes e travas automatizadas em ambientes de alta criticidade.

A gestão de acesso físico está alinhada ao princípio do menor privilégio e integra as práticas gerais de controle de acesso estabelecidas pela cooperativa.

4.3. SEGURANÇA AMBIENTAL

Para garantir a continuidade das operações e preservar a integridade de equipamentos e informações, a Cred Vale Doce adota medidas de segurança ambiental que mitigam riscos relacionados a incêndios, flutuações de energia, condições inadequadas de temperatura ou umidade, infiltrações, alagamentos e outros eventos que possam afetar a infraestrutura de TI ou arquivos sensíveis.

As medidas incluem:

- sistemas de detecção e combate a incêndio adequados ao ambiente tecnológico (como detectores de fumaça, alarmes e extintores compatíveis com equipamentos eletrônicos);
- uso de nobreaks (UPS), estabilizadores e redundâncias elétricas para garantir alimentação contínua e protegida;
- climatização controlada em salas técnicas, mantendo temperatura e umidade dentro de parâmetros recomendados;
- instalação de sensores ambientais e monitoramento remoto para detecção precoce de falhas;
- manutenção programada de sistemas elétricos, hidráulicos e estruturais;
- áreas de armazenamento físico protegidas contra luz solar excessiva, pragas, poeira e degradação ambiental.

Esses controles reduzem a probabilidade de interrupções, prolongam a vida útil dos equipamentos e reforçam a confiabilidade da infraestrutura da cooperativa.

5. SEGURANÇA DE REDES E COMUNICAÇÕES

A Segurança de Redes e Comunicações da Cred Vale Doce compreende um conjunto estruturado de controles destinados a garantir que as informações em trânsito ou armazenadas nos ambientes de rede permaneçam protegidas contra acessos não autorizados, interceptações, adulterações e interrupções. Esses controles são alinhados às práticas recomendadas pelo Banco Central do Brasil, pela ISO/IEC 27033 e pelos requisitos operacionais específicos do setor financeiro.

5.1. PROTEÇÃO DE REDES

A Cred Vale Doce mantém uma arquitetura de redes projetada para segregar ambientes e limitar a exposição a riscos cibernéticos. A proteção de redes é implementada por meio de camadas de defesa que incluem firewalls de última geração, sistemas de controle de acesso, segmentação de VLANs, gateways seguros e mecanismos de criptografia aplicados a dados sensíveis.

As redes internas que suportam sistemas financeiros e informações críticas são isoladas das redes corporativas gerais e das redes de convidados, reduzindo a probabilidade de movimentação lateral de ameaças. O tráfego de dados é avaliado continuamente, e configurações de segurança são revisadas periodicamente para assegurar conformidade com requisitos técnicos e regulatórios.

5.2. MONITORAMENTO E DETECÇÃO DE INTRUSÕES

O ambiente tecnológico da cooperativa é monitorado por ferramentas especializadas capazes de identificar comportamentos anômalos, tentativas de intrusão, varreduras não autorizadas e padrões de ataque. A Cred Vale Doce utiliza soluções de Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) e ferramentas de análise de eventos correlacionadas a um sistema de monitoramento contínuo.

Esse monitoramento permite identificar precocemente potenciais violações, garantindo resposta rápida e coordenada. Logs de rede, eventos de firewall e indicadores de risco são mantidos, analisados e armazenados de acordo com requisitos legais e auditorias internas.

5.3. CRIPTOGRAFIA E PROTEÇÃO DE DADOS

A Cred Vale Doce adota mecanismos avançados de criptografia para proteger informações em trânsito e em repouso.

- AES (Advanced Encryption Standard): utilizado para proteger dados sensíveis tanto em repouso quanto em trânsito, garantindo integridade e confidencialidade.
- HSMs (Hardware Security Modules): dispositivos físicos dedicados ao armazenamento seguro de chaves criptográficas e à execução de operações de criptografia, protegendo credenciais, certificados digitais e informações críticas da cooperativa, complementando a proteção em todos os níveis de armazenamento e transmissão.

A aplicação desses mecanismos complementa as políticas de controle de acesso, autenticação e monitoramento, reforçando a segurança de toda a infraestrutura tecnológica da cooperativa.

6. GESTÃO DE INCIDENTES DE SEGURANÇA

A Cred Vale Doce mantém um processo estruturado, contínuo e formalizado para identificação, tratamento e resolução de incidentes de segurança da informação. A gestão de incidentes tem como objetivo preservar a integridade dos sistemas, minimizar impactos operacionais, proteger dados sensíveis e assegurar conformidade com normas regulatórias, especialmente as diretrizes do Banco Central do Brasil e da LGPD. Esse processo envolve todas as áreas da cooperativa e depende tanto de mecanismos tecnológicos quanto de práticas organizacionais alinhadas ao Plano de Continuidade de Negócios e ao Plano de Resposta a Incidentes.

6.1. RESPOSTA A INCIDENTES

A resposta a incidentes é conduzida por um ciclo estruturado que compreende detecção, análise, contenção, erradicação e recuperação. Quando um evento suspeito é identificado — seja por alertas automáticos dos sistemas de monitoramento, seja por relatos de usuários — a equipe de segurança realiza uma avaliação inicial para classificar a gravidade do incidente e definir o fluxo de tratamento.

Em situações críticas, como ataques cibernéticos, comprometimento de credenciais, indisponibilidade de sistemas essenciais ou vazamento de dados de cooperados, medidas imediatas de contenção são executadas para limitar a propagação do impacto. Posteriormente, a equipe conduz ações de erradicação da causa raiz e trabalha para restaurar os serviços afetados com o mínimo de interrupção possível. Evidências do incidente são preservadas conforme boas práticas forenses, possibilitando análises posteriores e, quando necessário, apoio a investigações internas ou externas.

A comunicação interna é um elemento essencial desse processo, garantindo que as áreas afetadas sejam devidamente informadas e que medidas emergenciais sejam coordenadas de forma eficiente. Quando aplicável, são acionados os procedimentos de escalonamento para a alta direção e para os órgãos reguladores.

6.2. RELATÓRIOS DE INCIDENTES

Todos os incidentes, independentemente de sua criticidade, devem ser reportados à área de Segurança da Informação pelos colaboradores, prestadores, parceiros ou equipes técnicas. O registro deve ocorrer imediatamente após a identificação do evento, utilizando-se os canais oficiais previstos no Plano de Resposta a Incidentes, como sistema de chamados ou contato direto com a equipe responsável.

Os relatórios elaborados pela área de segurança descrevem detalhadamente a natureza do incidente, seu impacto, as ações corretivas adotadas, a análise das causas e as recomendações preventivas. Incidentes de maior gravidade, especialmente aqueles relacionados a dados pessoais ou que afetam a continuidade dos serviços bancários, podem demandar relatórios formais adicionais ao Banco Central do Brasil, à Autoridade Nacional de Proteção de Dados (ANPD) e à diretoria executiva, em conformidade com os requisitos legais e regulatórios.

7. CONSCIENTIZAÇÃO E TREINAMENTO EM SEGURANÇA

A Cred Vale Doce reconhece que a segurança da informação depende não apenas de mecanismos tecnológicos, mas também de comportamento humano. Por isso, investe continuamente na formação e no engajamento dos colaboradores para construir uma cultura organizacional orientada à proteção da informação, ao cumprimento de normas e à prevenção de riscos operacionais.

7.1. PROGRAMA DE CONSCIENTIZAÇÃO

O programa de conscientização em segurança tem caráter permanente e visa sensibilizar todos os colaboradores sobre a importância de práticas seguras no ambiente corporativo. A iniciativa compreende a divulgação de comunicados, campanhas internas, materiais instrucionais, simulações de ataques de engenharia social e orientações sobre políticas e procedimentos. A conscientização abrange temas como proteção de senhas, uso seguro de e-mail, prevenção a fraudes, manipulação de informações sensíveis, boas práticas digitais e responsabilidade individual na defesa do ambiente corporativo.

7.2. TREINAMENTO EM SEGURANÇA

Os treinamentos são fornecidos desde o momento da integração do colaborador e são renovados periodicamente conforme o nível de exposição, categoria de risco e função desempenhada. Equipes críticas, como TI, atendimento e áreas de operações financeiras, recebem treinamentos complementares e atualizações sempre que houver mudanças tecnológicas, novos sistemas ou revisão de políticas. A cooperativa busca garantir que todos compreendam claramente as suas responsabilidades e saibam agir adequadamente frente a incidentes ou comportamentos suspeitos.

8. AVALIAÇÃO E MELHORIA CONTÍNUA

A Cred Vale Doce mantém um processo sistemático de aprimoramento contínuo de sua segurança da informação. A avaliação constante de processos,

controles e mecanismos tecnológicos permite identificar falhas, corrigir vulnerabilidades e fortalecer a maturidade de segurança da cooperativa.

8.1. AUDITORIAS DE SEGURANÇA

Auditorias internas e externas são realizadas periodicamente com o propósito de verificar a conformidade da cooperativa às normas internas, regulamentações aplicáveis e boas práticas do mercado. As auditorias incluem revisões técnicas dos ambientes de TI, avaliação de processos administrativos, análise de controles internos e testes de aderência às políticas.

8.2. REVISÃO DE POLÍTICAS E PROCEDIMENTOS

As políticas de segurança, incluindo esta PSI, são revisadas em intervalos regulares ou sempre que mudanças tecnológicas, organizacionais ou normativas justificarem atualizações. Essa revisão contínua garante que as diretrizes permaneçam alinhadas às práticas modernas de segurança e às exigências do Banco Central, da LGPD e das normas ISO.

8.3. ANÁLISE DE RISCOS

A análise de riscos é conduzida para identificar ameaças potenciais, vulnerabilidades, impactos operacionais e probabilidades de ocorrência. Esse processo orienta a priorização de investimentos em segurança, a implementação de controles mitigatórios e a definição de estratégias que garantam a continuidade das operações em cenários adversos. A análise de risco também subsidia o planejamento do ambiente de rede da cooperativa, especialmente no que diz respeito à proteção dos dados financeiros e ao funcionamento de sistemas bancários críticos.

8.4. MEDIÇÃO DE DESEMPENHO

A eficácia das ações de segurança da informação é avaliada por meio de indicadores-chave de desempenho (KPIs) definidos pela cooperativa. Esses indicadores permitem monitorar incidentes, tempos de resposta, taxas de

vulnerabilidades corrigidas, adesão a treinamentos, sucessos e falhas de auditorias. Os resultados são analisados pela direção, permitindo a tomada de decisões baseadas em evidências e a melhoria constante dos controles.

9. CONFORMIDADE LEGAL E REGULATÓRIA

A Cred Vale Doce atua em conformidade com o conjunto de leis, regulamentações e normativas que orientam a proteção da informação no setor financeiro. A aderência regulatória é fundamental para garantir confiança, transparência e segurança nos serviços prestados aos cooperados.

9.1. CONFORMIDADE COM LEIS E REGULAMENTAÇÕES

A Cred Vale Doce compromete-se a cumprir a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e o Marco Civil da Internet (Lei nº 12.965/2014), bem como as normas emitidas pelo Banco Central do Brasil que disciplinam a segurança cibernética e a continuidade das operações no Sistema Financeiro Nacional. Em particular, observa a Resolução CMN nº 4.893/2021, que estabelece requisitos mínimos para a política de segurança cibernética e para a contratação de serviços de processamento, armazenamento de dados e computação em nuvem por instituições autorizadas pelo Banco Central. O cumprimento dessas normas assegura que a Cred Vale Doce atue com responsabilidade, governança adequada e em conformidade com o arcabouço regulatório, protegendo os cooperados e fortalecendo a confiança no sistema.

9.2. GERENCIAMENTO DE VULNERABILIDADES E PATCHES

A cooperativa mantém um processo formal para identificar, priorizar e corrigir vulnerabilidades nos sistemas, equipamentos e aplicações que suportam suas operações. Esse processo inclui varreduras periódicas, aplicação de patches de segurança, monitoramento de atualizações críticas e avaliação constante da exposição a riscos cibernéticos. A manutenção contínua do ambiente tecnológico reduz a probabilidade de exploração de falhas e reforça a confiabilidade dos sistemas bancários utilizados pela organização.

10. RESPONSABILIDADES

As responsabilidades por segurança da informação são organizadas conforme a estrutura hierárquica da cooperativa, garantindo clareza de atribuições e efetividade nos controles.

10.1. DIREÇÃO

A direção da Cred Vale Doce é responsável pelo apoio institucional às iniciativas de segurança, garantindo recursos adequados, alinhamento estratégico e supervisão dos programas implementados. A alta gestão valida políticas, acompanha indicadores e assegura que a segurança da informação esteja integrada aos objetivos organizacionais e às obrigações regulatórias.

10.2. EQUIPE DE SEGURANÇA DA INFORMAÇÃO

A equipe de Segurança da Informação é responsável pela implementação, monitoramento e manutenção dos controles estabelecidos nesta PSI. Suas atribuições incluem o tratamento de incidentes, a gestão de acessos, a análise de vulnerabilidades, a condução de treinamentos, o acompanhamento de auditorias e a atualização das políticas internas. Também compete a essa equipe orientar colaboradores e atuar como ponto de contato com órgãos reguladores quando necessário.

10.3. FUNCIONÁRIOS

Todos os colaboradores têm responsabilidade direta na proteção da informação e devem cumprir rigorosamente as políticas e procedimentos estabelecidos. Devem utilizar os sistemas corporativos de forma adequada, evitar práticas que elevem o risco operacional, resguardar dados sensíveis e reportar imediatamente qualquer situação suspeita ou incidente aos canais oficiais de segurança.

11. DOCUMENTOS DE REFERÊNCIA

A elaboração desta Política de Segurança da Informação da Cred Vale Doce baseou-se em um conjunto de normas, legislações, frameworks e documentos internos e externos amplamente reconhecidos no setor financeiro e nas práticas modernas de gestão da segurança da informação. Esses documentos serviram como fundamento para estruturar diretrizes, responsabilidades e controles que garantem aderência regulatória, robustez operacional e alinhamento às melhores práticas do mercado.

A seguir, estão listados os principais documentos considerados na construção desta PSI, organizados por natureza normativa e relevância para o contexto da cooperativa.

11.1 NORMAS E REGULAMENTAÇÕES NACIONAIS

A presente Política de Segurança da Informação foi elaborada em conformidade com o arcabouço jurídico e regulatório brasileiro aplicável ao tratamento de dados, à segurança cibernética e ao gerenciamento de riscos no setor financeiro. Entre os principais instrumentos normativos considerados, destacam-se:

Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709/2018)
Estabelece regras para o tratamento de dados pessoais, direitos dos titulares, bases legais aplicáveis e obrigações de controladores e operadores, impactando diretamente os processos de gestão da informação da cooperativa.

Marco Civil da Internet (Lei nº 12.965/2014)
Define princípios e garantias para o uso da internet no Brasil, incluindo diretrizes para guarda de registros, proteção da privacidade, neutralidade de rede e responsabilidades correlatas.

Normativos do Banco Central do Brasil e do Conselho Monetário Nacional, com destaque para:

- **Resolução CMN nº 4.893/2021** - Dispõe sobre a política de segurança cibernética das instituições financeiras, requisitos para contratação de serviços de processamento e armazenamento de dados e obrigações relacionadas à gestão de riscos tecnológicos. Revoga a Resolução CMN nº 4.658/2018.

- **Resolução CMN nº 4.557/2017** - Estabelece a estrutura de gerenciamento de riscos e controles internos, incluindo requisitos de estratégia, apetite de risco, processos de monitoramento e governança corporativa.

- **Resolução BCB nº 85/2021** - Regulamenta diretrizes para segurança cibernética, continuidade de negócios e comunicação de incidentes relevantes ao Banco Central do Brasil.

Essas normas orientam a implementação dos controles mínimos obrigatórios para instituições do Sistema Financeiro Nacional, assegurando que a Cred Vale Doce opere de forma segura, responsável e alinhada às expectativas dos órgãos supervisores.

11.2 NORMAS INTERNACIONAIS E BOAS PRÁTICAS

Para garantir alinhamento às melhores práticas e a padrões reconhecidos mundialmente, foram considerados os seguintes referenciais internacionais:

ISO/IEC 27001 – Sistemas de Gestão de Segurança da Informação
Define requisitos para implementação, operação, monitoramento, revisão e melhoria contínua de um SGSI, servindo como base metodológica para a estrutura desta política.

ISO/IEC 27002 – Controles de Segurança da Informação, Cibersegurança e Privacidade
Fornece diretrizes detalhadas e recomendações de controles técnicos, físicos e

organizacionais, abordando temas como controles de acesso, redes, gestão de ativos, resposta a incidentes e proteção física.

ISO/IEC 27005 – Gestão de Riscos de Segurança da Informação
Estabelece diretrizes para condução sistemática de identificação, análise, avaliação e tratamento de riscos, contribuindo para o modelo de gestão adotado pela cooperativa.

NIST Cybersecurity Framework (NIST CSF – Versão 1.1 / Versão 2.0)
Utilizado como referencial complementar para organização das capacidades de Identificar, Proteger, Detectar, Responder e Recuperar, fortalecendo a maturidade da postura de segurança cibernética.

Esses padrões internacionais forneceram suporte metodológico, apresentação de controles e benchmarks de maturidade aplicáveis ao contexto da Cred Vale Doce.

12. GLOSSÁRIO

AES (Advanced Encryption Standard)

Algoritmo de criptografia amplamente utilizado para proteção de dados sensíveis, garantindo confidencialidade e segurança em repouso e em trânsito.

API / APIs (Application Programming Interface)

Conjunto de padrões que permite a comunicação e integração entre sistemas internos e externos, incluindo parceiros e instituições financeiras.

BCB (Banco Central do Brasil)

Autoridade responsável pela regulação e supervisão do Sistema Financeiro Nacional, incluindo normas de segurança cibernética e continuidade de negócios.

CFTV (Circuito Fechado de Televisão)

Sistema de câmeras utilizado para vigilância, controle de acesso e monitoramento de áreas físicas da cooperativa.

CMN (Conselho Monetário Nacional)

Órgão regulador que estabelece diretrizes gerais para políticas monetárias, cambiais e de crédito, incluindo normas de segurança da informação e riscos.

CSF (Cybersecurity Framework – NIST)

Framework de segurança cibernética desenvolvido pelo NIST, estruturado nas funções Identificar, Proteger, Detectar, Responder e Recuperar.

Disponibilidade

Princípio de segurança que assegura que sistemas, serviços e informações estejam acessíveis sempre que necessários para as operações da cooperativa.

HSM / HSMs (Hardware Security Modules)

Dispositivos físicos que armazenam e processam chaves criptográficas com segurança, protegendo operações sensíveis e credenciais críticas.

IDS (Intrusion Detection System)

Sistema que monitora redes e sistemas para identificar tentativas ou comportamentos suspeitos, alertando a equipe de segurança sobre possíveis intrusões.

Integridade

Princípio que garante que dados e informações permaneçam completos, exatos e não alterados de maneira não autorizada.

IPS (Intrusion Prevention System)

Sistema que, além de detectar ameaças, é capaz de agir automaticamente para bloquear ataques antes que causem danos.

LGPD (Lei Geral de Proteção de Dados – Lei nº 13.709/2018)

Regulamenta o tratamento de dados pessoais, estabelecendo direitos, responsabilidades e obrigações para proteção da privacidade e segurança.

MFA (Autenticação Multifator – Multi-Factor Authentication)

Método de verificação que exige duas ou mais credenciais para confirmar a identidade do usuário, aumentando a segurança dos acessos.

Disponibilidade

Princípio de segurança que garante que sistemas e informações estejam acessíveis quando necessário para as operações corporativas.

PSI (Política de Segurança da Informação)

Documento que define princípios, controles, diretrizes e responsabilidades para a proteção dos ativos de informação da cooperativa.

RBAC (Role-Based Access Control)

Modelo de controle de acesso baseado em papéis, garantindo que cada usuário possua apenas as permissões necessárias para suas funções.

SSL / TLS (Secure Sockets Layer / Transport Layer Security)

Protocolos de criptografia utilizados para proteger dados em trânsito, garantindo comunicação segura entre sistemas, aplicações e usuários.

2FA (Two-Factor Authentication)

Método de autenticação que exige dois fatores de verificação (senha + código, senha + biometria, etc.), reforçando a segurança no acesso a sistemas.

TI (Tecnologia da Informação)

Área responsável pelos sistemas, infraestrutura tecnológica, segurança da informação, redes e suporte técnico da cooperativa.

UPS (Uninterruptible Power Supply)

Equipamento (nobreak) que fornece energia temporária em caso de falha elétrica, garantindo continuidade e proteção para equipamentos críticos.