

	Política De Segurança Da Informação		
	Versão: 1.0 Data: 01/08/2025	Departamento Emissor: Tecnologia da Informação	Aprovação: Diretoria Executiva

1. OBJETIVO

A presente Política de Segurança da Informação tem por objetivo estabelecer diretrizes, princípios, responsabilidades e controles para garantir a confidencialidade, integridade, disponibilidade e autenticidade das informações no âmbito da CredutPay.

Visa assegurar a proteção dos ativos informacionais, a continuidade dos negócios, a mitigação de riscos operacionais e a conformidade com requisitos legais, regulatórios e melhores práticas de mercado.

2. ABRANGÊNCIA

Esta Política aplica-se a:

- Todos os colaboradores, administradores e estagiários;
- Prestadores de serviços, parceiros e fornecedores;
- Sistemas, aplicações, infraestrutura tecnológica e ambientes operacionais;
- Informações em formato físico ou digital sob responsabilidade da CredutPay.

3. NORMAS E REFERÊNCIAS

A CredutPay adota esta Política em conformidade com:

- Lei Geral de Proteção de Dados (LGPD);
- Banco Central do Brasil;
- Resolução BCB nº 85/2021 (Segurança Cibernética e Serviços de Tecnologia);
- Resolução BCB nº 368/2024 (atualizações regulatórias aplicáveis);
- Normas e boas práticas internacionais, incluindo ISO/IEC 27001 (Sistema de Gestão de Segurança da Informação);
- Políticas internas da CredutPay e normativos corporativos.

4. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

A CredutPay estabelece, como fundamentos para a gestão e proteção de seus ativos informacionais, os seguintes princípios:

4.1 Princípios Fundamentais

	Política De Segurança Da Informação		
	Versão: 1.0 Data: 01/08/2025	Departamento Emissor: Tecnologia da Informação	Aprovação: Diretoria Executiva

- **Confidencialidade:** assegurar que o acesso às informações seja restrito exclusivamente a usuários, sistemas ou entidades devidamente autorizados, prevenindo divulgação, acesso ou uso indevido;
- **Integridade:** garantir que as informações sejam mantidas íntegras, completas e consistentes, protegidas contra alterações não autorizadas, acidentais ou maliciosas;
- **Disponibilidade:** assegurar que as informações e os sistemas estejam disponíveis e acessíveis sempre que necessário, de acordo com os níveis de serviço e requisitos operacionais estabelecidos;
- **Autenticidade:** garantir a veracidade da origem das informações, assegurando que sejam provenientes de fontes confiáveis e devidamente validadas;
- **Responsabilidade:** assegurar que todos os usuários utilizem os ativos informacionais de forma adequada, ética e segura, em conformidade com esta Política e demais normativos internos.

4.2 Diretrizes Complementares

Adicionalmente, a CredutPay adota as seguintes diretrizes:

- A segurança da informação constitui elemento essencial da governança corporativa, devendo estar integrada aos processos estratégicos e operacionais;
- A segurança da informação atua como facilitadora dos objetivos de negócio, promovendo confiança, continuidade operacional e mitigação de riscos;
- Os controles de segurança são definidos com base em análise de risco, considerando a criticidade dos ativos, o impacto potencial e a relação custo-benefício;
- A proteção das informações é responsabilidade de todos os colaboradores, parceiros, prestadores de serviços e terceiros que tenham acesso aos ativos informacionais da CredutPay.

4.3 Confidencialidade e Proteção de Informações Estratégicas

É expressamente vedado o compartilhamento, divulgação ou utilização indevida de informações estratégicas, confidenciais ou sensíveis sem a devida autorização formal.

A inobservância desta diretriz inclui, mas não se limita a, situações em que a divulgação não autorizada possa acarretar impactos:

- Financeiros;
- Reputacionais;
- Operacionais;
- Regulatórios.

	Política De Segurança Da Informação		
	Versão: 1.0 Data: 01/08/2025	Departamento Emissor: Tecnologia da Informação	Aprovação: Diretoria Executiva

Todos os usuários devem adotar postura diligente na proteção das informações sob sua responsabilidade, garantindo seu uso exclusivamente para fins legítimos e autorizados.

5. SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO (SGSI)

A CredutPay mantém um Sistema de Gestão de Segurança da Informação (SGSI) estruturado, baseado em boas práticas de mercado e alinhado aos requisitos legais e regulatórios aplicáveis, com o objetivo de assegurar a proteção dos ativos informacionais e a mitigação de riscos.

5.1 Objetivos do SGSI

O SGSI tem por finalidade:

- Identificar, avaliar e tratar riscos relacionados à segurança da informação, de forma contínua e estruturada;
- Implementar controles de segurança proporcionais ao nível de risco identificado, considerando a criticidade dos ativos e os impactos potenciais;
- Monitorar continuamente ameaças, vulnerabilidades e eventos de segurança;
- Promover a melhoria contínua dos processos, controles e práticas de segurança da informação.

5.2 Diretrizes e Estrutura do SGSI

O SGSI da CredutPay é estruturado com base nos seguintes elementos:

- Atendimento aos requisitos legais, regulatórios e normativos aplicáveis;
- Realização de análises de risco periódicas, com definição de planos de tratamento;
- Execução de auditorias internas e externas, visando avaliar a efetividade dos controles implementados;
- Observância dos direcionamentos estratégicos da alta administração;
- Definição formal de papéis e responsabilidades no âmbito da segurança da informação;
- Estabelecimento de reportes periódicos à alta administração sobre o nível de risco, incidentes e efetividade dos controles;
- Integração com as áreas de Compliance, Gestão de Riscos e Tecnologia da Informação, assegurando alinhamento organizacional.

	Política De Segurança Da Informação		
	Versão: 1.0 Data: 01/08/2025	Departamento Emissor: Tecnologia da Informação	Aprovação: Diretoria Executiva

6. CLASSIFICAÇÃO DA INFORMAÇÃO

As informações devem ser classificadas conforme os seguintes níveis:

- **Pública:** informações cuja divulgação é autorizada e não gera riscos à CredutPay, podendo ser acessadas por qualquer público;
- **Interna:** informações destinadas ao uso interno da organização, cujo acesso deve ser restrito a colaboradores e terceiros autorizados;
- **Confidencial:** informações que, se divulgadas indevidamente, podem causar impactos financeiros, operacionais ou reputacionais, devendo ter acesso rigorosamente controlado;
- **Restrita/Sensível:** informações de alta criticidade, incluindo dados pessoais, financeiros, estratégicos ou regulatórios, cujo acesso é altamente restrito e protegido por controles reforçados.

6.2 Diretrizes de Classificação

A classificação da informação determina os níveis de proteção, controle de acesso e regras de tratamento aplicáveis, devendo ser considerada ao longo de todo o ciclo de vida da informação.

Cada nível de classificação possui requisitos específicos relacionados a:

- **Armazenamento:** definição de locais e meios seguros para guarda das informações, conforme sua criticidade;
- **Compartilhamento:** restrição e controle de acesso, incluindo autorização formal para divulgação a terceiros;
- **Retenção:** definição de prazos de guarda, em conformidade com requisitos legais, regulatórios e de negócio;
- **Descarte seguro:** eliminação adequada das informações, de forma a impedir sua recuperação ou uso indevido.

6.3 Responsabilidades

Todos os colaboradores, parceiros e terceiros são responsáveis por:

- Classificar corretamente as informações sob sua responsabilidade;
- Garantir o cumprimento das diretrizes de proteção conforme o nível de classificação;
- Adotar medidas adequadas para prevenir acesso, uso ou divulgação não autorizados;
- Reportar imediatamente qualquer incidente ou violação relacionada à classificação da informação.

	Política De Segurança Da Informação		
	Versão: 1.0 Data: 01/08/2025	Departamento Emissor: Tecnologia da Informação	Aprovação: Diretoria Executiva

7. CONTROLE DE ACESSO

A CredutPay estabelece diretrizes e controles para o gerenciamento de acessos aos sistemas, informações e recursos tecnológicos, com o objetivo de assegurar que apenas usuários devidamente autorizados tenham acesso aos ativos informacionais, conforme suas atribuições e necessidades operacionais.

7.1 Princípios de Controle de Acesso

O controle de acesso deve observar os seguintes princípios:

- **Princípio do menor privilégio:** os acessos devem ser concedidos estritamente conforme a necessidade para o desempenho das funções do usuário;
- **Segregação de funções:** as permissões devem ser estruturadas de forma a evitar conflitos de interesse, fraudes ou acessos indevidos;
- **Necessidade de conhecimento (Need to Know):** o acesso às informações deve ser limitado àquilo que for essencial para a execução das atividades;
- **Responsabilização individual:** todas as ações realizadas nos sistemas devem ser rastreáveis e associadas a um usuário identificado.

7.2 Gestão de Identidades e Acessos

A CredutPay adota processos formais para gestão de identidades e acessos, contemplando:

- Concessão de acessos mediante solicitação formal, aprovação do gestor responsável e validação das áreas competentes;
- Revisão periódica dos acessos, visando garantir sua adequação às funções exercidas;
- Revogação imediata de acessos em casos de desligamento, mudança de função ou identificação de risco;
- Controle centralizado de usuários e perfis de acesso, sempre que aplicável;
- Utilização de identificadores únicos e intransferíveis para cada usuário.

7.3 Autenticação e Credenciais

Os mecanismos de autenticação devem garantir a segurança das credenciais de acesso, incluindo:

- Uso obrigatório de credenciais individuais, sigilosas e intransferíveis;
- Adoção de autenticação multifator (MFA) para acessos críticos, privilegiados ou sensíveis;
- Definição de requisitos mínimos de complexidade de senhas, incluindo:

	Política De Segurança Da Informação		
	Versão: 1.0 Data: 01/08/2025	Departamento Emissor: Tecnologia da Informação	Aprovação: Diretoria Executiva

- Comprimento mínimo;
- Combinação de caracteres alfanuméricos e especiais;
- Não reutilização de senhas anteriores;
- Implementação de mecanismos de bloqueio automático após tentativas inválidas de autenticação;
- Proibição do compartilhamento, armazenamento inadequado ou exposição de credenciais.

7.4 Acessos Privilegiados

Os acessos com privilégios elevados devem ser controlados de forma rigorosa, observando:

- Concessão restrita e devidamente justificada;
- Monitoramento contínuo das atividades realizadas;
- Revisão periódica e independente;
- Registro detalhado de logs para auditoria;
- Utilização, sempre que possível, de mecanismos de controle adicional, como cofre de credenciais ou sessões monitoradas.

7.5 Monitoramento e Registro de Acessos

A CredutPay mantém mecanismos de monitoramento e rastreabilidade, incluindo:

- Registro de logs de acesso e atividades relevantes;
- Proteção dos registros contra alteração ou exclusão indevida;
- Retenção dos logs conforme requisitos legais, regulatórios e internos;
- Monitoramento contínuo para identificação de comportamentos anômalos ou suspeitos;
- Utilização dos registros para fins de auditoria, investigação e conformidade.

7.6 Controle de Acesso a Sistemas e Dados

O acesso a sistemas, aplicações e dados deve observar:

- Definição de perfis de acesso baseados em função (RBAC);
- Restrição de acesso a ambientes críticos, como produção, dados sensíveis e sistemas financeiros;
- Segregação entre ambientes (desenvolvimento, homologação e produção);

	Política De Segurança Da Informação		
	Versão: 1.0 Data: 01/08/2025	Departamento Emissor: Tecnologia da Informação	Aprovação: Diretoria Executiva

- Controle de acesso a dados sensíveis, incluindo dados pessoais, financeiros e estratégicos, com base na classificação da informação;
- Uso de criptografia e outros mecanismos de proteção, quando aplicável.

7.7 Dispositivos e Acesso Remoto

O acesso por dispositivos e conexões remotas deve observar:

- Utilização de dispositivos autorizados e devidamente protegidos;
- Implementação de controles de segurança para acesso remoto (ex.: VPN, autenticação forte);
- Restrição de acesso a partir de redes públicas ou não confiáveis, salvo mediante controles adicionais;
- Aplicação de políticas de segurança para dispositivos corporativos e, quando aplicável, dispositivos pessoais (BYOD).

7.8 Responsabilidades

São responsabilidades dos usuários:

- Zelar pela confidencialidade de suas credenciais de acesso;
- Utilizar os acessos concedidos exclusivamente para fins profissionais e autorizados;
- Comunicar imediatamente qualquer suspeita de comprometimento de credenciais ou uso indevido;
- Cumprir integralmente as diretrizes estabelecidas nesta Política e demais normativos internos.

8. USO ACEITÁVEL DE RECURSOS

A CredutPay estabelece diretrizes para o uso adequado dos recursos tecnológicos e dispositivos, com o objetivo de garantir a segurança da informação, a integridade dos sistemas e a proteção dos ativos informacionais.

8.1 Diretrizes de Uso Aceitável

Os recursos tecnológicos disponibilizados pela CredutPay devem ser utilizados exclusivamente para fins profissionais, observando-se as seguintes diretrizes:

- Utilizar sistemas, equipamentos e informações de forma ética, responsável e em conformidade com as políticas internas;

	Política De Segurança Da Informação		
	Versão: 1.0 Data: 01/08/2025	Departamento Emissor: Tecnologia da Informação	Aprovação: Diretoria Executiva

- É vedado o uso dos recursos corporativos para atividades ilegais, não autorizadas ou que possam comprometer a segurança da informação;
- Não acessar, armazenar, compartilhar ou disseminar conteúdos inadequados, ilícitos ou que violem normas internas e legislação vigente;
- Não instalar, executar ou distribuir softwares, aplicações ou ferramentas sem autorização prévia da área responsável;
- Não burlar controles de segurança, incluindo mecanismos de autenticação, monitoramento ou restrições de acesso;
- Zelar pela integridade e confidencialidade das informações acessadas ou manipuladas.

8.2 Uso de Dispositivos Corporativos

Os dispositivos corporativos devem ser utilizados de forma segura e controlada, observando:

- Utilização exclusiva por usuários autorizados;
- Configuração e manutenção conforme padrões de segurança definidos pela CredutPay;
- Instalação de soluções de proteção, como antivírus, firewall e ferramentas de monitoramento;
- Atualizações periódicas de sistemas operacionais e aplicações;
- Bloqueio automático de tela e proteção por senha ou mecanismo equivalente;
- Proibição de desativação de controles de segurança implementados.

8.3 Uso de Dispositivos Pessoais (BYOD – Bring Your Own Device)

O uso de dispositivos pessoais para acesso a sistemas ou informações corporativas, quando permitido, deve atender aos seguintes requisitos:

- Autorização prévia da área responsável;
- Aplicação de controles mínimos de segurança, como senha de acesso, criptografia e bloqueio automático;
- Instalação de ferramentas corporativas de segurança, quando aplicável;
- Separação lógica entre dados pessoais e corporativos;
- Possibilidade de restrição ou revogação de acesso a qualquer momento, conforme necessidade de segurança.

	Política De Segurança Da Informação		
	Versão: 1.0 Data: 01/08/2025	Departamento Emissor: Tecnologia da Informação	Aprovação: Diretoria Executiva

8.4 Acesso à Internet e Correio Eletrônico

O uso de internet e e-mail corporativo deve observar:

- Utilização para fins profissionais, alinhados às atividades da organização;
- Proibição de envio ou recebimento de conteúdos maliciosos, fraudulentos ou não autorizados;
- Atenção a tentativas de phishing, engenharia social e outros ataques cibernéticos;
- Não compartilhamento de informações confidenciais sem autorização;
- Monitoramento do uso, em conformidade com as políticas internas e legislação aplicável.

8.5 Proteção de Informações em Dispositivos

Os usuários devem adotar medidas para proteger as informações armazenadas ou acessadas em dispositivos, incluindo:

- Não armazenar informações sensíveis em dispositivos não autorizados;
- Utilizar mecanismos de criptografia quando aplicável;
- Evitar o uso de dispositivos desconhecidos ou redes não confiáveis para acesso a sistemas corporativos;
- Garantir a proteção física dos dispositivos contra perda, furto ou acesso indevido;
- Reportar imediatamente incidentes envolvendo perda, roubo ou comprometimento de dispositivos.

8.6 Monitoramento e Conformidade

A CredutPay poderá realizar o monitoramento do uso dos recursos tecnológicos, com o objetivo de:

- Garantir a segurança dos sistemas e informações;
- Identificar comportamentos de risco ou uso indevido;
- Assegurar conformidade com esta Política e demais normativos internos.

Não há expectativa de privacidade no uso dos recursos corporativos, respeitados os limites legais e regulatórios aplicáveis.

8.7 Responsabilidades

São responsabilidades dos usuários:

- Utilizar os recursos tecnológicos de forma segura e conforme as diretrizes estabelecidas;

	Política De Segurança Da Informação		
	Versão: 1.0 Data: 01/08/2025	Departamento Emissor: Tecnologia da Informação	Aprovação: Diretoria Executiva

- Preservar a integridade dos dispositivos e informações;
- Cumprir as políticas de segurança da informação e demais normativos internos;
- Comunicar imediatamente qualquer incidente, falha de segurança ou uso indevido identificado.

9. PROTEÇÃO DE DADOS E PRIVACIDADE

A CredutPay realiza o tratamento de dados pessoais em conformidade com a legislação vigente, em especial a Lei Geral de Proteção de Dados Pessoais (LGPD), adotando medidas técnicas e administrativas aptas a proteger os dados contra acessos não autorizados, perda, destruição, alteração ou qualquer forma de tratamento inadequado ou ilícito.

O tratamento de dados pessoais observa, no mínimo:

- Finalidades legítimas, específicas e informadas ao titular;
- Adequação e necessidade do tratamento em relação às finalidades;
- Implementação de controles de segurança da informação;
- Restrição de acesso aos dados conforme o nível de classificação;
- Atendimento aos direitos dos titulares de dados;
- Comunicação de incidentes de segurança, quando aplicável, às autoridades competentes e aos titulares.

A CredutPay mantém estrutura adequada para governança de dados, incluindo definição de papéis e responsabilidades, bem como canal de atendimento ao titular por meio de seus canais oficiais disponibilizados no aplicativo e no site institucional.

10. SEGURANÇA DE SISTEMAS, REDES E INFRAESTRUTURA

A CredutPay adota controles de segurança para proteção de seus sistemas, redes e infraestrutura tecnológica, visando prevenir, detectar e responder a ameaças cibernéticas.

São estabelecidas, entre outras, as seguintes medidas:

- Monitoramento contínuo de sistemas, aplicações e transações;
- Gestão de vulnerabilidades, incluindo identificação, classificação e correção;
- Atualização periódica de sistemas e aplicações;
- Implementação de controles de segurança em aplicações, APIs e integrações;
- Proteção contra softwares maliciosos e ataques cibernéticos;

	Política De Segurança Da Informação		
	Versão: 1.0 Data: 01/08/2025	Departamento Emissor: Tecnologia da Informação	Aprovação: Diretoria Executiva

- Segmentação de redes e segregação de ambientes (desenvolvimento, homologação e produção);
- Utilização de mecanismos de criptografia para proteção de dados sensíveis.

11. GESTÃO DE INCIDENTES DE SEGURANÇA

A CredutPay mantém processo estruturado para gestão de incidentes de segurança da informação, com o objetivo de garantir resposta rápida, eficaz e rastreável.

Os incidentes devem ser:

- Identificados e reportados imediatamente;
- Registrados em sistema apropriado;
- Classificados conforme nível de criticidade e impacto;
- Tratados com ações corretivas e preventivas;
- Monitorados até sua completa resolução.

Quando aplicável, poderão ser adotadas medidas como:

- Adoção de medidas preventivas e corretivas para mitigação de riscos;
- Suspensão temporária de serviços;
- Comunicação às autoridades reguladoras e competentes;
- Comunicação aos clientes e titulares de dados, conforme exigido pela legislação.

Todos os incidentes devem ser documentados para fins de auditoria, rastreabilidade e melhoria contínua.

12. CONTINUIDADE DE NEGÓCIOS

A CredutPay mantém diretrizes e planos para assegurar a continuidade de suas operações em situações adversas.

Incluem-se:

- Plano de Continuidade de Negócios (PCN);
- Plano de Recuperação de Desastres (DRP);
- Estratégias de contingência para sistemas críticos;
- Execução de backups periódicos e testes de restauração;
- Avaliação contínua de riscos que possam impactar a operação.

	Política De Segurança Da Informação		
	Versão: 1.0 Data: 01/08/2025	Departamento Emissor: Tecnologia da Informação	Aprovação: Diretoria Executiva

13. SEGURANÇA EM TERCEIROS E FORNECEDORES

A CredutPay exige que terceiros, parceiros e fornecedores que tenham acesso a informações ou sistemas corporativos adotem padrões adequados de segurança da informação.

Para tanto:

- Devem cumprir esta Política e demais normativos aplicáveis;
- Estão sujeitos a processos de avaliação de risco (due diligence);
- Devem formalizar compromissos de confidencialidade;
- Devem demonstrar conformidade com requisitos legais e regulatórios.

A CredutPay poderá:

- Realizar auditorias e avaliações periódicas;
- Solicitar evidências de controles de segurança;
- Exigir adequações;
- Rescindir contratos em caso de não conformidade.

14. CONSCIENTIZAÇÃO E TREINAMENTO

A CredutPay promove ações contínuas de conscientização e capacitação em segurança da informação, visando fortalecer a cultura organizacional e reduzir riscos.

Incluem-se:

- Programas periódicos de treinamento;
- Campanhas de conscientização sobre riscos cibernéticos;
- Orientações sobre boas práticas de segurança;
- Capacitação específica para áreas críticas.

15. MONITORAMENTO E AUDITORIA

A CredutPay realiza monitoramento contínuo dos seus ambientes tecnológicos e atividades, com o objetivo de garantir a segurança e a conformidade.

Para tanto:

	Política De Segurança Da Informação		
	Versão: 1.0 Data: 01/08/2025	Departamento Emissor: Tecnologia da Informação	Aprovação: Diretoria Executiva

- Os acessos e atividades podem ser registrados e monitorados;
- Logs são mantidos e protegidos conforme requisitos regulatórios;
- Auditorias internas e externas são realizadas periodicamente;
- As evidências são utilizadas para avaliação de controles e melhoria contínua.

O monitoramento é realizado em conformidade com a legislação vigente, especialmente no que se refere à proteção de dados pessoais e à privacidade dos usuários.

16. RESPONSABILIDADES

A segurança da informação é responsabilidade de todos, sendo atribuídas as seguintes responsabilidades:

- **Alta Administração:** garantir a governança, recursos e efetividade da política;
- **Áreas de Tecnologia e Segurança:** implementar, monitorar e evoluir os controles;
- **Compliance e Riscos:** assegurar aderência regulatória e gestão de riscos;
- **Colaboradores e Terceiros:** cumprir as diretrizes estabelecidas nesta Política;

17. PENALIDADES

O descumprimento desta Política poderá resultar em medidas administrativas, disciplinares e legais, incluindo:

- Adoção de medidas cabíveis conforme legislação e contratos aplicáveis;
- Suspensão ou revogação de acessos;
- Encerramento de vínculo contratual;
- Responsabilização civil e criminal, quando aplicável;
- Comunicação às autoridades competentes.

18. REVISÃO E ATUALIZAÇÃO

Esta Política será revisada:

- No mínimo, anualmente;
- Sempre que necessário, para refletir alterações legais, regulatórias ou operacionais;
- Mediante recomendações de auditoria ou da alta administração.

	Política De Segurança Da Informação		
	Versão: 1.0 Data: 01/08/2025	Departamento Emissor: Tecnologia da Informação	Aprovação: Diretoria Executiva

19. DISPOSIÇÕES FINAIS

Esta Política constitui instrumento essencial para a proteção dos ativos informacionais da CredutPay, a mitigação de riscos e o fortalecimento da governança corporativa.

Sua efetividade depende do comprometimento da alta administração e do cumprimento rigoroso por todos os envolvidos.

20. VIGÊNCIA

Esta Política entra em vigor na data de sua aprovação pela Diretoria Executiva e permanece válida por prazo indeterminado.

Deverá ser revisada, no mínimo, anualmente, ou sempre que necessário para refletir alterações relevantes no ambiente regulatório, tecnológico ou nos riscos relacionados à segurança da informação.

A versão vigente estará sempre disponível nos canais oficiais da CredutPay.