



Política de Segurança da Informação (PSI)

VendeAI Tecnologia

POL-VDA-01 — versão 1.0

1 Introdução

A VendeAI Tecnologia (“VendeAI”) desenvolve e opera uma plataforma de tecnologia que utiliza inteligência artificial para simulação, análise e formalização de operações de crédito, atuando em parceria com instituições financeiras e bancos. No exercício dessa atividade, a VendeAI trata dados pessoais de clientes, colaboradores e parceiros, e por isso assume o compromisso formal de proteger a confidencialidade, integridade e disponibilidade da informação sob sua responsabilidade, em conformidade com a legislação brasileira aplicável.

Esta Política de Segurança da Informação (PSI) aplica-se a todos os colaboradores, prestadores de serviço, parceiros comerciais e demais pessoas que atuem em nome da VendeAI e tenham acesso a sistemas, dados ou ativos de informação da empresa.

2 Referência documental

Esta política observa, entre outras normas aplicáveis:

- CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988, Art. 5º, LXXIX — é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais;
- Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais — LGPD);
- Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet);
- Norma ISO/IEC 27000:2018 (SGSI — Visão geral e vocabulário) e boas práticas das normas ISO/IEC 27001, 27002 e 27701;
- Exigências contratuais e de compliance dos parceiros bancários e financeiros da VendeAI.

3 Definições

PSI — Política de Segurança da Informação, documento que estabelece diretrizes gerais de segurança da informação da VendeAI.

Ativo de informação — todo dado, sistema, equipamento ou serviço que armazena, processa ou transmite informação da VendeAI.

Confidencialidade, Integridade e Disponibilidade (CID) — os três pilares da segurança da informação: garantir que a informação seja acessada apenas por quem tem autorização (confidencialidade), que permaneça correta e completa (integridade), e que esteja acessível quando necessário (disponibilidade).

Incidente de segurança — qualquer evento que comprometa a confidencialidade, integridade ou disponibilidade de um ativo de informação.

Usuário da informação — colaborador, prestador de serviço ou parceiro com acesso autorizado a sistemas ou dados da VendeAI.

4 Propósito

Esta PSI tem por objetivo:

1. Estabelecer padrões de comportamento seguro no uso de sistemas, dados e equipamentos da VendeAI;
2. Orientar a implementação de controles técnicos e organizacionais de segurança da informação;

3. Resguardar a confidencialidade, integridade e disponibilidade dos ativos de informação;
4. Prevenir incidentes de segurança e mitigar responsabilidade legal decorrente de falhas evitáveis;
5. Minimizar riscos financeiros, operacionais e reputacionais para a VendeAI e seus parceiros.

5 Escopo

Esta política aplica-se a todo usuário da informação, incluindo colaboradores atuais, ex-colaboradores (quanto às obrigações remanescentes), prestadores de serviço e parceiros comerciais que tenham acesso a sistemas, ambientes de nuvem, código-fonte, bases de dados ou informações confidenciais da VendeAI.

5.1 Diretrizes de gestão

- A liderança da VendeAI (CEO e CTO) apoia formalmente esta política e provê os recursos necessários à sua implementação;
- Esta PSI e as normas dela derivadas serão revisadas periodicamente;
- Incidentes de segurança devem ser tratados conforme o **Plano de Resposta a Incidentes de Vazamento de Dados Pessoais** (POL-VDA-04);
- A VendeAI mantém práticas de continuidade de negócio, incluindo backup de dados e ambientes de produção redundantes, na medida do seu porte e maturidade operacional.

6 Papéis e responsabilidades

Todo colaborador e parceiro deve seguir as diretrizes desta PSI. O CTO/DPO é responsável por editar, manter e aprovar esta política e as normas de segurança derivadas, e por apoiar a resolução de incidentes e dúvidas técnicas relacionadas a segurança da informação.

A VendeAI mantém uma área dedicada de Segurança da Informação, composta por 4 colaboradores, responsável por avaliar periodicamente a segurança dos sistemas, analisar patches e atualizações que possam afetar a segurança, e produzir relatórios mensais de acompanhamento. Essa área atua em conjunto com o CTO/DPO nas questões de privacidade e proteção de dados.

7 Dos acessos

7.1 Concessão de acessos

O acesso a sistemas e dados é concedido pelo CTO ou por gestor de área, seguindo o princípio do menor privilégio: cada colaborador recebe apenas os acessos estritamente necessários para exercer sua função. Cada usuário deve possuir login individual — é proibido o compartilhamento de credenciais.

7.2 Aprovação de acessos

A concessão de acesso a sistemas críticos (produção, bases de dados de clientes, painéis de integração bancária) exige aprovação do CTO/DPO.

7.3 Revisão de acessos

Os acessos concedidos são revisados periodicamente (recomendado: trimestralmente) para identificar e remover privilégios não mais necessários.

7.4 Revogação de acessos

No desligamento de colaborador ou término de contrato com parceiro/prestador, todos os acessos devem ser revogados imediatamente pelo responsável de TI/infraestrutura.

7.5 Gestão de acessos privilegiados

Contas com privilégios administrativos (acesso root/admin a servidores, bancos de dados e provedores de nuvem) são restritas ao time técnico e não devem ser utilizadas para atividades rotineiras nem para fins de teste.

8 Uso e boas práticas

8.1 Sistemas e aplicações

A instalação de softwares em equipamentos corporativos ou de acesso a sistemas da VendeAI requer autorização prévia da área técnica.

8.2 E-mail e ferramentas de comunicação

Contas de e-mail corporativo são criadas no início do vínculo e de uso restrito ao titular. É proibido o reenvio de informações confidenciais a contas pessoais.

8.3 Senhas

Senhas de acesso a sistemas da VendeAI não devem conter nome, sobrenome, datas de nascimento, CPF, telefone ou sequências óbvias. Recomenda-se o uso de gerenciador de senhas e autenticação multifator (MFA) sempre que disponível.

8.4 Conscientização

A VendeAI promove, por meio de sua **Política e Cronograma de Treinamento** (POL-VDA-05), a capacitação periódica de colaboradores sobre segurança da informação e proteção de dados pessoais.

8.5 Dispositivos móveis e pessoais

O uso de dispositivos próprios (BYOD) para acessar sistemas ou dados da VendeAI segue as regras específicas da **Política de BYOD** (POL-VDA-07).

9 Penalidades

O descumprimento desta PSI pelos colaboradores pode resultar, conforme a gravidade e a reincidência, em advertência verbal, advertência escrita, restrição ou revogação de acessos a sistemas e, em casos graves, medidas disciplinares adicionais previstas na legislação trabalhista e nas normas internas da empresa. Parceiros e prestadores de serviço estão sujeitos às penalidades previstas em contrato para o mesmo tipo de descumprimento.

10 Gestão do documento

Este documento é de propriedade da VendeAI Tecnologia e permanece válido até que seja revisado ou substituído por nova versão, podendo ser atualizado a qualquer momento em razão de mudanças

legais, tecnológicas ou operacionais relevantes.

11 Responsáveis

Papel	Responsável
Autor	Gustavo Schewinski — CTO e DPO
Responsável da área	Gustavo Schewinski — CTO e DPO
Aprovador	Nicolas Ignacio Ryberg — CEO

12 Divulgação

A liderança da VendeAI comunicará a entrada em vigor desta política a todos os colaboradores e parceiros, disponibilizando o documento no repositório interno de políticas da empresa (canal a definir — ex.: Notion/Google Drive corporativo).