



Política de BYOD (Bring Your Own Device)

VendeAI Tecnologia

POL-VDA-07 — versão 1.0

1 Introdução

Esta Política de BYOD (“Bring Your Own Device”) estabelece as regras para uso de dispositivos pessoais (notebooks, smartphones, tablets) por colaboradores e parceiros da VendeAI Tecnologia (“VendeAI”) no acesso a sistemas, dados e ambientes corporativos, complementando a **Política de Segurança da Informação** (POL-VDA-01).

2 Objetivo

Permitir, de forma controlada, o uso de dispositivos pessoais para atividades de trabalho, sem comprometer a segurança da informação e a proteção de dados pessoais tratados pela VendeAI.

3 Escopo

Aplica-se a todo colaborador ou parceiro que utilize dispositivo pessoal para acessar e-mail corporativo, sistemas internos, repositórios de código ou dados de clientes da VendeAI.

4 Referência documental

Esta política observa, entre outras normas aplicáveis:

- CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988, Art. 5º, LXXIX — 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);
- Boas práticas da norma ISO/IEC 27002:2022;
- Política de Segurança da Informação da VendeAI (POL-VDA-01).

5 Regras de uso

- O acesso a sistemas corporativos a partir de dispositivo pessoal requer autenticação multifator (MFA) sempre que disponível;
- O dispositivo pessoal utilizado deve manter sistema operacional e antivírus atualizados;
- É proibido armazenar localmente, de forma permanente, bases de dados de clientes ou informações confidenciais da VendeAI em dispositivo pessoal — o acesso deve ocorrer preferencialmente via sistemas web/cloud, sem download definitivo de dados sensíveis;
- Dispositivos pessoais utilizados para acesso corporativo devem possuir bloqueio de tela por senha, PIN ou biometria;
- Em caso de perda, roubo ou comprometimento do dispositivo, o colaborador deve comunicar imediatamente a área técnica, para revogação de acessos e, se necessário, apagamento remoto de dados corporativos sincronizados (ex.: e-mail, MDM);
- O uso de redes Wi-Fi públicas ou não confiáveis para acesso a sistemas corporativos deve ser evitado; quando inevitável, deve-se utilizar VPN corporativa, se disponível;
- No desligamento do colaborador ou término do contrato do parceiro, todo acesso corporativo configurado no dispositivo pessoal (e-mail, aplicativos, VPN) deve ser removido.

6 Responsabilidades

O colaborador ou parceiro é responsável por manter seu dispositivo pessoal em conformidade com esta política enquanto o utilizar para fins corporativos. A área técnica é responsável por disponibilizar orientação sobre configuração segura (MFA, VPN, MDM quando aplicável) e por revogar acessos quando necessário.

7 Penalidades

O descumprimento desta política pode resultar em suspensão do acesso corporativo via dispositivo pessoal e, conforme a gravidade, medidas disciplinares nos termos das normas internas da empresa.

8 Responsáveis

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

9 Divulgação

O CTO/DPO informará a todos os colaboradores sobre a entrada em vigor desta política e a disponibilizará no repositório interno de políticas da empresa.