Política de Segurança da Informação

Ferrazio — CNPJ 64.008.257/0001-72 Versão 1.0 — vigente desde 03/11/2026 — revisão anual ou após mudança relevante Contato de segurança: privacidade@ferrazio.com

1. Objetivo e abrangência

Esta política define as regras que a Ferrazio adota para proteger a confidencialidade, a integridade e a disponibilidade das informações tratadas na plataforma **Ferrazio Hub** (ERP, integrações com marketplaces como o TikTok Shop, emissão de documentos fiscais e atendimento), no site ferrazio.com e nos ambientes internos da empresa.

Aplica-se a todos os sócios, colaboradores, prestadores de serviço e fornecedores que acessem sistemas ou dados da Ferrazio ou de seus clientes.

2. Princípios

- **Privilégio mínimo:** cada pessoa e cada sistema recebe apenas o acesso estritamente necessário à sua função.
- **Negação por padrão:** qualquer acesso não autorizado explicitamente é bloqueado.
- **Defesa em camadas:** nenhuma proteção isolada é considerada suficiente.
- **Segregação de clientes:** os dados de cada lojista (tenant) são logicamente isolados dos demais.
- **Rastreabilidade:** ações relevantes são registradas e auditáveis.

3. Papéis e responsabilidades

Papel	Responsabilidade
Direção	Aprovar esta política, prover recursos e aceitar formalmente riscos residuais
Responsável por Segurança e Encarregado de Dados (DPO)	Manter a política, coordenar a gestão de vulnerabilidades e a resposta a incidentes, atender titulares e autoridades
Equipe técnica	Aplicar os controles descritos, reportar falhas e incidentes imediatamente
Todos os usuários internos	Cumprir a política e o Termo de Confidencialidade

4. Classificação da informação

Classe	Exemplos	Tratamento
Restrita	Senhas, chaves de API e de assinatura, App Secret de marketplaces, tokens OAuth, certificados digitais A1, chaves de criptografia	Somente em cofre de segredos cifrado; nunca em código, e-mail, chat ou

Classe	Exemplos	Tratamento
		capturas de tela; acesso nominal e mínimo
Confidencial	Dados pessoais de compradores (nome, endereço, telefone, CPF/CNPJ), pedidos, mensagens de atendimento, notas fiscais, dados financeiros dos lojistas	Cifrados em trânsito e em repouso; acesso apenas por necessidade do serviço; isolados por cliente
Interna	Documentação técnica, código-fonte, métricas operacionais	Acesso restrito à equipe; repositórios privados com MFA
Pública	Site institucional, políticas publicadas	Sem restrição

Na dúvida, a informação é tratada na classe mais alta aplicável.

5. Criptografia

- **Em trânsito:** todo tráfego externo usa HTTPS/TLS 1.2 ou superior; comunicação interna entre serviços (ex.: mensageria) usa TLS com autoridade certificadora interna. Conexões sem criptografia são recusadas.
- **Em repouso:** discos e bancos de dados de produção são criptografados. Segredos, certificados digitais e arquivos dos clientes recebem uma camada adicional de criptografia com chaves de criptografia de chaves (KEK).
- **Gestão de chaves:** as chaves ficam em cofre com acesso restrito (permissão 0700), separado dos backups, e são rotacionadas imediatamente em caso de suspeita de exposição.
- **Senhas de usuários:** armazenadas apenas com hash forte e salt; nunca em texto claro.

6. Controle de acesso

6.1 Usuários da plataforma (lojistas)

- Autenticação com sessão opaca de curta duração e revogável a qualquer momento.
- Autenticação multifator (TOTP com códigos de recuperação) e **reautenticação obrigatória (step-up)** para ações sensíveis.
- Controle de permissões por papel (RBAC) em modo *fail-closed*: sem permissão explícita, o acesso é negado.
- Isolamento multi-tenant: toda consulta é filtrada pelo identificador do cliente.
- Limitação de tentativas (rate limiting) e mensagens de erro que não revelam informações internas.

6.2 Acesso administrativo e da equipe

- Contas individuais e nominais; contas compartilhadas são proibidas.
- **MFA obrigatório** em todos os sistemas corporativos e de fornecedores (repositórios de código, provedores de nuvem, CDN/DNS, e-mail, painéis de marketplaces).
- Acesso aos servidores somente por VPN (WireGuard) e SSH com chave criptográfica; login por senha e acesso direto como root desabilitados; bloqueio automático de tentativas (fail2ban).

- Concessão de acesso por necessidade, revisão trimestral e revogação imediata no desligamento ou troca de função.
- Acesso a dados de clientes pela equipe só ocorre para suporte solicitado ou obrigação legal, e é registrado.

7. Segurança da rede e da infraestrutura

- **Segregação de rede:** a plataforma fica atrás de CDN com firewall de aplicação (WAF), proteção contra DDoS e limitação de taxa. O servidor de origem aceita conexões web apenas dos endereços da CDN; bancos de dados, filas e cache não são expostos à internet e só escutam em interfaces internas.
- Serviços executam em contêineres sem privilégios de root (rootless), com limites de recursos e redes internas separadas.
- Ambientes de desenvolvimento, homologação e produção são separados; dados reais de clientes não são usados fora da produção.
- Sistemas operacionais e componentes recebem atualizações de segurança regularmente.
- Arquivos enviados pelos usuários passam por verificação antivírus (ClamAV) com quarentena antes de serem armazenados.

8. Linha de base das estações de trabalho

Todo computador usado para acessar sistemas da Ferrazio deve ter, obrigatoriamente:

- Antivírus/antimalware ativo e atualizado (ex.: Microsoft Defender);
- Sistema operacional e navegador com atualizações automáticas;
- Disco criptografado (ex.: BitLocker / FileVault);
- Bloqueio automático de tela em até 5 minutos de inatividade, com senha;
- Senha forte de login (mínimo 12 caracteres) e gerenciador de senhas;
- MFA em todas as contas de trabalho;
- Firewall do sistema operacional ativo.

É proibido armazenar dados Confidenciais ou Restritos em dispositivos pessoais não gerenciados, pendrives ou serviços de nuvem não aprovados.

9. Desenvolvimento seguro

- Código em repositórios privados, com revisão antes da integração.
- Verificação automática de vulnerabilidades em dependências (ex.: `cargo audit`) no pipeline de integração contínua.
- Proibição de segredos no código; segredos expostos acidentalmente são rotacionados imediatamente e removidos do histórico.
- Validação de entrada, verificação de assinatura em webhooks e processamento idempotente de eventos.

10. Gestão de vulnerabilidades

- Monitoramento contínuo de avisos de segurança das dependências e revisão semanal.

- Prazos de correção a partir da identificação: **crítica — até 7 dias; alta — até 30 dias; média — até 90 dias; baixa — próximo ciclo de manutenção**.
- Teste de intrusão (pentest) pelo menos uma vez por ano e após mudanças significativas de arquitetura; o último foi realizado em 28/08/2026, com plano de correção acompanhado.
- Canal para relato responsável de vulnerabilidades: privacidade@ferrazio.com, com resposta inicial em até 72 horas.

11. Registros e monitoramento

11.1 Motor de risco (detecção e bloqueio automático)

O gateway da plataforma possui um motor de risco, sempre ativo e sem interruptor de desligamento, que avalia cada requisição autenticada e atribui uma pontuação de risco por sessão de usuário e por chave de API. São monitorados, entre outros:

- **Tentativa de acesso a dados de outro cliente ou varredura de identificadores:** a requisição é negada com resposta opaca (o sistema não revela se o recurso existe ou pertence a outro cliente) e a tentativa soma pontos de risco;
- **Mudança de dispositivo ou de rede durante a sessão** (indício de sessão ou token roubado);
- **Tentativas repetidas de login, de MFA ou de uso de chaves de API inválidas**, com limitação por endereço e bloqueio temporário da conta;
- **Volume anormal de requisições**, com limitação de taxa por endereço, usuário e chave.

Ao ultrapassar os limiares, o motor primeiro **retarda** as respostas e depois **bloqueia** automaticamente o acesso. Para usuários, o bloqueio é progressivo dentro de 30 dias (temporário, depois mais longo e, na reincidência, definitivo, só revertido após análise). Para integrações, o bloqueio recai sobre a chave de API suspeita, que deve ser revogada. A emissão repetida de chaves bloqueadas leva ao bloqueio do usuário responsável. Todos os eventos ficam registrados em trilha de auditoria para investigação e podem acionar o Plano de Resposta a Incidentes.

11.2 Registros

- Registros de acesso, autenticação e eventos de segurança são centralizados e mantidos por 30 dias (ou mais, quando exigido por lei).
- Alertas para falhas de autenticação em massa, erros anormais e indisponibilidade.
- Os registros não armazenam senhas, tokens ou dados de cartão.

12. Backup e continuidade

- Backup diário automatizado de todos os bancos e arquivos, com verificação de integridade (hash).
- Cópia mantida fora do servidor principal.
- Teste de restauração semanal.
- Retenção de backups: 7 dias no servidor e 14 dias na cópia externa; após esse prazo são sobrescritos.

13. Fornecedores

Provedores de infraestrutura (hospedagem, armazenamento de objetos, CDN) são selecionados considerando suas certificações e práticas de segurança, e os dados são hospedados no **Brasil e nos Estados Unidos**. Fornecedores com acesso a dados pessoais assumem obrigações contratuais de confidencialidade e proteção de dados.

14. Incidentes

Incidentes de segurança são tratados conforme o **Plano de Resposta a Incidentes** da Ferrazio, que inclui comunicação a clientes, a marketplaces parceiros (como o TikTok Shop) e à ANPD nos prazos aplicáveis.

15. Conscientização

Todos os colaboradores recebem orientação de segurança e privacidade ao ingressar e reciclagem anual, e assinam Termo de Confidencialidade.

16. Descumprimento

O descumprimento desta política pode resultar em revogação de acessos, medidas disciplinares e contratuais, sem prejuízo das responsabilidades legais.