Plano de segurança de identidade

Resposta consolidada para pentest, política de senha, defesa contra tentativas, 2FA e acessos privilegiados.

Pontos da matriz	01/14 - pentest; 05/12 - senha e tentativas; 06 - 2FA; 07 - PAM

Documento de resposta técnica para a análise de aderência FTD. As metas e datas indicadas como propostas dependem de validação técnica, operacional e contratual; não constituem, isoladamente, SLA ou laudo.

Posição Jovens Gênios

Os controles existentes - Better Auth, sessões, papéis, rate limit por origem, ambientes Vercel e variáveis sensíveis - formam a base, mas não encerram os achados. A resposta assume um plano de fechamento com evidência e distingue capacidade nativa de controle efetivamente configurado.

Senha e bloqueio por conta

Camada	Situação / decisão	Evidência de aceite
Senha	Meta proposta de 12 caracteres para adultos e perfis privilegiados. Para estudantes, UX apropriada à idade, recuperação assistida e alternativa passwordless devem ser avaliadas antes da migração.	Configuração por aplicação, testes de cadastro/reset e plano de migração.
Rate limit	Better Auth aplica limites a requisições do cliente e regra mais estrita no sign-in; o limite padrão é rastreado por IP/origem, não por conta.	Configuração persistente adequada a serverless, resposta 429 e teste distribuído.
Bloqueio por conta	O plugin Admin permite banir e expirar banimentos, mas a regra '5 falhas/15 min' no primeiro fator exige contador persistente e automação/hook; não deve ser descrita como bloqueio automático nativo.	Teste que cobre 5 falhas, expiração, desbloqueio e não enumeração de e-mail.

Segundo fator

O plugin 2FA do Better Auth suporta TOTP, OTP, códigos de recuperação e dispositivos confiáveis. A implementação exige migração: o campo twoFactorEnabled no usuário e uma tabela twoFactor para segredo, códigos e estado de bloqueio. Para credenciais, a sessão autenticada só é emitida após validação do segundo fator.

• Obrigatório para administração e operação; opcional ou baseado em risco para usuários comuns.

• Tela de inscrição com QR, confirmação do primeiro código e exibição única dos códigos de recuperação.

• Recuperação com verificação forte, revogação de sessões, auditoria e reautenticação para desativar 2FA.

• Cobertura de magic link/OAuth com hook adicional, pois fluxos sem senha não são desafiados por padrão.

PAM, cofre e break-glass

Hoje, segredos de aplicação podem ser mantidos fora do código em GitHub/Vercel e marcados como sensíveis. Isso é gestão de segredos, não um programa PAM completo. O fechamento exige inventário de contas privilegiadas, menor privilégio, aprovação, rotação, trilha e uma conta break-glass lacrada e testada.

Marco	Entrega	Prazo proposto
M1	Inventário de contas, papéis, segredos e proprietários; remoção de acessos órfãos.	30 dias
M2	MFA obrigatório, variáveis sensíveis, rotação e revisão trimestral de privilégios.	60 dias
M3	JIT/JEA onde suportado, aprovação para produção, break-glass e exportação de auditoria.	90 dias
M4	Fechamento dos achados e novo pentest independente.	Até outubro/2026

Referências oficiais

Better Auth - Rate limit

Better Auth - 2FA, esquema e bloqueio do segundo fator

Better Auth - Plugin Admin (banimento e sessões)

Vercel - Variáveis de ambiente sensíveis