Relatório de Auditoria de Segurança | Check-up · Rodada 1 · Versão 1 | Exemplo anonimizado

PARA EMPRESA EXEMPLO · DOCUMENTO DE DEMONSTRAÇÃO

Plataforma Exemplo

Exemplo real de Relatório de Auditoria de Segurança IDDEIA, com nome, endereços e detalhes técnicos trocados para proteger o sistema auditado. Primeira rodada, o que foi analisado, o que encontramos, o que já foi corrigido e o que fazer a seguir.

VERSÃO AUDITADA	PERÍODO	RODADAS	RESPONSÁVEL
versão de out/2026	out/2026	1 (leitura do código)	IDDEIA

RESUMO PARA O DONO DO NEGÓCIO

Em uma página

7/10

Acima da média para um sistema desse tamanho. Nenhum segredo exposto e nada crítico ou alto. Os pontos fracos são o acesso do administrador, os limites contra abuso e a falta de um backup comprovado.

Os 3 riscos mais importantes

1. **A conta de administrador depende só do e-mail.** Quem entrar no e-mail do administrador vira administrador da plataforma: cria cupons, marca comissões como pagas e vê leads e custos.
2. **Os limites contra abuso quase não seguram.** Eles ficam na memória de cada cópia do servidor. Alguém com um script pode gastar a conta da API paga de busca de empresas e esgotar o atendente com IA dos sites dos clientes.
3. **Não dá para provar como está o banco nem como recuperá-lo.** As mudanças do banco foram aplicadas à mão e não há rotina de backup documentada para o banco nem para as fotos dos sites.

O que fazer primeiro

1. **Ligar a verificação em duas etapas no e-mail do administrador** · dono · esta semana
2. **Conferir e anotar o backup do banco** (plano, frequência, como restaurar) · dono · esta semana
3. **Alerta de orçamento e cota diária nas APIs pagas (busca e IA)** · dono · esta semana

Achados por gravidade

0	0	7	8
CRÍTICA	ALTA	MÉDIA	BAIXA

18 achados no total, sendo 3 apenas informativos · 1 já corrigido (PX-12, no mesmo dia) · 17 em aberto.

ESCOPO E MÉTODO

O que entrou na auditoria

Sistema	Plataforma Exemplo (criação de sites, painel do cliente, área de administração)
Ambiente	Código e configuração. Nenhum teste contra a produção nesta rodada.
Analisado	Todo o código versionado (dezenas de rotas de API e as páginas), os arquivos SQL do banco, as dependências, os nomes das variáveis de ambiente (sem copiar valores) e o histórico completo do repositório.
Fora do escopo	Configurações que só existem nos painéis (autenticação e backup do Supabase, firewall da Vercel) e o estado real do banco em produção. Ficam para a rodada 2.
Tecnologia	Next.js na Vercel, Supabase (Postgres e Storage), gateway de pagamento, API de busca de empresas e IA generativa
Rodadas	Rodada 1: leitura do código e da configuração nos 8 eixos. Rodada 2 (testes em ambiente de teste): a agendar.
Autorização	Autorização por escrito do dono do sistema.

Como trabalhamos: revisamos o código e a configuração com apoio de ferramentas de IA e conferimos cada achado no código antes de registrá-lo. Nesta rodada não houve teste ao vivo. Quando a conclusão depende do banco real, o achado diz "não verificado".

Gravidade

NÍVEL	QUER DIZER	PRAZO SUGERIDO
CRÍTICA	Alguém de fora consegue, sem esforço, acessar ou alterar dados ou dinheiro.	Imediato
ALTA	Acesso indevido a dados ou funções, com alguma condição (ex.: ter uma conta).	Até 7 dias
MÉDIA	Enfraquece uma defesa ou facilita um ataque combinado.	Até 30 dias
BAIXA	Boa prática que falta, sem caminho claro de ataque. Informativa: só registro.	Próxima versão

PLACAR

Os 8 eixos

EIXO	SITUAÇÃO	EM UMA FRASE
1. Chaves e segredos	ADEQUADO	Só a URL, a chave pública do banco e a do gateway de pagamento chegam ao navegador; nenhum segredo no histórico do código.
2. Login e permissão	ATENÇÃO	Toda rota confere a sessão e o dono do site no servidor, mas o administrador não tem segundo fator (PX-02).
3. Isolamento dos dados	ATENÇÃO	O código filtra pelo dono em todas as rotas e o SQL liga as regras de acesso, mas o estado real do banco não está comprovado (PX-04, PX-05).
4. Login sob ataque	ATENÇÃO	Não há senha para adivinhar, mas os limites das rotas abertas ficam só na memória (PX-01, PX-08, PX-09).
5. Tela e arquivos	ATENÇÃO	Upload reprocessa a imagem e não há HTML cru inseguro, mas faltam os cabeçalhos de segurança do navegador (PX-03, PX-11).
6. Pagamentos e integrações	ADEQUADO	O aviso do gateway de pagamento tem a assinatura conferida e o pagamento é buscado na fonte; faltam ajustes menores (PX-06, PX-07).
7. Dependências	ADEQUADO	Os avisos altos de produção foram corrigidos no mesmo dia (PX-12); hoje há 0 vulnerabilidades nas dependências de produção.
8. Registro, backup e recuperação	RISCO	Sem rotina de backup documentada para o banco nem para as fotos, e sem registro das ações do administrador (PX-14).

ADEQUADO sem achado acima de baixa · ATENÇÃO achado médio aberto · RISCO achado alto ou crítico aberto, ou recuperação não comprovada.

ACHADOS

O que encontramos

Do mais grave para o menos grave.

PX-01 Limite de requisições só na memória — MÉDIA

Eixo	4. Login sob ataque e abuso
Onde	Módulo de limite de requisições; única barreira nas rotas abertas de busca de empresas (API paga por consulta) e primeira camada no atendente com IA, métricas e importação
Como reproduzir	Em teste: de 200 a 500 pedidos paralelos em a rota de busca de empresas, de 2 ou 3 endereços, contando respostas aceitas e recusadas e o consumo no painel da API.
Impacto	Conta da API paga estourada e cota esgotada, o que derruba um recurso usado por clientes reais.
Como corrigir	Limitador compartilhado (Redis/KV ou função atômica no Postgres) por endereço, teto diário global nas rotas de busca de empresas, regra no firewall da Vercel e cota com alerta na chave da API.
Status	Aberto

PX-02 Administrador sem segundo fator — MÉDIA

Eixo	2. Login e permissão
Onde	Login por link no e-mail; perfil de administrador definido no servidor; nenhuma exigência de segundo fator
Como reproduzir	Com sessão de administrador de teste, conferir que nenhuma rota exige o nível de verificação em duas etapas; conferir no painel do Supabase se o MFA está ligado.
Impacto	Se o e-mail do administrador for invadido, o invasor cria cupons, marca comissões como pagas e vê leads e custos.
Como corrigir	Verificação em duas etapas forte no e-mail já; depois, ligar o MFA do Supabase e exigir o nível `aal2` nas rotas de administrador.
Status	Aberto

PX-03 Nenhum cabeçalho de segurança no navegador MÉDIA

Eixo	5. Tela e arquivos
Onde	Configuração do framework e da hospedagem: nenhum cabeçalho de segurança definido
Como reproduzir	Consultar os cabeçalhos de uma página do painel e abrir o painel dentro de um iframe em outra página.
Impacto	Clique enganado em ações do dono (publicar, aprovar respostas) e, se um dia surgir uma falha de injeção na tela, roubo de sessão sem segunda barreira.
Como corrigir	Cabeçalhos em na configuração do framework: bloqueio de iframe nas rotas da plataforma, `nosniff`, `Referrer-Policy`, `Permissions-Policy` e CSP começando em modo só-relatório.
Status	Aberto

PX-04 Mudanças do banco fora de controle de versão MÉDIA

Eixo	3. Isolamento dos dados · 8. Recuperação
Onde	Não há pasta de migrações versionadas; o SQL está espalhado em arquivos de anotação e documentos de planejamento, aplicado à mão
Como reproduzir	Comparar o esquema de produção com o SQL do repositório e listar as regras de acesso de todas as tabelas.
Impacto	Uma regra afrouxada no painel não aparece em revisão; uma restauração ou um ambiente novo pode subir sem as regras de acesso.
Como corrigir	Gerar uma migração-base do estado real, versionar em uma pasta de migrações, mudar o banco só por migração e testar automaticamente que toda tabela tem regra de acesso.
Status	Aberto

PX-05 Permissões padrão do banco ainda abertas MÉDIA

Eixo	3. Isolamento dos dados
Onde	Esquema público do banco: permissões padrão não revogadas; parte das tabelas antigas sem revogação individual (não verificado no banco real)
Como reproduzir	Consultar `pg_default_acl` e as permissões de `anon` e `authenticated`; chamar cada tabela com a chave pública.
Impacto	Hoje as regras de acesso seguram, mas uma tabela nova criada sem elas nasceria exposta pela chave pública, o caminho mais comum de vazamento em projetos Supabase.
Como corrigir	Revogar as permissões padrão de `anon` e `authenticated` para tabelas, funções e sequências, e revogar escrita onde ela é só do servidor.
Status	Aberto

PX-12 Dependências de produção com avisos de segurança MÉDIA

Eixo	7. Dependências
Onde	Duas bibliotecas usadas em produção, com avisos altos de travamento por descompressão e por excesso de memória
Como reproduzir	`npm audit --omit=dev`
Impacto	Travamento das funções que validam entrada anônima ou buscam sites de terceiros.
Como corrigir	Atualizar para as versões corrigidas e ligar alertas automáticos de dependência no GitHub.
Status	**Corrigido no mesmo dia** (já publicado): 0 vulnerabilidades nas dependências de produção; 3.124 testes passando. Falta ligar os alertas automáticos.

PX-14 Sem backup documentado e sem registro das ações do administrador

MÉDIA

Eixo	8. Registro, backup e recuperação
Onde	Nenhuma menção a backup ou restauração na documentação; fotos guardadas no Storage; cupons, comissões e transferência de site sem registro de quem fez
Como reproduzir	Conferir no painel do Supabase o plano, a frequência e a recuperação por ponto no tempo; ensaiar uma restauração num projeto de teste.
Impacto	Um apagamento errado, um ataque ou um erro de migração pode levar sites, assinaturas e fotos sem caminho de volta conhecido. O backup do banco não inclui as fotos.
Como corrigir	Documentar o backup e o passo a passo de restauração; agendar um dump diário do banco para fora do provedor e copiar as fotos; criar a tabela de auditoria do administrador; ensaiar a restauração a cada semestre.
Status	Aberto

PX-06 Aviso do gateway de pagamento sem proteção contra repetição BAIXA

Eixo	6. Pagamentos e integrações
Onde	Validação do aviso de pagamento aceita qualquer horário de assinatura; não há tabela de avisos processados
Como reproduzir	Em teste: reenviar dias depois um aviso assinado válido; ele é aceito e reprocessado.
Impacto	Com um aviso antigo capturado, dá para reativar um estado antigo em algum ramo menos protegido. A maioria dos ramos já ignora repetição.
Como corrigir	Recusar avisos com mais de 5 minutos e gravar o identificador de cada aviso numa tabela com chave única.
Status	Aberto

PX-07 Plano e domínio não conferem valor e moeda BAIXA

Eixo	6. Pagamentos e integrações
Onde	Ativação do plano e registro de domínio no aviso de pagamento; outros módulos do sistema já conferem
Como reproduzir	Em sandbox: pagamento de R$ 1 com os dados de um plano anual; o plano é ativado.
Impacto	Receita perdida se um dia houver uma cobrança criada errado ou manual.
Como corrigir	Conferir valor esperado (com ou sem cupom) e moeda BRL antes de ativar; senão, alerta para o administrador.
Status	Aberto

PX-08 Custo de IA na geração sem teto global BAIXA

Eixo	4. Abuso
Onde	Geração e edição de site com IA: a cota é contada e gravada em passos separados
Como reproduzir	Em teste: 15 pedidos simultâneos com uma conta, depois 10 contas descartáveis.
Impacto	Gasto com o provedor de IA.
Como corrigir	Função atômica no Postgres para a cota, teto diário global com alerta e alerta de orçamento no painel do provedor de IA.
Status	Aberto

PX-09 Visitante consegue esgotar o atendente com IA BAIXA

Eixo	4. Abuso
Onde	Atendente com IA dos sites publicados: teto diário por site e total; rota aberta e limite por endereço só na memória
Como reproduzir	Em teste: 61 mensagens para o mesmo site e conferir que o visitante real recebe "indisponível".
Impacto	Recurso pago fora do ar para um cliente, ou para todos até o dia seguinte. O custo segue protegido.
Como corrigir	Limitador compartilhado por endereço e por site (PX-01) e um desafio leve depois de algumas mensagens.
Status	Aberto

PX-10 Reivindicação de site não atômica BAIXA

Eixo	3. Isolamento dos dados
Onde	Link de reivindicação de site: troca de dono feita ao abrir a página, sem condição e sem conferir erro
Como reproduzir	Em teste: duas sessões abrem o mesmo link ao mesmo tempo; as duas veem "ok" e a última leva o site.
Impacto	Perda de posse do site, se o link vazar.
Como corrigir	Atualização condicional, transferindo só se o lead ainda não converteu, e mover a ação para um botão de confirmação.
Status	Aberto

PX-11 Campos de imagem aceitam endereços `javascript:` e `data:` BAIXA

Eixo	5. Tela e arquivos
Onde	Esquema de validação do conteúdo do site: endereços de imagem aceitam qualquer esquema
Como reproduzir	Em teste: gravar um site com o logo apontando para `javascript:`; a validação aceita.
Impacto	Baixo hoje (os campos só viram imagem); alto se algum modelo futuro usar o campo em um link.
Como corrigir	Aceitar só `https://`, de preferência só do Storage e de hosts conhecidos.
Status	Aberto

PX-13 CPF/CNPJ do titular do domínio em texto puro BAIXA

Eixo	3. Dados · 8. Retenção (LGPD)
Onde	Tabela de domínios comprados: documento, e-mail e telefone do titular, sem prazo de apagamento
Como reproduzir	Revisão de dados (não se aplica).
Impacto	Num vazamento do banco ou de um backup, o CPF dos clientes fica exposto, o que é incidente comunicável à ANPD.
Como corrigir	Cifrar o documento (o sistema já usa cifra forte em outro módulo) ou guardá-lo só enquanto o registro está pendente; documentar a retenção na política de privacidade.
Status	Aberto

PX-15 Proteção de origem tolerante e ausente em algumas rotas — BAIXA

Eixo	2. Login e permissão
Onde	Verificação de origem aceita pedido sem cabeçalho de origem; algumas rotas não fazem a verificação
Como reproduzir	Em teste: página num subdomínio que faz um POST para a prospecção com o administrador logado.
Impacto	Teórico hoje, porque os sites dos clientes não rodam script de terceiros.
Como corrigir	Conferir a origem em todas as rotas que mudam algo e tratar a origem ausente como inválida.
Status	Aberto

PX-16 Identificador do administrador na documentação — INFORMATIVA

Eixo	1. Chaves e segredos
Onde	Um documento de planejamento antigo no repositório
Impacto	Não dá acesso (não é segredo e o repositório é privado), mas indica qual conta é a de administrador.
Como corrigir	Trocar por um marcador no próximo commit.
Status	Aberto

PX-17 Chaves de poder total no arquivo local de ambiente — INFORMATIVA

Eixo	1. Chaves e segredos
Onde	Arquivo local de variáveis de ambiente na máquina de desenvolvimento (fora do repositório, como deve ser)
Impacto	A pasta tem cópia diária para a nuvem; falta confirmar que o arquivo fica de fora ou vai só para o cofre.
Como corrigir	Confirmar a exclusão de `.env*` no backup e trocar o token da hospedagem por um com escopo e validade.
Status	Aberto (não verificado)

PX-18 Pacotes instalados na máquina local defasados INFORMATIVA

Eixo	7. Dependências
Onde	Pasta local com versões anteriores às do arquivo de travamento de versões
Impacto	Os testes locais rodam versões diferentes das de produção.
Como corrigir	`npm ci` na pasta do projeto.
Status	Aberto

Conferido e sem problema

- Chave de serviço do banco só no servidor; o navegador recebe só a URL e a chave pública.
- Toda rota do dono confere o usuário no servidor e filtra pelo dono; não achamos acesso a site de outro cliente.
- Nenhuma consulta ao banco montada juntando texto.
- Proteção completa contra uso do servidor para acessar endereços internos na busca de sites de terceiros.
- Redirecionamento após o login protegido; tarefas agendadas exigem senha.
- Token de integração cifrado e o retorno do login externo assinado e ligado ao usuário.
- Upload de fotos reconvertido para JPEG, com limite de tamanho e quantidade.
- Rotas abertas que custam dinheiro (atendente e importação) têm teto gravado no banco e falham fechadas.

TESTES EXECUTADOS

O que foi verificado e o resultado

Nesta rodada a verificação foi pela leitura do código. Os testes ao vivo ficam para a rodada 2, em ambiente de teste.

EIXO	VERIFICAÇÃO	RODADA	ESPERADO	RESULTADO
1	Busca de chaves no código enviado ao navegador e em todo o histórico do repositório	R1	Nenhuma chave secreta	Ok
2	Conferência de sessão e de dono em todas as rotas	R1	Recusa sem login ou sem permissão	Ok no código
2	Segundo fator para o administrador	R1	Exigido	Achado PX-02
3	Acesso a site de outro cliente trocando o identificador	R1	Recusa	Ok no código; ao vivo na rodada 2
3	Regras de acesso (RLS) em todas as tabelas	R1	Todas protegidas	Ok no SQL; banco real não verificado (PX-04, PX-05)
3	Consulta montada com texto do usuário	R1	Nenhuma	Ok
4	Limites nas rotas que custam dinheiro ou enviam mensagem	R1	Limite compartilhado	Achados PX-01, PX-08, PX-09
5	HTML cru na tela e validação de endereços	R1	Tratado como texto	Ok; ressalva PX-11
5	Cabeçalhos de segurança do navegador	R1	Presentes	Achado PX-03
5	Upload de tipo e tamanho fora do permitido	R1	Recusa	Ok no código
6	Assinatura do aviso de pagamento	R1	Conferida	Ok
6	Aviso repetido e valor do pagamento	R1	Libera uma vez, com valor certo	Achados PX-06, PX-07
7	Relatório de vulnerabilidades das dependências de produção	R1	Nenhuma alta sem tratamento	Corrigido no mesmo dia (PX-12)

EIXO	VERIFICAÇÃO	RODADA	ESPERADO	RESULTADO
8	Backup documentado e restauração testada	R1	Restauração comprovada	Achado PX-14

BACKUP E RECUPERAÇÃO

Se tudo der errado, o sistema volta?

Onde fica a cópia	Não documentado. Backup do banco depende do plano do Supabase (a conferir no painel).
Fotos dos sites	Sem cópia conhecida. O backup do banco não inclui o Storage.
Teste de restauração	Não realizado nesta rodada.
Resultado	NÃO COMPROVADO · ver PX-14

PLANO DE CORREÇÃO

Próximos passos

FASE	O QUE FAZER	ACHADOS	PRAZO
0 · Urgente	Segundo fator no e-mail do administrador; conferir e anotar o backup; alerta de orçamento nas APIs pagas; confirmar que o backup local não leva o `.env.local`; `npm ci` local. *Dependências já atualizadas.*	PX-02, PX-14, PX-01, PX-08, PX-17, PX-18 · ~~PX-12~~	Esta semana
1	Limitador compartilhado e regras de firewall; cabeçalhos de segurança; permissões padrão do banco fechadas; MFA exigido para o administrador.	PX-01, PX-09, PX-03, PX-05, PX-02	2 semanas
2	Migrações versionadas e teste automático das regras de acesso; aviso de pagamento com prazo e valor conferido; cota atômica de geração; registro das ações do administrador e backup das fotos.	PX-04, PX-06, PX-07, PX-08, PX-14	1 mês
3	Só `https` nas imagens; origem obrigatória; reivindicação por botão; CPF cifrado; alertas automáticos de dependência.	PX-11, PX-15, PX-10, PX-13, PX-16	Contínuo

Recomendação: fazer a rodada 2 (testes ao vivo em ambiente de teste, incluindo o ensaio de restauração) depois das fases 0 e 1.

ALCANCE DESTE RELATÓRIO

Termo de responsabilidade

Este relatório descreve o estado do sistema auditado, na versão indicada, na data e no escopo indicados. Esta rodada foi de leitura do código e da configuração, sem testes ao vivo. Mudanças feitas depois no sistema, na hospedagem ou nos serviços conectados não estão cobertas.

A auditoria reduz riscos de forma significativa, mas nenhuma verificação garante a ausência total de falhas. Este documento não é certificação. É confidencial e foi preparado para uso exclusivo do cliente. Esta cópia é um exemplo anonimizado, para demonstração do serviço.

RESPONSÁVEL

IDDEIA · Auditoria de Segurança
Exemplo anonimizado de relatório real · out/2026

iddeia

Inteligência que Transforma Negócios

contato@iddeia.com.br · WhatsApp (41) 3798-4987

www.iddeia.com.br · HotMilk · Curitiba – PR

@iddeia.ai Marcos Faccin

MARCOS FACCIN ARQUITETURA E TECNOLOGIA LTDA · CNPJ 49.022.229/0001-16