AVIG 360

RESUMO PÚBLICO · PROGRAMA DE SEGURANÇA

Relatório de Segurança

Site institucional avig360.com e Control Tower

DATA DA VERIFICAÇÃO	PERÍODO	PRÓXIMA REVISÃO
24 de novembro de 2026	4º trimestre de 2026	Fevereiro de 2027

1 Resultado

SITUAÇÃO	CRÍTICA	ALTA	MÉDIA	BAIXA
Nenhuma vulnerabilidade identificada	0	0	0	0

Na verificação de 24/11/2026, todos os controles avaliados no site institucional e na Control Tower da AVIG 360 estavam **conformes**, sem vulnerabilidades em aberto de qualquer gravidade.

2 Escopo

SITE INSTITUCIONAL

avig360.com

Página principal, Espaço do Colaborador e Programa de Desenvolvimento Humano, com a interface de dados (API)

PLATAFORMA

Control Tower

avig360.com/controltower.html · painel de gestão de clientes e parceiros comerciais

3 Método

- Análise técnica do código-fonte e da configuração da versão publicada, com base no OWASP Top 10 (2021) e no OWASP ASVS 4.0.
- Revisão dos cabeçalhos de segurança, da política de conteúdo (CSP), do controle de acesso a arquivos e da proteção de credenciais.
- Verificação de dados pessoais e de autenticação conforme a LGPD (Lei 13.709/2018) e a Política AVIG-COMP-003.

O programa de segurança da AVIG 360 inclui, a cada trimestre, análise estática do código, análise das bibliotecas utilizadas e varredura automatizada do site no ar.

4 Controles verificados

Controle	O que foi verificado	Resultado
Conexão segura (HTTPS)	Todo o conteúdo servido por HTTPS, redirecionamento automático e HSTS com preload	✓ Conforme
Política de conteúdo (CSP)	Site, Control Tower e Espaço do Colaborador só executam scripts autorizados por assinatura, sem "unsafe-inline" nem "eval"	✓ Conforme
Scripts de terceiros	Nenhum script externo carregado nas páginas; nenhuma dependência de terceiros no navegador	✓ Conforme
Cabeçalhos de segurança	X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy e Cross-Origin-Opener-Policy	✓ Conforme
Proteção contra clickjacking	Páginas não podem ser incorporadas em sites de terceiros (frame-ancestors none)	✓ Conforme
Injeção de código (XSS)	Dados exibidos passam por escape; nenhum manipulador de evento embutido no HTML	✓ Conforme
Injeção de SQL	Todas as consultas ao banco de dados com parâmetros preparados	✓ Conforme
Arquivos sensíveis	Configuração, gabarito e banco de dados bloqueados ao acesso pelo navegador; listagem de pastas desativada	✓ Conforme
Credenciais e chaves	Nenhuma senha, token ou chave de acesso exposta no código público	✓ Conforme
Senhas e autenticação	Senhas com hash criptográfico, bloqueio após tentativas e código de verificação por SMS com validade de 10 minutos	✓ Conforme
Dados pessoais (LGPD)	CPF armazenado apenas como hash (HMAC-SHA256); páginas do colaborador fora dos buscadores	✓ Conforme
Integrações	Mensagens entre sistemas assinadas digitalmente (HMAC-SHA256)	✓ Conforme
Links externos	Links que abrem em nova aba isolados da página de origem (noopener)	✓ Conforme

5 Relatório técnico completo

Este resumo não traz detalhes de configuração, para não expor informações úteis a terceiros. O relatório técnico completo é disponibilizado a clientes, órgãos públicos e auditores mediante solicitação e termo de confidencialidade, pelo e-mail **dpo@avig360.com**.

ADRIANA G S D RIBEIRO

Adriana Ribeiro
CEO & Head de Expansão Global · AVIG 360

DOUGLAS S MOTA

Douglas da Silva Mota
Encarregado de Dados (DPO) · AVIG 360