RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

ingressossflamengo.com

Objeto investigado	ingressossflamengo.com - site que se apresenta como canal de venda de ingressos para jogos do Clube de Regatas do Flamengo (gTLD .com)
Natureza	Verificação de legitimidade e de risco ao consumidor / torcedor
Data da coleta	10/08/2026 (RDAP, DNS, HTTP/TLS, geolocalização, bundle JS) - reverificação em 11/08/2026
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · análise do app
Achado central	Cópia do site oficial de ingressos do Flamengo em domínio com "s" duplicado, com formulário de login próprio que captura e-mail/CPF e senha
Classificação	**RISCO ALTO**
Emissão do laudo	11/08/2026 as 08:53

1. Sumário Executivo

Este laudo documenta a investigação técnica do domínio **ingressossflamengo.com**, realizada em **10/08/2026** por técnicas de OSINT (inteligência de fontes abertas) e análise passiva - requisições equivalentes às de um visitante comum e consultas a bases públicas, **sem cadastro, sem login e sem envio de qualquer dado**. Toda evidência foi preservada em arquivo e teve seu hash SHA-256 calculado (Anexo A).

O domínio **está no ar** e entrega um site em português intitulado "Ingressos Flamengo | Compre Ingressos para Jogos do Flamengo", com listagem de próximas partidas (Brasileirao Serie A e CONMEBOL Libertadores, no Maracana e no Mineirao), botões "Comprar", menus "Login", "Cadastrar", "Biometria" e "Seja Nacao", e páginas institucionais de Termos de Uso, Aviso de Privacidade, Perguntas Frequentes e Política de Cancelamento.

O ponto central da investigação é que **este site é uma cópia do site oficial de ingressos do Flamengo**. A prova mais direta está no próprio código: a metatag OpenGraph do site copiado não foi alterada e ainda declara `og:url = https://ingressos.flamengo.com.br`, o endereço legítimo. Além disso, o site carrega imagens e recursos diretamente dos domínios oficiais do clube (`ingressos.flamengo.com.br`, `biometria.flamengo.com.br`, `nacao.flamengo.com.br`, `www.mengo.com.br`, `www.flapremios.com.br`) e reproduz os caminhos internos da plataforma oficial de bilheteria (`/lib/flamengo-nexo/` e `/lib/futebolcard/`). A página de Termos de Uso reproduz o texto da operadora oficial, citando a FutebolCard e o CNPJ do Clube de Regatas do Flamengo (33.649.575/0001-99) - identidades de terceiros usadas sem qualquer vínculo demonstrado com o domínio investigado.

O nome do domínio explora um **erro de digitação**: "ingresso**ss**flamengo" com **dois "s"**, construção típica de typosquatting. O domínio foi **registrado em 08/05/2026**, com **titular oculto**, via GoDaddy, e está hospedado em servidor compartilhado da própria GoDaddy nos Estados Unidos (Ashburn/VA), sobre Apache e PHP 8.3 - infraestrutura sem qualquer relação com a do clube.

O risco concreto ao torcedor está no **fluxo de compra**. Qualquer tentativa de comprar ingresso conduz a uma etapa de login ("Etapa 3 de 4"), cujo formulário envia **e-mail ou CPF e senha** por POST para `/datajson/login-process.php` - um endpoint **no próprio site copiado**. Ou seja, as credenciais digitadas por quem acredita estar acessando sua conta oficial de ingressos são entregues ao operador deste domínio. O site também exibe termo de consentimento para coleta de **biometria facial**, reproduzido da plataforma oficial. A coleta foi estritamente passiva: nenhum dado, credencial ou imagem foi enviado, e por isso o fluxo posterior ao login e a forma de pagamento não foram observados.

CLASSIFICAÇÃO DE RISCO	RISCO ALTO

Leitura: um site que cópia a bilheteria oficial de um clube, hospeda-se em domínio anônimo com "s" duplicado e recebe e-mail/CPF e senha em endpoint próprio oferece **risco elevado** de captura de credenciais e de venda de ingresso inexistente. Recomenda-se **não cadastrar, não fazer login, não pagar e não fornecer dados** (Seções 5 e 6).

2. Metodologia e Cadeia de Custódia

Empregaram-se exclusivamente **técnicas passivas**. As respostas de rede e de bases públicas foram salvas no momento da coleta e tiveram hash SHA-256 calculado. O DNS foi consultado via resolvedor público 1.1.1.1; o conteúdo, os cabeçalhos e o bundle JavaScript foram obtidos por requisição HTTPS de visitante comum. Nenhum formulário foi preenchido e nenhum dado pessoal foi enviado. Fuso de referência: UTC.

Etapa	Técnica / fonte	Evidência preservada
Registro do domínio	RDAP (Verisign / .com - registrador GoDaddy)	`rdap_raw.json`

DNS	dig (A, AAAA, NS, MX, TXT, SOA, CNAME) via 1.1.1.1	`dns_records.txt`
Conteúdo / cabeçalhos	curl HTTPS (visitante comum)	`corpo_home.html` · `headers_home.txt`
Fluxo de compra	curl HTTPS das rotas /buy/sector e /buy/express	`live_buy_sector_event_37145.html` · `live_express.html`
Páginas institucionais	curl HTTPS de /institutional/*	`live_institutional_terms-of-use.html` · `live_institutional_contact-us.html`
Aplicação (front-end)	Download do bundle JS	`bundle_js.txt`
Certificado TLS	openssl s_client / x509	`tls_cert.txt`
Geolocalização do IP	ipinfo.io · PTR reverso	`geoip.json`

3. Identificação Técnica (Domínio, DNS, Hospedagem e TLS)

Domínio	ingressossflamengo.com (gTLD .com - Verisign) - note o **"s" duplicado**
Registro	**08/05/2026** · expira 08/05/2027 (validade de 1 ano)
Idade na coleta	**~3 meses**
Titular	**Oculto** (o RDAP expõe apenas o registrador)
Registrador	GoDaddy.com, LLC (IANA 146) · abuse@godaddy.com
Status	clientDelete / clientRenew / clientTransfer / clientUpdate Prohibited (quatro travas)
Servidores de nome	ns69 / ns70.domaincontrol.com (GoDaddy)
DNS - A	132.148.176.245 · sem AAAA
DNS - MX / TXT	MX `smtp.google.com` (Google Workspace) · TXT `google-site-verification=tCWligDYg1QBqfXZL86G0XPnjdIdxLW-Csbdg6r1idg`
Hospedagem	AS26496 GoDaddy.com, LLC - Ashburn / Virginia (EUA), servidor compartilhado
PTR reverso	`245.176.148.132.host.secureserver.net`
Servidor web	Apache · `x-powered-by: PHP/8.3.31` · sessão PHPSESSID
Certificado TLS	CN=www.ingressossflamengo.com · emissor Let's Encrypt (DV) · válido 28/07/2026-26/10/2026
Origem do conteúdo	**og:url aponta para https://ingressos.flamengo.com.br** - metatag do site original, não alterada na cópia

Leitura técnica. Titular oculto, validade de 1 ano e hospedagem compartilhada em servidor norte-americano de proposito geral são incompatíveis com a operação de bilheteria de um clube de futebol brasileiro, que roda em plataforma dedicada. A presença de **MX do Google Workspace** e de registro de verificação do Google indica que o operador mantém **e-mail funcional no domínio** - recurso útil para enviar confirmações de compra com aparência oficial. O certificado DV gratuito comprova apenas o controle do domínio, **não a identidade de qualquer empresa** nem autorização do clube. Não se imputa conduta ao registrador nem a GoDaddy (hospedagem), meros provedores de infraestrutura.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

O site reproduz a interface da bilheteria oficial do Flamengo, incluindo a listagem de partidas, os menus de conta e biometria, os textos institucionais e os caminhos internos da plataforma oficial. A navegação de compra é curta e converge para uma única ação: **autenticar-se**. Ao clicar em "Comprar" em qualquer partida, o visitante é levado à "Etapa 3 de 4 - Login", com o formulário descrito abaixo.

Aspecto	Constatação
Tipo de serviço	Venda anunciada de ingressos para jogos do Clube de Regatas do Flamengo
Tecnologia	Site PHP 8.3 sobre Apache, em hospedagem compartilhada GoDaddy (EUA)
Relação com o original	**Cópia do site oficial** - og:url preservado apontando para ingressos.flamengo.com.br
Recursos de terceiros	Imagens e assets carregados de ingressos / biometria / nacao.flamengo.com.br, www.mengo.com.br, www.flapremios.com.br e museuflamengo.eleventickets.com
Caminhos internos copiados	`/lib/flamengo-nexo/` e `/lib/futebolcard/` - estrutura da plataforma oficial de bilheteria
Formulário de login	**POST para /datajson/login-process.php** no próprio domínio, com os campos `login` (e-mail ou CPF), `pass`, `security` e `redirect`
Barreira ao fluxo	Compra só avança após login ("Etapa 3 de 4") - o cadastro/autenticação é o objetivo imediato do funil
Dados anunciados como coletados	E-mail, CPF, senha e **biometria facial** (termo de consentimento reproduzido do site oficial)
Identidades de terceiros	Termos citam a FutebolCard e o CNPJ 33.649.575/0001-99 (Clube de Regatas do Flamengo), sem vínculo demonstrado com o domínio
Meio de pagamento	**Não observado** - o fluxo exige login, e a coleta foi estritamente passiva (nenhum dado enviado)

Leitura técnica. O elemento decisivo não é a semelhança visual - que sozinha poderia ser obra de um revendedor - mas o **destino das credenciais**: o formulário de login envia e-mail ou CPF e senha para um endpoint hospedado no próprio domínio copiado, e não para a plataforma oficial. Quem digita ali a senha da sua conta de ingressos entrega-a ao operador deste site; e, como muitos usuários reutilizam senhas, o alcance do dano pode ultrapassar o contexto da bilheteria. Some-se a isso o nome de domínio com "s" duplicado (captura de erro de digitação e de busca), o titular oculto e o carregamento de imagens dos domínios oficiais, que sustenta a aparência de autenticidade a custo zero. O fluxo de pagamento não foi observado porque exigiria cadastro e envio de dados, o que a metodologia passiva veda.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Formulário de login envia e-mail/CPF e senha para endpoint no próprio domínio copiado	`live_buy_sector_event_37145.html`	ALTA
2	Cópia do site oficial de ingressos do Flamengo - og:url original preservado no código	`corpo_home.html`	ALTA
3	Typosquatting: "ingresso**ss**flamengo" com "s" duplicado	`rdap_raw.json` · `corpo_home.html`	ALTA
4	Uso da marca e da identidade do Clube de Regatas do Flamengo e da FutebolCard sem vínculo demonstrado	`live_institutional_terms-of-use.html`	ALTA
5	Titular oculto, domínio de 1 ano, sem qualquer identificação do operador no site	`rdap_raw.json`	ALTA

6	Anuncio de coleta de biometria facial, com termo de consentimento copiado do site oficial	`live_buy_sector_event_37145.html`	MEDIA
7	Hospedagem compartilhada generica nos EUA, incompatível com bilheteria de clube brasileiro	`geoip.json · headers_home.txt`	MEDIA
8	Imagens e recursos carregados (hotlink) dos domínios oficiais do clube	`corpo_home.html`	MEDIA
9	E-mail funcional no domínio (MX Google Workspace) apto a enviar confirmações com aparência oficial	`dns_records.txt`	BAIXA
10	Certificado TLS DV gratuito - comprova apenas controle do domínio	`tls_cert.txt`	BAIXA

Síntese: 5 indicadores de severidade ALTA, 3 MEDIA e 2 BAIXA. **Nenhum fator de legitimidade** (identificação do operador, autorização do clube, vínculo com a plataforma oficial de bilheteria) foi constatado.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em 10/08/2026, conclui-se que **ingressossflamengo.com** é um site de **alto risco**: uma **cópia do site oficial de ingressos do Flamengo**, publicada em domínio anônimo com "s" duplicado (typosquatting), hospedada em servidor compartilhado nos Estados Unidos e sem qualquer identificação do operador, que carrega imagens dos domínios oficiais do clube, reproduz os termos da operadora oficial (FutebolCard) e o CNPJ do clube, e cuja etapa de compra converge para um **formulário de login que envia e-mail/CPF e senha para endpoint no próprio domínio copiado**. Classifica-se o caso como **RISCO ALTO** ao consumidor, tanto por captura de credenciais quanto pela venda anunciada de ingressos por quem não demonstra autorização para vende-los.

Recomendações ao consumidor / solicitante

- **Não fazer login, não se cadastrar, não pagar e não enviar documentos ou selfie** a este site.
- Comprar ingressos apenas pelo canal oficial - `ingressos.flamengo.com.br` -, conferindo o endereço na barra do navegador **letra por letra**: o domínio falso difere apenas por um "s" a mais.
- Preferir digitar o endereço oficial ou usar um favorito, em vez de clicar em links de anúncios, redes sociais ou grupos de WhatsApp.
- Se já houve login neste site: **trocar imediatamente a senha** da conta oficial de ingressos e de qualquer outro serviço onde a mesma senha seja usada, e ativar verificação em duas etapas onde disponível.
- Se já houve pagamento: acionar o banco e, no caso de Pix, o mecanismo **MED**; reunir comprovantes e registrar Boletim de Ocorrência e reclamação em **consumidor.gov.br**.

Recomendações de mitigação / denúncia

- Denunciar o domínio aos canais de abuse do registrador e da hospedagem (`abuse@godaddy.com`), anexando este laudo.
- Comunicar o **Clube de Regatas do Flamengo** e a operadora oficial de bilheteria (FutebolCard) sobre o uso não autorizado da marca, dos textos e do CNPJ, para as providências de propriedade intelectual e de segurança dos torcedores.
- Reportar o endereço aos mecanismos de navegação segura (Google Safe Browsing, Microsoft SmartScreen) e as plataformas onde o link eventualmente circule como anúncio.
- Preservar este relatório e as evidências (pasta `evidencias/`, com hashes SHA-256) para eventual uso administrativo ou judicial.

*Ressalva metodológica: este laudo baseia-se em fontes abertas e reflete o estado do domínio nas datas indicadas (coleta em 10/08/2026, reverificação em 11/08/2026). A classificação expressa um juízo técnico de risco e não substitui decisão de autoridade policial, administrativa ou judicial. Não se imputa conduta ilícita ao Clube de Regatas do Flamengo, a FutebolCard nem aos provedores de infraestrutura citados (GoDaddy, Google) - o clube e a operadora oficial figuram aqui como **titulares das identidades***

***usadas sem autorização demonstrada**. Nenhuma credencial, dado pessoal ou imagem foi enviada ao site durante a investigação.*

Anexo A - Manifesto de Integridade (SHA-256)

Hashes SHA-256 das evidências preservadas no momento da coleta (cadeia de custódia).

Arquivo	SHA-256
bundle_js.txt	098ff0ec57e4ee28c0fffc9b4abdaa9f06999879793a72af43452fa513581d45
corpo_home.html	e50e09d4ed63a3a18acf4435bcbaa1b8436c28be90c8315bd47295c902131a1e
dns_records.txt	b54c311136b2ed6ba10d70cf6b9158f2ee711af21e78588142c30ecf9f0d70af
geoip.json	de555021e477de0cbec55c5a1be28f7866c1505c8e28722dabe8dbadbccc46af
hash_manifest.txt	7bb956ccdd1b1f767f15eea44d2d8512ac3e4b4b5c9c84ec6338a6a73435cbe1
headers_home.txt	c12e9eee0d6d09745886aee458c61f13acb4dc154ead6535361f3ea5eb942750
live_buy_sector_event_37145.html	a1f764526cf3ffbea7659c0956f1026dcdceb7198b8e174101616d61e041cea2
live_express.html	091e7a36e810fd103ea5a5770569a528768bbb3944f48e2f433216fb259de34e
live_institutional_contact-us.html	5e8ea96945f6a7c7edab6b7781279933b25b3546b48b39dc434ded26f0d7b295
live_institutional_terms-of-use.html	1395dfa53fcc97eebca0bffab32ae30b5a96c708da6b48a9a6784f8ce53a6734
rdap_raw.json	65419b570eace64849591f014eed9e93a4b1f758bc771f98a2cc2f1b4d150dc6
tls_cert.txt	1a73e8e4f760590bd56b707b63f54fa210c284596a991c00b52fa36b993e2c8f

- Fim do relatório -