Guia de Brand Suitability e Combate à Fraude

Edição 2024

iab brasil

PREFÁCIO

Por Silvio Locali,
vice-presidente do Comitê de Brand Safety 2024 do IAB Brasil

Brand Suitability e combate à fraude são componentes essenciais no cenário da publicidade digital, com o objetivo de garantir que as marcas possam manter sua reputação e, ao mesmo tempo, maximizar a eficácia de suas campanhas.

Brand Suitability envolve alinhar o conteúdo da publicidade com os valores e padrões de uma marca, garantindo que os anúncios apareçam em ambientes apropriados e ressoem com o público-alvo. As tecnologias disponíveis de proteção alinham mecanismos de Ciência Semântica e *machine learning* para classificar o conteúdo com precisão e em tempo real. Isso permite que os anunciantes apliquem o nível certo de proteção da marca, mantendo ou melhorando a escala.

Combater a fraude é igualmente essencial, pois atividades fraudulentas podem impactar significativamente o retorno sobre o gasto com anúncios e a eficácia geral das campanhas publicitárias. Os mecanismos robustos disponíveis de prevenção de fraude pré-lance/SIVT (*Sophisticated Invalid Traffic* ou Tráfego Inválido Sofisticado) ajudam os anunciantes a detectar e prevenir vários tipos de fraude, incluindo fraude de site/aplicativo, *malware* e dispositivos sequestrados. Ao identificar e mitigar essas ameaças, garante que os anúncios sejam vistos por seres humanos reais em ambientes adequados à marca, protegendo assim a integridade dos esforços de publicidade.

Nosso compromisso no Comitê de *Brand Safety* do IAB Brasil é explorar temas relevantes para que as marcas possam continuar anunciando mesmo em momentos críticos como guerras, desastres ambientais e humanos, eleições entre outros, e que consigam responder rapidamente à evolução constante da nossa indústria - principalmente com o uso de IA.

Nosso objetivo com este *Guia de Brand Suitability e Combate à Fraude* é fornecer aos anunciantes as ferramentas que precisam para proteger sua marca, otimizar o desempenho da campanha e garantir que seus esforços de publicidade sejam eficazes e responsáveis.

SUMÁRIO

1 Introdução

A. Definição de *Brand Safety* e *Brand Suitability*

Brand Safety

***Brand Safety* é um conjunto de práticas** que as empresas são indicadas a aplicar em suas estratégias de mídia digital **para proteger suas marcas - evitando que sejam associadas a conteúdos ilegais, falsos e inseguros**, prejudicando com isso sua imagem junto aos consumidores e afetando direta/indiretamente o seu ROI.

Brand Suitability

Brand Suitability quer dizer o quanto uma marca se encaixa em um determinado ambiente, o que pode variar de acordo com o produto e o anunciante.

Recentemente, o tema foi destacado em um artigo da *Association of National Advertisers* (ANA) como uma das principais preocupações dos anunciantes, especialmente em um contexto em que as formas de comunicação com os usuários se tornam cada vez mais complexas. A adequação da marca vai além de categorias padrão e listas de bloqueio de palavras-chave, oferecendo uma proteção personalizada para quem anuncia.

O objetivo é maximizar a proteção sem comprometer a escala, personalizando a segurança da marca, a adequação e as configurações de fraude.

B. Diretrizes Gerais de *Brand Safety*

Para melhor garantir a segurança de marca, o mercado passou a adotar os padrões da *4A's Advertiser Protection Bureau (APB) Brand Safety Floor and Brand Suitability Framework*, apoiados pela *Global Alliance for Responsible Media* (GARM), de acordo com a necessidade de cada marca. Uma *versão das diretrizes da GARM* foi publicada em 2022 em português, em uma parceria entre o IAB Brasil e a ABA (Associação Brasileira de Anunciantes).

Mas, em agosto de 2024, a *WFA (World Federation of Advertisers)* decidiu interromper as atividades da GARM que, até então, era uma iniciativa da associação mundial de anunciantes que unia diferentes setores para combater o conteúdo prejudicial nas plataformas de mídia digital. A estrutura GARM *Brand Safety Floor + Suitability Framework* permitia avaliar a segurança e adequação dos anúncios nos conteúdos que os acompanham. Essa estrutura definia categorias de conteúdo sensível, com níveis de risco variados, e estabelecia diretrizes de monetização, desde conteúdos inadequados para publicidade (o *"Brand Safety Floor"*) até aqueles que podem ser adequados, mas que apresentam diferentes graus de sensibilidade para os anunciantes (o *"Suitability Framework"*).

Essas diretrizes permitiam às marcas trabalhar de forma ainda mais estratégica ao aplicar as regras restritivas de proteção. Quando as marcas reagem de forma genérica ao intenso ciclo de diferentes tipos de notícias, conteúdos podem ser incorretamente restringidos em massa, por causa, muitas vezes, de palavras-chave de bloqueio abrangentes demais, o que acaba prejudicando a escala e afetando editores legítimos. Por isso, é fundamental ir além da segurança e avançar para a adequação da marca.

A adequação da marca assegura que os anúncios sejam exibidos em contextos ideais, adaptando-se à relevância contextual e evitando conteúdos inadequados, mas sem deixar de aproveitar os veículos

verdadeiramente confiáveis. A *Taxonomia de Conteúdo do IAB Tech Lab*, que adotou as diretrizes da GARM, contribui para essa estratégia mais inteligente. Ela evoluiu para ajudar editores a organizar e diferenciar com mais precisão conteúdos como “esportes” em relação a “notícias”, por exemplo. O uso da taxonomia minimiza os riscos de bloqueio indiscriminado, por classificar e separar melhor as informações que podem ser sensíveis.

A Taxonomia de Conteúdo é uma “linguagem comum” para descrever conteúdos, usada para segmentação contextual e segurança da marca. A *versão 3.0* da taxonomia foi desenvolvida com atualizações para apoiar melhor áreas como Notícias, Vídeo/Conteúdo CTV, Podcasts, Rádio, Jogos e Lojas de Aplicativos.

Com a interrupção do trabalho da GARM, o mercado aguarda um novo consenso que possa definir regras universais de *suitability*.

C. Importância

A segurança da marca é crucial por vários motivos. Primeiro, ela protege a reputação de uma marca online. A internet está repleta de uma vasta gama de conteúdo, alguns dos quais podem ser inseguros ou inadequados, representando um risco de reputação para anunciantes globais. Isso pode variar de retórica inflamatória a terrorismo e notícias falsas. Dada a natureza dinâmica e imprevisível do reino digital, é fundamental garantir o alinhamento entre marca e conteúdo.

Em segundo lugar, a segurança da marca fornece controles precisos para melhor proteção - com mais de 100 categorias de prevenção de conteúdo disponíveis em 44 idiomas.

Em terceiro permite que as marcas estabeleçam uma governança global consistente, ao mesmo tempo em que permitem flexibilidade local, oferecendo cobertura abrangente pré e pós-lance e níveis elevados de proteção ao anunciante, gerando ganhos em eficiência operacional e desempenho da campanha.

D. Riscos Associados à Marca

Se um anunciante não usar a proteção de segurança da marca, ele se expõe a vários riscos. Um dos principais riscos é o potencial de sua marca ser associada a conteúdo inapropriado ou prejudicial. Isso pode incluir conteúdo extremo e gráfico, violação de direitos autorais, malware, phishing e spam. Essas associações podem prejudicar a reputação da marca e a confiança do cliente.

Além disso, sem proteção de segurança da marca, os anunciantes podem não conseguir aplicar o nível certo de proteção da marca enquanto mantêm ou melhoram a escala. Marcas diferentes têm preferências de adequação diferentes e, sem uma abordagem diferenciada, podem acabar anunciando em lugares que não são adequados para suas preferências específicas de marca.

Outro risco é o potencial de desempenho reduzido. Ser muito conservador com seleções - mais categorias, mais palavras-chave, etc. - normalmente não se traduz em melhor desempenho, pois pode impactar o alcance e aumentar os bloqueios (também conhecido como desperdício de mídia). Por outro lado, algumas marcas, especialmente aquelas novas na verificação, podem não ser conservadoras o suficiente com base no risco de sua marca.

Por fim, sem proteção de segurança da marca, as marcas podem não conseguir atingir efetivamente o público desejado. Por exemplo, a segmentação por idioma é um aspecto importante das campanhas globais e, sem as ferramentas certas, as marcas podem não conseguir evitar idiomas não apropriados para a marca ou campanha, ou identificar conteúdo em idiomas aceitáveis para cada campanha.

69%

dos consumidores estão **MENOS PROPENSOS** a comprar um produto se a marca estiver associada a desinformação.

74%

estão **MAIS PROPENSOS** a questionar a reputação da marca caso ela esteja associada a desinformação.

Fonte: Pesquisa feita pela Sapio para DV Global Insights Report 2024.

E. Regulamentação

Em vários países existem órgãos que desenvolvem diretrizes alinhadas com o mercado para promover práticas de proteção às marcas e criar diretrizes a serem seguidas. Os principais são:

Media Rating Council: O *Media Rating Council* (MRC) é uma organização que garante que os serviços de medição de audiência na indústria de mídia sejam válidos, confiáveis e eficazes. O MRC estabelece critérios mínimos e oferece um sistema de auditoria para garantir que as medições de audiência sigam esses critérios, com destaque para auditorias em visibilidade e fraude publicitária.

GARM Framework by WFA: A *Aliança Global para Mídia Responsável* (GARM), criada pela Federação Mundial de Anunciantes para combater o conteúdo prejudicial em plataformas digitais e sua monetização por meio da publicidade, deixou de existir em julho de 2024. O *framework* desenvolvido pela GARM fornecia uma estrutura para avaliar a segurança e adequação da marca em relação aos conteúdos publicados próximos dos anúncios, estabelecendo diretrizes sobre quais tipos de conteúdo são seguros ou arriscados para a publicidade.

4A's Advertiser Protection Bureau: O *Advertiser Protection Bureau* (APB) é uma iniciativa de segurança de marca liderada pelas agências americanas de mídia (associação 4A's) para promover um ambiente transparente e seguro para anunciantes, consumidores e publishers, abordando questões de segurança e adequação de marcas em ambientes de mídia, responsável por conteúdos como o *Cross-Industry Call to Action* e o *Misinformation/Disinformation*, e que poderia reassumir algumas funções da GARM, como o *Brand Safety Floor and Suitability Framework*.

Trustworthy Accountability Group (TAG): O *Trustworthy Accountability Group* (TAG) é uma iniciativa americana voltada a promover a transparência e combater atividades prejudiciais na indústria de publicidade digital, como fraude publicitária, *malware*, pirataria na internet e falta de transparência. Criado por grandes associações do setor, o TAG trabalha para elevar os padrões da indústria por meio de colaboração e melhores práticas.

Coalition for Better Ads: *A Coalition for Better Ads* (CBA) desenvolve e implementa padrões globais para melhorar a qualidade da publicidade online, alinhando-se às expectativas dos consumidores. Esses padrões, conhecidos como *Better Ad Standards*, são aplicáveis a ambientes de web em desktop e dispositivos móveis, buscando reduzir práticas publicitárias intrusivas.

WIPO Alert: A *WIPO Alert* é uma plataforma online gerenciada pela Organização Mundial da Propriedade Intelectual (WIPO), que permite às autoridades nacionais compartilharem listas de sites que violam direitos autorais. Anunciantes e agências podem usar sem custos essas listas para evitar que seus anúncios sejam exibidos em sites piratas, contribuindo para a proteção global da propriedade intelectual.

Code of Practice on Disinformation: O *Código de Prática sobre Desinformação* é uma iniciativa autorregulatória global para combater a disseminação de desinformação e notícias falsas na internet. O código, que é uma resposta da indústria às diretrizes da Comissão Europeia, inclui compromissos para melhorar a transparência na publicidade política e fechar contas falsas, promovendo melhores práticas para enfrentar a desinformação.

Memorandum of understanding on online advertising and IPR: O *Memorando de Entendimento* (MoU), da Comissão Europeia, é um *acordo voluntário* para reduzir a publicidade em sites e aplicativos móveis que violam direitos autorais ou promovem produtos falsificados. O objetivo é diminuir as receitas desses sites ilegais, monitorando o impacto da iniciativa e promovendo a cooperação entre os signatários.

European Viewability Steering Group: O *European Viewability Steering Groups* (EVSG) desenvolve os *Princípios Europeus de Visibilidade*, criados para elevar os padrões mínimos de qualidade na medição de publicidade digital, garantir a medição da exposição a anúncios, melhorar a experiência do usuário na internet e aumentar a confiança no ambiente de publicidade digital na Europa.

2 Estratégias de *Brand Safety*

A. Monitoramento Proativo

As marcas devem considerar cuidadosamente quais ferramentas fornecem o equilíbrio certo entre precisão, proteção e escala.

B. Diretrizes de Conteúdo Seguro

Categorias de conteúdo de verificação e níveis de adequação

As categorias de bloqueio variam de acordo com o parceiro de verificação, mas existem atualmente mais de 100 categorias de Brand Suitability disponíveis que podem incluir violência, terrorismo, discurso de ódio, acidente aéreo, guerras, terrorismo e muito mais. Certifique-se de que seu provedor esteja alinhado para fornecer cobertura e escala ideais.

Listas de palavras-chave

Seja estratégico em relação às suas listas de palavras-chave; considere notícias de última hora específicas e tópicos muito personalizados que você deseja evitar.

Exceções/controles granulares em nível de site

Exceções específicas em nível de site, aplicativo e página ajudam a ajustar seu perfil. Designe o conteúdo que você deseja exibir.

Listas de inclusão/exclusão

Identifique se existem sites e aplicativos específicos apropriados ou inadequados para suas campanhas. Considere listas de auditoria também.

C. Parcerias com Plataformas e Editores

Ferramentas para ajudar a gerenciar esforços de reputação da marca.

3 Implementação de Medidas de *Brand Safety e Brand Suitability*

A indústria de publicidade digital tem se transformado de forma constante e cada vez mais rápida na última década, especialmente com o advento da mídia programática e das redes sociais que automatizam os processos de compra de mídia digital e ampliam o alcance das campanhas. Todavia, com esse cenário cheio de possibilidades, nasce também a necessidade de proteção e adequação das marcas dentro desses ambientes - visto que um único anúncio no local e momento inadequados pode comprometer a equidade e reputação construída ao longo de anos. A maneira mais adequada para prevenção de danos é a construção e implementação de medidas de *Brand Safety e Suitability* dentro de suas políticas internas.

A. Desenvolvimento de Políticas Internas

Dada a complexidade de adequação das diferentes marcas dentro dos ambientes digitais, a construção de políticas internas que definem as diretrizes a serem seguidas pelas marcas é essencial. Para desenvolver esses pontos, contudo, é necessário realizar um minucioso levantamento de riscos para a marca, considerando não tão somente os valores, visão e missão, mas também fatores externos relevantes dentro do histórico global e local que possam ter oferecido algum risco à marca dentro de determinados contextos. Com uma política interna consolidada, será possível determinar os critérios para ter um *Brand Safety* e *Brand Suitability* bem estabelecidos e proteger a equidade e reputação da marca.

Para esse exercício é necessário trazer à tona alguns questionamentos, como: quais tipos de conteúdo e associações podem comprometer a integridade da marca? Quais plataformas e formatos de mídia oferecem maior ou menor risco em termos de *Brand Safety*? Como a marca pode se adaptar a novos cenários digitais sem comprometer sua identidade e reputação? Além disso, é importante avaliar como eventos sociais, culturais e políticos em constante mudança podem impactar a percepção da marca e influenciar o comportamento do público-alvo.

Outro ponto relevante é a definição de métricas claras para monitorar o desempenho das políticas de *Brand Safety* e *Suitability*, garantindo que elas sejam ajustadas conforme necessário. Essa flexibilidade é fundamental para lidar com a evolução rápida do ambiente digital e com possíveis crises de imagem que possam surgir. A integração dessas diretrizes com todas as áreas da empresa, como marketing, comunicação e compliance, também é essencial para garantir que as práticas estabelecidas sejam aplicadas de forma consistente e eficaz.

Com esses aspectos bem definidos, a marca estará mais preparada para navegar nos desafios do ambiente digital, protegendo seus valores e mantendo uma conexão autêntica com seu público.

B. Treinamento de Equipes

O treinamento de equipes é um pilar essencial para a implementação eficaz de políticas de *Brand Safety* e *Suitability*. As diretrizes estabelecidas pela empresa devem ser claramente comunicadas a todos os colaboradores, especialmente aos que atuam diretamente na criação, distribuição e monitoramento de conteúdo. A equipe precisa entender os riscos associados à exposição da marca a ambientes inadequados e a importância de proteger sua reputação em um cenário digital dinâmico e imprevisível.

Esse treinamento deve incluir não apenas o conhecimento das políticas internas, mas também a habilidade de identificar potenciais ameaças e oportunidades dentro dos ambientes digitais. Capacitar os colaboradores a reconhecer sinais de alerta e agir preventivamente reduz a exposição a conteúdos que possam comprometer a integridade da marca. Além disso, é importante que as equipes estejam atualizadas sobre as novas tecnologias e ferramentas de monitoramento, para que possam responder rapidamente a qualquer incidente e ajustar as estratégias conforme necessário.

Investir na formação contínua da equipe cria uma cultura de responsabilidade e cuidado com a marca, assegurando que todos estejam alinhados com os princípios de *Brand Safety* e *Suitability* e preparados para agir em situações críticas.

C. Auditoria e Avaliação de Riscos

A auditoria e a avaliação de riscos são etapas fundamentais no processo de construção e manutenção de uma estratégia robusta de Brand Safety e Brand Suitability. Realizar auditorias regulares permite identificar áreas vulneráveis onde a marca pode estar exposta a conteúdos ou contextos prejudiciais. Esse processo deve ser abrangente, analisando tanto a comunicação interna quanto os pontos de contato da marca com o público, incluindo canais de mídia social, publicidade programática e parcerias com influenciadores.

A avaliação de riscos, por sua vez, envolve uma análise profunda dos fatores que podem impactar a reputação da marca. Isso inclui a identificação de tópicos sensíveis, movimentos socioculturais e mudanças no comportamento do consumidor, que podem exigir ajustes nas diretrizes de Brand Suitability. Além disso, o mapeamento de riscos externos, como crises políticas, econômicas ou ambientais, é crucial para antecipar possíveis cenários que possam afetar a percepção da marca.

Uma auditoria eficiente não só revela potenciais ameaças, mas também oferece insights para melhorar continuamente as políticas internas, garantindo que a marca esteja alinhada com os valores que deseja comunicar. Por meio desse processo, é possível fortalecer a segurança da marca, preservando sua imagem e reputação em um ambiente digital complexo e em constante evolução.

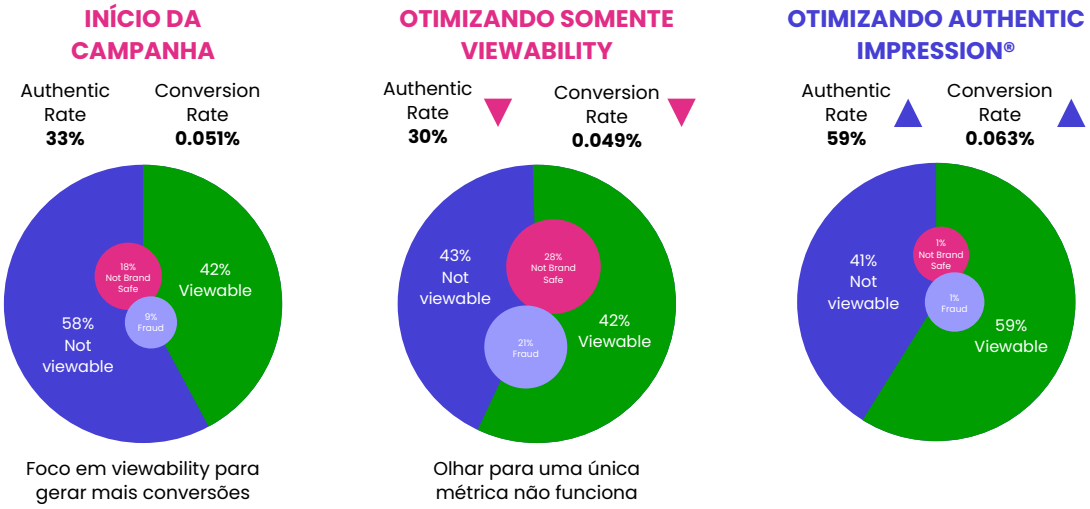
Ademais, o uso de plataformas de verificação é imprescindível em todo esse processo para dar suporte à auditoria e à avaliação de riscos. Essas plataformas fornecem relatórios detalhados sobre onde os anúncios estão sendo veiculados e monitoram o nível de adequação do conteúdo levando em conta as particularidades estabelecidas por cada marca e as diferentes estratégias de campanha. Com essas ferramentas, as marcas podem garantir maior transparência e controle sobre sua exposição, identificando rapidamente qualquer violação ou desvio das diretrizes de segurança e ajustando suas campanhas para manter a proteção da reputação.

4 Estudos de Caso e Exemplos

A. Experiências de Empresas com *Brand Safety*

CASE STUDY

Otimizando somente uma variável



Foco em viewability para gerar mais conversões

Olhar para uma única métrica não funciona

Fonte: DoubleVerify

*Grande empresa de telecomunicações busca impulsionar a aquisição de novos clientes

Lições Aprendidas

1. Uma grande marca de telecomunicações precisava aumentar as conversões em sua campanha de aquisição. A taxa de conversão de referência para a campanha foi de 0,051%.

Otimizando na taxa de visibilidade *(viewability)*

2. Ao otimizar apenas para *viewabilities* mais altos, não apenas a visibilidade aumentou, mas também a fraude, a inadequação da marca e as violações fora da geografia. Em alguns casos, mais de 50% das impressões estavam fora de seus alvos geográficos.

   Impressões fraudulentas e clientes fora do alcance geográfico do cliente podem ter altas taxas de *viewability*, mas não conseguem converter. O resultado — otimizar sem observar todas as métricas diminuiu a taxa de conversão.

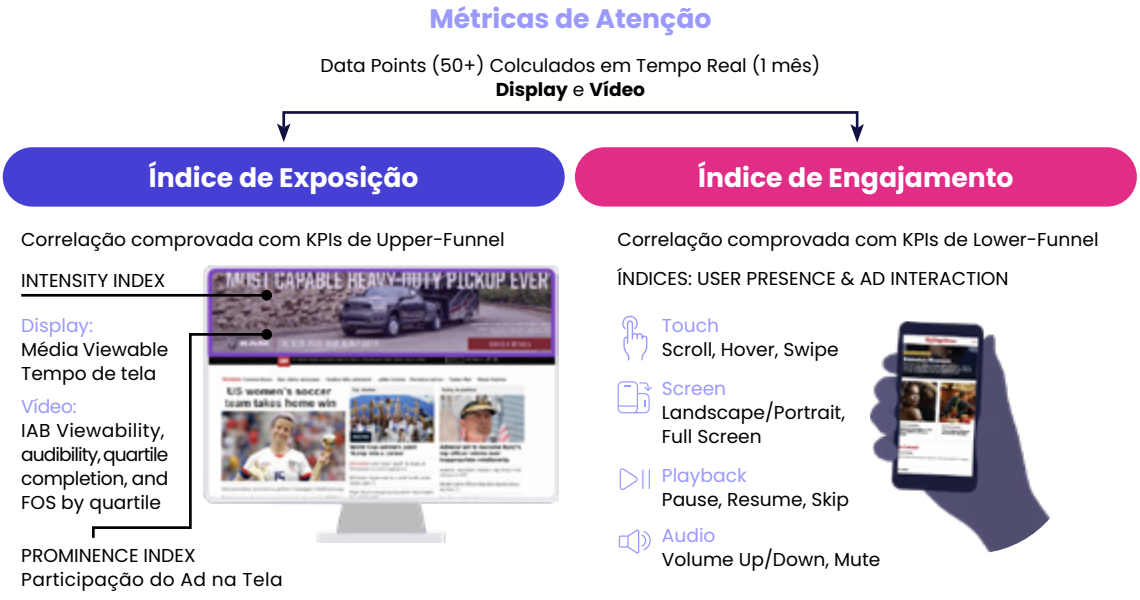
   Otimizando usando a taxa de autenticidade (impressões com viewability, livre de fraude, seguindo os parâmetros de brand suitability do anunciante e na geolocalização correta)

3. A otimização apenas no *viewability* não estava funcionando, então o cliente mudou sua estratégia de compra para otimizar buscando aumentar a taxa de autenticidade.

   O foco no inventário que foi totalmente visualizado, livre de fraudes, adequado à marca e na geografia certa, entregou impressões que tiveram a melhor oportunidade de desempenho. A taxa de conversão aumentou para 0,063%

5 Tendências Futuras e Desafios

A. Novas Tecnologias e Abordagens



Fonte: DoubleVerify

As métricas de atenção são uma solução de dados abrangente desenvolvida para medir e otimizar campanhas de publicidade digital. É uma solução credenciada pelo MRC que fornece dados quase em tempo real sobre a exposição e o engajamento de anúncios digitais, avaliando mais de 50 pontos de dados para entender como os anúncios são apresentados e como os consumidores interagem com eles.

As principais métricas incluem tempo em exibição, espaço na página, hovers, conclusões de quartil e interações como ajustes de volume. Esses insights ajudam os anunciantes a otimizar suas campanhas identificando os criativos e inventários de anúncios de melhor desempenho - o que, em última análise, impulsiona melhor desempenho da campanha.

Dados usados para Programática

B. Mudanças no Ecossistema Digital

O relatório *"State of Data 2024"*, desenvolvido pelo IAB US, trouxe um importante alerta ao mercado global de publicidade sobre transições significativas no ecossistema de mídia digital, especialmente no mercado de publicidade de mídia programática.

Com a intensificação das legislações de privacidade e a perda de sinais digitais, como cookies de terceiros, as empresas enfrentam mais desafios na coleta e utilização de dados de qualidade. Essa mudança atinge diretamente a personalização de mensagens e a eficácia das campanhas, exigindo que marcas, agências e veículos passem a usar novas estratégias e reorganizem estruturas internas para conseguir se adaptar ao novo cenário.

No mercado de publicidade programática, a precisão na segmentação e a personalização dependem fortemente da disponibilidade de dados confiáveis. A redução na *acessibilidade desses dados*

compromete a capacidade de alcançar os targets com mais precisão. A indústria está investindo em técnicas baseadas em inteligência artificial e modelagem probabilística, além de apostar em publicidade contextual e no fortalecimento do uso de dados primários. No entanto, a falta de interoperabilidade entre diferentes plataformas ainda dificulta a medição da efetividade das estratégias de marketing.

Nesse contexto de mudanças no ecossistema de mídia digital, é importante que as empresas adotem uma abordagem de privacidade desde o início ("privacy-by-design"), não apenas para cumprir regulamentações, mas também para fortalecer a confiança do consumidor. As organizações que integrarem a privacidade de forma estratégica e inovarem no uso de novas tecnologias de dados estarão mais bem posicionadas para liderar o mercado. Adaptar-se a essas transformações, focando na qualidade dos dados e na proteção da privacidade, é essencial para garantir o sucesso e a sustentabilidade da publicidade de mídia programática no futuro.

Por isso, o IAB Tech Lab lançou o ***Padrão de Transparência de Dados***, ou **Data Label**, que estabelece requisitos padronizados de divulgação para provedores de dados de audiência no mercado de publicidade digital. Funciona como um "rótulo nutricional" para conjuntos de dados, fornecendo informações detalhadas sobre a origem, qualidade e métodos de coleta dos dados, incluindo aspectos como recência, proveniência e critérios de segmentação. É um padrão que permite que os compradores de dados entendam exatamente o que estão adquirindo, promovendo maior transparência, confiança e conformidade com as regulamentações de privacidade no ecossistema de mídia programática.

C. Desafios

Entre os grandes desafios recentes da proteção às marcas está a descontinuação da *Global Alliance for Responsible Media (GARM)*, que desempenhou um papel relevante para o mercado de publicidade digital ao estabelecer diretrizes de segurança e adequação. Criada pela *World Federation of Advertisers (WFA)* em 2019, a GARM reuniu anunciantes, agências e plataformas de mídia para desenvolver padrões para evitar a associação de anúncios a conteúdos prejudiciais ou ilegais. Em colaboração com o IAB Tech Lab, foi também fundamental na criação do *Brand Safety Floor* e do *Brand Suitability Framework*, ferramentas que permitiram às marcas categorizar e monitorar o conteúdo de maneira consistente, garantindo que as campanhas publicitárias continuassem alinhadas com seus valores e responsabilidades corporativas.

Recentemente, a GARM teve suas atividades interrompidas pela WFA, apesar da reconhecida importância da aliança na redução de conteúdos nocivos e na proteção da reputação das marcas, especialmente na manutenção dos padrões de segurança e adequação.

Sem a liderança da GARM, as marcas podem ser incentivadas a buscar novos critérios uniformes para a avaliação de conteúdos, para evitar a fragmentação das práticas de segurança e a vulnerabilidade a associações indesejadas com conteúdos prejudiciais, que poderiam afetar negativamente a confiança dos consumidores. O IAB Tech Lab e o *Trustworthy Accountability Group (TAG)*, mesmo antes da criação da GARM, já assumiam papéis proeminentes, incentivando a colaboração intersetorial e desenvolvendo novas ferramentas e taxonomias que atendam às necessidades de segurança das marcas no ambiente digital.

Sites MFA

Sites MFA são definidos como aqueles cujo único propósito é entregar anúncios. Isso é evidente por meio de práticas de gerenciamento de monetização que levam a uma grande entrega de anúncios. É possível categorizar sites inteiros e seções ou páginas específicas como *Made for Advertising (MFA)*.

Essas seções são identificadas com base em várias características, como conteúdo clickbait, desordem de anúncios, conteúdo duplicado, vídeo fixo, conteúdo desatualizado, design de baixa qualidade, rolagem infinita e URLs principais de lista. No entanto, é importante observar que a classificação de um site ou seção como MFA não significa necessariamente que seja fraudulento.

Fonte: DoubleVerify

Sites (Qualidade de sites e usabilidade para usuários)

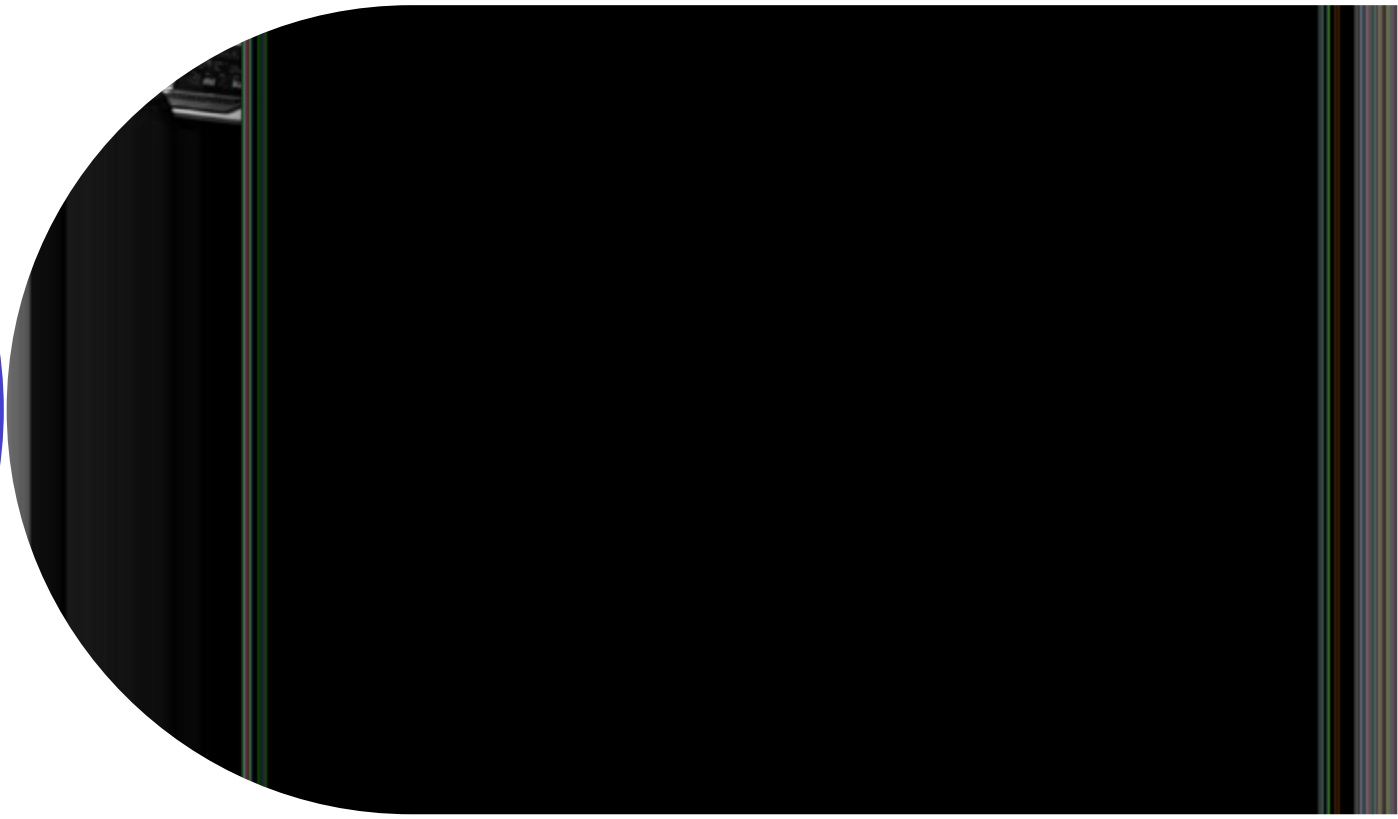
É importante analisar o local onde o anúncio está sendo entregue, da mesma forma que é analisado as métricas de acordo com os KPIs de cada campanha. Por exemplo, os sites MFA (descritos acima) são preparados para entregar resultados de *viewability*, mas é preciso avaliar se o contexto em que a publicidade está aparecendo está alinhado com os objetivos de proteção da marca.

Além dos sites MFA, é fundamental analisar o contexto do anúncio e o conteúdo da página. O *brand suitability* (ou adequação de marca) deve ser considerado além da exclusão básica de conteúdos, como notícias falsas, violência, discurso de ódio e pornografia. É necessário avaliar se o contexto pode apresentar alguma similaridade que traga desconforto para o usuário e para a marca.

Exemplos: numa segmentação geral de interesse por viagens, os anunciantes deste segmento podem veicular anúncios em páginas que noticiem um acidente. É preciso estar atento aos acontecimentos do cotidiano e à crescente produção de conteúdos em torno de determinados temas, que possam gerar combinações inadequadas com a campanha, evitando esse tipo de situação.

Outro ponto importante é a qualidade da usabilidade dos sites para os usuários. Mesmo com as iniciativas da *Coalition for Better Ads*, que indicam que a densidade ideal de anúncios seria de 30% da página, ainda existem sites que não seguem esses padrões, gerando desconforto para os usuários em relação às publicidades. Isso leva alguns usuários a adotarem bloqueios mais rígidos, deixando de ser impactados, mesmo em sites com uma boa densidade de anúncios, e perdendo a oportunidade de ver anúncios que poderiam ser relevantes para seu conhecimento e consumo.

Uma análise aprofundada de onde a campanha está sendo veiculada pode ajudar a evitar sites que não adotam esse tipo de cuidado. A poluição de informações pode gerar resultados falsos. À primeira vista, os resultados de *viewability* podem parecer bons, mas uma análise mais cuidadosa revelará a complexidade e a importância de considerar o contexto completo.



Atualização do MRC sobre IVT

Para melhorar os serviços de verificação, o **Media Rating Council (MRC)** divulgou em abril de 2024 *uma atualização nas diretrizes* de detecção e filtragem de **tráfego inválido (IVT)**, para fornecedores de medição digital usados por anunciantes para evitar a compra de inventário publicitário fraudulento. A atualização inclui novas exigências para conformidade com regulamentações de privacidade, além de introduzir mudanças importantes em como o tráfego inválido é identificado e relatado, tanto em nível de impressão quanto em nível de propriedade, ou seja, em domínios, subdomínios e IDs de aplicativos.

Um dos focos das atualizações é o impacto das **regulamentações de privacidade** na detecção de IVT. As novas diretrizes exigem que os fornecedores de medição garantam conformidade com essas regulamentações, especialmente à medida que navegadores e editores limitam o acesso a dados como endereços IP e User Agents, que são importantes para detectar tráfego inválido. O MRC destaca que a conformidade com as leis de privacidade é essencial, e fornecedores devem ajustar as metodologias para cumprir as exigências legais.

Outro ponto chave é a detecção de tráfego inválido em **TVs conectadas (CTVs)**, nas quais foram identificadas novas formas de falsificação de domínios e IDs de pacotes de aplicativos. A falsificação de IDs em CTV envolve a deturpação das informações de aplicativos e inventários, o que pode levar à compra de anúncios em espaços que não correspondem ao que foi originalmente negociado. As novas regras melhoram a detecção e o combate a essas práticas fraudulentas, ao exigir que os fornecedores façam comparações entre os IDs do leilão e os IDs dos espaços em que os anúncios são realmente exibidos.

Uma mudança significativa é a exigência de **relatórios em nível de propriedade**, uma novidade importante para melhorar a transparência na compra de mídia digital. Além de relatar IVT em nível de impressão, agora os fornecedores devem trazer dados sobre o tráfego inválido em um nível mais granular, como domínios e subdomínios. Isso vai permitir a anunciantes e compradores de mídia evitar sites que extrapolem um determinado limite de IVT, especialmente nas propriedades conhecidas como **"Feitas para Publicidade" (MFAs)**, que são sites com pouco conteúdo e alta densidade de anúncios.

A importância da distinção entre **tráfego inválido geral (GIVT)** e **tráfego inválido sofisticado (SIVT)** também faz parte da atualização. O **GIVT** envolve a filtragem de tráfego por métodos rotineiros e automatizados, como listas de bots e cabeçalhos de navegadores não identificados. Já o **SIVT** requer técnicas mais avançadas, como análises de padrões de comportamento e detecção de fraudes sofisticadas, incluindo a falsificação de IDs de aplicativos e manipulação de atividades do usuário, como cliques forçados.

O MRC reconhece que o cenário da publicidade digital está em constante mudança, especialmente com o surgimento de novos formatos de conteúdo, como sites gerados por inteligência artificial (IA). Apesar de essas propriedades não se enquadrarem nas diretrizes atuais de IVT, o MRC sinaliza que futuras atualizações podem incluir critérios qualitativos para garantir que essas novas formas de publicação digital sejam adequadamente avaliadas. Essas atualizações já estão em vigor e fazem parte do processo de acreditação dos fornecedores auditados pelo MRC, garantindo que o mercado de publicidade digital seja mais seguro e transparente para todos os envolvidos.

6 Por que o combate à fraude é importante?

A perda anual devido à fraude na internet é substancial e continua a crescer à medida que os fraudadores desenvolvem esquemas mais sofisticados.

Nos últimos anos, por exemplo, foram descobertos vários esquemas de fraude, como o esquema SSAI *"StreamScam"* e o botnet "MultiTerra", que têm o potencial de criar perdas financeiras massivas se não forem detectados.

Em geral, a fraude de anúncios pode ser responsável por uma parcela significativa das perdas por fraude na Internet - estimando-se que até 20% dos sites que veiculam anúncios são visitados exclusivamente por robôs de clique fraudulentos.

Esse tipo de atividade não afeta apenas os anunciantes, mas também prejudica a integridade do ecossistema de publicidade digital. A perda anual para o setor, segundo a DoubleVerify, gira em torno de US$12,5 bilhões, crescendo US$2 billhões YxY e sendo mais que o triplo do total computado em 2019.

O IAB Brasil entende que mitigar as fraudes na indústria de publicidade digital é prioritário. Por isso, temos nos dedicado a educar empresas de todo esse ecossistema, disponibilizando padrões e boas práticas para uma atuação cada vez mais transparente, segura, ética e sustentável para toda a cadeia.

Este guia tem o propósito de servir como uma ferramenta de recomendações globais e foi baseado em documentos disponibilizados pelo IAB US e da TAG *(Trustworthy Accountability Group)* – uma associação formada em 2015 a partir da união entre os interesses do IAB US, da 4A's *(American Association of Advertising)* e da ANA *(Association of National Advertisers)*, todas entidades representativas para veículos, anunciantes, agências e empresas de tecnologia.

7 Fraude? Tráfego Inválido?

No mercado da publicidade digital, a fraude nada mais é do que o uso de tráfego inválido com o objetivo de obter vantagem financeira – logo, trata-se da prática deliberada de tentar veicular anúncios que não têm potencial para serem vistos por um usuário humano. No entanto, aqui é importante ressaltar e se atentar ao fato de que isso não significa que todo tráfego inválido possa ser considerado fraudulento.

Para entender melhor esta questão, nossa sugestão é observar as diferentes categorias existentes nos dias de hoje e que, atualmente, se dividem pela complexidade de cada uma.

A. Tráfego Inválido Geral *(General Invalid Traffic - GIVT)*

Tráfego identificado por meio de filtragem de rotina, executado com listas ou outros parâmetros padronizados. Os principais exemplos são:

• **Tráfego de Data Centers:** tráfego não-residencial e nem corporativo, que normalmente não é humano. Pode ser filtrado a partir de listas de endereços conhecidos por serem uma fonte consistente de tráfego.

• **Tráfego Automatizado:** tráfego gerado por programas como spiders, robots e outros crawlers – ou seja, softwares usados para fazer varreduras de informação na internet, como mecanismos de busca e indexadores de preço. Pode ser filtrado a partir de listas de bots conhecidos.

• **Tráfego de Ferramentas Incomuns:** tráfego gerado por acessos que não foram feitos por um navegador padrão. Pode ser filtrado a partir de listas de navegadores conhecidos.

B. Tráfego Inválido Sofisticado *(Sophisticated Invalid Traffic - SIVT)*

Mais complexo e mais difícil de ser identificado, essas ferramentas foram idealizadas e construídas para a prática de fraude. São cenários que requerem ações como análises avançadas de ferramentas especializadas, colaboração em várias etapas e intervenção humana significativa para que se possa identificar este tipo de tráfego como fraudulento. Alguns exemplos são:

- **Bots sofisticados:** dispositivos legítimos que podem ser contaminados por um bot de diferentes maneiras. Por exemplo, baixando programas/ aplicativos de sites suspeitos ou clicando em links de e-mails fraudulentos. Neste caso, os bots são usados para mostrar anúncios sem o controle ou consentimento do usuário e tentam simular o comportamento humano para escapar de ferramentas de detecção, podendo até gerar impressões, cliques, viewability e até preencher cadastros, dependendo de sua complexidade;
- **Ad Stuffing:** os anúncios são intencionalmente escondidos, empilhados ou encobertos com a intenção de inflar os números. Na maioria das vezes, o anúncio não está visível e não pode ser clicado. Uma indicação da existência desse tipo de fraude é uma taxa de cliques muito abaixo do normal para um volume de views muito acima.

O MRC *(Media Rating Council)* publicou, em outubro de 2015, a primeira versão das diretrizes para reportar tráfego inválido.

C. URL *mismatches*

O termo "URL *mismatches*" (incompatibilidade de URL) normalmente se refere a discrepâncias entre a URL onde um anúncio é entregue e a URL declarada no leilão ou solicitação de lance.

É o caso em que a URL www.sbs.com.au/language/en, por exemplo, é relatada como *https://www.sbs.com.au/* no final, causando bloqueios. Esse problema está relacionado ao uso do Google Safeframe, que afeta a capacidade de extrair a URL completa da página.

Existem também as incompatibilidades de domínio, em que a URL do leilão difere da URL de entrega - como, por exemplo, *usatoday.com* sendo declarada, mas o anúncio sendo entregue em um subdomínio como *sports.usatoday.com*. Essas incompatibilidades não são necessariamente indicativas de fraude, mas podem resultar de razões técnicas ou níveis variados de detalhes nos dados do leilão.

Destacamos também casos em que URLs são tratadas de forma diferente nos lados antes e depois do lance, levando a incompatibilidades. Por exemplo, *https://d4builds.gg/* é tratado como uma página inicial no lado antes do lance, mas não no lado depois do lance, causando problemas de classificação.

MFA Subdomains Spoofing: exemplos de incompatibilidades benignas, como entrega em *weather.aol.com* enquanto a URL do leilão era *aol.com*. Essas incompatibilidades geralmente são devido à distribuição de subdomínios ou razões técnicas e não são automaticamente consideradas fraude.

D. CTV

A fraude de TV conectada (CTV) abrange vários tipos, cada um explorando diferentes vulnerabilidades dentro do ecossistema de CTV.

Aqui estão alguns tipos principais de fraude CTV:

Aplicativos fraudulentos: os fraudadores podem criar seus próprios aplicativos CTV e liberá-los para lojas de aplicativos abertas e fechadas. Esses aplicativos podem ter poucos *downloads*, mas geram milhões de impressões. Alguns fraudadores também criam ferramentas tecnológicas aparentemente legítimas que oferecem aos criadores de aplicativos, que são então usadas para cometer fraudes.

Fraude de inserção de anúncios do lado do servidor (SSAI): a tecnologia SSAI, embora benéfica, pode ser mal utilizada para gerar fraudes em escala. Os fraudadores podem criar seus próprios servidores ou comprar espaço na nuvem para falsificar informações sobre uma oportunidade de impressão (aplicativo/IP/dispositivo/etc.), gerando tráfego completamente falso. Isso pode resultar em milhões ou bilhões de impressões sendo disparadas de uma fazenda de servidores.

Falta de transparência: o ecossistema CTV geralmente carece de transparência, com os anunciantes não sabendo em quais aplicativos ou conteúdo estão anunciando. Os acordos programáticos geralmente incluem informações do aplicativo na forma de *BundleIDs*, mas essas informações podem não ser confiáveis e não seguir os padrões do setor. Essa falta de transparência facilita a operação de fraudadores sem serem detectados.

Vários IDs para aplicativos: qualquer aplicativo pode ter até 15 IDs, cada um potencialmente sendo um número aleatório. Apenas uma pequena porcentagem de leilões de CTV tem nomes de aplicativos que aderem às convenções do IAB, dificultando o rastreamento e a verificação do tráfego legítimo.

TV desligada: O problema da fraude de CTV *(Connected TV)* relacionada a "TV desligada" refere-se a uma situação em que os anúncios continuam a ser reproduzidos e a gerar impressões mesmo depois que a televisão foi desligada. Essa atividade fraudulenta pode levar a um desperdício significativo de gastos com anúncios, pois os anunciantes pagam por impressões que não estão sendo realmente visualizadas por ninguém.

De acordo com as descobertas, muitos dos principais aplicativos de CTV, incluindo aqueles das principais redes de TV, continuam a gerar impressões muito depois que a TV foi desligada. Isso pode acontecer por minutos, horas ou até indefinidamente. Esse problema é prevalente, com mais de um terço de todas as impressões de CTV potencialmente indo para ambientes onde a TV está desligada. Essa falta de sinalização e controle adequados no ecossistema CTV permite que tais atividades fraudulentas ocorram.

Para combater esse tipo de fraude existe a Certificação CTV *Fully On-Screen*, que garante que a reprodução e as impressões de vídeo sejam desabilitadas quando a TV é desligada. Essa certificação ajuda os anunciantes a validar que suas campanhas estão sendo veiculadas 100% na tela quando a TV é ligada, protegendo assim seus gastos com anúncios de serem desperdiçados em impressões não visíveis.

Segundo o DV *Global Insights Report 2024*, as fraudes/SIVT diminuíram 29% na América Latina, colocando a região em linha com a referência global de 1,1%. No entanto, A TV Conectada (CTV) registrou o índice mais alto de fraude/SIVT, com 4,9%, reforçando a necessidade da América Latina se adaptar ao rápido crescimento do total de impressões de CTV, que aumentou 98%.

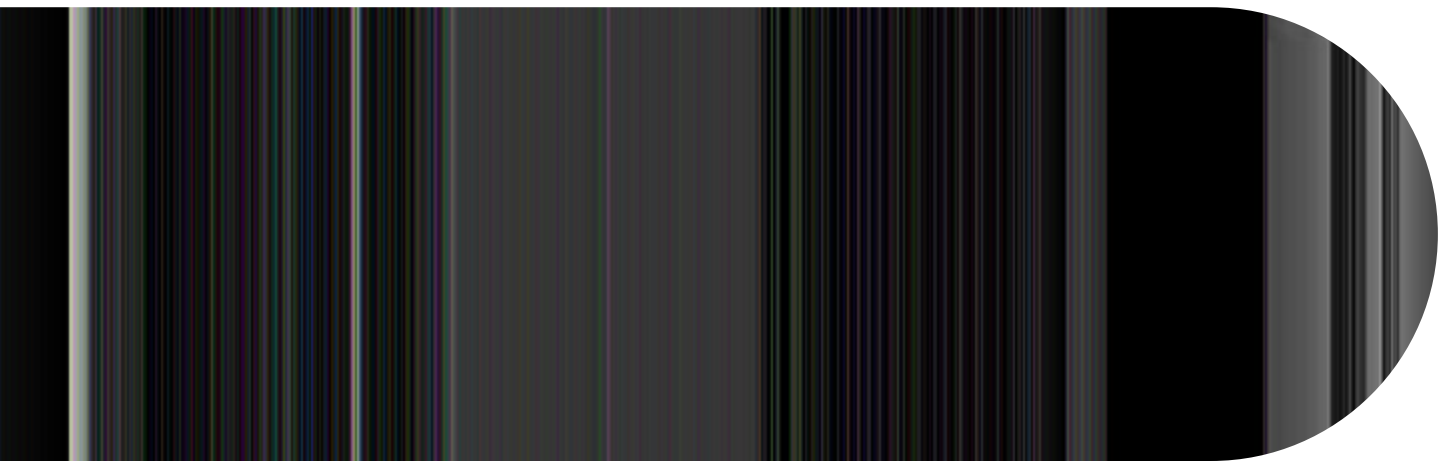
E. IA (Inteligência Artificial)

O futuro da segurança da marca *(Brand Safety)* e fraude no contexto da IA (Inteligência Artificial) é uma área em constante desenvolvimento. As tecnologias de IA estão sendo cada vez mais aproveitadas para aprimorar as medidas de *Brand Safety* e detectar atividades fraudulentas de forma mais eficaz.

Abaixo falamos um pouco sobre o que já está sendo colocado em prática:

IA na detecção de fraudes: utiliza bibliotecas de detecção de tráfego inválido e listas padrão para detectar e monitorar tráfego inválido. Isso envolve esforços de codificação personalizados, como a colaboração entre as equipes de engenharia de todo o ecossistema para coletar dados de vídeo em nível de evento por meio do *data warehouse* centrado em privacidade e medição baseado em nuvem.

Mídias sociais e IA: Em contextos de mídia social, estão disponíveis as categorias de *Brand Safety* e detecção de fraude em várias plataformas de grande abrangência. A integração com essas plataformas oferece visibilidade, segurança de marca e medição de fraude, garantindo que as campanhas dos anunciantes sejam protegidas de tráfego inválido e outras atividades fraudulentas.



8 Tendências futuras no Combate à Fraude

Espera-se que os avanços contínuos em IA e *machine learning* aprimorem ainda mais as capacidades em detectar e mitigar fraudes. À medida que os fraudadores evoluem continuamente suas táticas, as soluções baseadas em IA serão cruciais para permanecer à frente e garantir a integridade da publicidade digital.

Dark Channels: Refere-se a estratégias de marketing que utilizam canais menos convencionais e mais obscuros, muitas vezes invisíveis ao público em geral. Isso inclui o uso de redes sociais de nicho, fóruns especializados e campanhas de email marketing altamente direcionadas.

Influenciadores Robôs: Influenciadores digitais criados por computação gráfica e algoritmos, que não são pessoas reais, mas conseguem engajar e influenciar o público de maneira eficaz.

IA Influenciadora: Personalidades virtuais geradas por inteligência artificial que participam de campanhas publicitárias e têm seguidores reais. Elas oferecem vantagens como a ausência de escândalos e a capacidade de trabalhar 24/7.

Publicidade em Jogos AAA: A inclusão de anúncios dinâmicos em jogos de grande orçamento (AAA), que são direcionados aos gostos dos jogadores e integrados de forma não intrusiva nas experiências de jogos.

Esses temas refletem a contínua evolução do marketing digital e as novas oportunidades e desafios que surgem com o avanço da tecnologia.

9 Boas práticas no Combate à Fraude

Como em todo mercado de tecnologia, a evolução está sempre presente e acontece rápido. Além disso, o caminho para o controle e a eliminação do tráfego inválido e fraudulento é constante. As boas práticas a seguir ajudarão compradores e vendedores a negociarem publicidade on-line de qualidade, identificando e minimizando casos de fraude.

A. Boas Práticas para *Buyers* (Compradores)

Listamos, abaixo, algumas recomendações específicas na compra de mídia digital:

- **Atente-se para métricas que fogem do padrão.** CTRs extremamente altos ou taxas de conversão muito acima da média podem indicar fraude.
- **Busque benchmarks internos e/ou externos para entender se suas métricas estão dentro do praticado no mercado.** Caso seja possível, avalie os históricos da conta.
- **Verifique a qualificação da conversão.** Analise o que foi preenchido pelos usuários impactados. Fraudes podem apresentar e-mails falsos padronizados, mensagens sem sentido ou em outros idiomas. Vendas fraudulentas podem emitir boletos que nunca serão pagos.
- **Observe comportamentos suspeitos.** Com a ajuda de plataformas, analise métricas como tempo de permanência no site, número de páginas visitadas, bounce rate, tráfego vindo de países que não são alvo da campanha, referals ou dispositivos desconhecidos – esses são alguns exemplos de indicadores que podem ajudar.
- **Avalie o custo benefício da compra que você está fazendo.** Inventários de qualidade verificada podem ter um custo maior.

- **Exija transparência de seus parceiros e fornecedores.** Entenda quais relatórios e visões você pode ter da entrega e como é tratado o tema do controle de fraude pelas operações dos seus parceiros.
- **Se possível, utilize ferramentas antifraude** que automatizam rotinas, verificações e conseguem escalabilidade em processos manuais.
- **Utilize Filtros Antifraude/SIVT.** Empresas especializadas em verificação possuem filtros pre-bid disponíveis nas DSPs (Demand-Side Platforms) e até em veículos diretos. Esses filtros podem automatizar a compra de anúncios, evitando fraudes e SIVT (Tráfego Inválido Sofisticado).
- **Utilize Ferramentas Especializadas de Verificação de Fraude/SIVT**, pois podem ajudar de maneira determinística e incluem o monitoramento de fraudes sofisticadas que são mais difíceis de classificar. Essas ferramentas são essenciais para identificar e mitigar fraudes complexas, garantindo que o investimento publicitário seja utilizado de forma eficiente e segura.

B. Boas Práticas para Publishers

Como donos do inventário e elo entre os anunciantes e o público, os publishers têm papel fundamental no combate à fraude. Abaixo, você encontra algumas sugestões de como facilitar a detecção delas e contribuir com um ecossistema saudável:

- **Tem parceiros para conteúdo?** Avalie se eles operam dentro dos padrões que você deseja. Incentive inventários saudáveis e compartilhe boas práticas.
- **Precisa comprar tráfego externo?** A prática não é recomendada pela TAG, mas você pode minimizar riscos priorizando a qualidade, conhecendo o fornecedor e exigindo transparência dele.
- **Verifique frequentemente o seu inventário**, realize benchmarks e compare suas métricas. Faça tudo ao seu alcance para tratar falhas e aprimorar a qualidade.
- **Busque implementar iniciativas de transparência do mercado**, como o ads.txt e app-ads.txt.
- **Avalie o uso de plataformas de verificação** para complementar os pontos acima.

10 Participe da conversa

Todo o mercado se beneficia de um ecossistema mais saudável, transparente e responsável. Traga o assunto para seus pares, superiores, participe da discussão e ajude o mercado a evoluir. No combate à fraude é fundamental permanecer diligente e continuar buscando o conhecimento. Acompanhe as ações do IAB Brasil e participe dos nossos comitês!

Para mais informações sobre o IAB Brasil, escreva para *relacionamento@iabbrasil.org.br*.

11 Referências

ADPUSHUP. Why Ad Density Matters? A Must-Know for Every Publisher. Disponível em: *https://www.adpushup.com/blog/ad-density/*. Acesso em: 25 de outubro de 2024.

ANA, The Bot Baseline: Fraud in Digital Advertising. Disponível em: *https://www.ana.net/content/show/id/botfraud-2016*. Acesso em: 25 de outubro de 2024.

COALITION POR BETTER ADS. Ad Experience: Ad Density Higher Than 30%. Disponível em: *https://www.betterads.org/mobile-ad-density-higher-than-30/*. Acesso em: 25 de outubro de 2024.

IAB EUROPE. IAB Europe's Guide to Quality. Disponível em: *https://iabeurope.eu/wp-content/uploads/IAB-Europes-Guide-to-Quality-Feb-24.pptx.pdf*. Acesso em: 25 de outubro de 2024.

IAB USA, IAB Releases Final Best Practices For Reducing Risk Of Traffic Fraud. Disponível em: *https://www.iab.com/news/iab-releases-final-best-practices-for-reducing-riskof-traffic-fraud/*. Acesso em: 25 de outubro de 2024.

MEDIA RATING COUNCIL. Invalid Traffic Detection and Filtration: Guidelines Addendum. Disponível em: *https://mediaratingcouncil.org/101515_IVT%20Addendum%20FINAL%20(Version%201.0).pdf*. Acesso em: 25 de outubro de 2024.

MEDIA RATING COUNCIL. Media Rating Council Issues Update To Invalid Traffic Detection And Filtration Standards. Disponível em: *https://mediaratingcouncil.org/sites/default/files/News/General-Announcements/062520%20Media%20Rating%20Council%20Issues%20Update%20To%20Invalid%20Traffic%20Detection%20and%20Filtration%20Standards_Final.pdf*. Acesso em: 25 de outubro de 2024.

MEDIA RATING COUNCIL. 2024 IVT Interim Updates. Disponível em: *https://mediaratingcouncil.org/sites/default/files/News/2024_IVT_Interim_Updates_FINAL.pdf*. Acesso em: 25 de outubro de 2024.

TAG, Trustworthy Accountability Group. Disponível em: *https://www.tagtoday.net/*. Acesso em: 25 de outubro de 2024.

12 Agradecimentos

Este material é reflexo do trabalho desenvolvido voluntariamente por um Grupo do Comitê de *Brand Safety* 2024 do IAB Brasil. Agradecemos aos membros pelo comprometimento e pela entrega durante nossos encontros e discussões relevantes, que tanto contribuíram para o desenvolvimento do mercado brasileiro.

Colaboraram neste documento

Izadora Lombardi - DoubleVerify
José Calazans - Record
Pedro Abbud - DoubleVerify
Silvio Campideli Locali - DoubleVerify e Vice-Presidente do Comitê de Brand Safety 2024
Vivian Kato - Folha de S. Paulo

IAB Brasil

Denise Porto Hruby - CEO
Cris Duarte - Diretora de Produtos
Jovanka de Genova - Gerente de Conteúdo e Educação
Cristina de Paula - Coordenadora de Conteúdo
Talita Nunes - Community Manager

Revisão

Andre Akira Mizokami - DoubleVerify

Projeto Gráfico e Diagramação

Marcelo Vila Nova

12 Edições anteriores

O IAB Brasil revisita periodicamente seus guias e materiais para manter-se atualizado com o mercado. Caso queira acessar a edição de 2021 do nosso Guia de Combate à Fraude, *clique aqui*.

iabbrasil.com.br