RESIGeT On-Line
Revista Eletrônica de Sistemas de Informação e Gestão Tecnológica
Vol. 15 Nro. 1 2025
Uni-FACEF Centro Universitário Municipal de Franca

Content Delivery Network (CDN): Uma Revisão Bibliográfica sobre Arquiteturas, Aplicações e Tendências Futuras

Alyson Monteiro e Silva
Graduando em Ciência da Computação – Uni-FACEF
alyson_monteiros@hotmail.com

Henrique Cursino
Graduando em Ciência da Computação – Uni-FACEF
henriquecursino46@gmail.com

Prof. Geraldo Henrique Neto
Docente do Departamento de Computação – Uni-FACEF
geraldo.henriqueneto@gmail.com

Resumo

O crescimento exponencial da internet e a crescente demanda por conteúdos digitais impulsionaram a evolução das *Content Delivery Networks* (CDNs), tornando-as fundamentais para garantir desempenho, escalabilidade e segurança na distribuição de dados. Este trabalho apresenta uma revisão bibliográfica sobre as arquiteturas, aplicações e tendências futuras das CDNs, abrangendo sua história, componentes técnicos, desafios de segurança e impactos ambientais. Foram analisadas publicações acadêmicas e relatórios técnicos de 1990 a 2025, utilizando bases como IEEE Xplore, ACM *Digital Library* e relatórios de empresas líderes do setor. Os resultados mostram a importância das CDNs na melhoria da experiência do usuário, no fortalecimento de estratégias de *Search Engine Optimization* (SEO) e na redução de custos operacionais. Além disso, discute-se a integração das CDNs com tecnologias emergentes como *Edge Computing*, 5G, IoT e Inteligência Artificial, apontando para uma evolução contínua em direção a redes mais inteligentes, distribuídas e sustentáveis.

Palavras-chave: *content delivery network, cdn, edge computing.*

Abstract

The exponential growth of the internet and the increasing demand for digital content have driven the evolution of Content Delivery Networks (CDNs), making them essential for ensuring performance, scalability, and security in data distribution. This study presents a literature review on the architectures, applications, and future trends of CDNs, covering their history, technical components, security challenges, and environmental impacts. Academic publications and technical reports from 1990 *to 2025 were analyzed, using databases such as IEEE Xplore, ACM Digital Library, and reports from leading industry companies. The findings highlight the role of CDNs in improving user experience, strengthening SEO strategies, and reducing operational costs. Furthermore, the study discusses the integration of CDNs with emerging technologies such as Edge Computing, 5G, IoT, and Artificial Intelligence, pointing towards a continuous evolution towards more intelligent, distributed, and sustainable networks.*

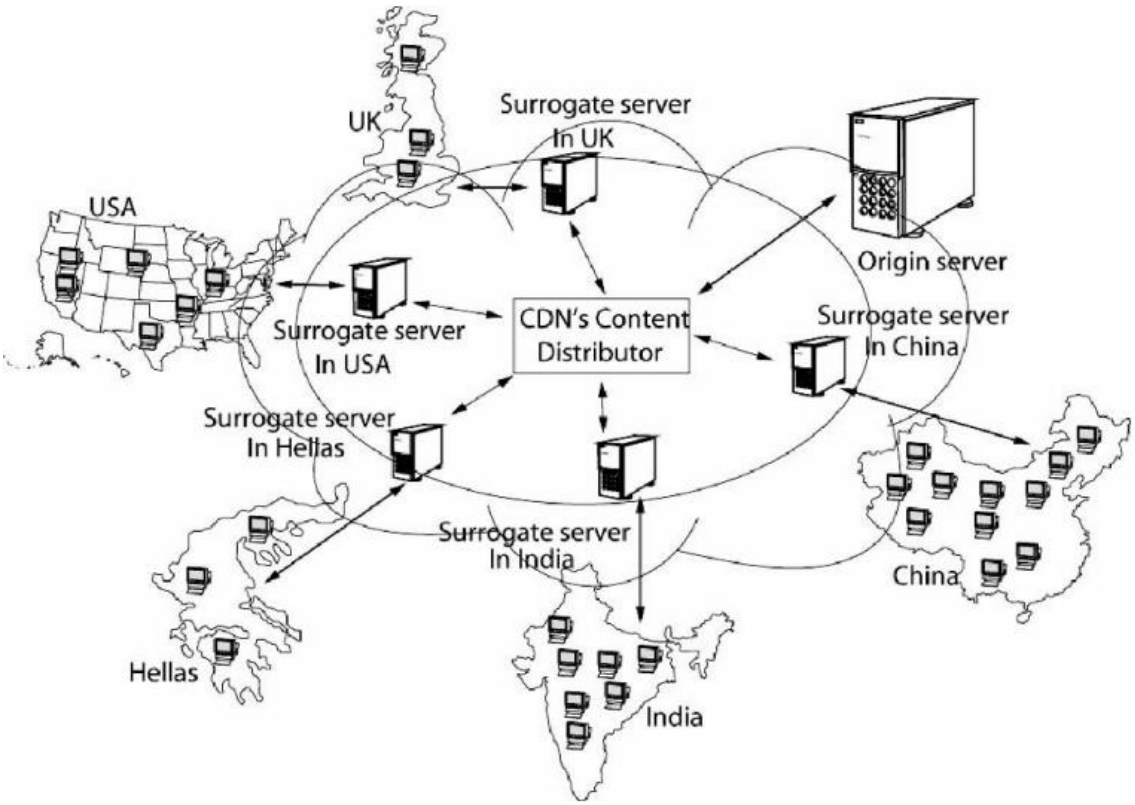
Keywords: *content delivery network, cdn, edge computing.*

1 Introdução

1.1 Definição e importância de CDNs

As *Content Delivery Networks* (CDNs) são sistemas distribuídos de servidores estrategicamente posicionados em diversos pontos de presença (PoPs) ao redor do mundo, que trabalham em conjunto para armazenar e entregar conteúdos tanto estáticos, como imagens e vídeos, quanto dinâmicos de forma rápida e eficiente. Em vez de concentrar a origem do conteúdo em um único servidor, as CDNs replicam os dados em múltiplos locais, o que aproxima o conteúdo do usuário final e melhora significativamente a experiência de acesso como demostrado na figura 1. (Peng, 2018)

Figura 1 Modelo de uma CDN



Fonte: Stamos et al. (2009, p. 3).

A infraestrutura distribuída das CDNs é uma resposta direta à necessidade de reduzir a distância entre o conteúdo solicitado e o usuário que o acessa. Quando uma requisição é realizada, o tráfego é direcionado para o servidor ou PoP mais próximo, reduzindo a latência e garantindo uma navegação mais rápida e fluida. Essa distribuição não só diminui os tempos de resposta, mas também minimiza o congestionamento de rede, pois a carga é compartilhada entre vários

servidores, permitindo que o sistema mantenha sua estabilidade, mesmo em momentos de pico de tráfego.

> "Embora o tempo de carregamento do conteúdo dos principais sites da Internet tenha melhorado constantemente ao longo dos últimos anos, a latência geral de acesso ao conteúdo da Web ainda está na faixa de alguns segundos, o que é várias vezes maior do que o limite considerado ideal para a leitura e escaneamento humano." (Peng 2018, p.2)

Além disso, a performance das conexões web proporcionada pelas CDNs tem um impacto direto na lucratividade dos negócios digitais. Sites que apresentam carregamento rápido e conexões estáveis oferecem uma experiência de usuário superior, o que se reflete em taxas de abandono menores e níveis mais altos de engajamento. Essa qualidade na entrega de conteúdo também influencia positivamente o ranking dos sites em mecanismos de busca, já que a velocidade de carregamento é um dos critérios avaliados para SEO (*Search Engine Optimization*). Em última análise, melhorias mesmo que discretas no desempenho podem gerar aumentos significativos nas taxas de conversão.

Em um cenário cada vez mais digital e competitivo, a adoção de CDNs torna-se imprescindível para empresas que desejam oferecer serviços online com alta qualidade. A crescente demanda por conteúdo multimídia, unida à necessidade de proporcionar uma experiência consistente e segura em diferentes dispositivos e regiões, obriga as organizações a investirem em soluções que otimizem a entrega de dados. Assim, a infraestrutura distribuída das CDNs não só garante a robustez e a segurança da comunicação, mas também se adapta de forma eficaz às novas demandas tecnológicas, como o advento do 5G e a expansão da Internet das Coisas (IoT). (Peng, 2018)

1.2 Justificativa do estudo

A crescente demanda por conteúdo multimídia, o aumento do tráfego na internet e a necessidade de mitigar riscos de falhas e ataques cibernéticos justificam uma análise aprofundada das CDNs. Estudar sua evolução e aplicação não só esclarece os mecanismos que possibilitam a alta performance dos serviços digitais, mas também evidência os desafios e as oportunidades de inovação nesse campo.

1.3 Objetivos da pesquisa

Este estudo tem como objetivos revisar as principais arquiteturas e mecanismos de funcionamento das CDNs, apresentar as aplicações e benefícios atuais desse modelo de distribuição, discutir os desafios, limitações e comparações entre abordagens tradicionais e novas práticas emergentes, e identificar tendências futuras, como a integração com *Edge Computing*, 5G, IoT e a aplicação de inteligência artificial.

1.4 Metodologia utilizada para a revisão bibliográfica

A pesquisa foi realizada por meio da análise e síntese de artigos acadêmicos, estudos de caso, publicações técnicas e relatórios do setor. Foram consultadas bases de dados especializadas como IEEE Xplore, ACM Digital Library e Springer, além de repositórios digitais e relatórios técnicos de grandes empresas como Akamai Technologies, Cisco Systems, Google, Cloudflare e Microsoft Azure, permitindo uma visão abrangente sobre a evolução e as inovações nas redes de distribuição de conteúdo (CDNs). A seleção dos materiais ocorreu considerando fatores como relevância, atualidade, impacto das contribuições na área e a abrangência temática relacionada à tecnologia e segurança em CDN.

O intervalo temporal dos materiais analisados abrange publicações de 1990 a 2025, assegurando uma compreensão evolutiva e contemporânea do tema. Essa ampla janela permitiu observar desde os conceitos fundamentais e primeiras aplicações até as recentes inovações tecnológicas impulsionadas por inteligência artificial, aprendizado de máquina, segurança avançada, redes 5G e computação de borda. A diversidade e a quantidade dos artigos e relatórios revisados garantem a robustez e a profundidade da pesquisa realizada.

1.5 Estrutura do trabalho

O trabalho está organizado em oito seções, iniciando com a introdução e contextualização histórica das CDNs, seguida da análise de sua arquitetura e funcionamento. Posteriormente, são discutidas as aplicações e benefícios atuais, os desafios e limitações enfrentados, além de uma comparação entre as abordagens tradicionais e as novas técnicas emergentes. Finalmente, o estudo explora as tendências futuras e encerra com as conclusões e sugestões para futuras pesquisas.

2. História e Evolução das CDNs

Nesta seção, é realizada uma análise histórica da evolução das *Content Delivery Networks* (CDNs), contextualizando os fatores tecnológicos, sociais e econômicos que impulsionaram seu surgimento. Abordam-se os desafios enfrentados pelas infraestruturas tradicionais da internet, como alta latência, gargalos de banda e dificuldades de escalabilidade, que motivaram a criação de mecanismos mais eficientes para distribuição de conteúdo digital. Em seguida, são discutidos os principais marcos no desenvolvimento das CDNs, desde as primeiras implementações até as inovações recentes, como a integração com computação em nuvem, *Edge Computing* e inteligência artificial. Essa perspectiva histórica permite compreender como as CDNs se tornaram elementos essenciais para a performance, disponibilidade e segurança na internet contemporânea.

2.1 Contextualização do cenário tecnológico

Nas últimas décadas, o crescimento exponencial da internet e a diversificação de conteúdos digitais criaram um ambiente onde a velocidade e a eficiência na entrega de dados se tornaram essenciais. Esse cenário impulsionou o desenvolvimento de soluções que pudessem atender a uma demanda global e heterogênea.

> "O surgimento de novas formas de conteúdo na Internet, como *streams* de mídia, torna o problema de desempenho da Internet ainda mais grave devido à irregularidade no atraso de acesso." (Peng 2018, p.2)

2.2 Surgimento das CDNs

O conceito de *Content Delivery Network* (CDN) surgiu na década de 1990 como uma resposta aos desafios de desempenho e escalabilidade enfrentados pela Internet em expansão. A crescente demanda por distribuição eficiente de conteúdo digital, impulsionada pelo aumento do tráfego na web e pelo surgimento de aplicações multimídia, evidenciou a necessidade de um modelo mais eficiente para a entrega de dados. Pioneiros como a Akamai Technologies surgiu a partir de um projeto de pesquisa do MIT voltado para a solução do problema de *flash crowd* (pico de acessos ao servidor original). Com uma abordagem baseada na observação de que fornece conteúdo da Web a partir de um único local pode causar sérios problemas de escalabilidade, confiabilidade e desempenho do site. Assim, desenvolveram um sistema para atender às requisições por meio de um número variável de servidores de origem substitutos na borda da rede. (Dilley, 2002)

2.3 Principais marcos na evolução das CDNs

Nos anos 2000, as CDNs passaram por um processo de expansão global, aumentando significativamente o número de Pontos de Presença (PoPs) para garantir uma cobertura mais ampla e eficiente. Além disso, novas técnicas de balanceamento de carga foram introduzidas para otimizar a distribuição do tráfego entre servidores e garantir alta disponibilidade dos serviços. Durante essa fase, também se intensificou o uso de algoritmos avançados de roteamento de requisições, permitindo que as CDNs escolhessem dinamicamente o servidor mais próximo e menos congestionado para atender às solicitações dos usuários. (Padmanabhan, 2001)

Com o avanço da computação em nuvem e do *Edge Computing*, as CDNs modernas passaram a incorporar serviços mais sofisticados, incluindo processamento distribuído e *caching* inteligente baseado em inteligência artificial. Além disso, a segurança das CDNs se tornou uma prioridade, especialmente para mitigar ataques cibernéticos como os ataques de negação de serviço distribuído (DDoS). Atualmente, grandes provedores de CDN integram *firewalls* de aplicativos web (WAFs), autenticação avançada e análise de tráfego em tempo real para garantir a proteção de sites e aplicações.

Esses avanços refletem a evolução das CDNs de simples mecanismos de *cache* para plataformas inteligentes e altamente distribuídas, desempenhando um papel fundamental na infraestrutura digital global.

2.4 Tendências e inovações recentes

Nos últimos anos, as CDNs têm evoluído significativamente devido ao avanço das tecnologias de rede e computação distribuída. O advento do 5G e a crescente adoção da Internet das Coisas (IoT) têm sido fatores determinantes para a

modernização dessas redes, permitindo a entrega de conteúdos com menor latência e maior eficiência. Com o 5G, a capacidade de transmissão de dados aumentou exponencialmente, possibilitando que as CDNs operem mais próximas dos dispositivos dos usuários, reduzindo o tempo de resposta e melhorando a experiência de acesso a serviços em tempo real, como streaming e aplicações interativas. (Peng, 2018)

Além disso, a crescente disseminação da IoT gerou uma demanda por processamento distribuído e descentralizado, impulsionando a integração das CDNs com *Edge Computing*. Essa abordagem permite que os dados sejam processados mais próximos da origem, reduzindo congestionamentos na infraestrutura principal e otimizando a entrega de conteúdo em larga escala. (Peng, 2018)

Outra inovação relevante é a aplicação de inteligência artificial (IA) e aprendizado de máquina no gerenciamento e na distribuição do tráfego de dados. Modelos preditivos baseados em IA possibilitam a alocação dinâmica de recursos, a identificação de padrões de tráfego e a prevenção de ataques cibernéticos, aumentando a segurança e a eficiência das CDNs. Empresas do setor têm investido em soluções automatizadas para otimizar a entrega de conteúdo e reduzir custos operacionais, garantindo que a infraestrutura CDN seja escalável e resiliente frente ao aumento da demanda global. (Akamai, 2021)

Dessa forma, as CDNs estão se tornando cada vez mais inteligentes, distribuídas e integradas com novas tecnologias, preparando-se para os desafios da próxima geração da Internet.

3. Arquitetura e Funcionamento das CDNs

Nesta seção, são explorados os componentes técnicos e os mecanismos operacionais que constituem uma *Content Delivery Network* (CDN). Primeiramente, descrevem-se os principais elementos estruturais dessas redes, como servidores de cache, balanceadores de carga e *proxies* reversos. Em seguida, são discutidas as estratégias de distribuição de conteúdo, os tipos distintos de CDNs públicas, privadas e híbridas e as abordagens de segurança e privacidade adotadas por essas infraestruturas. A análise técnica apresentada aqui fornece as bases necessárias para compreender como as CDNs operam de forma eficiente, escalável e resiliente frente às exigências do tráfego digital global.

3.1 Componentes básicos de uma CDN

Uma *Content Delivery Network* (CDN) é composta por diversos elementos que trabalham em conjunto para otimizar a entrega de conteúdos na internet. Esses componentes desempenham funções essenciais para reduzir latência, melhorar a escalabilidade e garantir a disponibilidade dos serviços. Entre os principais elementos de uma CDN, destacam-se:

Servidores de *Cache*: São responsáveis por armazenar cópias dos conteúdos estáticos e dinâmicos em locais distribuídos geograficamente. Esse armazenamento reduz a necessidade de recuperar o conteúdo do servidor de origem, melhorando a velocidade de carregamento e reduzindo o consumo de largura de banda da infraestrutura principal (Dilley et al., 2002).

Proxies Reversos: Atuam como intermediários entre os usuários e os servidores da CDN, redirecionando as requisições para os servidores de *cache* mais próximos ou menos congestionados. Essa abordagem melhora o tempo de resposta e protege o servidor de origem contra sobrecargas e ataques mal-intencionados (Krishnamurthy; Wills, 2006).

Sistemas de Gerenciamento de Conteúdo: São responsáveis por sincronizar e atualizar os dados distribuídos entre os servidores da CDN. Essas plataformas permitem que novos conteúdos sejam replicados rapidamente em diversos pontos da rede, garantindo consistência e disponibilidade global (Pathan; Buyya, 2008).

Balanceadores de Carga: Distribuem dinamicamente as requisições entre os servidores da CDN, evitando sobrecargas e maximizando o desempenho. Esses sistemas analisam métricas como latência, taxa de transferência e carga do servidor para tomar decisões sobre o direcionamento do tráfego (Berman et al., 2017).

A combinação desses componentes permite que as CDNs entreguem conteúdos de forma eficiente, confiável e escalável, minimizando os impactos de congestionamentos e falhas na infraestrutura de rede.

3.2 Mecanismos de distribuição de conteúdo

As *Content Delivery Networks* (CDNs) empregam diversas estratégias para otimizar a distribuição de conteúdo, garantindo maior velocidade, disponibilidade e eficiência na entrega de dados aos usuários. Entre as principais técnicas utilizadas, destacam-se:

Caching: O armazenamento temporário de conteúdos em servidores de borda permite que as requisições dos usuários sejam atendidas sem a necessidade de acessar repetidamente o servidor de origem. Esse método reduz a latência, melhora a eficiência da rede e diminui a carga sobre os servidores centrais. O *caching* pode ser estático, quando o conteúdo é armazenado por longos períodos, ou dinâmico, onde a CDN atualiza os dados conforme necessário para garantir informações atualizadas (Pathan; Buyya, 2008).

Replicação: Para garantir redundância e alta disponibilidade, as CDNs replicam conteúdos em vários servidores distribuídos geograficamente. Dessa forma, se um servidor falhar ou apresentar sobrecarga, o tráfego pode ser redirecionado para outro servidor disponível, mantendo a qualidade do serviço (Berman et al., 2017). A replicação também contribui para a resiliência da rede, protegendo contra-ataques DDoS e falhas em infraestrutura (Ghojloo et al., 2020).

Roteamento Dinâmico: A escolha do melhor caminho para a entrega do conteúdo é fundamental para o desempenho da CDN. O roteamento dinâmico ajusta automaticamente a trajetória dos dados com base em fatores como proximidade geográfica do usuário, congestionamento da rede e disponibilidade dos servidores. Esse processo melhora a velocidade de resposta e a qualidade da experiência do usuário, garantindo que as requisições sejam direcionadas ao servidor mais eficiente (Krishnamurthy; Wills, 2006).

A combinação dessas técnicas permite que as CDNs forneçam um serviço otimizado, garantindo entrega rápida de conteúdo, escalabilidade e eficiência na distribuição de dados.

3.3 Tipos de CDNs e suas características

As CDNs podem ser classificadas em diferentes tipos, de acordo com suas características operacionais e os objetivos para os quais foram projetadas. Cada modelo apresenta vantagens e desafios específicos, sendo adotado conforme a necessidade de desempenho, segurança e escalabilidade da organização. Os principais tipos de CDNs são:

CDNs Públicas: São operadas por grandes provedores de serviços, como Akamai, Cloudflare e Amazon CloudFront, que oferecem infraestrutura global para atender a múltiplos clientes. Esse modelo permite que empresas de todos os portes utilizem a infraestrutura de terceiros para distribuição eficiente de conteúdo, sem a necessidade de investir em servidores próprios. A principal vantagem desse tipo de CDN é a escalabilidade, já que os provedores possuem milhares de pontos de presença (PoPs) ao redor do mundo, garantindo alta disponibilidade e desempenho otimizado (Krishnamurthy; Wills, 2006).

CDNs Privadas: Desenvolvidas e mantidas por grandes organizações que precisam de controle total sobre o tráfego de dados, segurança e personalização. Empresas como Netflix e Facebook optam por construir suas próprias CDNs para garantir qualidade de serviço (QoS) e reduzir dependência de provedores terceirizados. As CDNs privadas são ideais para organizações com grande volume de tráfego e requisitos específicos, mas exigem altos investimentos em infraestrutura e manutenção (Böttger et al, 2016).

CDNs Híbridas: Combinam características de CDNs públicas e privadas, oferecendo um equilíbrio entre custo, flexibilidade e desempenho. Nesse modelo, uma organização pode utilizar uma infraestrutura própria para conteúdos críticos e sensíveis, enquanto recorre a provedores externos para aumentar a capacidade em momentos de pico (Ghojloo et al., 2020). Esse tipo de CDN é especialmente útil para empresas que precisam de redundância, otimização de custos e alta escalabilidade (Zhang et al., 2018).

Cada modelo de CDN apresenta vantagens específicas, e a escolha entre eles depende dos objetivos da organização, do volume de tráfego e das demandas de segurança e personalização dos serviços. As diferenças de modelo e preços entre provedores podem ser vistas na Tabela abaixo (Cloudflare, s.d.; BlazingCDN, 2024; Stegmann, 2015).”

Conforme a Tabela 1, provedores públicos adotam cobrança por plano ou por GB, enquanto a Netflix opera uma CDN privada com custos estimados por usuário (Cloudflare, s.d.; BlazingCDN, 2024; Stegmann, 2015).”

Tabela 1 Tabela de preços

Provedor	Tipo	Modelo de cobrança / plano típico	Preço	Observações principais
Cloudflare	Pública	Planos “Free”, “Pro”, “Business” + tarifas de uso em alguns casos.	Free: US$ 0/mês. Pro: US$ 20/mês (anual) para o plano CDN.	Para volumes maiores ou uso empresarial, preços customizados.
Akamai	Pública	Modelo por GB em “tiers” de volume + contrato personalizado.	~US$ 0,049/GB para 0-10 TB/mês; ~US$ 0,045/GB para 10-50 TB/mês.	Grandes volumes recebem forte desconto; negociação obrigatória.
Netflix	Privada	Sistema interno de distribuição (Open Connect).	Estima-se custo de distribuição entre **US$ 0,12 e US$ 0,75 por usuário/mês** para custos de interconexão e transit.	Não público: valores reais de custo por GB ou por TB não são disponibilizados.

3.4 Aspectos de segurança e privacidade

A segurança nas CDNs é essencial para proteger os dados durante sua transmissão e armazenamento, assegurando a integridade e a privacidade das informações dos usuários. A criptografia desempenha um papel fundamental nesse contexto, utilizando protocolos avançados como TLS *(Transport Layer Security)* e SSL (*Secure Sockets Layer*). Esses protocolos garantem conexões seguras entre usuários e servidores, protegendo contra-ataques de interceptação, conhecidos como *man-in-the-middle* (Müller et al., 2019). Além disso, técnicas avançadas de criptografia ponta a ponta é adotada cada vez mais para reforçar a privacidade e prevenir o vazamento de dados sensíveis (Liu; Dai, 2020).

Outro aspecto crítico na segurança das CDNs é a mitigação de ataques de negação de serviço distribuídos (DDoS - *Distributed Denial of Service*), que visam sobrecarregar servidores e indisponibilizar serviços. Para combater esses ataques, são implementadas estratégias como a filtragem proativa de tráfego malicioso, análise em tempo real dos padrões de requisições e o uso de redes distribuídas para distribuir e dissipar cargas ofensivas (Cloudflare, 2022). Além disso, mecanismos como *rate limiting e firewalls* inteligentes auxiliam na identificação e no bloqueio de tráfego suspeito antes que causem danos significativos à infraestrutura (Akamai 2021).

Além das medidas técnicas de segurança, as CDNs precisam estar alinhadas com regulamentações rigorosas de proteção de dados pessoais, como o Regulamento Geral de Proteção de Dados (GDPR) na Europa e a Lei Geral de Proteção de Dados (LGPD) no Brasil. Isso implica a adoção de políticas robustas de segurança, incluindo anonimização dos dados, obtenção de consentimento explícito dos usuários para coleta e uso de informações e a realização frequente de auditorias para verificar conformidade. Para atender essas exigências, muitos provedores de

CDN oferecem recursos adicionais como *geofencing* e controles detalhados de acesso baseados em políticas regionais, assegurando que os dados sejam processados e armazenados conforme as especificidades legais de cada localidade (Fernandes et al., 2021; Tang et al., 2020).

4. Aplicações e Benefícios das CDNs na Atualidade

As *Content Delivery Networks* (CDNs) viabilizam entrega rápida e confiável de conteúdo em larga escala. Seus benefícios concentram-se em quatro eixos: desempenho, SEO e experiência do usuário, eficiência/custos e disponibilidade, escalabilidade e segurança. A seguir, sintetizam-se os resultados e implicações mais relevantes para plataformas digitais modernas (Pathan; Buyya, 2008).

4.1 Aumento de desempenho e velocidade de carregamento

CDNs reduzem latência ao aproximar conteúdo do usuário em Pontos de Presença (PoPs), diminuindo hops e tempo de resposta. O uso combinado de *cache* na borda para conteúdo estático e dinâmico, *origin shielding* e técnicas de compressão (p. ex., Brotli) eleva a taxa de *cache hit*, reduz *origin fetches* e melhora a vazão percebida (Pathan; Buyya, 2008). Protocolos modernos (HTTP/2, HTTP/3/QUIC) e otimizações de transporte contribuem adicionalmente para menor tempo de carregamento e maior estabilidade sob variação de rede (Kim et al., 2019; Tomiyama et al., 2020).

4.2 Melhoria em SEO e experiência do usuário

O tempo de carregamento é determinante para visibilidade e retenção. Ao reduzir latência e bytes transferidos, CDNs favorecem métricas de experiência (p. ex., *Core Web Vitals* como LCP, FID e CLS), facilitam o trabalho de *crawlers* e contribuem para menor taxa de rejeição em dispositivos móveis e redes variáveis (Pathan; Buyya, 2008; Kim et al., 2019; Liu; Jiang, 2021). O resultado é renderização mais rápida, navegação mais fluida e maior probabilidade de conversão em contextos como e-commerce e streaming.

4.3 Redução de custos e eficiência

A descentralização da entrega diminui dependência de grandes data centers e de *backhaul*, aliviando a infraestrutura de origem e otimizando largura de banda (Pathan; Buyya, 2008; Zhang; Li, 2021; Xiao et al., 2020). Em cenários contemporâneos, a integração com *edge computing* e modelos *pay-as-you-go* amplia elasticidade e permite alocar processamento próximo ao usuário, beneficiando inclusive aplicações de IoT e IA (Singh; Sharma, 2022; Dewitt et al., 2021).

4.4 Alta disponibilidade, escalabilidade e segurança

A distribuição geográfica e a redundância entre PoPs favorecem disponibilidade e continuidade de serviço mesmo sob picos ou falhas locais (Xiao et al., 2021; Buyya; Pathan, 2008). Mecanismos de balanceamento de carga (*load balancing*) p. ex.,

round-robin, least connections e IP hashing evitam concentração de tráfego e sustentam elasticidade sem intervenção manual (Kim et al., 2020). Em segurança, a mitigação de *DDoS, Anycast, rate limiting* e camadas como WAF e *bot management* reduzem risco de indisponibilidade e abuso, preservando desempenho e confiabilidade (Xiao et al., 2020).

4.5 Exemplos de uso em diferentes indústrias

As CDNs são amplamente adotadas por diversos setores que dependem de desempenho, escalabilidade e alta disponibilidade para atender a um grande volume de usuários. A capacidade das CDNs de armazenar, distribuir e otimizar conteúdos torna-as essenciais para *e-commerce*, *streaming* de vídeo, portais de notícias, redes sociais e muitos outros segmentos. A seguir, estão apresentados alguns exemplos de uso:

- E-commerce: experiência de compra rápida e eficiente

  Em lojas virtuais, a velocidade de carregamento e a fluidez da navegação impactam diretamente a conversão: um atraso de 100 ms pode reduzir taxas em até 7% (Akamai, 2021). CDNs melhoram a performance ao aplicar *cache* de imagens e páginas dinâmicas, distribuir o tráfego entre servidores para absorver picos de acesso e reforçar camadas de segurança contra DDoS e fraude (Cloudflare, 2023). Grandes varejistas como Amazon, Mercado Livre e Alibaba dependem de CDN para manter experiência rápida e estável em diferentes regiões.

- Streaming de vídeo: alta definição sem interrupções

  Plataformas como Netflix, YouTube e Disney+ utilizam CDN para garantir baixa latência e qualidade consistente. Destaca-se o *adaptive bitrate streaming (ABR)*, que ajusta a qualidade conforme a rede do usuário, o uso de servidores distribuídos para aliviar a origem e a redução de custos de largura de banda via *cache* (Cisco, 2022). A Netflix, por exemplo, entrega mais de 90% do tráfego pelo *Open Connect*, sua própria CDN, reduzindo a sobrecarga na internet pública (Netflix, 2022).

- Portais de notícias: informação em tempo real

  Veículos como BBC, CNN e The New York Times precisam publicar com rapidez, sobretudo em coberturas ao vivo. CDNs agilizam o acesso por meio de pré-posicionamento de conteúdos de alta demanda, compactação para acelerar carregamentos (especialmente em dispositivos móveis) e elasticidade para suportar picos imprevisíveis (Fastly, 2023). Além disso, contribuem para resiliência contra-ataques e tentativas de bloqueio, preservando o acesso à informação (Akamai, 2022).

- Redes sociais: comunicação em massa e escalabilidade

  Facebook, X/Twitter, Instagram e TikTok lidam com volumes bilionários de

requisições. CDNs possibilitam carregamento quase instantâneo de imagens e vídeos a partir de nós próximos aos usuários, sincronização em tempo real sem degradar o desempenho e escalabilidade global para eventos que geram tráfego extremo (Meta, 2023). No TikTok, a entrega de vídeos curtos com mínima latência é fortemente apoiada por infraestrutura de CDN (Cloudflare, 2022).

5. Desafios e Limitações das CDNs

Embora as CDNs ofereçam inúmeras vantagens, sua implementação e operação ainda enfrentam diversos desafios. Esta seção aborda os principais obstáculos técnicos, operacionais e regulatórios associados ao uso de CDNs, incluindo questões de segurança, privacidade, cobertura geográfica limitada e impactos ambientais. São analisadas vulnerabilidades comuns, como ataques DDoS, complexidades de integração com infraestruturas legadas e dificuldades de conformidade com legislações como GDPR e LGPD. A compreensão dessas limitações é essencial para uma visão crítica e realista sobre o papel das CDNs no cenário tecnológico atual.

5.1 Problemas de segurança e privacidade

As *Content Delivery Networks* (CDNs) desempenham um papel essencial na otimização do desempenho e escalabilidade da internet, mas, apesar de seus benefícios, elas não estão imunes a ameaças de segurança e desafios de privacidade. Como armazenam e distribuem grandes volumes de conteúdo em diferentes servidores ao redor do mundo, as CDNs podem ser alvos de ataques cibernéticos, violações de dados e problemas regulatórios.

1. Ataques DDoS e a Mitigação de Sobrecarga

Um dos principais desafios de segurança enfrentados pelas CDNs são os ataques de negação de serviço distribuídos (DDoS - *Distributed Denial of Service)*. Nesses ataques, criminosos utilizam uma grande quantidade de dispositivos comprometidos (*botnets*) para sobrecarregar os servidores da CDN, tornando os sites e serviços indisponíveis.

Em 2021, a Akamai reportou um dos maiores ataques DDoS da história, que atingiu um pico de 800 Gbps e teve como alvo uma grande empresa do setor financeiro (Akamai, 2021).

Plataformas como Cloudflare e Fastly implementam firewalls avançados e filtragem de tráfego malicioso para mitigar esses ataques antes que atinjam os servidores de origem (Cloudflare, 2023).

Estratégias como *Rate Limiting* e *Anycast Routing* ajudam a dissipar o tráfego malicioso distribuindo as requisições entre múltiplos servidores da CDN (Fastly, 2022).

2. Interceptação de Dados e Ataques *Man-in-the-Middle* (MITM)

As CDNs são intermediárias no processo de entrega de conteúdo, o que pode torná-las alvos potenciais para ataques *Man-in-the-Middle* (MITM). Esses ataques ocorrem quando hackers interceptam a comunicação entre um usuário e o servidor da CDN para roubar ou modificar informações sensíveis.

Medidas para mitigar esses riscos incluem:

Criptografia TLS/SSL: Implementação do HTTPS com TLS 1.3 para evitar que dados sejam interceptados por terceiros (Google, 2018).

Certificados SSL gerenciados: Empresas como Let's Encrypt fornecem certificados gratuitos para garantir que todas as conexões sejam seguras (ISRG, 2023).

Proteção contra *downgrade* de protocolo: Ataques como POODLE e BEAST exploram falhas em versões antigas do TLS, tornando crucial o suporte apenas a versões mais seguras (Owasp, 2022).

3. Exploração de Vulnerabilidades em Aplicações Web

As CDNs geralmente armazenam e aceleram o carregamento de aplicações web dinâmicas, mas isso também pode abrir brechas de segurança, como *Cross-Site Scripting* (XSS) e *Injection Attacks.*

Em 2017, a falha "Cloudbleed" da Cloudflare permitiu que dados sensíveis de usuários, como cookies e credenciais, fossem expostos devido a um bug em seu parser HTML (Cloudflare, 2017).

Para mitigar riscos, muitas CDNs oferecem *Web Application Firewall*s (WAFs) que analisam e bloqueiam códigos maliciosos antes que cheguem aos usuários (Imperva, 2023).

Implementação de *Content Security Policy* (CSP) para restringir fontes externas de scripts e evitar injeção de código malicioso (Mozilla, 2023).

4. Privacidade e Conformidade com Regulamentações (GDPR, LGPD, CCPA)

As CDNs processam grandes quantidades de dados de usuários, incluindo endereços IP, cookies e preferências de navegação. Isso levanta preocupações relacionadas à privacidade e conformidade com legislações internacionais, como:

GDPR (*General Data Protection Regulation* - Europa): Regulamenta a coleta e armazenamento de dados pessoais, exigindo que CDNs adotem anonimização e consentimento explícito para rastreamento de usuários (European Commission, 2023).

LGPD (Lei Geral de Proteção de Dados - Brasil): Exige que as empresas informem os usuários sobre o uso de seus dados e forneçam opções para exclusão (Governo do Brasil, 2023).

CCPA (*California Consumer Privacy Act* - EUA): Concede aos consumidores o direito de saber quais dados são coletados, como são usados e exigir sua remoção (California DOJ, 2023).

Empresas de CDN precisam garantir que não violem essas regulamentações, especialmente ao operar em mercados internacionais. Algumas soluções incluem:

Armazenamento descentralizado para evitar a transferência de dados para regiões não regulamentadas.

Redução do rastreamento de IPs e cookies para minimizar a coleta de informações pessoais desnecessárias.

Relatórios de transparência e auditorias regulares para demonstrar conformidade com as leis de proteção de dados.

5.2 Desafios na implementação de CDNs

A implementação de uma *Content Delivery Network* (CDN) envolve uma série de desafios técnicos e operacionais, especialmente para empresas que precisam distribuir conteúdo de forma eficiente e confiável em escala global. Algumas das principais dificuldades incluem a integração com infraestruturas preexistentes, a configuração de pontos de presença (PoPs) em diferentes regiões e a garantia da consistência dos dados replicados nos servidores da CDN.

1. Complexidade da Integração com Infraestruturas Existentes

Empresas que adotam CDNs frequentemente precisam garantir que seus sistemas já estabelecidos possam se comunicar corretamente com a rede de distribuição. Problemas comuns incluem:

Compatibilidade com aplicações legadas que não foram projetadas para funcionar com múltiplos servidores distribuídos (Akamai, 2022).

Configuração de DNS e regras de *cache* para evitar inconsistências na entrega do conteúdo (Cloudflare, 2023).

Latência na sincronização de dados dinâmicos entre a origem e os servidores distribuídos (Fastly, 2022).

2. Manutenção e Gerenciamento dos PoPs (Pontos de Presença)

Uma CDN é composta por diversos PoPs distribuídos geograficamente, mas gerenciá-los de forma eficiente é um grande desafio. Empresas precisam considerar fatores como:

Monitoramento constante de desempenho para garantir baixa latência e evitar gargalos de rede (Imperva, 2023).

Segurança e mitigação de falhas para evitar ataques e interrupções (AWS, 2023).

Distribuição inteligente de tráfego, garantindo que os usuários sempre acessem o servidor mais próximo e menos congestionado (Microsoft Azure, 2022).

3. Garantia da Consistência dos Conteúdos Distribuídos

A replicação de dados em múltiplos servidores pode resultar em problemas de versionamento e consistência. Quando um conteúdo é atualizado, as versões antigas podem permanecer em *cache* por períodos indesejados, levando a inconsistências entre servidores diferentes. Técnicas para evitar isso incluem:

Cache Purging Automático, removendo conteúdos obsoletos rapidamente (Google, 2018).

Versionamento de arquivos e validação de integridade para garantir que os usuários sempre acessem a versão mais recente (IBM, 2022).

5.3 Limitações de Escalabilidade e Cobertura

Apesar de serem projetadas para escalabilidade, as CDNs enfrentam desafios para atingir cobertura verdadeiramente global, especialmente em regiões com infraestrutura limitada.

1. Cobertura Limitada em Regiões Remotas

Embora provedores como Cloudflare, Akamai e AWS CloudFront tenham centenas de PoPs distribuídos pelo mundo, regiões menos desenvolvidas ainda sofrem com baixa cobertura. Algumas dificuldades incluem:

Falta de infraestrutura de telecomunicações adequada para suportar servidores de borda eficientes (*World Economic Forum*, 2023).

Regulações locais restritivas, que dificultam a operação de servidores estrangeiros, como ocorre em países como China e Rússia (Forbes, 2022).

Baixa adoção de tecnologias de rede de alta velocidade, como fibra óptica e 5G, que impactam o desempenho da CDN (ITU, 2023).

2. Dependência de Provedores de Nuvem e ISPs

CDNs frequentemente dependem de provedores de serviços em nuvem e Internet Service Providers (ISPs) para expandir sua cobertura. No entanto, essa dependência pode gerar custos elevados e barreiras operacionais, além de criar gargalos quando os provedores não possuem capacidade suficiente em certas regiões (Google, 2018).

3. Custos de Expansão da Infraestrutura

A criação de novos PoPs envolve investimentos significativos em hardware, infraestrutura elétrica e conectividade, tornando o crescimento geográfico da CDN um processo caro e demorado. Empresas precisam balancear custo-benefício ao expandir sua rede para novas áreas (Aws, 2023).

5.4 Impactos Ambientais e Consumo Energético

O crescimento das CDNs ocorre em paralelo à expansão de data centers e redes de transmissão, o que traz desafios ambientais relevantes. Estimativas recentes indicam que data centers e redes de transmissão respondem por cerca de 1% das emissões/consumo de eletricidade relacionados à energia no mundo (IEA, 2023), e que o consumo elétrico de data centers cresceu mais rapidamente que a demanda elétrica total desde 2017, alcançando aprox. 1,5% do consumo elétrico

global em 2024 (IEA, 2025). Esse cenário é pressionado por cargas de trabalho intensivas (streaming, IA, jogos e aplicações em tempo real), o que exige eficiência e descarbonização contínuas.

Métricas e conceitos fundamentais

PUE (*Power Usage Effectiveness)* – razão entre a energia total do data center e a energia destinada à TI. Valores mais próximos de 1,0 indicam maior eficiência. Relatórios recentes de provedores de nuvem reportam PUEs inferiores à média do setor; por exemplo, a AWS reportou PUE global de 1,15 em 2024 (mazon, 2025).

CFE% (*Carbon-Free Energy*) – percentual de energia livre de carbono consumida por região/horário. O Google disponibiliza CFE% por região e orientações para levar essa métrica em conta na escolha da localidade de workloads (Google, 2018).

Escopos de emissões (GHG *Protocol*) – Escopo 1 (diretas), 2 (energia comprada) e 3 (cadeia de valor). Inventários corporativos de CDNs e nuvens detalham metodologias *location-based* (intensidade média da rede local) e *market-based* (contratos/PPAs), fundamentais para interpretar números e comparações (Cloudflare, 2024; Cloudflare, 2025; Akamai, 2025; Microsoft, 2025).

Onde está o consumo energético nas CDNs

O consumo de energia associa-se (i) à operação dos servidores de borda (CPU, memória, discos) e (ii) ao transporte de dados em redes de longa distância. Estudos mostram que discos podem representar 40–55% da energia por servidor de CDN; políticas de desligamento/agrupamento de discos em períodos de baixa, com controle de *cache* hit e degradação aceitável, podem economizar ~30% de energia de disco (Sundarrajan; Kasbekar; Sitaraman, 2016). Em paralelo, *caching* na borda e colaboração entre nós reduzem misses e encurtam o caminho de entrega, diminuindo energia por GB entregue ao reduzir *backhaul* e *origin fetches* (Lin; Liang, 2024).

Computação verde aplicada a CDNs (práticas)

Elevar *cache-hit* e reduzir tráfego de origem: *tiered caching, request coalescing e pre-positioning* diminuem a dependência de *backbone* e a energia associada ao transporte (Lin; Liang, 2024).

Reduzir bytes transferidos: compressão Brotli para texto e formatos de imagem WebP/AVIF trazem ganhos diretos de energia em rede (prática de mercado consolidada e referenciada em guias de fornecedores).

Otimizar transporte: HTTP/3/QUIC reduz *handshakes* e melhora robustez em redes com perda/latência, reduzindo custo energético por objeto entregue (Iea, 2024).

Gestão de armazenamento: conforme (Sundarrajan; Kasbekar; Sitaraman, 2016), políticas de desligamento de discos com controle de hit rate e replicação podem reduzir significativamente energia mantendo QoE.

Alocação geográfica consciente: selecionar regiões/PoPs e origens com CFE% mais alto sem comprometer latência e SLAs (Google, 2018).

Data centers modulares, que utilizam menor quantidade de energia e podem ser realocados conforme a demanda.

Servidores otimizados para eficiência energética, reduzindo desperdícios e melhorando a distribuição da carga computacional.

Parcerias com projetos de compensação de carbono, como reflorestamento e captura de CO_2 atmosférico.

6. Estudo de Caso: Netflix Open Connect (CDN privada)

Este estudo de caso examina a Open Connect, a rede de entrega de conteúdo privada da Netflix, como um exemplo paradigmático de arquitetura orientada à borda para vídeo sob demanda em escala global. A escolha da Open Connect se justifica pela combinação de escala, transparência técnica (documentação pública de implantação) e relevância prática para o contexto brasileiro

6.1 Contexto e motivação

A Open Connect é a rede de entrega de conteúdo (CDN) privada da Netflix, criada para aproximar o conteúdo do assinante e reduzir custos de trânsito e latência. O programa disponibiliza *appliances* de *cache* OCA (*Open Connect Appliance*) para ISPs (Provedores de Serviços de Internet) e para IXPs (*Internet Exchange Points*), de modo a localizar o tráfego e minimizar o caminho percorrido até o usuário, com ganhos diretos de QoE (Qualidade da Experiência) e eficiência operacional (Netflix, [s.d.] “Open Connect — Overview”).

6.2 Arquitetura (plano de dados × plano de controle)

A arquitetura separa plano de dados clusters de OCAs servindo objetos de mídia a partir da rede do ISP/IXP e plano de controle, hospedado na nuvem da AWS (*Amazon Web Services*), que orquestra estado dos OCAs, rotas aprendidas, preenchimento de catálogo e saúde dos nós. Publicações técnicas e estudos de caso indicam o uso de FreeBSD e NGINX na camada de entrega do plano de dados, com anúncios e seleção de rotas via BGP (Border Gateway Protocol) (Netflix, [s.d.] “Overview”; FREEBSD FOUNDATION, 2021).

6.3 Operação e abastecimento de conteúdo

O conteúdo é pré-posicionado nos OCAs durante janelas de preenchimento (*fill windows*) fora do horário de pico. Esse mecanismo reduz *origin fetches* e tráfego de longa distância, elevando *cache-hit* e estabilidade em lançamentos e picos de audiência. A própria Netflix descreve o modelo operacional e publica guias de implantação para parceiros com os requisitos e rotinas recomendadas (Netflix, 2025 “Deployment Guide”; Netflix, [s.d.] “Appliances”).

6.4 Implantação em ISPs/IXPs e requisitos

A Netflix mantém uma política de *peering* aberto e guia de implantação para OCAs incorporados (embedded OCAs) em redes de acesso: requisitos de portas (10/100 GbE), *racking*, energia/resfriamento e critérios para distribuição geográfica que maximizem *offload local*. Quando há volume significativo de tráfego, OCAs embutidos tendem a ser a opção mais benéfica para o ISP (Netflix, [s.d.] "*Peering with Open Connect*"; Netflix, 2025 "*Deployment Guide*"; Netflix, [s.d.] "*Open Connect* — en_gb").

6.5 Evidências independentes e benefícios observados

Medições acadêmicas mostram que a Open Connect explora intensamente IXPs como substrato para entrega de grande parte do tráfego global, reduzindo dependência de trânsito e melhorando o desempenho; há destaque para a presença no Brasil, onde a colocação de OCAs em IXPs/ISPs locais impacta latência e estabilidade (Böttger et al., 2016; Böttger et al., 2018). Esses achados convergem com o objetivo declarado do programa de "localizar tráfego" e melhorar a experiência do assinante (Netflix, [s.d.] "Open Connect — home").

6.6 Relação com "computação verde"

Ao encurtar o caminho de entrega mais Pontos de Presença próximos ao usuário e elevar *cache-hit*, a *Open Connect* reduz *backhaul* e, consequentemente, energia por GB entregue, alinhando-se a princípios de computação verde. O impacto final depende, porém, do mix elétrico onde os OCAs operam e da eficiência PUE (*Power Usage Effectiveness*) dos locais de instalação; por isso, recomenda-se relacionar esse estudo de caso à sua seção de sustentabilidade (Seção 5.4), discutindo onde os PoPs/OCAs estão e quais métricas ambientais regionais se aplicam (Netflix, 2025 "Deployment Guide"; FreeBSD Foundation, 2021).

6.7 Limitações e generalização

A viabilidade de uma CDN privada desse porte está ligada a escala de catálogo VOD *(Video on Demand),* previsibilidade de demanda e relações com ISPs/IXPs *(Internet Service Providers* (provedores de acesso) / *Internet Exchange Points* (pontos de troca de tráfego)). Serviços com tráfego muito dinâmico ou menor volume podem preferir CDNs públicas ou estratégias multivendor. Logo, a Open Connect deve ser lida como exemplo de fronteira de otimização (custo/latência/energia) quando há controle integral do plano de dados e parceria estreita com redes de acesso (Netflix, [s.d.] "Overview"; Böttger et al., 2018).

7. Prova de Conceito: Mini-CDN baseada em contêineres

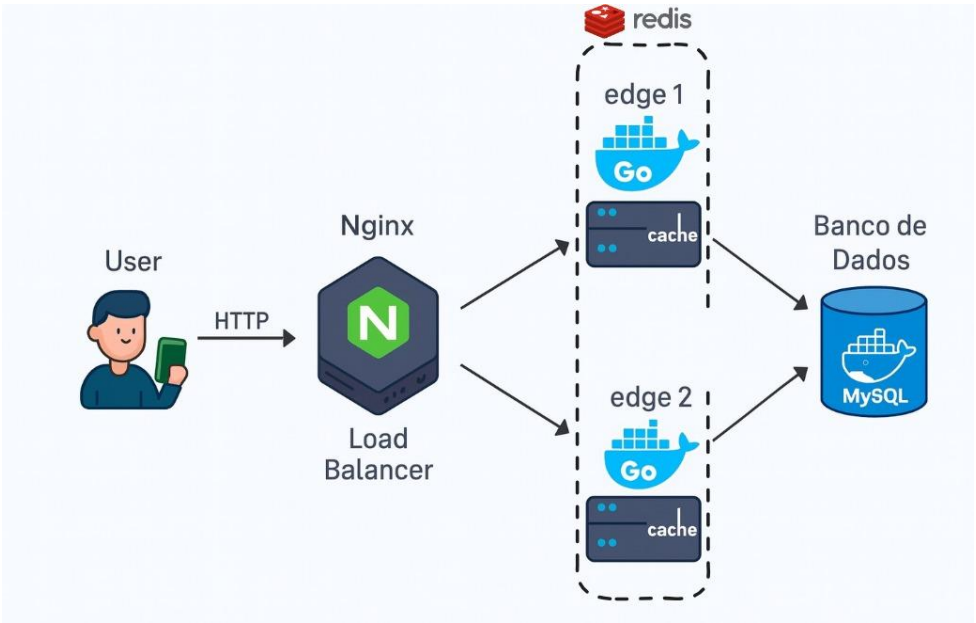
Esta seção apresenta uma prova de conceito (PoC) de uma CDN (*Content Delivery Network*) em ambiente controlado, construída com contêineres e serviços mínimos para espelhar os elementos essenciais de produção

7.1 Objetivo e escopo

Esta prova de conceito (PoC) implementa, em ambiente controlado, os elementos essenciais de uma CDN (*Content Delivery Network*): servidores de borda, balanceamento de carga e roteamento de requisições, com orquestração por contêineres. O objetivo é demonstrar o comportamento de *cache* na borda e os efeitos de direcionamento de tráfego, aproximando conceitos teóricos de um arranjo prático e reprodutível.

7.2 Arquitetura e mapeamento conceitual

Figura 2 Simulador de uma CDN



Fonte: elaboração própria (2025).

A arquitetura simula uma CDN em topologia de borda, como mostrado na figura 2:

Servidores de borda (*edge servers*): nós independentes escritos em Go (Golang), cada um utilizando Redis com *cache* em memória, responsáveis por atender requisições de conteúdo. Nesta PoC, eles correspondem ao papel de PoPs (Pontos de Presença) simplificados.

Proxy reverso/balanceador: um Nginx na “frente” recebe as requisições dos clientes e as distribui entre os *edges*, simulando o encaminhamento típico de CDNs (afinidade, disponibilidade e alívio de carga).

Origem (*origin*): um banco de dados MySQL armazena os valores associados às chaves de conteúdo, representando o repositório/serviço de origem.

Orquestração: *Docker Compose* instancia e conecta os serviços (Nginx, edges e MySQL), permitindo isolar e reproduzir o experimento.

Nesse arranjo, a resposta do *edge* pode ser *cache hit* (conteúdo atendido localmente) ou *cache miss* (consulta ao *origin* e posterior preenchimento do *cache*).

O *sleep* artificial no acesso ao banco emula a latência de origem (p.ex., distância geográfica).

7.3 Implementação

Na implementação, cada requisição passa por um fluxo simples:

1. O *handler* HTTP em Go recebe a chave solicitada.
2. O sistema consulta primeiro o *cache* em memória.
   - Se for um *cache hit*, o valor é retornado imediatamente.
   - Se for um *cache* miss, o *handler* consulta o banco de dados MySQL, armazena a resposta em memória e então a retorna ao usuário, já acompanhada de um *timestamp* para registro da operação.

Cada nó da CDN (por exemplo, *edge1* e *edge2*) é identificado por uma variável de ambiente, permitindo verificar se o balanceamento está funcionando corretamente.

O Nginx atua como ponto de entrada único. Ele recebe as requisições externas e as distribui entre os nós de borda.

A orquestração é feita pelo Docker Compose, que define as redes internas e as dependências necessárias, como a conexão entre o Nginx, os nós de borda e as credenciais de acesso ao MySQL.

Observação: no código de referência em Go foi utilizado um *time.Sleep(5 * time.Second)* apenas para simular a latência do servidor de origem. Em um ambiente real, essa latência seria causada por fatores como distância de rede ou gargalos de entrada e saída (I/O).

7.4 Metodologia de avaliação

Para evidenciar o comportamento de CDN, recomenda-se medir:

Latência de resposta por endpoint: diferença entre *cache hit* e *cache miss*;

Distribuição de requisições por nó: verificar a ação do balanceador (equilíbrio/afinidade);

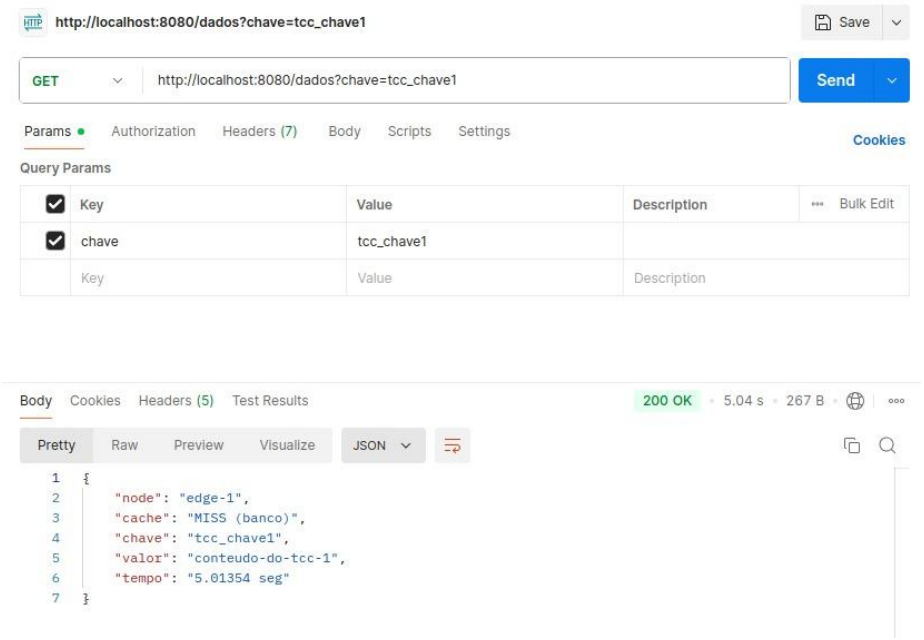
Impacto da latência de origem: variar artificialmente o tempo de espera em 5 segundos e observar o ganho relativo do cache.

Resiliência simples: desligar temporariamente um *edge* e observar continuidade de atendimento via Nginx.

7.5 Resultados

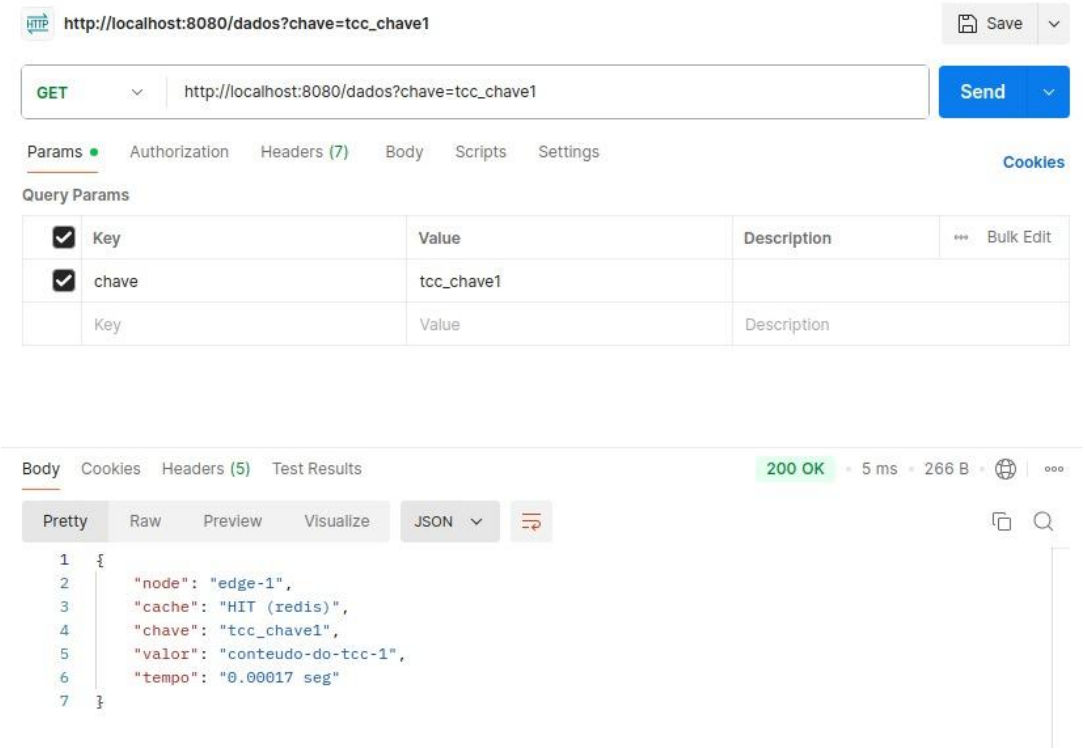
Nesta seção são apresentados os resultados dos testes de desempenho realizados para avaliar o impacto da latência de origem e o efeito do uso do *cache* Redis.

Figura 3 Requisição 1



Fonte: elaboração própria (2025).

Figura 4 Requisição 2



Fonte: elaboração própria (2025).

Para a chave tcc_chave1, observou-se:

Requisição 1 (Figura 3) — *MISS* (*origin*/banco): resposta 200 OK em aproximadamente 5,04 s (tempo interno reportado pelo serviço: 5,01354 s), com cache: "*MISS* (banco)".

Requisição 2 (Figura 4) — HIT (Redis): resposta 200 OK praticamente instantânea (tempo interno: 0,00017 s, ≈ 0,17 ms), com cache: "HIT (redis)".

O atendimento via *cache* Redis reduziu a latência em cerca de 5 segundos, representando um ganho de ordem de ≈30.000× em relação ao acesso ao *origin* para a mesma chave. Esse resultado confirma, mesmo em ambiente controlado, o benefício central de CDNs: reuso de conteúdo e eliminação de chamadas ao *origin*, com impacto direto na experiência do usuário e no tráfego de *backhaul*. Em linha com a discussão de computação verde (Seção 5.4), ao evitar o *origin* reduz-se também a energia por GB entregue, condicionada ao mix elétrico e à eficiência (PUE) da infraestrutura utilizada.

7.6 Limitações e ameaças à validade

A PoC não modela roteamento global, políticas de *peering*, diversidade de ASN, controle de congestionamento multi-região, HTTP/3/QUIC ou estratégias avançadas de *tiered caching* e *coalescing*. Também não contempla escalabilidade horizontal massiva, replicação consistente entre PoPs ou *cache* distribuído em disco. Assim, os resultados não devem ser extrapolados diretamente para ambientes de produção; servem como demonstração didática e base para experimentos controlados.

8. Conclusões

8.1 Principais achados da revisão bibliográfica

A revisão mostrou que CDNs (*Content Delivery Networks*) são hoje um pilar de desempenho, resiliência e segurança para serviços digitais sob alta demanda multimídia. Do ponto de vista arquitetural, a literatura converge para modelos com *cache* na borda, roteamento dinâmico, *tiered caching* e proteções em múltiplas camadas (WAF, mitigação de DDoS, *bot management*), apoiados por protocolos modernos (HTTP/2, HTTP/3/QUIC). Evidenciou-se que práticas como compressão (Brotli), formatos eficientes (WebP/AVIF) e *origin shielding* reduzem latência e tráfego de *backhaul*, impactando diretamente custo e experiência do usuário.
O estudo de caso da Netflix Open Connect ilustra os ganhos de localização de tráfego via *appliances* de borda em ISPs/IXPs, com *pre-positioning e peering* aberto, e a prova de conceito (PoC) confirmou, em ambiente controlado, a diferença substancial entre *cache hit e cache miss* sob latência de origem. Por fim, a discussão de computação verde indicou que energia por GB entregue tende a diminuir com *cache* eficiente e proximidade, ainda que o impacto final dependa de PUE e CFE% das regiões envolvidas.

8.2 Implicações para o uso de CDNs

À luz da demanda crescente por conteúdo multimídia, do aumento do tráfego e da necessidade de mitigar falhas e ataques (justificativa 1.2), as seguintes implicações práticas se destacam:

Projeto e governança: priorizar borda com *tiered caching, request coalescing e origin shielding;* adotar HTTP/3/QUIC e TLS 1.3; monitorar TTFB, *cache-hit e origin fetches* como SLOs operacionais.

Segurança e resiliência: integrar mitigação DDoS e *bot management;* avaliar multi-CDN com *failover* automatizado para reduzir risco de *single point of failure.*

Custo e sustentabilidade: incluir precificação regional e egress no TCO; otimizar bytes/req (Brotli, WebP/AVIF) e considerar localidades com CFE% superior quando a latência permitir, conectando desempenho a metas de ESG.

Adoção de novas práticas: explorar *Edge Computing*, 5G e IoT para *offloading* de lógica (p.ex., functions/serverless at *edge*, WASM), bem como IA para pre-positioning e controle adaptativo de cache.

Contexto Brasil/AmSul: testar provedores com PoPs (Pontos de Presença) próximos aos ASNs-alvo; medir in loco (São Paulo, RJ, NE) por 7–14 dias para capturar variação diurna/regional.

8.3 Sugestões para futuras pesquisas

Benchmarks independentes e reprodutíveis no Brasil entre múltiplas CDNs (desempenho, custo e segurança), incluindo métricas de sustentabilidade (energia/GB, estimativas de CO_2eq com base em PUE/CFE% regionais).

Modelos de IA para previsão de demanda e pre-positioning orientado a custo/energia, comparando ganhos de hit e redução de backhaul versus consumo adicional de armazenamento.

Efeitos do 5G e de mobilidade (*handover*, perda, *bufferbloat*) em HTTP/3/QUIC, avaliando QoE em streaming ao vivo e VOD sob diferentes políticas de cache.

Edge Computing e funções na borda: estudo de latência fim-a-fim, consistência de *cache* e observabilidade quando lógica de aplicação migra para PoPs, inclusive implicações de LGPD (dados pessoais na borda).

Resiliência e segurança avançadas: avaliação de multi-CDN com roteamento baseado em SLO em tempo real, testes de estresse contra DDoS aplicacional e análise de eficácia de bot management em cenários de fraude/abuso.

Economia e regulação: modelagem de TCO (incluindo *egress*, logs e add-ons de segurança), e estudo de políticas de interconexão/*peering* que afetam desempenho e custo em ASNs nacionais.

Este trabalho atingiu os objetivos propostos: (i) revisou arquiteturas e mecanismos das CDNs; (ii) descreveu aplicações e benefícios com evidências práticas (Netflix Open Connect e PoC); (iii) discutiu desafios e limitações, incluindo segurança e sustentabilidade; e (iv) apontou tendências e frentes de inovação (*Edge*, 5G, IoT, IA). Diante da trajetória de crescimento do tráfego e do risco crescente de falhas e ataques, CDNs bem projetadas e governadas continuam sendo estratégicas

para assegurar desempenho, resiliência e responsabilidade ambiental nos serviços digitais.

Referências

ALSALEM, Thanaa Saad; ALMAIAH, Mohammed Amin; LUTFI, Abdalwali. Cybersecurity Risk Analysis in the IoT: A Systematic Review. Electronics, v. 12, n. 18, 3958, 2023. Disponível em: https://www.mdpi.com/2079-9292/12/18/3958. Acesso em: 27 abr. 2025.

AKAMAI TECHNOLOGIES, Inc. Akamai 2024 ESG Impact Report. Cambridge, MA, 2025. Disponível em: https://www.akamai.com/site/en/documents/corporate/2025/akamai-2024-esg-impact-report.pdf. Acesso em: 20 jun. 2025.

AKAMAI TECHNOLOGIES, Inc. State of the Internet / Security: Year in Review. Cambridge, MA, 2021. Disponível em: https://www.akamai.com/blog/security/soti-security-year-end-review. Acesso em: 20 jun. 2025.

AMAZON. 2024 Amazon Sustainability Report: AWS Summary. Seattle, 2025. Disponível em: https://sustainability.aboutamazon.com/2024-amazon-sustainability-report-aws-summary.pdf. Acesso em: 16 set. 2025. (PUE global de 1,15 em 2024.)

AMAZON. 2024 Amazon Sustainability Report. Seattle, 2025. Disponível em: https://sustainability.aboutamazon.com/2024-amazon-sustainability-report.pdf. Acesso em: 16 set. 2025.

AOUEDI, Ons; PIAMRAT, Kandaraj; PARREIN, Benoît. Intelligent Traffic Management in Next-Generation Networks. Future Internet, v. 14, n. 2, p. 44, 2022. Disponível em: https://www.mdpi.com/1999-5903/14/2/44. Acesso em: 26 abr. 2025.

BÖTTGER, Timm; CUADRADO, Felix; TYSON, Gareth; CASTRO, Ignacio; UHLIG, Steve. Open Connect Everywhere: A Glimpse at the Internet Ecosystem through the Lens of the Netflix CDN. arXiv preprint, 2016. Disponível em: https://arxiv.org/abs/1606.05519. Acesso em: 12 set. 2025

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 16 set. 2025.

BUYYA, Rajkumar; PATHAN, Mukaddim; VAKALI, Athena (Eds.). Content Delivery Networks. Berlim: Springer-Verlag, 2008 (Lecture Notes in Electrical Engineering). ISBN: 978-3-540-77886-8. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=p2C2cZkTrmsC&oi=fnd&pg=PA3&dq=Content+Delivery+Networks&ots=gfyh0zon7x&sig=P4tS1IKRuwaobITHMzXlosnVw-E&redir_esc=y#v=onepage&q=Content%20Delivery%20Networks&f=false. Acesso em: 27 abr. 2025.

BLAZINGCDN. Akamai CDN Pricing: An In-Depth Analysis. Blog BlazingCDN, 18 nov. 2024. Disponível em: https://blog.blazingcdn.com/en-us/what-is-the-price-per-tb-of-akamai-cdn. Acesso em: 20 out. 2025.

CISCO SYSTEMS. The Cisco Content Delivery Network Solution for the Enterprise. White Paper. Cisco Systems, 2000. Disponível em: https://doi.org/10.3390/electronics12183958. Acesso em: 27 abr. 2025.

CLOUDFLARE, Inc. 2024 Impact Report. San Francisco, 2024. Disponível em: https://cf-assets.www.cloudflare.com/slt3lc6tev37/7bEraZE4BmpaCFfYYHxbaU/20dda9014ac14793e61daaff0783eee5/2024_Cloudflare_Impact_Report.pdf. Acesso em: 14 set. 2025.

CLOUDFLARE, Inc. Cloudflare Emissions Inventory 2024. San Francisco, 2025. Disponível em: https://cf-assets.www.cloudflare.com/slt3lc6tev37/2lg914L21Lyfpcya6weavX/1f239ca65b697e5b3b1ce89bb7141c41/Cloudflare_2024_Emissions_Inventory.pdf. Acesso em: 15 set. 2025.

CLOUDFLARE, Inc. DDoS Attack Threat Landscape 2022. San Francisco, 2022. Disponível em: https://www.cloudflare.com/static/0eff061e8d56da7d6a5ad3b1327dd11e/BDES-3514_DDoS-Trends-Report-Q2-2022-WP-A4.pdf. Acesso em: 19 set. 2025

CLOUDFLARE. CDN da Cloudflare. [s.d.]. Disponível em: https://www.cloudflare.com/pt-br/application-services/products/cdn/. Acesso em: 20 out. 2025.

DILLEY, John; MAGGS, Bruce; PARIKH, Jay; PROKOP, Harald; SITARAMAN, Ramesh; WEIHL, Bill. Globally Distributed Content Delivery. University of Massachusetts - Amherst, 2002. Disponível em: https://ieeexplore.ieee.org/abstract/document/1036038. Acesso em: 14 fev. 2025.

GOOGLE. Carbon-free energy for Google Cloud regions. Disponível em: https://cloud.google.com/sustainability/region-carbon. Acesso em: 16 set. 2025.

GOOGLE. Modernizing transport security. Google Security Blog, 2018. Disponível em: https://security.googleblog.com/2018/10/modernizing-transport-security.html. Acesso em: 04 set. 2025.

INTERNET SECURITY RESEARCH GROUP (ISRG). 2023 Annual Report. 2023. Disponível em: https://www.abetterinternet.org/documents/2023-ISRG-Annual-Report.pdf. Acesso em: 16 set. 2025.

INTERNATIONAL ENERGY AGENCY. Data Centres and Data Transmission Networks. Paris: IEA, 2023. Disponível em: https://www.iea.org/energy-

system/buildings/data-centres-and-data-transmission-networks. Acesso em: 13 set. 2025.

INTERNATIONAL ENERGY AGENCY. Electricity 2024: Analysis and Forecast to 2026. Paris: IEA, 2024. Disponível em: https://iea.blob.core.windows.net/assets/6b2fd954-2017-408e-bf08-952fdd62118a/Electricity2024-Analysisandforecastto2026.pdf. Acesso em: 13 set. 2025.

INTERNATIONAL ENERGY AGENCY. Energy and AI: Executive Summary. Paris: IEA, 2025. Disponível em: https://www.iea.org/reports/energy-and-ai/executive-summary. Acesso em: 13 set. 2025.

KRISHNAMURTHY, Balachander; WILLS, Craig E. On the use and performance of content distribution networks. In: Proceedings of the 1st Internet Measurement Workshop (IMW '01). San Francisco, CA: ACM, 2001. Disponível em: https://dl.acm.org/doi/10.1145/505202.505224. Acesso em: 05 set. 2025.

LECONTE, Mathieu; LELARGE, Marc; MASSOULIÉ, Laurent. Adaptive Replication in Distributed Content Delivery Networks. Technicolor - INRIA, Microsoft Research - INRIA Joint Center, 2014. Disponível em: https://arxiv.org/abs/1401.1770. Acesso em: 23 abr. 2025.

LIN, Zhi; LIANG, Jiarong. Edge Caching Data Distribution Strategy with Minimum Energy Consumption. Sensors (Basel), v. 24, n. 9, p. 2898, 2024. DOI: 10.3390/s24092898. Disponível em: https://pmc.ncbi.nlm.nih.gov/articles/PMC11086164/. Acesso em: 05 set. 2025.

MICROSOFT. Environmental Sustainability Report 2025. Redmond, 2025. Disponível em: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/2025-Microsoft-Environmental-Sustainability-Report.pdf. Acesso em: 16 set. 2025.

MANDAVA, Sarath Krishna. Web Performance Optimization in the Age of 5G: New Opportunities and Challenges. Educational Administration: Theory and Practice, v. 27, n. 1, p. 1098-1109, 2021. Disponível em: https://doi.org/10.53555/kuey.v27i1.8395. Acesso em: 24 abr. 2025.

MELLUK, Abdelhamid; HOCEINI, Said; TRAN, Hai Anh. Quality of Experience for Multimedia: Application to Content Delivery Network Architecture. Londres: ISTE Ltd.; Hoboken, NJ: John Wiley & Sons, 2013. ISBN: 978-1-84821-563-4. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=HhcfAgAAQBAJ&oi=fnd&pg=PR13&dq=Quality+of+Experience+for+Multimedia&ots=LotDv3tJgE&sig=wD2KlDWUg_PriqtCd4vMCbqhNMs&redir_esc=y#v=onepage&q=Quality%20of%20Experience%20for%20Multimedia&f=false. Acesso em: 27 abr. 2025.

MIRHEIDARI, Seyed Ali et al. Cached and Confused: Web Cache Deception in the Wild. In: 29th USENIX Security Symposium, 12-14 agosto 2020. Disponível em:

https://www.usenix.org/conference/usenixsecurity20/presentation/mirheidari. Acesso em: 27 abr. 2025.

MISHRA, Atul; KATYAL, Mayanka. A Comparative Study of Load Balancing Algorithms in Cloud Computing Environment. J.C. Bose University of Science & Technology, YMCA, 2014. Disponível em: https://arxiv.org/abs/1403.6918. Acesso em: 23 abr. 2025.

MOZILLA DEVELOPER NETWORK (MDN). Transport Layer Security (TLS). 5 maio 2025. Disponível em: https://developer.mozilla.org/en-US/docs/Web/Security/Transport_Layer_Security. Acesso em: 07 set. 2025.

NETFLIX. Open Connect Overview. [S. l.], [s. d.]. Disponível em: https://openconnect.netflix.com/Open-Connect-Overview.pdf. Acesso em: 10 set. 2025.

NETFLIX. Open Connect Appliances. [S. l.], [s. d.]. Disponível em: https://openconnect.netflix.com/appliances/. Acesso em: 10 set. 2025.

NETFLIX. Open Connect Deployment Guide. 22 ago. 2025. Disponível em: https://openconnect.netflix.com/deploymentguide.pdf. Acesso em: 10 set. 2025.

NETFLIX. Peering with Open Connect. [S. l.], [s. d.]. Disponível em: https://openconnect.netflix.com/peering/. Acesso em: 10 set. 2025.

NETFLIX. Open Connect Home. [S. l.], [s. d.]. Disponível em: https://openconnect.netflix.com/. Acesso em: 10 set. 2025.

NYGREN, Erik. The Akamai Network: A Platform for High-Performance Internet Applications. ACM SIGOPS Operating Systems Review, v. 36, p. 28-29, 2002. Disponível em: https://dl.acm.org/doi/abs/10.1145/1842733.1842736. Acesso em: 27 abr. 2025.

OWASP. Transport Layer Security Cheat Sheet. [s.d.]. Disponível em: https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Security_Cheat_Sheet.html. Acesso em: 04 set. 2025.

PADMANABHAN, Venkata N. et al. Distributing Streaming Media Content Using Cooperative Networking. In: NOSSDAV'02: 12th International Workshop on Network and Operating System Support for Digital Audio and Video, Miami, Florida, EUA, 2002. Disponível em: https://dl.acm.org/doi/abs/10.1145/507670.507695. Acesso em: 27 abr. 2025.

PATHAN, A. M. K.; BUYYA, Rajkumar. A Taxonomy of CDNs. In: BUYYA, R.; PATHAN, M.; VAKALI, A. (orgs.) Content Delivery Networks. Berlin: Springer, 2008. Disponível em: https://link.springer.com/chapter/10.1007/978-3-540-77887-5_2. Acesso em: 20 fev. 2025.

PENG, Gang. CDN: Content Distribution Network. 2018. Dissertação (Mestrado em Ciência da Computação) – State University of New York at Stony Brook, Stony Brook, 2018. Disponível em: https://arxiv.org/abs/cs/0411069. Acesso em: 14 fev. 2025.

QIU, Lili; PADMANABHAN, Venkata N.; VOELKER, Geoffrey M. On the Placement of Web Server Replicas. In: Proceedings IEEE INFOCOM 2001, Anchorage, Alaska, EUA, 2001. Disponível em: https://ieeexplore.ieee.org/abstract/document/916655. Acesso em: 27 abr. 2025.

STAMOS, Konstantinos; PALLIS, George; VAKALI, Athena; DIKIAKOS, Marios D. Evaluating the Utility of Content Delivery Networks. In: UPGRADE-CN'09 – International Workshop on the Use of P2P, GRID and Agents for the Development of Content Networks, 9 jun. 2009, Munich, Germany. DOI: 10.1145/1552486.1552509. Disponível em: https://doi.org/10.1145/1552486.1552509. Acesso em: 14 fev. 2025.

SU, Zhou et al. Edge Caching for Layered Video Contents in Mobile Social Networks. IEEE Transactions on Multimedia, 2017. DOI: 10.1109/TMM.2017.2733338. Disponível em: https://ieeexplore.ieee.org/abstract/document/7995075. Acesso em: 27 abr. 2025.

STEGMANN, Pascal. Netflix's Distribution And Interconnections: What Are The Economics Today? ARK Invest, 30 mar. 2015. Disponível em: https://www.ark-invest.com/articles/analyst-research/cdns-netflix-networks. Acesso em: 20 out. 2025.

SUNDARRAJAN, Aditya; KASBEKAR, Mangesh; SITARAMAN, Ramesh K. Energy-efficient disk caching for content delivery. In: e-Energy '16 – 7th International Conference on Future Energy Systems. New York: ACM, 2016. DOI: 10.1145/2934328.2934348. Disponível em: https://groups.cs.umass.edu/wp-content/uploads/sites/3/2019/12/Energy-efficient-disk-caching-for-content-delivery.pdf. Acesso em: 16 set. 2025.

UNIÃO EUROPEIA. Regulation (EU) 2016/679 (General Data Protection Regulation GDPR). Bruxelas, 2016. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng. Acesso em: 07 set. 2025.

VAKALI, Athena; PALLIS, George. Content Delivery Networks: Status and Trends. IEEE Internet Computing, nov.-dez. 2003, p. 68-74. Disponível em: https://ieeexplore.ieee.org/abstract/document/1250586. Acesso em: 27 abr. 2025.
YANG, Huixiang; PAN, Hanlin; MA, Lin. A Review on Software Defined Content Delivery Network: A Novel Combination of CDN and SDN. IEEE Access, 2023. Disponível em: https://ieeexplore.ieee.org/abstract/document/10103706. Acesso em: 20 abr. 2025.

YU, Yifan; LV, Huazhang; CHEN, Dan. Towards the Seamless Integration of OTT CDN and Mobile Edge Computing System. In: Proceedings of IEEE International Conference, 2023. Disponível em: https://ieeexplore.ieee.org/abstract/document/8647347. Acesso em: 27 abr. 2025.