ARTIGO

O APAGÃO DIGITAL: LIÇÕES DO INCIDENTE DE DNS NA AWS E A VULNERABILIDADE DA INFRAESTRUTURA DE NUVEM NA INTERNET GLOBAL

Edgar Yukio Ishibashi
Silvio César Bogsan

RESUMO

A crescente consolidação de serviços digitais críticos em um número limitado de provedores de nuvem levanta questões fundamentais sobre a resiliência da infraestrutura. Se uma organização coloca suas operações “core” na nuvem, ela espera alta disponibilidade. Este estudo de caso investiga o incidente generalizado ocorrido na Amazon Web Services (AWS) em 20/10/2025, que resultou em um vasto "apagão digital", com paralisação de operações em setores como financeiro, aviação e comunicação. Por meio da análise de relatos públicos, mapeamos a propagação da falha central para milhares de aplicações dependentes, em forma de cascata. O evento serve como um alerta crítico sobre a vulnerabilidade decorrente da dependência de um único ponto de controle, sublinhando a necessidade imperativa de que as organizações revisitem e implementem estratégias de continuidade de negócios baseadas em diversificação e arquiteturas verdadeiramente *cloud-agnostic* (independentes de um provedor específico), o que impõe novas demandas de redundância interna aos próprios provedores de nuvem.

Palavras-chave: Autenticação no DNS, Cibersegurança, Computação em Nuvem, DNSSec, Integridade de Dados, Protocolo DNS, Vulnerabilidade.

ABSTRACT

The growing consolidation of critical digital services within a limited number of cloud providers raises fundamental concerns about infrastructure resilience. When an organization migrates its core operations to the cloud, it expects high availability. This case study investigates the widespread incident that occurred at Amazon Web Services (AWS) on October 20, 2025, which resulted in a vast “digital blackout,” halting operations across areas such as finance, aviation, and communications. Through the analysis of public reports, we mapped out how the central failure propagated in a cascading manner to thousands of dependent applications. The event serves as a critical warning about the vulnerability arising from reliance on a single point of control, emphasizing the imperative for organizations to revisit and implement business continuity strategies based on

diversification and truly cloud-agnostic architectures (independent of any single provider). It imposes new internal redundancy requirements on the cloud providers themselves.

Keywords: DNS Authentication, Cybersecurity, Cloud Computing, DNSSEC, Data Integrity, DNS Protocol, Vulnerability.

1 INTRODUÇÃO

A última década testemunhou uma migração acelerada da infraestrutura de Tecnologia da Informação para o modelo de nuvem pública, com a ascensão dos serviços Infrastructure as a Service (IaaS) e Software as a Service (SaaS). Este movimento, intensificado pela necessidade de escalabilidade imposta pela crise sanitária de 2019/2020, permitiu que organizações de todos os portes substituíssem a posse e manutenção de recursos computacionais — como servidores, backups e atualizações — pela contratação de serviços baseados em assinatura. Embora essa transição ofereça vantagens significativas em termos de redução de custos operacionais (CapEx para OpEx) e transferência de responsabilidades técnicas especializadas, ela introduz um novo vetor de risco: a concentração da dependência operacional em um número restrito de grandes provedores globais.

Segundo Richter (2025), a AWS é o maior provedor da nuvem pública, com aproximadamente 30% do faturamento. A Microsoft, através da Azure vem em seguida, e depois o Google, como os maiores provedores. Essa dominância demonstra a profunda interdependência entre a saúde operacional de um único fornecedor e a estabilidade de grande parte do ecossistema digital mundial. Essa dependência foi dramaticamente exposta em 20/10/2025, quando um evento de indisponibilidade centrado na região US-EAST-1 da AWS não apenas paralisou serviços internos da Amazon, como também gerou um efeito dominó que afetou operações em setores cruciais como o financeiro, a aviação e plataformas de comunicação.
Fonte: statista.com

Diante deste cenário, este artigo quer ir além do relato técnico da falha. O objetivo central é analisar as implicações sistêmicas do "Apagão Digital" de 20/10/2025, avaliando cuidadosamente a propagação da disrupção entre diferentes setores, bem como a vulnerabilidade da infraestrutura de nuvem globalmente centralizada. Conclui-se, a partir deste evento, a necessidade imperativa de revisão das estratégias de continuidade de negócios, focando na adoção de arquiteturas que sejam cloud-agnostic (independentes de um provedor específico). Para tal, detalharemos o incidente em si, seguida de uma discussão sobre as lições aprendidas para a governança de TI e, finalmente, as conclusões do estudo.

2 REFERENCIAL TEÓRICO

Resiliência, Disponibilidade e a Base da Nuvem

A infraestrutura de Nuvem Pública, embora prometa escalabilidade, opera sobre componentes eletrônicos sujeitos a falhas inerentes, como defeitos de hardware, indisponibilidade energética e fatores ambientais. Neste cenário, o conceito de Resiliência torna-se fundamental. Resiliência refere-se à capacidade de um sistema, serviço ou organização de TI se recuperar rapidamente de falhas, interrupções ou eventos adversos, mantendo níveis aceitáveis de operação (AXELOS, 2019).
Para tangibilizar essa resiliência, a área de Tecnologia da Informação e Comunicação (TIC) formalizou a Governança de TI, trazendo especificações e melhores práticas para a implementação de soluções redundantes, segurança e garantia de Alta Disponibilidade (HA) dos serviços oferecidos. Grande parte dos padrões seguidos pela indústria foram, ironicamente, estabelecidos pelos próprios provedores de nuvem, que criaram ecossistemas robustos em suas regiões primárias.

Mecanismos de Tolerância a Falhas em Escala Global

A arquitetura de sistemas distribuídos, como a Nuvem, exige mecanismos sofisticados que vão além da simples redundância física. Sistemas distribuídos devem incorporar mecanismos automatizados para monitorar a saúde dos componentes (health checks), acionar sistemas de reserva (failover) de forma automática e realizar o balanceamento de carga (load balance) entre servidores para mitigar sobrecargas localizadas. Essas medidas, historicamente projetadas para escopo local, precisam operar atualmente em uma capacidade global, dada a dependência de organizações em diferentes fusos horários e jurisdições.

O Ponto de Falha Centralizado

A extrema dependência desse ecossistema global foi severamente testada em 20/10/2025. Neste dia, um incidente na infraestrutura da Amazon Web Services (AWS), especificamente um colapso no serviço de Domain Name System (DNS) em um de seus “data centers” centrais (US-EAST-1), demonstrou o risco inerente à centralização. Uma falha em um componente fundamental de "diretório" da nuvem resultou na paralisação de serviços de terceiros, expondo a fragilidade das estratégias de resiliência quando a falha reside no provedor central.

O DNS (Domain Name System) é um protocolo da camada de aplicação do modelo OSI e é um dos pilares da Internet moderna, porém é um dos pontos mais vulneráveis se não for bem protegido.

O protocolo DNS é o sistema de nomes de domínio, responsável por traduzir nomes legíveis (como www.google.com) em endereços IP (como 142.250.190.68) que os

computadores usam para se comunicar em rede. O protocolo DNS, na sua forma original (definido na década de 1980 — RFC 1034/1035), não foi projetado com segurança em mente. Ele transmite dados em texto puro (sem criptografia) e confia amplamente em respostas sem autenticação robusta, isso o torna suscetível a diversos tipos de ataques. Técnicas como do DNS Spoofing / Cache Poisoning, DNS Hijacking, Amplificação de DNS utilizados em DDoS, Interceptação e espionagem (Privacy Leaks), além de falhas geradas pela configuração e dependência centralizada, se não implementadas através de mecanismos como o DNSSec, DoH / DoT (criptografia nas consultas DNS), mitigação de ataques de negação de serviços (DoS), distribuição de servidores globalmente para resiliência e performace (Anycast DNS).

3 ESTUDO DE CASO: O INCIDENTE DE OUTUBRO DE 2025 NA AWS

Esta seção concentrar-se-á em detalhar a natureza da falha, sua propagação e a diversidade de setores impactados, servindo como evidência empírica para o que foi apresentado no referencial teórico. Criada em 2006, a AWS é a maior provedora de computação em nuvem do mundo. Com milhões de clientes em mais de 190 países, sua estrutura sustenta o funcionamento de inúmeros sites, aplicações corporativas e bancos de dados. Em 2.024, a divisão foi responsável por US$ 108 bilhões em receita, concentrando a maior parte dos lucros da Amazon. (Exame, 2.025).

Essa falha se soma a episódios anteriores registrados em 2.020, 2.021 e 2.023, todos com efeito em cascata e impacto global. Em comum está a origem dos problemas: a região US-EAST-1, localizada no norte da Virgínia, considerada o núcleo mais antigo e sobrecarregado da AWS. A US-EAST-1 concentra uma série de funções críticas, como autenticação, monitoramento e roteamento de tráfego. Este empilhamento de funções críticas é herança do crescimento acelerado da AWS na década de 2.010, fazendo com que falhas no norte da Virgínia gerem impactos em outras regiões do mundo. (Exame, 2.025)

3.1. Diagnóstico Técnico

O Componente Crítico que ocasionou todo problema foi a falha de Resolução de DNS, afetando os endpoints (dispositivos físicos ou virtuais que trocam dados) do serviço DynamoDB. O Amazon DynamoDB é um serviço de banco de dados NoSQL (não relacional) totalmente gerenciado, oferecido pela Amazon Web Services (AWS). Ele foi projetado para aplicações que precisam de alta performance, baixa latência e escalabilidade massiva, fornecendo acesso a dados de forma rápida e previsível. Sendo NoSQL, os itens dentro de uma mesma tabela não precisam ter os mesmos atributos. Basta ter uma chave primária, e os demais campos podem variar. A grande vantagem é a oferta de baixa latência (acesso a dados em milissegundos) em qualquer escala,

mesmo com grandes volumes de dados. A AWS cuida da infraestrutura, gerenciamento, manutenção e atualizações, permitindo que a infraestrutura por baixo do serviço não precise ser gerenciada, provisionada ou escalada manualmente por você. (AWS, 2.025).

3.2. A Propagação da Disrupção (O Efeito Dominó)

Uma falha sistêmica e generalizada pode sobrecarregar ou comprometer o subsistema responsável por esse monitoramento, sobrecarregando ou impedindo os mecanismos internos de health check e failover da AWS de funcionarem corretamente. O processo de failover (transferência automática de recursos para uma zona de disponibilidade saudável) depende diretamente do sucesso dos health checks. Se o sistema de monitoramento não funciona corretamente, a ação de failover não é acionada, e as aplicações continuam a tentar se conectar a recursos inacessíveis, causando atrasos significativos na recuperação (aproximadamente 15 a 16 horas, com recuperação total levando a maior tempo). (G1, 2.025).

Além disso, empresas tiveram dificuldades para criar novos servidores virtuais no serviço Elastic Compute Cloud (EC2). A AWS afirmou ter identificado alguns sinais de recuperação após adotar medidas para resolver os problemas ligados ao EC2 e que estava tomando medidas semelhantes nos locais que ainda enfrentavam problemas. Os erros impactaram outras funcionalidades na AWS. O AWS Lambda permite que você utilize servidores sem precisar lidar com todo o gerenciamento da infraestrutura, possibilitando um desenvolvimento mais rápido, melhor desempenho, maior segurança e eficiência de custos (AWS, 2025). Por volta das 18h30, 76 recursos da plataforma ainda tinham algum tipo de instabilidade. Outros 66 apareciam como resolvidos na página do serviço. (G1, 2025).

3.3. Impacto Intersetorial Global

Segundo a agência Reuters, o site Downdetector, que monitora instabilidades em sites e aplicativos no mundo todo, mais de 4 milhões de usuários relataram problemas devido ao incidente. (G1, 2.025). Diversos serviços tiveram falhas:

- Serviços de Consumo: Snapchat, Fortnite, Netflix, Alexa, Clash of Clans, Clash Royale, HBO, Prime Video;
- Serviços Críticos/Financeiros: Coinbase, Robinhood, bancos no Reino Unido, Mercado Pago, Stone, Banco Pan, PicPay;
- Infraestrutura de Suporte: Claro, Amazon;
- Companhias aéreas: Delta, United;
- Serviços de produtividade: Slack, Zoom, Canva, Lyft, iFood, Duolingo.

4. DISCUSSÃO

4.1. A Falha da Abstração de Infraestrutura

A popularidade dos serviços de Nuvem Pública está fundamentalmente na abstração da complexidade para o cliente. Serviços como DynamoDB, EC2 e Lambda são vendidos sob a premissa de que a infraestrutura subjacente — hardware, manutenção, gerenciamento de capacidade — é de total responsabilidade do provedor (AWS, 2.025). Essa delegação de tarefas técnicas, conforme estabelecido na Governança de TI, permite que as empresas se concentrem em seu “core business”.

No entanto, o incidente de 20/10/2025 demonstrou que essa abstração carece ao proteger o cliente quando à falha em um componente de infraestrutura básica e transversal, como o Sistema de Nomes de Domínio (DNS) para o DynamoDB. A falha não ocorreu em um serviço de nicho, mas em uma camada fundamental de comunicação que sustenta inúmeras aplicações de missão crítica.

A concentração de funções críticas — como o roteamento de tráfego e a autenticação — na região US-EAST-1 (Exame, 2025) agrava este ponto. Ao empilhar um número desproporcional de funções essenciais em um único hub geográfico, a AWS criou um vetor de risco sistêmico que transcende os limites de falha esperados de um único cliente. O que pretendia ser um risco isolado (falha de um banco de dados) se tornou um risco sistêmico para milhares de clientes que, baseados nos SLAs (Níveis de Serviço Contratados) e na promessa de alta disponibilidade, não implementaram barreiras de contenção eficazes fora daquela região. A falha evidenciou, portanto, que a dependência de um único ponto de controle, por mais robusto que pareça, anula a resiliência que o cliente tenta construir em níveis de serviço mais altos.

Essa situação levanta uma questão crítica para a Governança de TI: onde termina a responsabilidade do provedor e onde começa a responsabilidade do cliente na arquitetura de resiliência, seja recuperação de desastre ou continuidade dos negócios?

4.2. Insuficiência de Mecanismos Internos de Resiliência

O Referencial Teórico evidenciou que a operação moderna de sistemas distribuídos depende de mecanismos automatizados, como health checks e failover (G1, 2025). A expectativa implícita de um serviço gerenciado como o DynamoDB é que, em caso de degradação de desempenho, o sistema automaticamente redireciona o tráfego para locais íntegros, garantindo a continuidade do serviço.

O incidente demonstrou uma falha crítica nesta cadeia de contenção:

- Comprometimento do Health Check: A falha de resolução de DNS para os endpoints do DynamoDB impediu que os sistemas de monitoramento internos (que dependem do DNS para validar a saúde dos serviços) funcionassem corretamente. Se o

sistema não consegue confirmar a localização de um recurso, ele não pode validar, se ele está saudável ou doente.

- Paralisia do Failover: O processo de failover (transferência automática de carga para uma Zona de Disponibilidade, AZ, saudável) depende intrinsecamente do sucesso dos health checks e da capacidade de iniciar novos recursos, como o lançamento de instâncias EC2. A AWS notou a dificuldade em lançar novas instâncias EC2 (G1, 2025), o que sugere que a falha inicial no nível de conectividade e descoberta de serviços (DNS) impediu a orquestração necessária para mover a carga de trabalho de forma autônoma.

Essa falha sistêmica revela uma hierarquia de dependências: a resiliência em camadas superiores (serviço de banco de dados) foi anulada por uma falha em uma camada fundamental (o serviço de endereçamento/DNS) que, teoricamente, deveria ser o mais estável. Para o cliente, isso significa que o isolamento geográfico dentro da US-EAST-1 (como o uso de múltiplas AZs) pode ter se tornado ineficaz, pois a falha não foi isolada a uma única máquina ou AZ, mas à capacidade fundamental de encontrar e se comunicar com os recursos, independentemente de sua localização física dentro da região, vazando para outras regiões geográficas, multiplicando o problema.

4.3. Caminhos para a Resiliência Futura: A Necessidade de Diversificação

A análise da falha na AWS em outubro de 2025 reforça um princípio negligenciado na era da alta conveniência da nuvem: a diversificação é a única proteção contra falhas sistêmicas em provedores centrais. O incidente demonstrou que a confiança excessiva na redundância dentro de um único ecossistema de nuvem pode levar à ilusão de segurança, especialmente quando a falha reside em um serviço de infraestrutura fundamental (como o DNS) que impacta múltiplas camadas de serviço.

4.3.1. A Estratégia Multi-Cloud

Para mitigar o risco de concentrar num único provedor todos os sistemas da organização, a literatura acadêmica e as melhores práticas de mercado apontam para a adoção de estratégias Multi-Cloud. Esta abordagem envolve a utilização ativa de serviços de pelo menos dois provedores distintos (e.g., AWS e Azure). A lição para as organizações é que a continuidade de negócios exige que as cargas de trabalho mais críticas (como autenticação e serviços transacionais) sejam arquitetadas para operar em ambientes isolados entre diferentes provedores. A falha da AWS evidencia que, para serviços de core business, a redundância regional não é suficiente; a redundância entre fornecedores é obrigatória.

O Gartner aponta ainda que há uma tendência entre as grandes empresas de adotarem soluções que incluam nuvens híbridas, em que uma parte da infraestrutura funciona em cima de uma nuvem privada, da própria empresa, e outra na nuvem pública,

oferecida por um ou mais provedores. O mercado de armazenamento em nuvem híbrida abrange diversos padrões de implementação com tecnologias subjacentes que endereçam uma ampla variedade de tipos de dados. Os produtos neste mercado devem facilitar serviços de dados contínuos (seamless) por meio de de diferentes ambientes, incluindo datacenters distintos, locais de co-localização (“collocations”), locais de borda (edge locations) e infraestrutura de nuvem pública. As soluções de dados em nuvem híbrida são oferecidas por vários meios, como infraestrutura híbrida distribuída (DHI), plataformas de armazenamento em nuvem híbrida, dispositivos de transferência de dados, soluções hiper convergentes, arrays de armazenamento, produtos de software-defined storage (SDS) e softwares abrangentes de gerenciamento de dados. (Gartner, 2025)

4.3.2. Arquiteturas Cloud-Agnostic

A viabilidade de uma estratégia Multi-Cloud depende da adoção de arquiteturas cloud-agnostic (independentes de um provedor específico). Conforme evidenciando anteriormente, isso implica no desenvolvimento de sistemas que evitam o uso de APIs proprietárias e serviços de gerenciamento exclusivos de um provedor principal. Tal design confere a flexibilidade necessária para realizar migrações rápidas ou failover em tempo real entre plataformas, um passo crucial que muitas aplicações atuais ainda não completaram.

4.3.3. Implicações para os Provedores de Nuvem

Esse evento impõe uma nova responsabilidade aos próprios provedores. A expectativa de resiliência do mercado não pode mais se limitar à robustez de uma única região. A falha sistêmica na US-EAST-1 sinaliza que os provedores dominantes precisam reavaliar a arquitetura de seus serviços fundamentais (como DNS, gerenciamento de identidade e serviços de storage básicos). A longo prazo, a verdadeira resiliência global pode exigir que os provedores trabalhem com padrões de redundância que cruzem os limites de suas próprias regiões ou que garantam uma separação mais estrita entre as camadas de controle e as camadas de aplicação do cliente.

CONSIDERAÇÕES FINAIS

Este artigo teve como objetivo geral analisar o "Apagão Digital" de 20/10/2025, investigando a propagação da falha originada na AWS US-EAST-1 e avaliando as lições aprendidas para a resiliência da infraestrutura de nuvem global. A análise confirmou que, apesar dos avanços em Governança de TI e dos mecanismos de tolerância a falhas

embutidos na nuvem, a dependência de um único provedor para funções críticas expõe as organizações a riscos sistêmicos inaceitáveis.

Os achados demonstram que a falha em um componente transversal, como o serviço de DNS para o DynamoDB, comprometeu a eficácia de soluções de resiliência de nível superior, como health checks e failovers automáticos. Esse evento ressalta a fragilidade inerente à confiança na abstração de infraestrutura: quando a camada mais fundamental falha, a resiliência contratada pelo cliente torna-se irrelevante.

Sendo assim a principal lição extraída é a necessidade imperativa de mover a estratégia de resiliência corporativa de um modelo puramente reativo (esperar que o provedor resolva) para um modelo proativo de diversificação. A adoção de estratégias Multi-Cloud e o investimento em arquiteturas cloud-agnostic — que permitem a migração de serviços críticos entre plataformas — deixam de ser um diferencial competitivo e se consolidam como uma exigência mínima para a continuidade de negócios na economia digital moderna. Como desdobramento, impõe-se também aos grandes provedores a responsabilidade de garantir que seus serviços de controle e endereçamento sejam resilientes até mesmo contra a falha catastrófica de uma região inteira.

Pesquisas futuras devem focar na quantificação do custo-benefício da adoção Multi-Cloud e no desenvolvimento de padrões de interoperabilidade para facilitar a migração de dados e serviços em cenários de falha de provedor em larga escala.

REFERÊNCIAS BIBLIOGRÁFICAS

RICHTER, Felix. The Big Three Stay Ahead in Ever-Growing Cloud Market: Cloud Infrastructure Market. 21 ago. 2025. Statista. [S.l.]. Disponível em: https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers. Acesso em: 21 out. 2025.

ITIL-AXELOS. ITIL Foundation. 1. ed. Londres: TSO, 2019. Disponível em: https://www.itil.com/. Acesso em: 21 out. 2025.

EXAME. O calcanhar de Aquiles da internet: por que a região US-EAST-1 da AWS ainda causa tantos problemas? [S.d.]. Exame.com. Disponível em: https://exame.com/tecnologia/o-calcanhar-de-aquiles-da-internet-por-que-a-regiao-us-east-1-da-aws-ainda-causa-tantos-problemas/. Acesso em: 21 out. 2025.

AMAZON WEB SERVICES (AWS). O que é o Amazon DynamoDB?. [S. l.], [2025?]. Disponível em: https://docs.aws.amazon.com/pt_br/amazondynamodb/latest/developerguide/Introduction.html. Acesso em: 21 out. 2025.

G1. Apagão na Amazon: o que se sabe sobre a pane que afetou apps e serviços no mundo todo. 20 out. 2025. G1. Rio de Janeiro: Globo.com. Disponível em: https://g1.globo.com/tecnologia/noticia/2025/10/20/apagao-na-amazon-o-que-se-sabe-sobre-a-pane-que-afetou-apps-e-servicos-no-mundo-todo.ghtml#instabilidade. Acesso em: 21 out. 2025.

GARTNER. Market Guide for Hybrid Cloud Storage. [S.l.]: Gartner, 2025. Disponível em: