Zero Trust: O Papel da Observabilidade para Segurança em Nuvem

José Augusto de Jesus Júnior [#1], Robson de Oliveira Albuquerque [#2]
[#]*Programa de Pós-Graduação Profissional em Engenharia Elétrica (PPEE; Departamento de Engenharia Elétrica, Campus Universitário Darcy Ribeiro; Universidade de Brasília (UnB), Asa Norte, 70910-900, Brasília/DF, Brasil*
#1 augusto.jose@aluno.unb.br
#2 robson@redes.unb.br

Resumo: Este artigo aborda a complexa relação entre confiança e a capacidade real de visibilidade que as organizações possuem em ambientes de nuvem pública. Enquanto analisa o funcionamento e entendimento atual sobre Zero Trust ele também discute sobre a real capacidade de observabilidade em uma nuvem e demonstra a percepção que as organizações possuem sobre a segurança de seus dados. O estudo identifica as ações concretas que alguns países realizaram em busca da preservação da sua soberania sobre os dados e discute as medidas que o Brasil já possui e que pode adotar para aumentar a segurança das suas informações estratégicas. Em seguida, mediante análise e discussões sobre os fatos que perpassam a segurança cibernética, confiança e Zero Trust, o artigo procura explicar que sem o estabelecimento de confiança por meio de um processo real de verificação contínua uma organização tende a tarefas repetitivas buscando satisfazer requisitos de compliance e confiando na análise de terceiros que podem não conhecer o negócio.

Palavras-chave: Zero trust, confiança, modelo de maturidade, nuvem computacional, observabilidade, zero trust architecture.

Abstract: This article addresses the complex relationship between trust and the actual visibility capabilities that organizations possess within public cloud environments. While analyzing the operation and current understanding of Zero Trust, it also discusses the real capacity for observability in a cloud and demonstrates the perception that organizations have regarding the security of their data. The study identifies concrete actions that some countries have taken in pursuit of preserving their data sovereignty and discusses the measures that Brazil already has in place and those it could adopt to enhance the security of its strategic information. Subsequently, through analysis and discussion of facts encompassing cybersecurity, trust, and Zero Trust, the article seeks to explain that without the establishment of trust through a genuine process of continuous verification, an organization tends toward repetitive tasks, seeking to satisfy compliance requirements and relying on third-party analyses that may not understand the business.

Keywords: Zero trust, trust, maturity model, cloud computing, observability, zero trust architecture.

I. INTRODUÇÃO

Segurança em nuvem para ser considerada efetiva deve ser composta de políticas, controles, tecnologias, sistemas, dados, dispositivos e pessoas devidamente alinhados, suportados e embasados por uma política de segurança que, por sua vez, devem ser aderentes a um framework. Esse framework deve considerar as ameaças e oportunidades do negócio e do ambiente em que a instituição está inserida. Nesse sentido, um modelo de segurança consistente não deriva de paredes e perímetros impenetráveis, mas sim de uma visibilidade profunda e contínua dos fluxos e relacionamentos dos dados ao longo das redes e sistemas. Ao analisar esses aspectos, entende-se que uma arquitetura de segurança deve considerar conceitos e práticas que englobam um modelo de segurança como o Zero Trust, que foi desenhado para o ambiente de nuvem computacional e permite estabelecer múltiplos critérios para alcançar um nível de confiança que redefine e eleva a proteção dos ativos e acessos em uma nuvem.

Muitas organizações estão levando seus dados e sistemas para os diversos provedores de nuvem existentes, mas a falta de um entendimento e de um acompanhamento efetivo do que é realizado com cada um destes dados se desdobram em riscos que devem ser avaliados sob a perspectiva do controle e soberania das informações e da continuidade dos serviços utilizados pela sociedade.

Por este motivo, propõe-se que a observabilidade do que de fato ocorre nas infraestruturas de nuvem não deve ser vista somente como um componente do modelo de segurança Zero Trust ou uma capacidade que sinaliza o nível de maturidade em cibersegurança, mas sim como uma premissa para a fundação e sustentação dos pilares de uma arquitetura de segurança moderna, dando o real sentido à filosofia de nunca confiar e sempre verificar.

Nesse contexto, este artigo discute a filosofia de Zero Trust e os conceitos fundamentais associados à sua implementação, ao mesmo tempo que demonstra as características de uma arquitetura de nuvem e destaca a necessidade de compreender os riscos de não gerenciar e não monitorar os dados armazenados em provedores de nuvem pública.

As principais contribuições deste trabalho envolvem dois pontos principais:

a) Esclarecer que as organizações não possuem capacidade real de acesso, monitoria e observabilidade completa ambientes de nuvem pública;
b) A necessidade de um processo prático que oriente a implementação da arquitetura Zero Trust;

Este artigo está organizado conforme se segue. Após essa breve introdução, o capítulo II apresenta o referencial teórico sobre os conceitos relacionados ao tema do artigo, no capítulo III são discutidos os problemas de observabilidade em nuvem,

no capítulo IV são apresentadas as soluções para os problemas identificados e o capítulo V conclui demonstrando os benefícios alcançados e sugerindo trabalhos futuros.

II. REFERENCIAL TEÓRICO

Esse capítulo apresenta os conceitos dos temas relevantes para compreender confiança, nuvem e Zero Trust. Ao conceituar confiança é possível compreender como ela é estabelecida sob a ótica humana até ser organizada em um processo computacional. Em seguida demonstra o funcionamento de uma nuvem e a sua organização em camadas. A conceituação é finalizada ao apresentar os conceitos associados à Zero Trust e as características técnicas da sua implementação.

Para compreender sobre Zero Trust é preciso antes identificar sua origem e organizar os principais conceitos relacionados ao tema, esta análise facilita o entendimento sobre sua estrutura e fundamentos. Uma abordagem de Zero Trust em nuvem é concretizada por meio de uma Zero Trust Architecture [1] e avaliada através de um Zero Trust Maturity Model [2], que, são interdependentes e fundamentais para o entendimento, planejamento e uma implementação bem-sucedida de um modelo de segurança adequado e eficaz para infraestruturas modernas.

A necessidade de organizar um modelo de segurança da informação que se difere das abordagens tradicionais já era discutida por outros pesquisadores antes da consolidação do Zero Trust, a publicação *A Layered Trust Information Security Architecture* (TISA) [3] demonstra que as plataformas de segurança existentes já não conseguiam tratar os diversos aspectos do uso da informação. A sua organização em camadas que se apoiam em um pilar de confiança permitiu compreender a importância de integrar todos as dimensões de uma informação. Como resultado desta organização, foi possível compreender que a confiança não é alcançada por meio de apenas um dos componentes e aspectos do dado, mas somente com a integração e verificação contínua de cada camada envolvida no seu armazenamento, processamento ou transporte.

Com a popularização na oferta de serviços na internet a utilização de ambientes de nuvem foi impulsionada devido à sua praticidade, a consequência foi a criação de novos serviços e a migração de muitos sistemas que até então eram hospedados e consumidos apenas internamente nas organizações, esta necessidade de acesso externo desencadeou a migração tanto de infraestruturas quanto de aplicações e dados até então locais para Data Centers e provedores de serviço distribuídos geograficamente.

Este movimento obrigou a adequação dos provedores – seus sistemas, serviços, funcionários, fornecedores e infraestruturas – e a redefinição de conceitos, tecnologias, políticas e normativos de verificação e conformidade para que eles obtivessem a confiança necessária para oferecer seus serviços para empresas e governos.

Com o tempo, empresas e governos passaram a utilizar este modelo de serviço em larga escala e, conscientes ou não, passaram a confiar nos provedores. Mesmo sem entender claramente os riscos e desafios envolvidos para garantir a segurança dos seus dados e aplicações que agora estavam em uma nuvem remota e desconhecida.

A. Confiança

Para entender confiança ao utilizar uma tecnologia, é necessário antes compreender como ela é vista sob uma ótica mais interna e pessoal. Para o ser humano, a confiança [4] é um nível de probabilidade subjetiva de cada indivíduo ao avaliar outra pessoa ou grupo. Ela não é um sentimento cego, mas está associada ao cálculo de risco que consiste em identificar e determinar a possibilidade do outro indivíduo, especialmente em ocasiões em que não há monitoramento, agir de maneira favorável, indiferente ou desfavorável, para que a partir daí seja possível iniciar uma cooperação.

Este risco só está presente porque os agentes envolvidos possuem a liberdade de decepcionar ou de trair, exigindo que eles estabeleçam meios para medir e gerenciar os riscos envolvidos na decisão de iniciar e manter a confiança. Por isso, é comum iniciar a confiança utilizando frações menores ou menos significativas, até que ela possa progredir e alcançar um nível satisfatório.

Decidir confiar consiste em realizar uma análise de risco subjetiva que resulta em uma escala que pode ser medida entre desconfiança completa e confiança completa, é o resultado desta análise que irá justificar o início, perda ou retrocesso da confiança no individuo ou grupo. Para Gambetta [4], estabelecer confiança se torna uma aposta baseada em reputação, familiaridade ou crença.

Ao analisar confiança utilizando um ambiente de tecnologia, Cofta [5] considera que a confiança humana pode ser modelada de uma maneira algorítmica, tornando-a, portanto, em uma confiança computacional. Este conceito permite associar que a confiança é definida como um mecanismo racional de autopreservação, através do qual um sistema, seja ele um indivíduo ou uma organização, opta por minimizar o risco à sua própria existência através da gestão da sua complexidade interna.

Neste caso, em vez de ser primariamente uma avaliação da confiabilidade de um terceiro, a confiança é conceituada como uma decisão estratégica desencadeada pela necessidade de um confiante – *trustor* – em reduzir a sua "carga computacional" interna. Por isso, quando a complexidade de um sistema se aproxima de um nível insustentável – ameaçando a sua capacidade de responder ao seu ambiente e, em última análise, a sua integridade – ele pode optar por exportar parte dessa complexidade para outro sistema, o confiável – *trustee*.

Essa decisão de confiar não é um ato cego ou puramente instintivo, mas o resultado de um cálculo que visa selecionar a opção de menor risco global. Em muitos casos, a decisão de confiar envolve considerar elementos como complexidade interna, risco para si próprio ou até mesmo o risco de não confiar e ter de enfrentar as consequências sozinho.

O sistema – um indivíduo ou organização – avalia se o risco combinado de delegar uma tarefa, considerando as probabilidades de sucesso e de quebra da confiança, é menor

do que o risco de uma falha interna por sobrecarga de complexidade. Assim, a confiança manifesta-se como o comportamento externo de se tornar vulnerável a outro, impulsionado por uma necessidade interna de sobrevivência.

Essa perspectiva é particularmente útil para explicar fenômenos aonde a confiança parece desafiar a lógica da escolha, como a confiança em monopólios ou em entidades tidas como pouco confiáveis, sob a argumentação de que, sob certas condições de pressão interna, confiar pode ser uma ação mais racional para a autopreservação do que decidir simplesmente por não confiar em alguém.

Por estar associado a culturas e crenças, o conceito de confiança é naturalmente mais próximo ao ser humano, e justamente por isto, a busca por esclarecer e estruturar uma visão de confiança é o que permite modelar um processo humano em um algoritmo que possa estabelecer um modelo de confiança computacional.

De modo similar ao que acontece com o comportamento humano, estabelecer confiança é gerenciar risco [6]. Portanto, espera-se de um modelo computacional que no momento que ocorre a quebra da confiança ou o comprometimento de um dos elementos que a sustentam, haja a garantia de que os outros agentes não se tornem uma vulnerabilidade, caso contrário, deve-se assumir que todos os envolvidos não são mais confiáveis.

Essa premissa permite estabelecer que se a confiança for quebrada, ela volta para seu estado inicial – zero, sendo necessário recomeçar todo o processo de validação.

B. Nuvem

A utilização de ambientes de nuvem computacional, também conhecida como nuvem, exige a compreensão do conceito, composição e funcionamento do próprio ambiente. Quando observadas sob a ótica do usuário, uma nuvem computacional pode ser abstraída em serviços que são consumidos de maneira simples e dinâmica. Mas ao analisar estas características com o olhar dos provedores e fornecedores envolvidos é possível identificar a sua complexidade e necessidade de integração com diversos sistemas que trabalham de maneira distribuída e coordenada.

A computação em nuvem é definida [7] como um modelo criado para oferecer e consumir serviços por meio de qualquer dispositivo com conectividade de rede, o acesso a esses serviços não exige conhecimento avançado nem configurações complexas e é realizado sob demanda, sem que seja necessário aguardar aprovações ou processos manuais. Os recursos de computação existentes são compartilhados e podem envolver desde as camadas mais inferiores como rede, processamento e armazenamento até as camadas mais superiores como sistemas operacionais, aplicações e serviços. Todos eles são provisionados de acordo com a necessidade de utilização, funcionando com a elasticidade esperada para cada recurso envolvido.

As características essenciais de uma nuvem computacional podem ser vistas em todos os modelos de serviço (Fig. 1) e de implantação [7]. A utilização de cada um destes modelos impacta em como a nuvem será gerenciada, no nível de acesso dos usuários e na capacidade de observabilidade dos dados processados dentro do ambiente.

Ao optar pela utilização de uma Nuvem Privada, o controle da infraestrutura e dos sistemas se torna maior, consequentemente também eleva a capacidade de observabilidade do ambiente. Já ao utilizar uma Nuvem Pública, essa capacidade fica limitada ao provedor de nuvem que administra o ambiente.

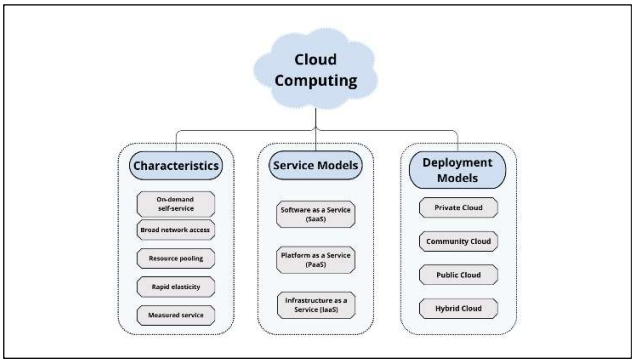

Fig. 1 - NIST: Computação em Nuvem

Em todos os cenários de nuvem previstos há a predominância de características que tornam estes ambientes dinâmicos, distribuídos e sem perímetro. É justamente a presença destes fatores que tornou legado os modelos de segurança até então baseados em uma rede local e em confiança implícita, tornando-os incompatíveis com a nuvem e com os serviços que ela fornece.

C. Zero Trust

O termo Zero Trust (ZT) aponta para uma mudança na forma de pensar segurança cibernética, reajustando o foco oriundo de um modelo baseado em confiança implícita – tudo que estava dentro do perímetro da rede era confiável – para um processo de confiança realizada com base em verificação contínua – independentemente de estar dentro ou fora da rede. Trata-se de uma filosofia de segurança que permite orientar decisões, políticas e práticas que alcançam todas as pessoas, ambientes, equipamentos e tecnologias envolvidas.

Sua lógica está baseada em uma premissa simples de compreender, porém complexa de implementar, a de que nenhum usuário, dispositivo ou sistema deve ser confiável por padrão, independente da sua localização geográfica, rede ou nível de acesso, mesmo para aqueles que em algum momento já foram considerados confiáveis.

Nela, os elementos envolvidos precisam percorrer todas as etapas pré-estabelecidas para que alcancem o status de confiável, este processo se repete infinitamente a cada necessidade de acesso e de maneira independente da permissão e da confiança recebidas anteriormente.

Considerar a metodologia humana de confiança [5] e que ela é uma camada transversal que sustenta os pilares de qualquer modelo de segurança [3], facilita a compreensão da filosofia ZT, pois elas reconhecem que para confiar é preciso antes verificar os agentes envolvidos. Uma vez estabelecido um

nível aceitável de confiança é concedido um privilégio mínimo e limitado, similar ao já analisado [4] nas relações humanas, que assume o fato de que diante do risco de decepção ou traição exige-se uma confiança estrita e limitada, pois, caso ela se confirme, os danos serão drasticamente reduzidos.

Para ZT tanto a crença humana quanto a incerteza residual da análise do risco não são aceitas. Assim, um modelo de segurança em nuvem com base nesta abordagem assume que uma violação de segurança já ocorreu ou que ela é iminente. Como resultado, cada acesso é tratado como uma ameaça em potencial e não possui autorização prévia, estabelecendo que nunca se deve confiar até que sejam realizadas todas as verificações computacionais necessárias.

Ela é resumida e amplamente conhecida pela expressão "*never trust, always verify*". Sua raiz aponta para o provérbio Russo "*доверяй, но проверяй -- Dovorey no provorey*" (*trust, but verify*) e foi popularizada no Ocidente por Reagan em 1987 durante as negociações do *Intermediate-Range Nuclear Forces Treaty*, segundo o acervo do Presidente [8], ele fazia o uso literal deste provérbio em alguns dos seus discursos daquele período.

A sua utilização no contexto de Segurança Cibernética tem início em 2010, quando um Analista desta área publica [9] que a expressão já conhecida "*trust, but verify*" seja alterada para "*verify and never trust*". Esta proposta fez com que nos anos seguintes os acadêmicos e as empresas de tecnologia adaptassem a afirmação para a expressão como a conhecemos hoje, "*never trust, always verify*".

Em 2021, já consolidada, ela passa a ser adotada como uma premissa de segurança para todo o Governo dos Estados Unidos [10] e consequentemente para diversas nações e organizações ao redor do mundo, que passavam a fornecer e consumir diversos serviços nuvem. Em 2024 é divulgado o *Federal Zero Trust Data Security Guide* [11], que aborda o nível tático da estratégia de implementação do ZT e atua na tradução dos princípios de alto nível em um roteiro prático e acionável para a mudança de paradigma fundamental do ZT. Agora a segurança passa a proteger os dados e abandona o antigo modelo de "castelo e fosso" focado no perímetro local e que não se adequa à realidade de computação em nuvem.

Devido à falta de alinhamentos e definições no início do ZT, havia muita dúvida sobre a sua gestão e operacionalização. Por este motivo, iniciativas como o estabelecimento de grupos de trabalho na *Cloud Security Alliance* (CSA) [12] e publicações específicas como as do NIST, permitiram o amadurecimento por meio da definição [1], organização [2] e orientação [11] de um modelo de segurança moderno para os serviços em nuvem.

Desde o seu surgimento até a sua consolidação, a filosofia de ZT busca romper com a ideia de perímetros confiáveis e de redes internas seguras, substituindo-a por uma confiança condicional e dinâmica, justificada em evidências coletadas e analisadas em tempo real. O foco passa a ser a proteção de recursos ao invés de segmentos de rede, orientado para minimizar a incerteza na aplicação de permissões de acesso e na concessão de privilégios mínimos, considerando que qualquer ambiente de nuvem já está comprometido.

Por apresentar conceitos, valores e premissas de uso seguro da nuvem, o ZT não fornece um modelo prático de implementação, mas permite adotar uma postura cética de segurança antes mesmo da aquisição dos produtos e tecnologias necessários para a implantação de uma arquitetura de segurança moderna.

Como não é um produto único, mas sim uma estratégia de cibersegurança, a sua efetivação e utilização em um ambiente cibernético depende da adoção de frameworks, arquiteturas e de maturidade organizacional, que variam conforme a tecnologia, cultura e orçamento de cada instituição, mas que não podem ser negligenciadas.

D. Zero Trust Architecture

Uma Zero Trust Architecture (ZTA) [1] consiste em um guia que auxilia na materialização dos princípios de Zero Trust em uma arquitetura de segurança concreta e focada em componentes, processos e fluxos técnicos. Seu objetivo é fornecer um conjunto de orientações para a criação de um plano prático e estruturado que pode ser aplicado por uma organização que deseja proteger os seus recursos.

Ao estabelecer uma ZTA, uma organização estará planejando a implementação de um plano de segurança cibernética utilizando os conceitos de ZT, enquanto analisa e projeta os relacionamentos dos seus ativos, fluxos de trabalho e políticas de acesso.

Em uma ZTA existem sete princípios fundamentais:

1) Todas as fontes de dados e serviços de computação são consideradas recursos;
2) Toda a comunicação deve ser segura, independentemente da localização da rede;
3) O acesso a recursos empresariais individuais é concedido por sessão;
4) O acesso aos recursos é determinado por políticas dinâmicas;
5) A organização monitora e mede a integridade e a postura de segurança de todos os ativos próprios e associados;
6) Toda a autenticação e autorização de recursos são dinâmicas e estritamente aplicadas antes que o acesso seja permitido, em um ciclo contínuo de avaliação;
7) A empresa coleta o máximo de informações possível sobre o estado atual dos ativos, infraestrutura de rede e comunicações para melhorar sua postura de segurança;

Cabe destacar os princípios cinco (5) e sete (7), pois eles estão diretamente relacionados ao "Papel da Observabilidade para Segurança em Nuvem" e podem ser diretamente associados ao trecho "*always verify*" da filosofia ZT. Sem eles, todos os outros se tornam ineficientes, pois a coleta e monitoria dos ativos e comunicações é justamente o que permite validar se os outros princípios estão sendo atendidos.

Ao optar pela implementação de uma ZTA, a organização poderá seguir três (3) abordagens principais de execução. Em todas elas (Tabela I) há a presença de componentes lógicos (Tabela II), sendo que uma arquitetura completa possivelmente irá incluir elementos de cada uma delas e é

particularmente adequada para organizações que possuem alguma das características citadas (Tabela III).

Tabela I - Abordagens de Execução de uma ZTA [1]

ZTA - Abordagens	
Enhanced Identity Governance	Utiliza a identidade dos atores como o componente chave para a criação de políticas.
Micro-Segmentation	Isola recursos individuais ou grupos de recursos em segmentos de rede únicos, cada um protegido por um gateway de segurança (PEP).
Network Infrastructure and Software Defined Perimeters (SDP)	Utiliza a infraestrutura de rede, como uma rede de sobreposição, para implementar a ZTA, onde o PA atua como um controlador de rede.

Tabela II - Componentes Lógicos de uma ZTA [1]

ZTA - Componentes Lógicos		
Plano de Controle	Policy Engine (PE)	Responsável pela decisão final de conceder, negar ou revogar o acesso a um recurso.
	Policy Administrator (PA)	Estabelece ou encerra o caminho de comunicação entre um sujeito e um recurso. É quem executa a decisão do PE.
	Policy Decision Point (PDP)	É formado pelo Policy Engine (PE) e pelo Policy Administrator (PA).
Plano de Dados	Policy Enforcement Point (PEP)	Responsável por habilitar, monitorar e, eventualmente, encerrar as conexões entre um sujeito e um recurso.

Por causa do papel que desempenha, o PDP é inútil sem informações e a sua capacidade de decisão é tão boa quanto os dados que recebe. Por este motivo, a observabilidade se torna o sistema nervoso central da arquitetura, já que não é possível verificar as características e o comportamento de um dispositivo, rede ou usuário sem dados em tempo real sobre seu estado e ações.

Tabela III - ZTA: Características das Organizações [1]

ZTA - Características das Organizações
Utilização de estruturas com filiais remotas que se conectam via links dedicados (MPLS).
Contratação de dois ou mais provedores de nuvem (multi-nuvem) para hospedar aplicações, serviços ou dados, a necessidade de conceder acesso limitado à recursos para visitantes e prestadores de serviço contratados.
Empresas que oferecem serviços voltados ao público que podem ou não exigir registro e autenticação de usuários.

Existem outros cenários possíveis que justificam a adoção de uma ZTA, mas em todos eles a confiança passa a ser estabelecida com base em uma política automatizada que é executada diante de fatos evidentes e somente após a análise de dados obtidos em tempo real.

Ao considerar que não se confia mais em nenhum dos componentes e acessos sem que antes tenham sido verificados, o uso da expressão "*never trust*" não implica em afirmar que a confiança foi eliminada, mas que ela deixou de ser implícita e herdada, sendo transferida dos *endpoints*, sistemas, redes, senhas e locais físicos para os componentes da própria ZTA.

Consequentemente, é importante realizar uma análise crítica e compreender que não basta confiar na ZTA e nos seus mecanismos de validação, pois, caso seja feito, esta seria apenas a transferência do risco para um conjunto de sistemas, retornando ao conceito de confiança subjetiva citado.

Assim, a maneira mais adequada de alcançar confiança utiliza uma avaliação de risco [6] dinâmica e alicerçada em evidências obtidas por meio da observabilidade contínua, não se limitando à verificação executada automaticamente pelos componentes da arquitetura, mas acompanhando como as estruturas de decisão são executadas e qual a legitimidade das informações que subsidiaram a obtenção de confiança.

E. Zero Trust Maturity Model

O Zero Trust Maturity Model (ZTMM) [2] fornece um guia prático para auxiliar as agências federais dos Estados Unidos a planejar e executar a implantação de uma Arquitetura de ZTA.

Ele está alinhado às etapas de transição para o ZT do NIST e por não ter sido criado como um conjunto rígido de requisitos, pode ser utilizado como um guia para apoiar diversas organizações na transição progressiva para uma postura de segurança moderna em ZT.

Este modelo de maturidade é estruturado em cinco pilares – identidade, dispositivos, redes, aplicações com suas cargas de trabalho e dados. Todos são apoiados e integrados por três capacidades transversais – visibilidade e análise, automação com orquestração e governança – que, conforme destacado na Fig. 2, suportam os pilares e permitem que eles se comuniquem de maneira eficiente.

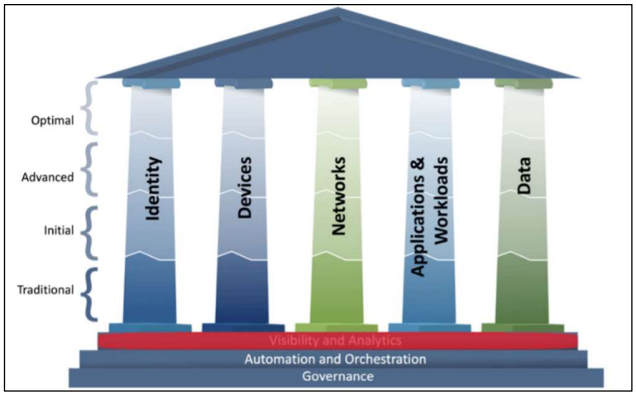

Fig. 2 - CISA: Pilares e Maturidade em ZT [2] (adaptada)

Uma organização que opta pela implementação de um ZT pode analisar seu estágio de maturidade (Tabela IV) e iniciar a sua jornada para alcançar o estado ideal.

A relevância do ZTMM é que ele é uma ferramenta de avaliação e planejamento que fornece um roteiro estruturado para auxiliar na tarefa de transição de uma segurança em perímetro para o modelo de segurança ZT, permitindo uma

implementação gradual enquanto auxilia na resposta às ameaças modernas.

Tabela IV - ZTMM: Estágios de Maturidade [2]

ZTMM - Estágios de Maturidade	
Tradicional	Processos manuais; Segurança baseada no perímetro; Monitoria focada em firewalls;
Inicial	Baixa automação; Presença de MFA; Segmentação de rede; Coleta reativa de logs;
Avançado	Existência de controles automatizados; Coleta de logs centralizada; Correlacionamento de dados; Alertas baseados em métricas; Investigações iniciais de segurança;
Ideal	Predominância de processos automatizados; Políticas de acesso "*just-in-time*" e "*just-enough*"; Decisões de acesso dinâmicas embasadas em telemetria e com privilégios mínimos; Análises de *machine learning* são aplicadas nos dados coletados para detectar ameaças de forma proativa; A segurança passa a ser um sistema adaptativo e otimizado;

Um modelo de maturidade em ZT transforma um conceito até então abstrato em um plano de ação concreto, permitindo que as organizações, independentemente do seu ponto de partida, evoluam sua postura de segurança de maneira lógica, mensurável e progressiva.

F. Conceitos Associados ao Zero Trust

Após a análise dos conceitos e referências associados a ZT é possível identificar que eles não são concorrentes, e sim camadas interdependentes que permitem formular uma estratégia de segurança em nuvem moderna e coesa.

A Tabela V é o resultado da análise e do correlacionamento das principais características de cada um dos componentes citados até então sobre ZT, ela consolida o entendimento e fornece um guia objetivo para a escolha e utilização de cada conceito associado.

Tabela V - Características dos Conceitos de Zero Trust

ZT - Características e Conceitos			
	ZT	ZTA	ZTMM
Conceito	Filosófico; Estratégico; Mindset; Princípios;	Blueprint; Framework Técnico; Modelo Lógico;	Ferramenta de Avaliação; Roadmap; Guia de Medição;
Objetivo Principal	Eliminar confiança implícita; Reduzir superfície de ataque; Assumir que a violação é inevitável;	Fornecer um guia; Projetar e construir um ambiente; Implementar os princípios de ZT;	Medir a postura de segurança atual; Guiar a implementação incremental; Justificar investimentos;
Foco	O que fazer; Por que não confiar; O que verificar;	Como fazer; Como os componentes, fluxos de dados e políticas interagem;	Quão madura é a implementação; O que fazer para evoluir;
Componentes Chave	Verificação explícita; Acesso com privilégio mínimo; Segmentação de rede; Presunção de violação;	Componentes lógicos; PE; PA; PDP; PEP; Fontes de dados (SIEM, logs, etc.);	Pilares; Capacidades Transversais;
Diferença Fundamental	Visão estratégica abstrata; Orienta todas as decisões de segurança; Agnóstico à tecnologia;	Projeto concreto; Permite construir o sistema; Tecnologias específicas;	Gerencia a jornada de construção e melhoria do sistema;

III. DISCUSSÃO DO PROBLEMA

Esse capítulo aborda a discussão do problema de observabilidade em nuvem e unifica todos os conceitos apresentados. Eles são utilizados para justificar a necessidade de adoção de um modelo de segurança para a nuvem. Em seguida discute as limitações técnicas que impedem a confiança em nuvem pública para os que buscam realizar a verificação contínua exigida pelo Zero Trust. Por fim, demonstra que mesmo grandes empresas e nações possuem desafios para executar o princípio de verificação contínua.

Toda nuvem é implementada provendo um ambiente de computação com propriedades como elasticidade, serviços criados e configurados pelo próprio usuário e alocação de recursos realizada sob demanda [7], ela também possui, obrigatoriamente um (1) modelo de implantação e um (1) ou mais modelos de serviço (Fig. 1).

Essas características não são um problema em si, pois oferecem ao usuário níveis de abstração que facilitam a administração de recursos tecnológicos e reduzem os custos associados com manutenção e evolução do ambiente.

Contudo, a capacidade de coleta e análise do que ocorre dentro deste ambiente é vista como um problema, pois é reduzida à medida que o nível de abstração aumenta, gerando obstáculos que afetam a capacidade das organizações para observar por conta própria se os seus dados estão sendo tratados na nuvem conforme o esperado.

Esses obstáculos foram identificados e organizados em tópicos, que permitem uma análise progressiva por meio de uma discussão encadeada dos problemas. Essa organização facilita a aplicação das soluções que buscam tratar as limitações de observabilidade em ambientes de nuvem.

A. *Camadas na Nuvem sem Observabilidade*

Em todas as suas implementações, uma nuvem possui camadas (Fig. 3) – aqui chamadas de inferiores – que são de acesso exclusivo de quem administra a infraestrutura necessária para o seu funcionamento. Elas realizam o armazenamento, processamento e transferência dos dados e são determinantes para que as camadas – aqui chamadas de superiores – possam utilizar e exibir as informações e aplicações desejadas. As camadas não caracterizam um problema, já fazem parte da arquitetura e sem elas uma nuvem não pode existir.

Mas ao optar por utilizar algum dos modelos de serviço (*IaaS, PaaS ou Saas* [7]) de nuvem, é necessário compreender que o acesso a estas camadas será diretamente afetado e irá comprometer a visibilidade do que ocorre no ambiente.

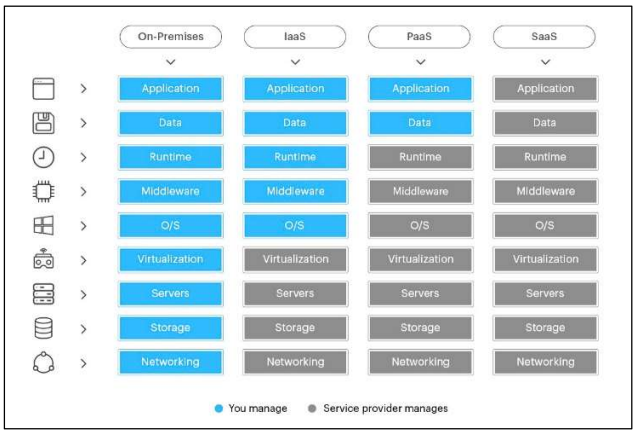

Fig. 3 - Camadas da Nuvem [13] (adaptada)

Apesar de existirem em qualquer nuvem, estas camadas inferiores nem sempre estão acessíveis ao usuário final, e por característica, elas sempre agrupam equipamentos e *softwares* de diversos fabricantes que funcionam sob licenciamento proprietário ou de *software* livre com código aberto. Essas camadas e seus componentes são parcialmente ou totalmente desconhecidas para diversas organizações que contratam um provedor de nuvem e principalmente para os usuários dos serviços oferecidos neste ambiente.

Em nuvens privadas, caracterizadas pela propriedade, gerência e uso exclusivo de uma única organização [7], os recursos de *hardware*, *software* e dados são hospedados localmente (*on-premises*) dentro de suas instalações. Este é o modelo tradicional de TI, que apesar de ser mais oneroso em diversos aspectos, permite acessar física e logicamente os componentes de cada camada – rede, armazenamento, servidor, virtualização, sistema operacional, APIs e sistemas, ambiente de execução de aplicações, arquivos ou bancos de dados e aplicações.

Neste modelo de nuvem local, é possível gerenciar, visualizar e coletar metadados, indicadores, telemetria e logs detalhados. Isto proporciona um conhecimento mais técnico do ambiente e permite que uma organização alcance maior observabilidade do que ocorre na sua nuvem.

Fatores como aquisição e manutenção de equipamentos, acompanhados de licenciamento e suporte de softwares, sistemas operacionais, bancos de dados, patches de segurança e serviços de TI geram altos custos ao optar por manter ambientes hospedados localmente, os valores aumentam ao considerar custos com equipes especializadas, energia, refrigeração e manutenção do espaço físico.

Estes custos impulsionam as organizações a migrarem toda ou parte das suas aplicações e serviços para nuvens públicas gerenciadas por um *Cloud Service Provider* (CSP), reduzindo seus gastos com infraestruturas e recursos locais e tornando transparente todo o trabalho necessário para manter a infraestrutura da nuvem ou o serviço contratado.

Em contrapartida, elas perdem a capacidade de acesso às camadas inferiores e consequentemente deixam de ter observabilidade destas camadas da nuvem.

B. *Legislações e Normativos*

Organizações que optam por manter ambientes *on-premises* são caracterizadas por serem altamente regulamentadas e por lidarem com informações sigilosas ou sensíveis, podendo ser tanto de governos – como setores estratégicos, órgãos de segurança ou de defesa – quanto informações relacionadas à intimidade de indivíduos – como dados financeiros, de saúde, de orientação política ou religiosa.

Nestes casos o foco está no controle absoluto das informações sob sua custódia, essas características exigem um nível de isolamento que somente ambientes computacionais de propriedade, gerência e uso próprio e exclusivo podem permitir.

Como estes dados se diferem dos outros pelo seu uso e pela sua essência, é preciso garantir que a sua residência e localização física sejam conhecidas e, em alguns casos, restritas ao perímetro da organização. Isto evita dúvidas sobre jurisdição legal – que apesar de ser possível, é muito complexo ao utilizar nuvens públicas – e permite definir políticas personalizadas para o acesso, manuseio e ciclo de vida da informação.

Dado a sua criticidade de custódia e residência dos dados, muitas organizações já operam sob alguma forma de controle regulatório, como a Lei Geral de Proteção de Dados (LGPD) [14] em conjunto com a IN nº 5/21 [15] no Brasil, na Europa estes dados estão protegidos pelo *General Data Protection Regulation* (GDPR) [16], já nos EUA a *Health Insurance Portability and Accountability Act* (HIPAA) [17] protege dados de saúde da população.

Por causa destas regulamentações os CSPs se adequaram para atender aos normativos de diversos países, criando processos de validação das suas infraestruturas e sistemas acompanhados de métodos de verificação e *compliance* [18] [19] [20] dos dados para cada uma destas normas.

Para as organizações sujeitas a essas regulamentações, é fundamental que seus provedores de nuvem e outros fornecedores de tecnologia permaneçam em conformidade e apliquem os métodos de proteção aos dados dos seus clientes, além de oferecer mecanismos claros de verificação e controle dos dados e dos seus acessos.

Apesar da existência de uma aprovação e da possibilidade de verificação dos relatórios de conformidade, o problema da legislação para a residência dos dados é a incapacidade de os usuários validarem a confiança nestes ambientes. Não há um método prático e visível para realizar a verificação do que é

realizado, restando "confiar" na conformidade (*compliance*) de cada fornecedor envolvido.

A legislação, apesar de existente, não garante que a organização que contratou a plataforma possua a capacidade de verificar que os seus dados estão sendo tratados de acordo com o normativo legal. Resta a eles confiarem na conformidade sem que tenham a observabilidade, mesmo em ambientes que afirmam possuir o ZT implementado.

C. Confiança em Nuvens Públicas

Organizações estratégicas de governo e instituições com atribuições singulares – como as da área financeira – ainda possuem dificuldade em confiar a custódia dos seus dados em nuvens públicas, mesmo as que oferecem métodos de segregação lógica de dados acompanhados de mecanismos de controle de acesso e auditoria. O *State of the Cloud Report* [21] concluiu que em 2024 a segurança (Fig. 4) ocupou o segundo lugar entre as preocupações dos gestores e usuários de serviços em nuvem.

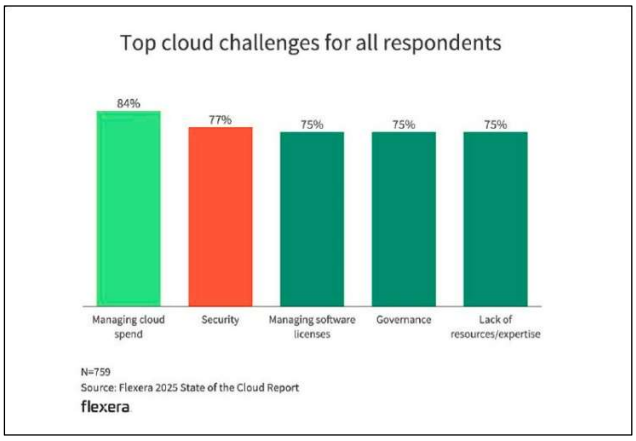

Fig. 4 - Nuvem: Principais Desafios [21] (adaptada)

Essa preocupação está associada ao controle, visibilidade e localização dos dados, resultado da custódia e gerenciamento do que é hospedado em uma infraestrutura de terceiros. Mesmo diante de acordos legais e mecanismos tecnológicos de *compliance* por parte dos CSPs, ainda permanece o fato das organizações precisarem conceder a custódia dos seus dados para provedores estrangeiros e sujeitos às legislações do seu país sede.

Apesar da certeza técnica que já existia sobre a real capacidade de acesso aos dados na nuvem, restava a dúvida sobre a capacidade legal. Ela foi esclarecida em 06/2025 durante um inquérito no Senado Francês que tratava justamente da soberania digital da União Europeia, aonde o representante de um provedor de nuvem pública afirmou "não poder garantir a soberania dos dados dos seus clientes" [22], devido à obrigação da sua organização em seguir o *CLOUD Act* [23] no seu país de origem.

Diante das certezas técnicas e legais sobre a capacidade de acesso aos dados, a segurança exigida para ambientes de nuvem – mesmo *on-premises* – caracterizados pela ausência de perímetro, pode ser alcançada utilizando uma arquitetura ZT [1], desde que seja realmente ajustada para atender ao princípio da verificação contínua. Visto que no ZT a confiança é obtida por meio de uma política automatizada e com dados coletados em tempo real.

Porém, essa confiança se torna difícil de ser alcançada em ambientes de nuvem pública, já que não é possível acessar as camadas inferiores que armazenam e processam dados de diversas organizações e os trafegam simultaneamente por meio de dispositivos compartilhados por toda a nuvem.

Ao considerar a capacidade de acesso às camadas da nuvem (Fig. 3) oferecida de acordo com o modelo de serviço utilizado, é possível afirmar que o acesso e o controle dos dados, em maior ou menor parte, é restrito ao CSP e se torna altamente limitado para o usuário ao optar pelo modelo *Software as a Service* (SaaS). Em contrapartida, à medida que se utiliza o modelo *on-premises*, o acesso e a coleta de dados se tornam mais completos.

Essa capacidade de acesso às camadas se refere à organização que contratou um provedor de nuvem, ela recebe permissão em uma interface para administrar e provisionar recursos e serviços. Essas tarefas são executadas por profissionais de TI da organização, com privilégios de administração e capacidade técnica para configurar e alocar os diversos tipos de recursos disponíveis. Para estes, ainda sim, todas as camadas inferiores não são visíveis nem gerenciáveis, só em ambientes *on-premises*.

Por este motivo, ao utilizar um ambiente de nuvem é necessário ter ciência não apenas das vantagens, mas das limitações técnica inerentes a este tipo de serviço. Que impedem a coleta, processamento e monitoria dos componentes físicos e lógicos (Fig. 3). Além da verificação do processo de obtenção de confiança realizado pelo ZT a cada acesso ou transação realizada nas diversas camadas.

D. Responsabilidade na Nuvem

Quando o usuário ou o provedor – CSP – falham na implementação ou na utilização das medidas de proteção em uma das camadas da nuvem, os seus dados podem ser expostos até mesmo para quem não possui a intenção de visualizá-los. Porém, a proteção destes dados não é responsabilidade apenas do provedor, os usuários também possuem responsabilidade pelo que armazenam na nuvem.

Contudo, os usuários da nuvem não possuem os acessos necessários para verificar onde suas informações estão "fisicamente" armazenadas, nem possuem permissão para observar como e por onde seus dados são trafegados e tratados neste ecossistema restrito aos CSPs.

Por este motivo, estes CSPs passaram a oferecer recursos de proteção por meio de controle de acesso e criptografia nativa dentro dos seus sistemas, o objetivo era para reduzir o risco de visualização e acesso indevido aos dados por terceiros.

Mas, uma vez superada a barreira de permissão de acesso, o usuário da nuvem não possui uma garantia real de que os seus dados não foram visualizados por algum dos recursos e pessoas que fazem parte deste ecossistema, já que ele não dispõe de um modo efetivo de monitoria dos acessos aos diversos dados existentes nestas camadas inferiores e mais especificamente aos dados que são de sua propriedade.

Por conseguir acessar somente as camadas superiores (Fig. 3), é responsabilidade do usuário tornar seus dados confidenciais por meio da utilização de uma criptografia forte. Este é o principal mecanismo de proteção disponível, pois se seus dados forem acessados ou capturados, ainda sim estarão protegidos contra visualização ou manipulação indevida.

Além da proteção dos seus dados em repouso, as organizações que contratam uma plataforma de nuvem também possuem o papel de garantir a segurança das suas informações, esta responsabilidade varia de acordo com o modelo de nuvem contratado.

Grandes provedores de nuvem – CSP – adotam um modelo de responsabilidade compartilhada [24] [25] [26], que segmenta a responsabilidade pelos dados de acordo com o serviço e modelo de nuvem contratado. Todos eles convergem para o fato da responsabilidade (Fig. 5) associada à organização que decidiu hospedar seus dados em um ambiente de nuvem pública.

Quem contrata algum destes serviços deve ter em mente que está transferindo, em maior ou menor parte, algumas das suas responsabilidades para o CSP e que elas variam de acordo com o modelo contratado – Iaas, PaaS ou SaaS. Além do fato de que, para exercer a sua responsabilidade, o CSP precisará realizar o acesso aos seus dados.

Logo, ao contratar uma nuvem pública com maior nível de abstração – SaaS – a organização aceita possuir menos visibilidade e gerência técnica do ambiente em troca da "comodidade" de não precisar administrar uma infraestrutura complexa, e concorda em transferir uma parte da sua responsabilidade ao CSP.

Em contrapartida, ao contratar uma nuvem de menor nível de abstração – IaaS – a organização passa a ter mais visibilidade e responsabilidade sobre os seus dados dentro do CSP e uma maior gerência técnica do ambiente.

Já ao optar por implementar de nuvem local (*on-premises*) toda gerência e responsabilidade ficam com o dono da nuvem.

Contudo, em nenhum dos cenários de utilização de nuvem pública, a organização está isenta da responsabilidade sobre o que insere neste ambiente e principalmente da obrigatoriedade de estabelecer meios para verificar se o CSP está cumprindo com o estabelecido.

Ao utilizar ZT, a responsabilidade de proteção do ambiente de nuvem e do controle de acesso aos dados só pode ser considerada real se esta confiança puder ser verificada.

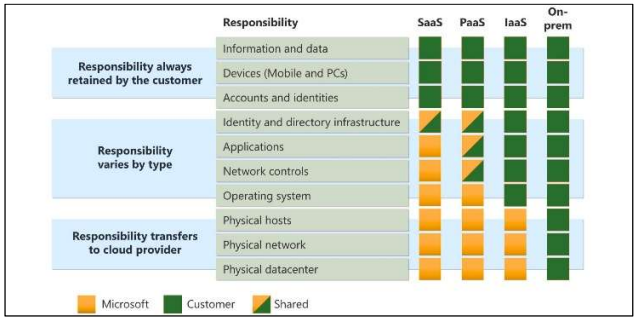

Fig. 5 - Microsoft: Responsabilidade Compartilhada [26] (adaptada)

E. Auditoria na Nuvem

Diante dos diversos dados hospedados nos CSPs, a consciência da necessidade de auditoria na nuvem possui um papel fundamental para que as organizações adotem uma postura proativa, deixando de apenas confiar nos controles e proteções – por mais eficientes que sejam – disponíveis e passando a enfrentar o desafio de verificar e auditar as ações realizadas no ambiente contratado. Esta necessidade se baseia no entendimento de que a responsabilidade nunca é exclusiva do CSP, e sim compartilhada (Fig. 5) entre quem contratou e quem é o provedor da nuvem.

Ações como verificar se o provedor contratado permite a realização de auditorias no seu ambiente, ou o planejamento de capacitação da equipe para realizar estas auditorias, demonstram a capacidade que uma organização possui de confiar na segurança de uma nuvem por meio da verificação e observabilidade.

Organizações como a ISACA possuem orientações e planos de capacitação que auxiliam na auditoria [27] de ambientes de nuvem, oferecendo desde políticas específicas [28] [29] para auditoria dos maiores CSPs até guias práticos para validar um modelo de segurança ZT já implementado.

A *Cloud Security Alliance* (CSA) [12], organização referência em ZT, também possui a *Cloud Control Matrix (CCM)* [30] que é organizada em 17 domínios que auxiliam na análise de segurança de um CSP e permitem que uma empresa possa elaborar, implementar e avaliar um programa de auditoria para gerenciar os controles da nuvem sob sua responsabilidade.

Ao implementar auditoria na nuvem a organização alcança outro benefício além da já esperada visibilidade, ela também se torna capaz de medir os custos (*FinOps*) e identificar desperdícios financeiros. Dados do *State of the Cloud Report* [21] apontam que gerenciar os gastos com a nuvem (Fig. 4) ainda é o principal desafio das organizações, que em 2024 observaram seus orçamentos ultrapassarem os 17% com provedores e serviços de nuvem justamente por causa da necessidade manter ativos os seus serviços já migrados e que muitas vezes poderiam ser mantidos com um custo menor.

Normas como a ISO 27017 [31] – que esclarece as responsabilidades de segurança entre o provedor de nuvem e o o contratante, e fornece controles e diretrizes específicos para a nuvem – e a ISO 27018 [32] – que possui foco em privacidade e proteção de informações de identificação pessoal (PII) em nuvens públicas – preenchem as lacunas que apoiam a auditoria de um ambiente de nuvem.

Para alcançar o ZT na nuvem, seja ela pública ou privada, é necessário compreender que a auditoria é o principal meio pelo qual se demonstra o entendimento da primeira parte da expressão – *never trust* – e pelo qual se valida a capacidade técnica de execução da segunda parte – *always verifiy.*

A auditoria também permite validar a eficácia das políticas implementadas no plano de controle por meio o PDP (Tabela II) e identificar como elas respondem às tentativas de acesso não autorizadas, o foco deixa der ser o perímetro e passa a ser a auditoria de cada transação.

Ao adotar este modelo de segurança, quanto melhor a auditoria mais fácil será comprovar que a verificação obrigatória em ZT está sendo realizada e mais efetiva será a coleta e observabilidade dos acessos, identidades, permissões, dados, APIs e suas conexões em uma nuvem.

A auditoria contribui diretamente para o aumento da conformidade do que é realizado na nuvem e garante que a verificação não é apenas uma ideia, mas uma realidade comprovável.

IV. PROPOSTA DE SOLUÇÃO

Esse capítulo apresenta as soluções para os problemas identificados e justifica a necessidade de adoção de um modelo de segurança em nuvem. O objetivo é alcançar o real controle e observabilidade dos dados para garantir que os princípios de Zero Trust sejam aplicados.

A. Gestão de Segurança com Zero Trust

A definição e adesão a um Sistema de Gestão da Segurança da Informação (SGSI) conforme orienta a ISO 27001 [33], permite elevar a maturidade e a gestão da segurança de uma organização.

Mas, conforme demonstrado anteriormente, atingir conformidade com normas e relatórios de *compliance* não é suficiente para garantir segurança. Estar aderente à normas é importante, mas elas fornecem um retrato estático da aderência a controles prescritos e revela que a segurança real não se alcança somente com a conformidade, ela exige capacidade dinâmica de enxergar, interpretar e reagir a eventos no ambiente.

Um SGSI para sistemas e infraestruturas em nuvem que não considera princípios de ZT até pode garantir conformidade, mas prescinde de eficácia prática na detecção e resposta a ameaças modernas. Por outro lado, uma implementação de ZT sem um SGSI pode gerar uma proteção fragmentada, sem governança e sem alinhamento estratégico.

Consequentemente, ao integrar um SGSI com um modelo de segurança focado em ZT, a organização alcança uma solução que implementa aspectos maduros de governança e de gestão de riscos. Ao mesmo tempo, considera requisitos dinâmicos e contínuos de segurança que permitem um alinhamento com o cenário real de ameaças enfrentadas pela organização.

B. Nuvem Local com Verificação Contínua

Devido às diversas camadas existentes em uma infraestrutura de nuvem pública, o alcance da verificação contínua proposta pelo ZT deve ser analisado com profundidade pelas organizações que lidam com dados sensíveis e temas relacionados à soberania nacional.

Por caraterística, uma nuvem tem necessidade de abstrair suas diversas camadas e entregar serviços de forma transparente sem que seus usuários precisem entender ou sequer conhecer o ambiente que os mantêm.

Ao utilizar nuvens públicas, empresas e agências de governo devem compreender o real o alcance da verificação contínua proposta pelo ZT, já que as camadas mais inferiores e a capacidade de coleta e visualização dos dados contidos nelas estão restritas aos CSPs e são inacessíveis para qualquer organização, até mesmo para um outro país com capacidade financeira e legal de requisitar este acesso.

Portanto, uma organização que não tenha a capacidade legal e principalmente técnica de observar o uso dos dados em todas as camadas – principalmente as que são invisíveis aos usuários e estão fora do alcance de uma auditoria independente – não possui de fato o controle dos seus dados e a garantia da observabilidade completa de como suas informações são tratadas por terceiros.

Diante da impossibilidade da análise do tratamento dos seus dados, mesmo àqueles armazenados em Data Centers no país, as organizações não podem adotar o comportamento de "confiar sempre" nos sistemas, políticas e legislações impostas. Tampouco no nível de *compliance* dos provedores de serviço e das soluções de terceiros, pois por mais sérias e capazes que sejam, elas não oferecem a garantia de uma efetiva, literal e completa verificação do acesso e tratamento dos seus dados em um ambiente que não permite acesso às suas camadas inferiores. A confiança nestes casos se mostra mais como uma "acreditação" e não uma real aplicação do conceito *Never Trust, Always verify*.

O alcance do princípio fundamental do Zero Trust se torna factível ao ter sob o seu domínio e custódia todas as camadas envolvidas no processamento, armazenamento e trânsito das informações.

Por este motivo, declarações como a ouvida pelo Senado Francês [22] confirmam a impossibilidade de garantir que os dados de um país não sejam ser entregues a outro. Logo, é possível afirmar que não há como uma nação exercer a sua soberania [34] enquanto permitir que provedores externos possuam a custódia e o acesso aos seus dados. Existem sérios riscos em avançar na dependência de empresas e órgãos estrangeiros para manter e regular informações nacionais.

C. Guia Prático sobre Zero Trust

Os EUA publicaram uma série de normativos [1] [10] [35] [2] [11] que permitiram fornecer uma direção estratégica acompanhada de uma orientação prática para a implementação de ZT. Ao tomar essa ação, o país habilitou suas agências de governo e a iniciativa privada para requisitarem dos seus parceiros de negócio controles e ações específicas de ZT que demonstrem o foco na proteção do novo perímetro imposto pelas arquiteturas de nuvem.

De modo semelhante, Singapura também publicou o normativo *Government Zero Trust Architecture* (GovZTA) [36], que fornece uma estrutura para todo o governo implementar ZT. Ao reconhecer o impacto financeiro e o crescimento dos ataques cibernéticos aos serviços do governo, o país optou por elevar a postura de segurança cibernética de todas as suas agências governamentais. A arquitetura proposta possui quatro princípios-chave, cinco pilares técnicos e dois facilitadores associados com governança, todos eles têm como base os conceitos já conhecidos de uma ZTA [1] e de um ZTMM [2].

Já o governo do Reino Unido identificou 8 princípios e publicou o guia *Zero trust architecture design principles* [37] com as definições de uma ZTA e orientações para que os setores público e privado possam desenhar e implementar internamente cada princípio.

De maneira similar, o Canadá divulgou sua diretriz de segurança cibernética *Zero Trust security model* [38] e utilizou os conceitos do NIST [1] e do CISA [2] como parte de sua política de conscientização para as agências de governo.

Em ambos os casos, as publicações não possuem um papel normativo para as agências do governo, atuando mais como uma recomendação.

No Brasil, a Estratégia Nacional de Governo Digital [39] surgiu para guiar a modernização dos sistemas de governo.

Diversas agências do governo que passam por essa transformação digital também já contam com o Programa de Privacidade e Segurança da Informação (PPSI) [40], criado pela Secretaria de Governo Digital (SGD) do Ministério da

Gestão e da Inovação em Serviços Públicos (MGI). Este programa oferece grupos de controle que permitem elevar a segurança e a privacidade e contribuem significativamente para a maturidade de segurança em todo o governo.

Já a Estratégia Nacional de Cibersegurança - E-Ciber [41] cita necessidades como:

- Elaborar um modelo nacional de maturidade em cibersegurança;
- Reduzir o débito tecnológico do país;
- Desenvolver a capacidade de avaliação continuada de conformidade em segurança de produtos, serviços e tecnologias de cibersegurança;
- E estímulo ao estabelecimento de parcerias com institutos brasileiros de pesquisa e desenvolvimento para ampliar as residências tecnológicas em cibersegurança.

Todas essas ações demonstram as iniciativas do Brasil para criar condições que contribuem para o maior controle dos dados em nuvem.

Adicionalmente, apesar de não abordar especificamente o ZT, o Gabinete de Segurança Institucional da Presidência da República (GSI/PR) publicou a Instrução Normativa nº 8/25 [42]. Ela revogou a restrição existente na IN nº 5/21 [15] que vedava o tratamento de informação classificada em qualquer grau de sigilo, e passou a permitir que informações classificadas nos graus reservado e secreto no âmbito da Administração Pública Federal sejam tratadas em nuvens privadas geridas por órgãos nacionais ou empresas habilitadas.

A IN nº 8/25 [42] ainda traz uma série de orientações para garantir a segurança e auditoria dos CSPs contratados e obriga que as agências de governo adotem requisitos rígidos para a seleção e publicação de serviços em nuvem pública.

A publicação deste normativo representa uma ação concreta em busca da soberania e contribui para a maturidade do governo e das empresas de tecnologia. Ao restringir o tratamento de informação classificada nos graus reservado e secreto a uma nuvem privada, e ao impedir que informação ultrassecreta seja tratada em qualquer tipo de nuvem, o governo brasileiro confirma a impossibilidade de alcançar observabilidade nas diversas camadas de uma nuvem pública.

Como a capacidade de coletar e visualizar os dados em todas as camadas da nuvem é limitada, o normativo do Brasil demonstra que é mais confiável utilizar nuvens privadas e nacionais.

Contudo, diversos dados e serviços já migrados para CSPs continuam sendo utilizados por agências de governo, e com o avanço da digitalização este uso tende a aumentar ano após ano, resultando na migração de novos ou ao menos na permanência de serviços e dados governamentais não classificados – mas ainda sim potencialmente sensíveis – em provedores de nuvem pública.

Apesar das publicações do governo brasileiro que permitem o avanço da maturidade cibernética, é possível notar a falta normativos específicos que guiem as agências governamentais na adoção de uma estratégia de segurança em ZT, essa lacuna dificulta a conscientização necessária para garantir a confiança por meio da observabilidade e da auditoria indispensáveis nestes ambientes. O resultado é a percepção de iniciativas locais e isoladas dentro do governo para a implementação de ZT, como a do SERPRO, que em 2025 implementou o modelo ZT no acesso à rede (ZTNA) dentro da sua plataforma de segurança para nuvem – Govshield [43] – ou iniciativas de bancos públicos, que por serem alvos constantes de ataques sofisticados, precisam investir com antecedência em tecnologias e soluções de segurança.

É necessária a criação de políticas de governo que estabeleçam as diretrizes e guiem os órgãos na adoção de uma estratégia madura de ZT, não tratando apenas os níveis Táticos e Operacionais, mas lidando com a conscientização e a responsabilização dos gestores [44] do nível Estratégico para a necessidade de implantação dos pilares de ZT em todas as agências governamentais. Estas políticas devem ser seguidas de ações que permitam a custódia dos dados sensíveis para o país, principalmente os que possuem sigilo e são relacionados com a segurança nacional. A proteção desejada para estes dados pode ser alcançada por meio da criação e gestão de infraestruturas de nuvem local administradas por instituições previamente habilitadas.

D. Nunca Confiar, Sempre Verificar

Ao optar pela custódia local de todas as camadas na nuvem, ainda é necessário considerar que ações de incentivo e normativos legais não garantem por si só o controle sobre os dados.

É necessário considerar que o monitoramento contínuo deve ser visto como um componente ativo da segurança. Ele tem o papel de evidenciar e fundamentar todas as decisões, impedindo que ações sejam executadas com base em deduções, possibilidades e configurações específicas dos fabricantes – majoritariamente externos – de cada uma das soluções de *hardware* e *software* utilizadas.

Dentro de qualquer ambiente de nuvem sempre existirão tecnologias de vários fornecedores, cada uma com características técnicas e capacidade de visibilidade distintas.

Com isso, alcançar a observabilidade necessária em uma arquitetura de ZT só é possível ao combinar ferramentas e técnicas especificas que permitam a telemetria através da coleta, análise, e correlacionamento dos eventos gerados em cada camada pelos usuários, ativos e sistemas na nuvem.

Os desafios de integração destas soluções e a dificuldade de compreensão e implementação de uma arquitetura de ZT tornam mais complexo o uso deste modelo de segurança, principalmente ao tentar implementar e auditar a observabilidade identificada aqui como essencial para permitir que a confiança não seja somente uma crença.

O relatório *In Whose Tech We Trust* [45] publicado em 2025 pela *Australian Strategic Policy Institute* (ASPI) demonstra que os principais países do Indo-Pacífico tiveram iniciativas isoladas para proteger sua soberania digital.

Ele demonstra que Singapura decidiu contratar apenas fornecedores que permitem auditoria dos equipamentos e sistemas e garantem a nacionalização dos seus dados. A Coreia do Sul criou o programa de certificação *Cloud Security Assurance Program* (CSAP) [46] para garantir que somente os fornecedores certificados pudessem hospedar os dados e sistemas do governo. Já a Austrália, permite que seus dados sejam enviados para o exterior, desde que os destinatários garantam cumprir os princípios de privacidade [47] do país de origem. Em alguns dos casos, os países decidiram estabelecer

critérios de confiança e verificação para criar listas de fornecedores autorizados a fornecer serviços e produtos.

Possuir um modelo de ZT é essencial para buscar a observabilidade, mas é necessário fazer uso de todos os mecanismos anteriores que permitiram a implantação de uma segurança orientada à confiança por observabilidade.

Todos os normativos, frameworks, equipamentos, sistemas, equipes, dados coletados e relatórios de conformidade utilizados na implantação do ZT são necessários. Contudo, se eles não fornecerem uma capacidade real de auditoria e dados visíveis sobre a confiança estabelecida, não terão cumprido o seu papel de oferecer segurança em nuvem por meio da observabilidade.

É necessário realizar verificações contínuas para garantir que o acesso a uma informação é legítimo. O responsável pela conformidade deve ter a capacidade de demonstrar que o acesso a um dado percorreu todas as etapas de validação necessárias.

E. Confidential Computing

Uma solução ainda pouco utilizada e que oferece um nível adicional de segurança contra acesso indevido aos dados em nuvem é o *Confidential Computing* [48].

Essa tecnologia surgiu para aumentar a proteção dos dados durante o seu uso, ou seja, enquanto são processados dentro da infraestrutura do provedor. Alguns CSPs [49] [50] [51] já o oferecem como recurso adicional de segurança em nuvem.

O pilar deste recurso é a utilização de técnicas de *hardware* que fornecem isolamento durante a execução do código de *software*. Ele impede que os dados utilizados pela aplicação sejam vistos e alterados por outros recursos – como processador, disco e memória – que por serem compartilhados na nuvem, processam simultaneamente dados de diversos clientes.

Seu desenvolvimento exige conhecimento específico para que seja validado em conjunto com o CPU e possa ser utilizado em um ambiente de execução confiável – *Trusted Execution Environments* (TEEs). Sua utilização é direcionada para ambientes de nuvem pública e surgiu para remover a necessidade de confiar no CSP.

Contudo, o uso desta tecnologia ainda precisa ser direcionado para casos muito específicos que justifiquem os custos associados à sua utilização, já que a instituição [52] que a define declara que estabelecer um TEE baseado em *hardware* possui desafios relacionados a limitações de velocidade, do volume dos dados processados e na escalabilidade horizontal deste ambiente quando comparado com um ambiente de computação em nuvem tradicional.

Para as aplicações executadas, também há a necessidade de escrever e certificar o código em conjunto com o CPU e os *drivers* utilizados para garantir que a tecnologia forneça a proteção esperada.

Como ela não garante proteção contra todos os tipos de ameaças, o *Confidential Computing* deve ser utilizado de modo complementar às outras soluções já apresentadas.

F. Soluções Mapeadas

A Tabela VI sintetiza e relaciona os problemas identificados com as soluções propostas.

Tabela VI - Observabilidade em Nuvem: Problemas e Soluções

Mapeamento de Observabilidade em Nuvem		
#	**Problema**	**Solução**
1	Camadas na Nuvem sem Observabilidade	Nuvem Local com Verificação Contínua
2	Lesligação e Normativos	Orientação Prática sobre ZT
3	Confiança em Nuvens Públicas	Nunca Confiar, Sempre Verificar
4	Responsabilidade na Nuvem	Gestão de SI com ZT
5	Auditoria na Nuvem	*Confidential Computing*

Os tópicos a seguir oferecem um resumo dos problemas identificados e das soluções apresentadas na Tabela VI.

1) Problema x Solução 1:

Uma nuvem possui camadas que realizam o processamento e transporte dos dados, ao utilizar nuvens públicas elas não podem ser acessadas pelos usuários. Essas características afetam a observabilidade do tratamento realizado nestes ambientes. Ao propor a implementação de uma nuvem local com ZT as organizações alcançam a visibilidade completa do tratamento dos seus dados em todas as camadas da nuvem.

2) Problema x Solução 2:

As legislações atuais oferecem meios de proteção aos dados armazenados em nuvem e impedem que informações classificadas utilizem este ambiente, mas elas não especificam um meio de verificar o tratamento e não exigem uma segurança que permita a observabilidade do tratamento dos dados. Ao propor um guia prático de ZT com observabilidade para agências do governo, busca-se elevar a capacidade de verificação dos acessos e aumento da confiança em nuvem.

3) Problema x Solução 3:

A dificuldade de verificação das camadas inferiores diminui o nível da confiança em nuvem pública. Ao buscar o modelo ZT os CSPs oferecem uma melhor significativa na segurança para o usuário. A solução proposta exige que organizações país apliquem o real conceito de verificação contínua em nuvem e estabeleçam critérios de validação prévia dos fornecedores envolvidos.

4) Problema x Solução 4:

As organizações têm utilizado a nuvem pública e enviado diversos dados, a responsabilidade compartilhada exige que cliente e provedor cumpram seus papéis, mas para o usuário não há uma capacidade real de verificação. Como solução, a adoção de um SGSI com ZT que permita verificação contínua oferece visibilidade e aumenta a segurança do ambiente.

5) Problema x Solução 5:

A auditoria é o principal meio pelo qual se valida a confiança na nuvem. Mesmo com a implantação de ZT é necessário auditar e garantir que os componentes deste modelo de segurança seguem as políticas implementadas. Como esta verificação existe profundo conhecimento e acesso aos componentes da tecnologia, a utilização de *Confidential Computing* contribui para isolar as aplicações e seus dados ao serem executadas em uma nuvem, aumentando a proteção em nível de *hardware*.

V. CONCLUSÕES E TRABALHOS FUTUROS

Esse capítulo traz as conclusões do artigo, demonstra as iniciativas existentes e oferece sugestões de trabalhos futuros que podem contribuir para o aumento da confiança em nuvem.

Zero Trust não é um produto que se compra, mas uma filosofia de segurança que se implementa e se aprimora continuamente. O sucesso e a maturidade de uma estratégia de segurança moderna são diretamente proporcionais à capacidade de observabilidade do ambiente de nuvem.

Este artigo demonstrou alguns dos desafios reais que ajudaram a fundamentar a necessidade de conscientização para que usuários de nuvem decidam abandonar a confiança implícita e busquem adotar uma verificação explícita e baseada em evidências, que devem ser visíveis e constantes.

Ao identificar e relacionar o entendimento sobre diversos componentes como o funcionamento e as camadas de uma nuvem, um modelo de segurança com verificação contínua, as responsabilidades do cliente e do provedor de nuvem, a importância da publicação de guias e normativos e a necessidade de utilização de meios de coleta e auditoria das ações realizadas neste ambiente, este artigo contribui para iniciativas nacionais que busquem compreender e aumentar da confiança por meio da observabilidade.

Procurou-se demonstrar a importância de uma organização em conhecer as características de uma nuvem, a necessidade de identificação dos dados e as limitações de auditoria que impactam na observabilidade e como elas afetam o processo de obtenção de confiança. Este entendimento permite analisar qual o impacto do processamento e armazenamento de informações sigilosas ou de interesse nacional e ajuda na definição de quais dados podem ser utilizados em uma nuvem.

Neste projeto, os logs, métricas e traces de equipamentos e sistemas deixam de ser vistos apenas como dados operacionais para equipes de infraestrutura, serviços, DevSecOps, segurança e de auditoria, e se tornam dados brutos essenciais para a tomada de decisões de segurança em tempo real. Se corretamente utilizados, eles transformam uma ZTA de um conceito estratégico para uma segurança efetiva, visível e auditada. Entende-se que ao decidir não confiar em nada passamos a depender de tudo o que podemos observar.

Um país que deseja alcançar soberania digital e realizar a proteção dos seus dados, da sua população e consequentemente da sua competitividade precisa formular uma estratégia de segurança clara e aplicável para os setores público e privado.

Ao demonstrar como outros países estão buscando um conjunto de soluções para proteger suas informações no meio cibernético, este artigo traz a importância da edição de guias e normativos nacionais e principalmente da necessidade de realização de ações concretas para manter a custódia, administração e auditoria contínua do que é realizado com os dados distribuídos entre os diversos provedores de serviço. Agências de governo e instituições especializadas em outros países já reconhecem esta dificuldade até mesmo para quem adota os mais modernos modelos de segurança.

Por fim, qualquer confiança assumida ou que tenha como base uma intuição não é real, ela só pode existir com evidências que permitem a sua comprovação. Um país que não possui uma definição clara de como alcança confiança nos seus fornecedores, sistemas, equipamentos [45] e serviços acaba se limitando a relatórios de conformidade atestado por outros ou assumindo uma confiança que já foi estabelecida por terceiros.

Portanto, este artigo entende que é necessário avançar na formação de uma conscientização sobre a confiança e necessidade de visibilidade real em ambientes de nuvem, seguidas de ações concretas para implementação desta capacidade. Estas ações contribuem para a maturidade de segurança das instituições públicas e privadas, e consequentemente da nação, ao demonstrar que não basta confiar, é preciso verificar pessoalmente.

Trabalhos futuros podem aprofundar os desafios na proteção da computação em nuvem por meio de um TEE [52] em conjunto com tecnologias de *attestation* [48] para computação confidencial, ela está sendo padronizada justamente para auxiliar na verificação da confiabilidade de quem determina que uma informação é confiável, permitindo que usuários de nuvem pública possam suprir uma preocupação ainda não resolvida, ou seja, ver por si mesmo a evidência de que a tecnologia utilizada está realmente protegendo seus dados. Contudo, por ter o *hardware* como um dos principais componentes de segurança, o *attestation* exige a confiança no fabricante do chip.

A Arquitetura de Zero Trust também é uma oportunidade futura para ser adicionada nativamente em protocolos de redes sem fio [53], permitindo que os benefícios deste modelo alcancem também pequenas empresas e usuários domésticos.

A sugestão de uma auditoria da própria Arquitetura de Zero Trust por meio de uma análise prática dos seus componentes também se mostra necessária, visto que mesmo ao utilizar este modelo de segurança é importante compreender que será preciso confiar principalmente nos seus planos de controle, de dados [1] e no método interno que eles utilizam para realizar as análises que garantem a confiança proposta. Nestes casos, também deve ser considerado que qualquer tecnologia está suscetível a falhas humanas no momento da definição e da configuração das políticas.

REFERÊNCIAS

[1] National Institute of Standards and Technology, NIST, “Zero Trust Architecture,” 8 2020. [Online]. Available: ttps://doi.org/10.6028/NIST.SP.800-207. [Acesso em 02 Setembro 2025].

[2] Cybersecurity and Infrastructure Security Agency, CISA, “Zero Trust Maturity Model Version 2.0,” 4 2023. [Online]. Available: https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf. [Acesso em 24 Setembro 2025].

[3] R. de Oliveira Albuquerque, L. J. García Villalba, A. L. Sandoval Orozco, F. Buiati e T. H. Kim, “A layered trust information security architecture,” *Sensors (Switzerland),* vol. 14, nº 12, pp. 22754-22772, 12 2014.

[4] D. Gambetta, “Can We Trust Trust?,” *Trust: Making and Breaking Cooperative Relations,* pp. 213-237, 1988.

[5] P. Cofta, “Trust, choice, and self-preservation: a computational approach,” *Cognition, Technology & Work,* vol. 23, nº 1, pp. 85-101, 2 2021.

[6] ISO, “31000: Risk management,” International Organization for Standardization, 2018. [Online]. Available: https://www.iso.org/standard/65694.html. [Acesso em 04 Nov. 2025].

[7] National Institute of Standards and Technology, NIST, “The NIST

Definition of Cloud Computing," Set. 2011. [Online]. Available: https://doi.org/10.6028/nist.sp.800-145. [Acesso em 02 Set. 2025].

[8] R. Reagan, "Remarks on Signing the Intermediate-Range Nuclear Forces Treaty," Jan 1987. [Online]. Available: https://www.reaganlibrary.gov/archives/speech/remarks-signing-intermediate-range-nuclear-forces-treaty. [Acesso em 02 Outubro 2025].

[9] J. Kindervag, S. Balaouras e L. Coit, "No more chewy centers: Introducing the zero trust model of information security," Forrester Research, 2010. [Online]. Available: https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf. [Acesso em 02 Outubro 2025].

[10] Executive Office, President, "Executive Order 14028, Improving the Nation's Cybersecurity," 12 5 2021. [Online]. Available: https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity. [Acesso em 02 Outubro 2025].

[11] Chief Information Security Officer (CISO); Chief Data Officer (CDO); Office of Management and Budget (OMB), "Federal Zero Trust Data Security Guide," 10 2024. [Online]. Available: https://www.cio.gov/assets/files/Zero-Trust-Data-Security-Guide_Oct24-Final.pdf. [Acesso em 24 Novembro 2025].

[12] CSA, "Working Group Zero Trust," Cloud Security Alliance, [Online]. Available: https://cloudsecurityalliance.org/research/working-groups/zero-trust. [Acesso em Set. 2025].

[13] EgInnovations, "Key Difference between SaaS, PaaS and IaaS: Level of Control," 27 Ago. 2024. [Online]. Available: https://www.eginnovations.com/blog/saas-vs-paas-vs-iaas-examples-differences-how-to-choose/. [Acesso em 01 Nov. 2025].

[14] BRASIL, "Lei Geral de Proteção de Dados Pessoais (LGPD)," Presidência da República, 15 Ago. 2018. [Online]. Available: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. [Acesso em 07 Nov. 2025].

[15] BRASIL, "Instrução Normativa GSI/PR nº 5," Gabinete de Segurança Institucional da Presidência da República, 30 Ago. 2021. [Online]. Available: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-5-de-30-de-agosto-de-2021-341649684. [Acesso em 08 Nov. 2025].

[16] EU, "General Data Protection Regulation," European Union, 04 Mai. 2016. [Online]. Available: https://gdpr-info.eu/. [Acesso em 05 Nov. 2025].

[17] Department for Health and Human Services, "Health Insurance Portability and Accountability Act," USA, 21 Ago. 1996. [Online]. Available: https://www.hhs.gov/hipaa/index.html. [Acesso em 05 Nov. 2025].

[18] AWS, "Brazil Data Privacy," Amazon, Ago. 2020. [Online]. Available: https://aws.amazon.com/pt/compliance/brazil-data-privacy/. [Acesso em 06 Nov. 2025].

[19] Google, "Cloud Compliance," [Online]. Available: https://business.safety.google/intl/pt-BR/compliance/. [Acesso em 06 Nov. 2025].

[20] Azure, "Proteção de Dados e LGPD," Microsoft, [Online]. Available: https://www.microsoft.com/pt-br/microsoft-365/business/lgpd. [Acesso em 05 Nov. 2025].

[21] Flexera, "State of the Cloud Report," 2025. [Online]. Available: https://info.flexera.com/CM-REPORT-State-of-the-Cloud-2025. [Acesso em 07 Nov. 2025].

[22] Forbes, "Microsoft Can't Keep EU Data Safe From US Authorities," 22 Jul. 2025. [Online]. Available: https://www.forbes.com/sites/emmawoollacott/2025/07/22/microsoft-cant-keep-eu-data-safe-from-us-authorities/. [Acesso em 07 Nov. 2025].

[23] US Congress, "CLOUD Act," USA, 02 Jun. 2018. [Online]. Available: https://www.congress.gov/bill/115th-congress/house-bill/4943. [Acesso em 07 Nov. 2025].

[24] AWS, "Shared Responsibility Model," Amazon, [Online]. Available: https://aws.amazon.com/pt/compliance/shared-responsibility-model/. [Acesso em 12 Set. 2025].

[25] Google, "Shared Responsibilities and Shared Fate on Google Cloud," 21 Ago. 2023. [Online]. Available: https://cloud.google.com/architecture/framework/security/shared-responsibility-shared-fate. [Acesso em 12 Set. 2025].

[26] Azure, "Shared Responsibility in the Cloud," Microsoft, 29 Set. 2024. [Online]. Available: https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility. [Acesso em 12 Set. 2025].

[27] ISACA, "Audit Programs and Tools," Information Systems Audit and Control Association, [Online]. Available: https://www.isaca.org/resources/insights-and-expertise/audit-programs-and-tools. [Acesso em 07 Nov. 2025].

[28] ISACA, "AWS Audit Program," Information Systems Audit and Control Association, 01 Mai. 2019. [Online]. Available: https://www.isaca.org/about-us/newsroom/press-releases/2019/isaca-launches-new-resources-for-auditing-amazon-web-services-aws. [Acesso em 07 Nov. 2025].

[29] ISACA, "Google Cloud Platform Audit Program," Information Systems Audit and Control Association, 19 Jul. 2023. [Online]. Available: https://www.isaca.org/about-us/newsroom/press-releases/2023/isaca-introduces-new-google-cloud-platform-audit-program. [Acesso em 07 Nov. 2025].

[30] CSA, "Cloud Controls Matrix (CCM)," Cloud Security Alliance, [Online]. Available: https://cloudsecurityalliance.org/research/cloud-controls-matrix. [Acesso em 07 Nov. 2025].

[31] ISO, "27017: Code of practice for information security controls based on ISO/IEC 27002 for cloud services," International Organization for Standardization, 2015. [Online]. Available: https://www.iso.org/standard/43757.html. [Acesso em 07 Nov. 2025].

[32] ISO, "27018: Guidelines for protection of personally identifiable information (PII) in public clouds acting as PII processors," International Organization for Standardization, 2025. [Online]. Available: https://www.iso.org/standard/27018. [Acesso em 07 Nov. 2025].

[33] ISO, "27001: Information security, cybersecurity and privacy protection," International Organization for Standardization, 2022. [Online]. Available: https://www.iso.org/standard/27001. [Acesso em 05 Nov. 2025].

[34] J. F. Cassino, "Soberania Fatiada: Controle das Infraestruturas e Subordinação da Autoridade Pública no Mundo Digital," *Universidade Federal do ABC,* 2025.

[35] Office of Management and Budget (OMB), "M-22-09 - Federal Zero Trust Strategy," 26 1 2022. [Online]. Available: https://www.federalregister.gov/d/2021-10460. [Acesso em 24 Setembro 2025].

[36] Singapore Government, "Government Zero Trust Architecture (GovZTA)," 23 Set. 2025. [Online]. Available: https://www.developer.tech.gov.sg/guidelines/standards-and-best-practices/government-zero-trust-architecture.html. [Acesso em 06 Nov. 2025].

[37] NCSC, United Kingdom, "Zero trust architecture design principles," National Cyber Security Centre, 23 Jul. 2021. [Online]. Available: https://www.ncsc.gov.uk/collection/zero-trust-architecture. [Acesso em 06 Nov. 2025].

[38] Canada, "Zero Trust security model," Canadian Centre for Cyber Security, Nov. 2022. [Online]. Available: https://www.cyber.gc.ca/en/guidance/zero-trust-security-model-itsap10008. [Acesso em 05 Nov. 2025].

[39] BRASIL, "Estratégia Nacional de Governo Digital," Ministério da Gestão e da Inovação em Serviços Públicos, 21 Jun. 2024. [Online]. Available: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2024/Decreto/D12069.htm. [Acesso em 07 Nov. 2025].

[40] BRASIL, "Programa de Privacidade e Segurança da Informação (PPSI)," Ministério da Gestão e da Inovação em Serviços Públicos, 28 03 2023. [Online]. Available: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca. [Acesso em 05 Nov. 2025].

[41] BRASIL, "Estratégia Nacional de Cibersegurança - E-Ciber," Gabinete de Segurança Institucional da Presidência da República, 04 Ago. 2025. [Online]. Available:

https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/D12573.htm. [Acesso em 07 Nov. 2025].

[42] BRASIL, “Instrução Normativa GSI/PR nº 8,” Gabinete de Segurança Institucional da Presidência da República, 06 Out. 2025. [Online]. Available: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-gsi/pr-n-8-de-6-de-outubro-de-2025-660716869. [Acesso em 08 Nov. 2025].

[43] SERPRO, “Novas Funcionalidades no Govshield,” Serviço Federal de Processamento de Dados, 30 Set. 2025. [Online]. Available: https://www.serpro.gov.br/menu/noticias/noticias-2025/govshield-funcionalidades. [Acesso em 05 Nov. 2025].

[44] A. Marcilio, “Dificuldades na implementação de segurança da informação no serviço público brasileiro: a responsabilidade da alta administração,” *Universidade de Brasilia (UnB),* 15 Ago. 2025.

[45] J. Bassi, S. Gilding, A. Suriyasenee e J. Corera, “In Whose Tech We Trust,” Australian Strategic Policy Institute, ASPI, 11 Nov. 2025. [Online]. Available: https://www.aspi.org.au/report/in-whose-tech-we-trust-part-i-mapping-indo-pacific-security-approaches-to-foreign-owned-controlled-or-influenced-technology/. [Acesso em 12 Nov. 2025].

[46] KISA, “Cloud Security Assurance Program (CSAP),” Korea Internet & Security Agency, [Online]. Available: https://www.kisa.or.kr/EN. [Acesso em 12 Nov. 2025].

[47] Australian Government, “Australian Privacy Act 1988,” 12 Mar. 2014. [Online]. Available: https://www.legislation.gov.au/C2004A03712/2014-03-12/text. [Acesso em 11 Nov. 2025].

[48] Confidential Computing Consortium, CCC, “A Technical Analysis of Confidential Computing Changelog Table,” 11 2022. [Online]. Available: https://confidentialcomputing.io/wp-content/uploads/sites/10/2023/03/CCC-A-Technical-Analysis-of-Confidential-Computing-v1.3_unlocked.pdf. [Acesso em 20 Out. 2025].

[49] AWS, “Confidential Computing,” Amazon, [Online]. Available: https://aws.amazon.com/pt/confidential-computing/. [Acesso em 24 Nov. 2025].

[50] Azure, “Confidential Computing Overview,” Microsoft, 07 05 2025. [Online]. Available: https://learn.microsoft.com/en-us/azure/confidential-computing/overview. [Acesso em 24 Nov. 2025].

[51] Google, “Cloud Confidential Computing,” [Online]. Available: https://cloud.google.com/security/products/confidential-computing?hl=en-US. [Acesso em 24 Nov. 2025].

[52] CCC, “A Technical Analysis of Confidential Computing v1.3,” Confidential Computing Consortium, Nov. 2022. [Online]. Available: https://confidentialcomputing.io/resources/white-papers-reports/. [Acesso em 24 Nov. 2025].

[53] NIST, “Zero Trust Networks Project,” National Institute of Standards and Technology, 2024. [Online]. Available: https://www.nist.gov/programs-projects/zero-trust-networks. [Acesso em 06 Nov. 2025].

[54] Gart, “IT Infrastructure Components: Essential Components for Modern Business,” 25 Jun. 2025. [Online]. Available: https://gartsolutions.com/it-infrastructure-components/. [Acesso em 01 Nov. 2025].