ARQUITETURA DE INFRAESTRUTURA EM NUVEM E O MODELO ZERO TRUST COMO ESTRATÉGIA DE CIBERSEGURANÇA

ARTIGO ORIGINAL

TEODORO, Douglas Diego Rocha[1]

TEODORO, Douglas Diego Rocha. **Arquitetura de infraestrutura em nuvem e o modelo zero trust como estratégia de cibersegurança.** Revista Científica Multidisciplinar Núcleo do Conhecimento. Ano. 07, Ed. 11, Vol. 13, pp. 204-232. Novembro de 2022. ISSN: 2448-0959, Link de acesso: https://www.nucleodoconhecimento.com.br/tecnologia/modelo-zero-trust, DOI: 10.32749/nucleodoconhecimento.com.br/tecnologia/modelo-zero-trust

RESUMO

Desde o surgimento da internet, o crescimento vertiginoso do uso dos meios eletrônicos cresce na mesma proporção em que ocorrem os crimes cibernéticos, aplicados de forma cada vez mais sofisticada. Além desses dois fatores que impactam o uso da internet, destaca-se a velocidade com que evoluem os recursos e ferramentas inerentes à área de Tecnologia da Informação e Comunicação (TICs), que potencializam a necessidade de serem desenvolvidos e aperfeiçoados, continuamente, os meios de proteção de dados sensíveis de pessoas e organizações públicas e privadas. Nesta perspectiva, surge a *Cloud Computing*, que permite o armazenamento de dados, redes e aplicações, e demais recursos por meio de ambientes integrados através da internet, a partir de provedores coletivos, em contraponto ao sistema *on-premise*, que se baseia na guarda e acesso por meio de servidores locais, inclusive *mainframes*, que ainda são mantidos em boa parte das organizações de grande porte, como o sistema bancário, por exemplo. Ao *Cloud Computing* somem-se as práticas do *Zero Trust*, cuja principal inovação consiste na adoção de várias camadas de verificação de acesso. Este artigo foi elaborado adotando como metodologia a pesquisa bibliográfica. A pergunta que surge sobre o tema é: de que forma a *Zero Trust* confere maior segurança aos usuários das redes? Como objetivo pretende-se demonstrar as vantagens da segurança proporcionadas pela *Zero Trust*, aliadas à *Cloud Computing*. Diante da literatura analisada, foi possível concluir a existência de dois aspectos principais trazidos pela *Zero Trust*: o acesso do internauta

somente a partir de 7 camadas de verificação, e a mitigação das vulnerabilidades, entre elas a ideia sobre navegação responsável pelos diferentes usuários.

Palavras-chave: Crimes cibernéticos, Segurança em TI, *Mainframes, Cloud Computing*, *Zero Trust*.

1. INTRODUÇÃO

Desde o surgimento das Tecnologias da Informação (TI), a questão da segurança de dados sempre esteve no topo da pauta dos especialistas. Proteger os dados sensíveis dos usuários é algo prioritário, face às reincidentes atividades maliciosas, entre elas os *ransomwares* e *phishings*, que comprometem os dados dos usuários, assim como as redes internas, afetando inclusive os ativos digitais das organizações (IBM, 2022).

O fato é que ao longo do tempo as empresas desenvolveram sistemas computacionais internos, resultando na implantação de processos informacionais complexos e onerosos, que requeriam investimentos em equipamentos, instalação e manutenção de programas e equipes de especialistas para o cuidado com sua infraestrutura de TI, sistema conhecido como *on-premise*.

Foi a fase em que as exigências mercadológicas conflitavam entre si, ao exigirem dos profissionais de infraestrutura acentuados esforços na busca pela preservação dos controles seguros necessários, enquanto os profissionais de desenvolvimento eram levados a atuar na identificação de “novas funcionalidades para aplicações cada vez mais rápidas” (CASTRO, 2019, p.1). Tais movimentos mantinham muitas dificuldades para a implantação efetiva de soluções integradas que pudessem promover a homogeneidade das plataformas.

Neste sentido, a *Cloud Computing* surge como uma redefinição nas práticas das TICs, tanto na perspectiva do uso individual das redes e sistemas acessados pelos cidadãos, como dentro das organizações (CASTRO, 2019). Gravar um documento, responder a um *email* ou ouvir uma música no *streaming* são ações

que já são feitas naturalmente nos dias atuais, e que são possíveis a partir da evolução das TICs, já que tudo isso é feito por meio de *Cloud Computing*.

Aliado à segurança oferecida pela nuvem, surge o conceito *Zero Trust*, para aperfeiçoar a proteção de dados sensíveis dos usuários, em oposição à segurança de rede padrão, que atua para interromper as possíveis ameaças advindas de fora da rede, as quais podem, ocasionalmente, deixar dados vulneráveis, permitindo que sejam eventualmente roubados de dados dentro dessa rede. O princípio básico da *Zero Trust* consiste em reforçar a autenticação dos usuários, por meio da utilização de várias camadas de controle avançado de acesso, tanto para dispositivos de rede, quanto para os servidores que suportam tais recursos (ORACLE, 2022).

Este artigo científico foi elaborado com base em extensa pesquisa bibliográfica, ensejando responder à seguinte pergunta: de que forma a *Zero Trust* confere maior segurança aos usuários das redes? O objetivo deste estudo consiste em demonstrar as vantagens da segurança proporcionadas pela *Zero Trust*, aliada à *Cloud Computing*.

2. AMBIENTES *ON-PREMISE*

Ambiente local ou sistema *on-premise* é aquele que requer a aquisição e manutenção de licenças para sua instalação. Pode ser gerenciado pela equipe interna da organização, requerendo a "realização de *upgrades* e mudanças no sistema interno sem exigir acesso à internet" (BRESSANIN, 2021).

Seu funcionamento requer a instalação de um programa nos servidores da empresa, e, dependendo do formato da aplicação, deve ser instalado, também, em cada máquina de uma rede interna. Tais necessidades tornam sua instalação mais demorada, requerendo a configuração de cada um de seus módulos em cada máquina da rede interna da empresa. Sua instalação é feita a partir da

contratação de pacotes de serviços, que podem ser definidos previamente, e sintonizados a cada segmento. Apesar de ser um processo trabalhoso e demorado, a utilização de um sistema *on-premise* permite várias possibilidades de personalização, aspecto atrativo quando a empresa "requer integração e desenvolvimento" (BRESSANIN, 2021).

Quando se fala sobre ambientes corporativos, no tocante aos investimentos necessários à instalação e manutenção do ambiente *on-premise*, e, considerando-se a complexidade e demora para sua implantação, uma das possibilidades é adotar um modelo de solução informatizada conhecido como Sistema ERP - *Enterprise Resource Planning*, que permite a otimização de todos os processos operacionais da organização, permitindo maior eficiência e produtividade, além da redução de custos (BRESSANIN, 2021).

O sistema ERP foi desenvolvido para dar suporte à gestão dos processos organizacionais, entre eles as áreas de planejamento, vendas, emissão de notas fiscais e controles financeiros (SALESFORCE, 2016). A estas funcionalidades, acrescentam-se as melhorias nos processos internos e a integração das atividades dos vários setores, como o estoque e de recursos humanos. O uso do ERP permite a integração das informações em uma única plataforma, tornando-as compartilháveis mais facilmente, assim como toda a comunicação organizacional que fica mais leve e ágil (TOTVS, 2022).

No que se refere aos custos necessários à implantação de um sistema *on-premise* suportado por um ERP de gerenciamento, o investimento inicial é maciço, já que são necessários: equipamentos específicos; aquisição das licenças para *hardwares* e *softwares*, necessárias a esse sistema; custos para manutenção dos *hardwares*, além da complexidade e demora em sua implantação (BRESSANIN, 2021).

De uma forma resumida, pode-se observar a tabela 1, que apresenta a evolução do sistema *On-Premise* para a *Cloud Computing*.

Tabela 1 – Evolução das Tecnologias Emergentes, por empresa e modelo de negócios

Década	Tecnologia Emergente	Empresa Paradigma (data do IPO*)	Modelo de Negócio
1960 - 1970	*Mainframe*	IBM	Integração vertical Venda e locação de *hardware*
1970 - 1980	Minicomputador	DEC HP	Venda de *hardwares* e *softwares* proprietário, mas incorporando periféricos de terceiros
1980 - 1990	Computador pessoal	Intel Apple (1980) Microsoft (1986)	*Hardware* como *commodity* Licenciamento de *software*
1990 - 2000	Internet	Microsoft Netscape (1995)	Licenciamento de *software* Mecanismos de acesso (*browser*)
2000 - 2010	Web 2.0	Microsoft Amazon Google (2004)	Prestação de serviços de busca, *home banking*, comércio eletrônico, telecomunicações etc.
2010 -	Computação em nuvem	Google, Apple, Facebook	Serviços avançados de busca, redes sociais e publicidade dirigida
*IPO – (*Initial Public Offering*) - Oferta inicial de ações			

Fonte: Tigre e Noronha (2013, p.116).

3. ARQUITETURA PARA *CLOUD COMPUTING*

Por definição, “arquitetura de nuvem é a forma como as tecnologias individuais são integradas para criar nuvens. Elas são ambientes de TI que abstraem, agrupam e compartilham recursos escaláveis em uma rede” (REDHAT, 2019). Armazenar dados em nuvens significa “migrar dados, sistemas e aplicações para

a arquitetura em nuvem (...)", sendo considerada, no presente, uma "grande tendência tecnológica" (CLARANET, 1996-2002).

Para Sousa, Moreira e Machado (2019, p.5) a *cloud computing* surge para oferecer basicamente três benefícios aos usuários das redes virtuais: reduzir os investimentos em infraestrutura, que pode ser por demanda ou com recursos heterogêneos; flexibilizar tal modelo quanto às necessidades por *hardware* e *software*; conferir facilidade e abstração de acesso aos seus usuários.

Pedrosa e Nogueira (2011) definem que a computação por meio de nuvem é um modelo inovador, permitindo aos usuários finais acessarem grandes quantidades de conteúdos e de soluções a partir de qualquer lugar, independentemente de uma plataforma específica.

Por sua vez, Falcão e Silva (2021, p.101) referem que a computação em nuvem surgiu no final do século XX, mas popularizou-se logo no início do século XXI, face à "evolução de tecnologias de virtualização e ampla disponibilidade através dos provedores públicos de computação na nuvem". Com a finalidade de viabilizar sistemas em TI, sua proposta era "facilitar e otimizar a alocação de recursos gerando economia financeira e eficiência gerencial de recursos computacionais e humanos". Assim, a *Cloud Computing* ocasionou, também, mudanças nas áreas de Engenharia e Arquitetura de *Software*.

Se na fase anterior foram desenvolvidos inúmeros sistemas com "arquitetura monolítica" implantados em servidor único, o conceito de computação em nuvem, reforçado pela sequente evolução das diferentes TICs, permitiu a criação de sistemas completamente distribuídos, inclusive do "padrão arquitetural de microsserviços". Já naquilo que se refere à "hospedagem dos sistemas em nuvem, devido à similaridade de princípios, como a facilidade e rapidez na alocação e desalocação de recursos e serviços", por exemplo (FALCÃO e SILVA, 2021, p. 101-2)

Diante da disponibilização de todos os recursos computacionais em nuvem, os indivíduos passaram a precisar ter em seus dispositivos eletrônicos, apenas, “um sistema operacional, um navegador e acesso à internet” (SOUSA et al., 2009, p.4). A esta definição, acrescenta-se o conceito elaborado pela TD Synnex (2022), ao definir que “o objetivo do pesquisador era que a conexão pudesse ser feita de qualquer lugar e que estivesse disponível a qualquer horário. Ou, de outra forma, disponibilidade e acessibilidade”.

Figura 1 – Visão geral de uma nuvem computacional

Fonte: Sousa, Moreira e Machado (2009, p.3).

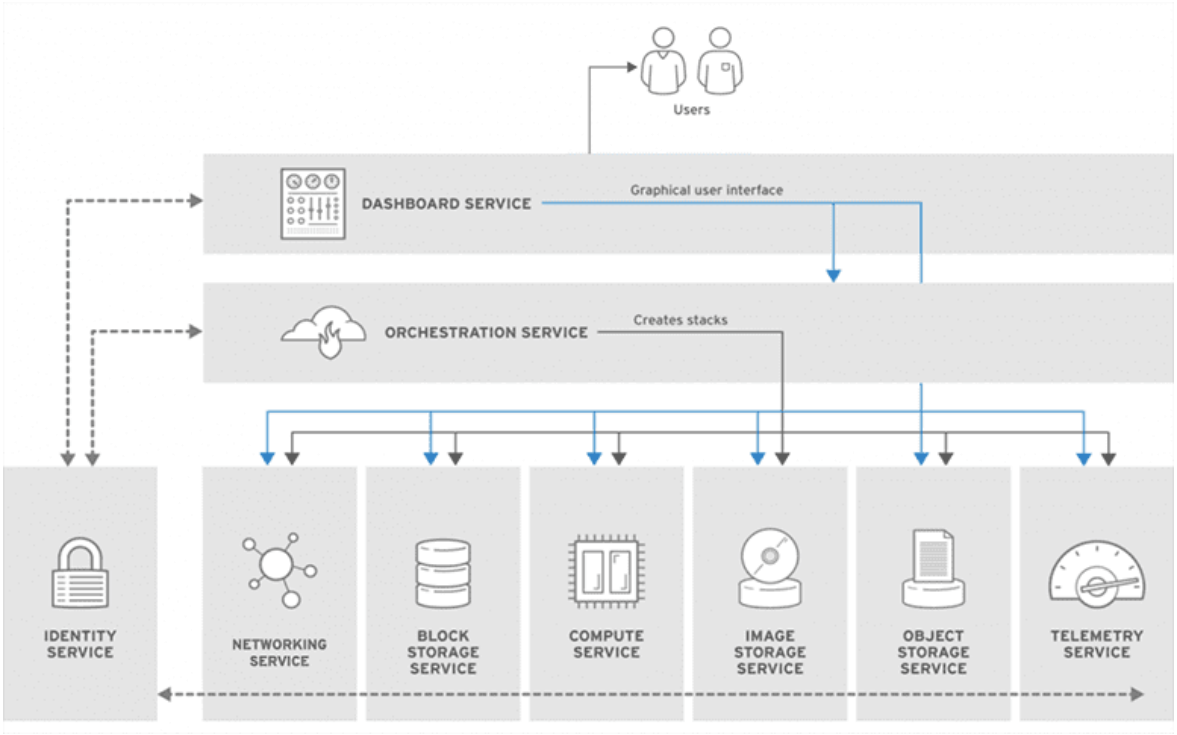
Por analogia, pode-se mencionar o exemplo dado por Redhat (2019), quando diz que pensar em infraestrutura de segurança é algo semelhante à construção de uma casa, cuja estrutura inclui os materiais necessários, como os tijolos, areia, cal, cimento, madeira, pinceis, tinta, etc.; nessa perspectiva, a estrutura da arquitetura seria a planta do imóvel em construção.

A comparação acima permite afirmar que o efetivo desenvolvimento da arquitetura de nuvem requer a existência dos “componentes e recursos necessários, os quais deverão estar conectados de modo a permitir a construção de uma plataforma *online* em que as aplicações deverão ser executadas” (REDHAT, 2019).

Significa que a arquitetura de nuvem pode variar conforme as necessidades a serem desenvolvidas; porém, seja qual for a finalidade de sua instalação, serão necessários “um *software* de automação, gerenciamento, *middleware* e *hardware*” (REDHAT, 2019).

Outro aspecto importante a destacar consiste na velocidade com que os recursos computacionais ficam obsoletos, tornando o uso da *Cloud Computing* uma solução inteligente, já que se utiliza de plataformas terceirizadas; além disso, é uma solução mais funcional e econômica, levando diferentes usuários aos acessos de seu interesse, sem que tenham maiores conhecimentos técnicos em TI. Cabe dizer ainda que tais acessos são realizados sob a demanda dos interessados (SOUSA et al., 2009).

Figura 2 – Composição de uma arquitetura básica de nuvem



Fonte: Redhat (2019).

A computação em nuvem foi desenvolvida para atender às demandas da área de TI, visando ser, também, um recurso global no atendimento das necessidades virtuais dos diferentes tipos de usuários, isto é, desde “o usuário final que hospeda seus documentos pessoais na internet até empresas que terceirizam toda infraestrutura de TI para outras empresas” (SOUSA et al., 2009, p. 3)

A virtualização para abstrair os recursos de *hardware* em *data lakes* com gerenciamento central também é utilizada pela infraestrutura de nuvem. Já outras nuvens conhecidas como *bare-metal* conectam os clientes diretamente ao *hardware* (REDHAT, 2019).

Do ponto de vista estratégico e comercial, existem vantagens competitivas importantes para as organizações na adoção da arquitetura de nuvem, entre elas a redução de custos e a maior segurança dos dados eletrônicos existentes. Além

disso, “permite que cargas de trabalho sejam executadas remotamente pela internet, por meio do uso de *data center* comercial que se utilize do modelo de nuvem pública” (CLARANET, 1996 - 2022).

A título de ilustração, existem na atualidade grandes fornecedores de nuvem pública, entre eles a *Amazon Web Servives* (AWS), a *Microsoft Azure* e *Google Cloud*. Os mais utilizados em 2020 foram: *Alibaba Cloud* / Oracle / IBM / *Tencent Cloud* / *Amazon web Services* / Microsoft / Google (MONTEIRO e BORGES, 2021).

Em uma breve linha do tempo obtida no portal TD Synners (2022), pode-se observar a evolução sobre a *Cloud Computing* no intervalo entre 1950 até 2000, que se assemelha àquela já apresentada por Tigre e Noronha (2013):

- **1950**: Os sistemas operacionais das organizações eram desenvolvidos em *mainframes*. Eram máquinas caras, e dessa forma, existiam apenas algumas em cada empresa;
- **1960**: Inicia-se a concepção do conceito sobre nuvem. John McCarthy, considerado o pai da Inteligência Artificial (IA) lança a ideia *Utility Computing*, criando também a programação *Lisp*;
- **1960**: Joseph C.R. Licklider colabora com o desenvolvimento da Rede de Agências e Projetos de Pesquisa Avançada (ARPANET);
- **1990**: Parte das empresas de telecomunicações criam redes virtualizadasde qualidade por baixo custo. Inicia-se o fornecimento do acesso compartilhado em uma mesma infraestrutura física. Na mesma fase popularizou-se o acesso às tecnologias;
- **1997**: o Professor Ramnath Chellapa usa pela primeira vez a expressão: “computação em nuvem” em uma palestra acadêmica. Tal expressão inspirou-se na ideia de “algo que está no ar”, como é o caso da internet;
- **2000**: a tecnologia *Cloud Computing* ganha força quando começa a ser oferecida para uso comercial. Nessa fase, surgem oportunidades de

empresas e particulares ofertando seus computadores virtuais para locação e plataformas de *streaming*, como por exemplo a *Amazon*, *Google*, *Microsoft Azure*e *Netflix*. Trata-se da disponibilização de assinaturas de um conjunto de serviços para armazenamento, computação e inteligência humana, baseados em nuvem.

A projeção de uma plataforma de nuvem compreende alguns pilares que permitem a projeção da estrutura da arquitetura de nuvem, e ainda, os recursos computacionais dos componentes de *hardware* (REDHAT, 2019).

Nesse sentido, destaca-se a existência de três plataformas ou pilares que são comumente utilizadas para a criação da arquitetura de nuvem, plataformas essas que conferem maior eficiência às organizações, além da redução de seus investimentos com infraestrutura local, a destacar: PaaS, SaaS, IaaS (REDHAT, 2019; CLARANET, 1996-2022).

O pilar PaaS consiste em plataforma voltada à arquitetura de nuvem que oferece a seus usuários uma infraestrutura de TI em camadas (REDHAT, 2019). Trata-se de um modelo de plataforma também denominado como plataforma de serviço, já que oferece aos seus usuários um “conjunto de serviços destinados aos desenvolvedores, especificamente” O PaaS fornece “ferramentas, processos e APIs, os quais, ao serem compartilhados, ocasionam a aceleração do desenvolvimento, teste e implantação de aplicações” (CLARANET, 1996-2022).

Cabe mencionar que as Interfaces de Programação de Aplicativos (APIs) promovem a conexão entre os sistemas, *softwares* e aplicativos, requerem da arquitetura de nuvem um desenvolvimento mais aprofundado, que permita “a incorporação e a conteinerização, orquestração, interfaces de programação de aplicações (APIs), roteamento, segurança, gerenciamento e *software* de automação” (REDHAT, 2019).

Por sua vez, o pilar SaaS é um modelo de distribuição de *software* de serviço, que permite acesso integrado aos aplicativos de *software* de determinado provedor, isto é, ao invés de ser baixado em uma determinada localidade, ele é hospedado em um provedor terceirizado e acessado por seus usuários a partir da interface de um navegador *web*, a partir de qualquer máquina (CLARANET, 1996-2022).

Já o pilar IaaS consiste em ser uma estrutura de serviço, ou seja, forma de computação em nuvem onde o *hardware* é fornecido e gerenciado por provedores externos. De outra forma, trata-se de um *hardware* que pode incluir servidores virtuais e até conexões de rede; é uma máquina virtual que permite às empresas dimensionar melhor suas soluções tecnológicas (CLARANET, 1996-2022).

O IaaS confere vantagens importantes a seus usuários: 1. escalabilidade, que pode ser conquistada por meio de assinatura; permite acesso aos sistemas de TI a qualquer momento, de forma rápida e eficiente, ao mesmo tempo que reduz a inatividade; 2. manutenção reduzida com *hardware* que antecede ao IaaS, gerando economia em sua manutenção para as empresas; 3. acesso sob demanda, que permite a redução dos custos relativos ao seu uso (CLARANET, 1996 - 2022).

Duas são as redes de nuvens disponíveis. A nuvem pública, que transpõe o espaço físico das organizações, sendo fornecida e operada por terceiros. Já a rede privada é instalada dentro de um ambiente empresarial, isto é, funciona como *intranet* ou *data center*, que consiste nos equipamentos necessários à área de TI (CLARANET, 1996 - 2022).

4. COMPARAÇÕES ENTRE *ON-PREMISE VS CLOUD COMPUTING*

Cloud Computing é um tipo de acesso à internet que permite aos usuários armazenar, gerir e compartilhar dados, *softwares*, aplicações e serviços na internet, com praticidade, agilidade e segurança (TD SYNNEX, 2022). Para Sousa,

Moreira e Machado (2009, p.3), “a computação em nuvem é uma tendência recente de tecnologia cujo objetivo é proporcionar serviços de Tecnologia da Informação (TI) sob demanda com pagamento baseado no uso”.

Observa-se que a migração do padrão ambientes para a *Cloud Computing* tornou-se tão natural quanto necessária. Nesta perspectiva, o portal TI Inside (2022) refere que em dezembro de 2021 a multinacional Accenture, especializada em gestão de tecnologia da informação e *outsourcing*, realizou um estudo *on-line* intitulado "*The great cloud mainframe migration: what banks need to know*", sobre a intenção dos banqueiros na migração de seus dados ainda mantidos em *mainframes* para *cloud*.

Tal pesquisa contou com a participação de 150 executivos de TI e inovação de bancos de 16 países entre os cinco continentes, entre eles: Alemanha, Austrália, Arábia Saudita, Brasil, Canadá, China, Espanha, EUA, França, Índia, Itália, Japão, México, Singapura, Suécia e Reino Unido. Constatou-se que alguns planejam migrar suas principais funções para a nuvem, enquanto outros já deram início a esse processo.

Na prática, as vantagens econômicas, gerenciais e na otimização de recursos humanos e físicos têm levado boa parte dos banqueiros a migrarem as funcionalidades de seus negócios, os novos produtos e seus aplicativos para o sistema *cloud*. Contudo, a dependência dos *mainframes* ainda persiste, sendo comum em algumas empresas de grande porte, a exemplo dos bancos, no que se refere aos registros de clientes, pagamentos, investimentos, risco e conformidade, ainda persistem (TI INSIDE, 2022).

Destaca-se que a migração para a nuvem dos serviços bancários móveis e *on-line* já é realidade em vários bancos, assim como as ferramentas necessárias à atuação de seus empregados, como por exemplo, *e-mails* e videoconferências que já operam no sistema *cloud* (TI INSIDE, 2022).

Entre as porcentagens no interesse de banqueiros para os diferentes aspectos relativos à migração do sistema *on-premise* para nuvem, consideram-se: “velocidade e agilidade (43%); segurança (41%); capacidade de acrescentar novos recursos (37%)”. Contudo, há riscos que têm sido considerados relevantes para tal migração, como por exemplo: “interrupção dos negócios; falta de compreensão sobre o funcionamento do código; capacidade de atrair e reter profissionais especializados em TI, e a regulação de riscos de segurança e conformidade” (TI INSIDE, 2022).

À *Cloud Computing*, soma-se a proteção conferida pela *Zero Trust* que compreende ações que visam nivelar todos os aspectos de segurança dos milhões de internautas, tendo por base o pressuposto de que “ninguém é confiável por padrão de dentro ou de fora da rede”. É um modelo de segurança de rede baseado na ideia de “nunca confie, sempre verifique”, ou seja, é um sistema que prima pela autenticação e verificação segura de um usuário que busca um acesso (ORACLE, 2022).

A adoção da *Zero Trust* implica no impedimento das diversas vulnerabilidades permitidas pelos métodos de segurança padrão, que atuam na interrupção das ameaças advindas de fora da rede, por meio da utilização de *firewalls*, *Virtual Private Network*” (VPNs), de controles de acesso, *Instrusion Detection System* (IDS), *Instrusion Prevention System* (IPS), SIEMs e *gateways* a *emails*. Uma vez que os criminosos se tornam cada vez mais especializados, suas habilidades permitem a “violação de *sites*, aplicativos ou quaisquer dispositivos eletrônicos conectados à internet” (ORACLE, 2022).

Para melhor visualizar os aspectos de maior impacto na tomada de decisão das organizações, são reproduzidas a seguir as tabelas 2, 3 e 4, com base nas indicações oferecidas pela plataforma *Mandic Cloud Platform* (MCP), que é dedicada à automatização e integração de fluxos de trabalho de diferentes

serviços e produtos, voltados aos diferentes modelos de negócios (MANDIC, sem data).

Tabela 2 – Comparativo dos Aspectos Estruturais entre o Ambiente *On-Premise vs. Cloud Server*

ON-PREMISE	*CLOUD SERVER*	*CLOUD SERVER GERENCIADO*
Customização e implantação por conta da empresa.	Possibilidade de aumento de recursos de memória, processamento, disco e banda, quando necessário.	Possibilidade de aumento de recursos de memória, processamento, disco e banda, quando necessário.
Hardwares de alto custo que ocupam um grande espaço dentro da empresa.	*Hardwares* fora da empresa.	*Hardwares* fora da empresa.
Licença dos *softwares* por conta da empresa.	Controle total na gestão de servidores e acesso ao *root*/admin do servidor.	Maior tempo de dedicação ao negócio, uma vez que você tem uma equipe de especialistas trabalhando para a sua empresa.

Fonte: Mandic (sem data).

Tabela 3 – Comparativo dos Aspectos Operacionais entre o Ambiente *On-Premise vs. Cloud Server*

ON-PREMISE	*CLOUD SERVER*	*CLOUD SERVER* GERENCIADO
Atualização de *softwares* e de *hardwares* por conta da empresa.	Atualização constante de aplicativos disponibilizados pela contratada; porém, quem faz é o operacional da empresa contratante.	Atualização constante de aplicativos, nos quesitos de funcionamento de segurança.
A empresa tem total domínio sobre o servidor. Pode fazer as alterações e ajustes que achar necessário.	O controle do servidor é da empresa contratada.	O controle do servidor é da empresa contratada.
Instalação de aplicativos e estratégias de segurança por conta da empresa.	Precisa de um conhecimento técnico para operacionalizar o painel de controle do servidor.	Sem necessidade de conhecimentos técnicos, facilita a criação de sites e gestão de aplicações.
Treinamento de pessoal por conta da empresa.	Equipe especializada do provedor.	Equipe especializada do provedor.

RC: 133524
Disponível em: https://www.nucleodoconhecimento.com.br/tecnologia/modelo-zero-trust

Downtime ruim.	Estabilidade garantida, com recursos realocados automaticamente em caso de *downtime.*	Estabilidade garantida, com recursos realocados automaticamente em caso de *downtime.*
Suporte somente em horário comercial.	Suporte 365x24x7	Suporte 365x24x7

Fonte: Mandic (sem data).

Tabela 4 – Comparativo dos Aspectos Financeiros entre o Ambiente *On-Premise vs. Cloud Server*

ON-PREMISE	*CLOUD SERVER*	*CLOUD SERVER* GERENCIADO
A empresa banca os custos de compra e licença de *hardwares* e de *softwares*. Custo também com a manutenção e atualização dos mesmos. Necessidade de ter técnicos especializados em *cloud* dentro da empresa ou que possam atender a qualquer emergência, seja qual for o horário.	A empresa banca a contratação de um provedor *cloud* e este cuida da manutenção da infraestrutura. O cliente faz as configurações necessárias no *cloud* para rodar as suas aplicações e precisa arcar com os possíveis problemas em qualquer horário.	A empresa banca somente a contratação de um provedor, que faz o gerenciamento da infraestrutura e das configurações necessárias, estando disponível a qualquer momento se houver problema, sem que você precise se preocupar.
Custo oscila de acordo com a necessidade mensal. Licença de *softwares* e licenças necessárias também são por conta da empresa.	Custo fixo mensal sem a necessidade de gastar com licenças de *softwares*.	Custo fixo mensal sem a necessidade de gastar com licenças de *softwares*.

Fonte: Mandic (sem data).

5. *ZERO TRUST SECURITY MODEL*

Em 2010, John Kindervag, então vice-presidente da empresa *Forrester Research,* que é considerado um dos maiores especialistas em segurança cibernética do mundo, criou o conceito *Zero Trust.* Seu objetivo era acabar com a ideia sobre “rede confiável ou não confiável”, isto é, que os modelos de segurança existentes pressupunham que tudo o que havia dentro de determinada rede deveria ser

RC: 133524
Disponível em: https://www.nucleodoconhecimento.com.br/tecnologia/modelo-zero-trust

confiável, e que todos que a acessassem navegavam com responsabilidade (PALO ALTO, 2022).

Acontece que sob a ótica *Zero Trust*, “confiança é uma vulnerabilidade”. Outro aspecto que compromete a segurança de uma rede ou sistema reside na presunção sobre o fato de que “a identidade de um usuário não seja comprometida e que todos os usuários ajam com responsabilidade e sejam confiáveis”. Tais aspectos estão relacionados ao fato de “uma vez na rede, os usuários – incluindo agentes de ameaças e usuários internos mal-intencionados – são livres para mover-se lateralmente e acessar ou transferir quaisquer dados aos quais tenham acesso” (PALO ALTO, 2022).

Por sua vez, definição obtida no portal Oracle (2022) defende que *Zero Trust* é um modelo de segurança de rede cuja filosofia parte do princípio de que nenhum internauta e nenhum dispositivo, dentro ou fora da rede de uma empresa, pode acessar determinado sistema de TI sem ser verificado de várias maneiras, para que possa obter sua autenticação.

Outra forma de conceituar *Zero Trust* é por meio de outra definição que também é conhecida como segurança sem perímetro. Consiste na “validação de identidades de usuários, direitos de acesso associados a um sistema específico e permite que as organizações gerenciem as identidades digitais dos usuários garantindo o acesso apropriado” (ORACLE, 2022).

A adoção de várias camadas de controle de acesso avançado para acessar os diferentes dispositivos de rede e/ou servidores permite o rastreamento das atividades dos usuários, a partir da criação de relatórios sobre tais atividades, com a finalidade do desenvolvimento de melhores políticas de boas práticas (ORACLE, 2022).

Segundo o portal *Palo Alto Networks Incorporation* (2022), multinacional especializada em segurança cibernética, podem ser relacionados ao *Zero Trust*

alguns *gateways* fragmentados, que irão fornecer visibilidade granular do tráfego, a partir de 7 camadas de inspeção e controle de acesso, ou seja, com política granular da Camada 7.

Trata-se do método Kipling, que abrange os seguintes aspectos: “quem”, “o quê”, “quando”, “onde”, “porquê” e “como” (PALO ALTO, 2022). Com isso, impede-se o acesso de usuários não autorizados à superfície protegida, possível somente na Camada 7. Esta prática impede a transferência não autorizada de dados confidenciais.

Entre os fatores que a *Zero Trust* abrange, estão vários que merecem ser destacados (PALO ALTO, 2022):

1. não significa tornar um sistema confiável, mas sim retirar o aspecto da confiança nas interações entre usuários e sistemas;
2. é uma iniciativa estratégica que ajuda a prevenir violações de dados, eliminando o conceito de confiança da arquitetura de rede de uma organização;
3. baseia-se no princípio de “nunca confie, sempre verifique”;
4. visa proteger ambientes digitais modernos, aproveitando a segmentação de rede, evitando o movimento lateral, fornecendo prevenção de ameaças da Camada 7 e simplificando o controle granular de acesso do usuário;
5. este modelo de confiança continua a estar relacionado com credenciais utilizadas indevidamente;
6. permite a identificação de uma “superfície de proteção”. A superfície de proteção é composta pelos dados, ativos, aplicativos e serviços mais importantes e valiosos da rede – DAAS (*Desktop as a Service*);
7. as superfícies de proteção são exclusivas para cada organização. Como contém apenas o que é mais crítico para as operações de uma organização, a superfície de proteção é muito menor do que a superfície de ataque e sempre pode ser conhecida;

8. uma vez identificada a superfície de proteção, pode-se identificar como o tráfego se move na organização em relação à superfície de proteção, ou seja, entender quem são os usuários, quais aplicativos eles estão usando e como estão se conectando é a única maneira de determinar e aplicar a política que garante o acesso seguro aos seus dados;
9. ao entender as interdependências entre DAAS, infraestrutura, serviços e usuários, os controles devem ser colocados o mais próximo possível da superfície de proteção, criando ao redor da superfície um micro perímetro**,** que vai se mover com a superfície de proteção para onde o usuário se direcionar.

Por sua vez, o portal Oracle (2022) lista os princípios da arquitetura de Zero *Trust* segundo definições do *National Institute of Standards and Technology* (NIST):

1. todas as fontes de dados e serviços de computação são consideradas recursos;
2. toda a comunicação é segura, independentemente da localização da rede; localização da rede não implica confiança;
3. o acesso a recursos empresariais individuais é concedido por conexão; a confiança no solicitante é avaliada antes que o acesso seja concedido;
4. o acesso aos recursos é determinado pela política, incluindo o estado observável da identidade do usuário e o sistema solicitante, e pode incluir outros atributos comportamentais;
5. a empresa garante que todos os sistemas próprios e associados estejam no estado mais seguro possível e monitora os sistemas para garantir que permaneçam no estado mais seguro possível;
6. a autenticação do usuário é dinâmica e estritamente imposta antes que o acesso seja permitido; esse é um ciclo constante de acesso, verificação e avaliação de ameaças, adaptação e autenticação contínua.

6. IMPORTÂNCIA DA SEGURANÇA *ZERO TRUST* PARA OS ESTADOS UNIDOS

As inseguranças existentes na proteção de dados sensíveis de usuários de diferentes sistemas e redes virtuais não são recentes. Há relatos que os vírus surgiram no final da década de 1970, inicialmente infectando *drives* ou disquetes (SANTOS, 2022). Contudo, dez anos depois os crimes cibernéticos projetaram exponencialmente seus níveis de periculosidade, chegando ao momento atual com diferentes modalidades e grupos de criminosos especializados no mundo virtual, como demonstra o quadro I.

Quadro 1 – Surgimento de Vírus e *Malwares* entre 1980 e 2012

Data	Tipo de Vírus/Malware	Histórico/Criador	Fonte de consulta
1982	Elk Cloner	Foi o primeiro vírus utilizado de forma massiva. Atingiu computadores com o sistema Apple II.	Pimentel (2021)
1984	Core Wars	Foi criado nos laboratórios Bell Computers. Mais forte que os vírus anteriores, comprometia a memória RAM das máquinas.	Pimentel (2021)
1985	Brain e Bouncing	Considerado o primeiro vírus capaz de contaminar computadores pessoais.	Pimentel (2021)
1989-1990	Trojan ou Cavalo de Troia. Considerado o primeiro *ransomware*.	Foi desenvolvido por Joseph Frank Popp. Sua finalidade era infectar computadores. No início, afetava apenas a plataforma Windows. Ao evoluir, passou a atingir as plataformas Apple, Android e Linux, e no presente, atingem até os *smartwatches*.	Pimentel (2021, p.3-4); Formasier (2020); Lema e Freitas (2021)
1992	Vírus Michelângelo	Criado para ser inativo e indetectável até o dia 06 de março, aniversário do artista, e a partir dessa data, ele corrompia os arquivos, sobrescrevendo caracteres aleatórios.	Pimentel (2021, p.3-4)
1999	Vírus Melissa	Criado por David L. Smith, considerado o primeiro a empregar engenharia social	Pimentel (2021, p.3-

RC: 133524
Disponível em: https://www.nucleodoconhecimento.com.br/tecnologia/modelo-zero-trust

		para ser espalhado, que ocorre por *email*, partindo de um dos contatos da vítima.	4)
2000	Vírus *I love you*	Infectou milhões de usuários do Windows, incluindo o Pentágono e a CIA. Espalhava-se por email, contendo um anexo denominado Love-letter-for-you, que, ao ser executado, retransmitia a mensagem para todos os contatos do usuário.	Pimentel (2021, p.3-4)
2005-2006		A empresa Trend Micro, na Rússia, descobre *malwares* que compactam e sobrescrevem alguns tipos de arquivos, ocasionando sequestro de dados. O objetivo era pedir resgate dos dados.	Brito (2016)
2012		Disseminação de casos pela Europa e América do Norte	Brito (2016)

Fonte: Santos (2022, p. 138-9).

Os graves ataques que ocorreram a partir dos anos 1990, realizados por meio de *malwares* muito aperfeiçoados foram transformados em *ransonwares*, ou seja, são novos *malwares*, que realizam o bloqueio, sequestro e embaralhamento dos dados pessoais e financeiros existentes nos dispositivos eletrônicos, com o objetivo de obter o pagamento de resgate (LEMA e FREITAS, 2021, apud SANTOS, 2022).

Nesta perspectiva, cabe descrever as invasões mais recentes feitas contra empresas de porte norte-americanas.

Em matéria publicada pelo jornal espanhol *El País*, Saiz (2014) reporta que em 2013 a proteção aos dados governamentais era pauta prioritária do Governo Obama, devido ao fato de as “incursões de piratas informáticos causaram prejuízos de 24 a 120 bilhões de dólares (57,9 a 289,5 bilhões de reais) às empresas em 2013, segundo um relatório do Centro de Estudos Estratégicos e Internacionais (CSIC)”. À época, o exército chinês foi apontado como responsável por esse ataque, tanto pelo governo norte-americano, quanto pelos meios de comunicação e empresas multinacionais.

Em 09 de maio de 2021 a Colonial Pipeline, maior gasoduto norte-americano, que distribui diariamente mais de 2,5 milhões de barris de óleo - volume equivalente a 45% do abastecimento de diesel, gasolina e querosene de aviação da costa leste dos EUA - foi vítima de um dos maiores ataques cibernéticos da história daquele país (BBC NEWS, 2021).

Ainda segundo o portal BBC News (2021), “um grupo de *hackers* desconectou completamente a rede e roubou mais de 100 GB de informações do oleoduto da empresa Colonial”. O golpe foi atribuído ao grupo *hackers DarkSide*, que se infiltrou na rede. Ao detectar o problema e, para defender seu sistema de dados, a empresa desligou parte dos sistemas para conter a ameaça, ação essa que interrompeu temporariamente todas as operações daquele oleoduto.

O fato levou o governo americano a “decretar estado de emergência em 17 estados, além de suspender as restrições nos horários do transporte rodoviário de combustíveis” até à normalização daquela ocorrência (BBC NEWS, 2021). Neste sentido, Stracqualursi (2021) alega que, mais uma vez, evidenciam-se as vulnerabilidades da infraestrutura do país.

Por sua vez, em junho de 2021 foi a vez da JBS, gigante da indústria de alimentos, que teve todas as suas fábricas e fazendas de suínos instaladas nos Estados Unidos afetadas por um ataque cibernético de grande porte, em dia comemorativo naquele país. Como resultado, o preço da carne bovina subiu exponencialmente (INFOMONEY, 2021).

Para evitar que o ataque atingisse todo o seu sistema e o vazamento de dados, e ainda, ensejando solucionar o reabastecimento com a maior velocidade possível, em uma decisão inédita a JBS optou pelo pagamento de um resgate milionário, da ordem de US$ 11 milhões, contrariando todas as orientações legais (G1, 2021).

Como consequência, o Presidente Joe Biden assinou uma nova Ordem Executiva (GUGELMIN, 2021), relativa à segurança cibernética, na qual foram descritas

algumas exigências sobre a criação de novas soluções, entre elas (BBC NEWS, 2021):

1. que todas as empresas prestadoras de soluções de segurança àquele governo adotem os mesmos padrões;
2. que os fornecedores informem aos órgãos contratantes eventuais falhas identificadas em seus sistemas;
3. que sejam adotadas, em curtos intervalos de tempo, tecnologias de criptografia e autenticação para o governo;
4. criação de uma lista de regras sobre como reagir a ataques futuros.

Com a recente guerra promovida pela Rússia contra a Ucrânia, as autoridades norte-americanas sugerem que empresas e órgãos norte-americanos permaneçam vigilantes contra possíveis ataques cibernéticos russos (CNN BRASIL, 2022).

Gugelmin (2021) refere alguns especialistas em segurança, consultados sobre a referida Ordem, sendo obtidas diferentes opiniões, demonstradas no quadro 2.

Quadro 2 – Opiniões de especialistas sobre a nova Ordem Executiva para Segurança de Dados

Entrevistados	Posição no Mercado	Avaliação	Sugestões
Diversos especialistas	Não informada	Elogiaram a decisão de uma nova Ordem Executiva; questionaram sua efetividade.	-x-
Jeff Hudson	CEO da *Venafi Inc*., empresa privada e especializada em segurança cibernética, chaves criptografadas e certificados digitais	Defende que de nada adiantará uma regulação preventiva a futuros ataques, devido ao fato de aquele governo não deter a velocidade necessária ao acompanhamento do desenvolvimento de *softwares*.	Sugeriu que a indústria de segurança seja incentivada na criação de aplicativos mais seguros
	CEO da *Traceable and Harness*	Concorda com Jeff Hudson.	Sugere que a aplicação de novas decisões sobre

RC: 133524
Disponível em: https://www.nucleodoconhecimento.com.br/tecnologia/modelo-zero-trust

Jyoti Bansal			segurança seja adotada no ciclo de criação de um software, e não quando já estão sendo produzidas
Amit Yoran	CEO da *Tenable* e ex-oficial no Departamento de Segurança Nacional	Considera que uma nova Ordem Executiva é um bom começo.	Reflete sobre a efetividade de uma única iniciativa governamental ou tecnológica ter o poder de evitar novos ataques.

Fonte: Gugelmin (2021).

7. AS BOAS PRÁTICAS DE SEGURANÇA *ZERO TRUST*

Entre as boas práticas necessárias à segurança de máxima confiança, estão os aspectos relacionados à avaliação, detecção e meios de impedir qualquer tipo de fraude. A avaliação está relacionada ao sistema existente, permitindo a implantação de planos de correção; a detecção relaciona-se às tentativas de acesso fora da política existente, e à identificação de eventuais anomalias no momento do acesso aos dados; o impedimento ao acesso dos dados proporciona maior visibilidade dos usuários e das atividades de uma organização (ORACLE, 2022).

Dessa forma, na perspectiva do modelo *Zero Trust*, pode-se considerar o seguinte modelo (ORACLE, 2020):

1. **Princípios de design de segurança como prioridade:**com segurança incorporada para reduzir o risco; virtualização de rede isolada; separação granular de responsabilidades; acesso mínimo ao privilégio;
2. **Segurança automatizada:**para reduzir a complexidade e evitar erros humanos; mitigação e correção automatizadas de ameaças;
3. **Segurança contínua:**para uma proteção perfeita: criptografia onipresente, ativada por padrão; monitoramento contínuo de comportamentos do usuário; autenticação adaptativa com conhecimento de contexto.

8. CONCLUSÃO

A realidade dos fatos obtidos na literatura e apresentados ao longo deste artigo, aliada às práticas profissionais cotidianas me permitem emitir algumas conclusões a respeito de aspectos avaliativos sobre segurança de dados.

Observa-se uma evolução muito significativa do ambiente On-Premise para o ambiente Cloud Computing, tanto no quesito acessibilidade de dados, tão necessária aos usuários em determinado momento, e independentemente de sua localização física, assim como naquilo que se refere às medidas de segurança que visam impedir a ocorrência de ataques criminosos e acesso aos dados sensíveis dos usuários.

Tal evolução surge com o avanço dos recursos das tecnologias de informação, aliados à alta disponibilidade de dados de interesse do usuário onde e quando precisar.

Outra forma de analisar a evolução do ambiente *On-Premise* para *Cloud Computing* consiste no fato de que tal evolução se realiza mediante novas estratégias de recursos, contando com as várias possibilidades para o formato de arquitetura do sistema de arquivo e acesso de dados.

Além desses aspectos específicos, há outro tão importante quanto os mencionados, que reside na questão relativa aos investimentos necessários à cibersegurança, já que a *Cloud Computing* permite a otimização do orçamento existente para a área de TI, além de garantir a continuidade dos negócios, conciliados à manutenção da privacidade de dados.

Por fim, e não menos relevante está a questão da *Zero Trust,* cujos objetivos são pragmáticos: criar barreiras reais aos intrusos quanto ao acesso de dados sensíveis dos indivíduos, por meio das 7 camadas de verificação: “quem, o que, quando, onde, porque e como”, além da sétima camada; eliminar o conceito sobre

navegação responsável por parte de usuários, já que sua premissa consiste em "nunca confiar, sempre verificar".

A adoção da *Zero Trust* visa ainda evitar a ocorrência de ataques cibernéticos, ao invés de apenas interromper sua ocorrência; visa, também, evitar o acesso indevido de dados pessoais e seu vazamento, assim como proteger os ambientes de navegação e todos os sistemas envolvidos.

REFERÊNCIAS

BBC NEWS BRASIL. **O ataque de hackers a maior oleoduto dos EUA que fez governo declarar estado de emergência**. Matéria publicada em 10 mai 2021. Disponível em: https://www.bbc.com/portuguese/internacional-57055618; acesso em 13 out 2022.

BRESSANIN, Lilian. ***On Premises Vs Cloud***: a polarização no ambiente na nuvem. Artigo publicado em 03 ago 2021. Disponível em:

https://www.selectsolucoes.com.br/2021/08/03/on-premises-vs-cloud-a-polarizacao-do-ambiente-na-nuvem/; acesso em 21 set 2022.

CASTRO, Klayton Rodrigues de. **Cloud.Jus**: Arquitetura de Nuvem Comunitária para Provisionamento de Infraestrutura como Serviço no Poder Judiciário da União. Dissertação de Mestrado Profissional em Computação Aplicada, apresentada à Universidade de Brasília (UnB). Brasília, 2019.

CLARANET. **Arquitetura em nuvem**: entenda o conceito do *cloud computing*. 1996-2022. Disponível em: https://br.claranet.com/blog/arquitetura-em-nuvem-entenda-o-conceito-do-cloud-computing; acesso em 14 set 2022.

CNN BRASIL. **FBI alerta para possíveis ataques de *ransomware* após sanções à Rússia**. Disponível em: https://www.cnnbrasil.com.br/internacional/fbi-alerta-para-possiveis-ataques-de-ransomware-apos-sancoes-a-russia/; acesso em 13 out 2022.

FALCÃO, Eduardo; SILVA, Matteus; SOUZA, Clenimar; BRITO, Andrey. **Autenticando aplicações nativas da nuvem com identidades. Capítulo 3.** XXI Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg 2021) p. 100-144. 2021. Disponível em: https://sol.sbc.org.br/livros/index.php/sbc/catalog/download/71/310/566-1?inline=1; acesso em 14 set 2022.

GUGELMIN, Felipe. **Biden assina ordem executiva para combater ataques virtuais nos EUA**. Matéria publicada em 14 mai 2021. Disponível em: https://canaltech.com.br/seguranca/biden-assina-ordem-executiva-para-combater-ataques-virtuais-nos-eua-185034/; acesso em 11 out 2022.

G1. **JBS diz que pagou US$ 11 milhões em resgate a ataque hacker em operações nos EUA.** Matéria publicada em 09 jun 2021. Disponível em:

https://g1.globo.com/economia/noticia/2021/06/09/jbs-diz-que-pagou-11-milhoes-em-resposta-a-ataque-hacker-em-operacoes-nos-eua.ghtml; acesso em 13 out 2022.

IBM. **Soluções de segurança *Zero Trust***. 2022. Disponível em: https://www.ibm.com/br-pt/security/zero-trust; acesso em 14 set 2022.

INFOMONEY. **Prejuízo do ataque hacker contra JBS se estendeu à indústria de alimentos dos EUA**. Matéria publicada em 11 jun 2021. Disponível em: https://www.infomoney.com.br/mercados/prejuizo-do-ataque-hacker-contra-jbs-se-estendeu-a-industria-de-alimentos-dos-eua/; acesso em 13 out 2022.

SANTOS, Levi Alves dos. **Os ataques *ransomware* e a camada de proteção em sistemas governamentais.** Revista Científica Multidisciplinar Núcleo do Conhecimento. Ano. 07, Ed. 08, Vol. 04, pp. 132-161. Agosto de 2022. ISSN: 2448-0959, Link de acesso: https://www.nucleodoconhecimento.com.br/tecnologia/ataques-ransomware, DOI: 10.32749/nucleodoconhecimento.com.br/tecnologia/ataques-ransomware.

MANDIC – *A Claranet Group Company*. ***On premise vs Cloud Computing***. Artigo sem data. Disponível em: https://blog.mandic.com.br/artigos/on-premise-vs-cloud-servers/; acesso em 21 set 2022.

MONTEIRO, Matheus Antonio; BORGES, Leandro. **Viabilidade da arquitetura em nuvem para instituições educacionais.** Revista Eletrônica de Computação Aplicada, vol. 1, p.142-161.

ORACLE. **Modelo de segurança de confiança zero**. 2022. Disponível em: https://www.oracle.com/br/security/what-is-zero-trust/; acesso em 14 set 2022.

PALOALTO NETWORKS. **O que é arquitetura de Confiança Zero**? 2022. Disponível em: https://www.paloaltonetworks.com.br/cyberpedia/what-is-a-zero-trust-architecture; acesso em 14 set 2022.

PEDROSA, Paulo H. C.; NOGUEIRA, Tiago. **Computação em Nuvem.** Artigo publicado em 2011. Disponível em:

https://www.ic.unicamp.br/~ducatte/mo401/1s2011/T2/Artigos/G04-095352-120531-t2.pdf

REDHAT. **O que é a arquitetura de nuvem?** Publicado em: 24 de junho de 2019. Disponível em: https://www.redhat.com/pt-br/topics/cloud-computing/what-is-cloud-architecture; acesso em 14 set 2022.

SALESFORCE. **CRM ou ERP? CRM e ERP? Entenda a diferença**. Artigo publicado em 27 dez 2016. Disponível em: https://www.salesforce.com/br/blog/2016/10/CRM-ou-ERP-Entenda-a-diferenca.html; acesso em 27 set 2022.

SAIZ, Eva. **Os EUA criam uma rede de segurança para proteger as empresas contra ataques cibernéticos**. Matéria publicada em 12 fev 2014. Disponível em: https://brasil.elpais.com/brasil/2014/02/12/internacional/1392230992_753620.html; acesso em 11 out 2022.

SANTOS, Levi Alves dos. **Os ataques *ransomware* e a camada de proteção em sistemas governamentais**. Revista Científica Multidisciplinar Núcleo do Conhecimento. Ano. 07, ed. 08, vol. 04, pp. 132-161. Agosto de 2022. ISSN: 2448-0959, Link de acesso: https://www.nucleodoconhecimento.com.br/tecnologia/ataques-ransomware, DOI: 10.32749/nucleodoconhecimento.com.br/tecnologia/ataques-ransomware; acesso em 13 out 2022.

SOUSA, Flávio R. C.; MOREIRA, Leonardo O.; MACHADO, Javam C. **Computação em Nuvem: Conceitos, Tecnologias, Aplicações e Desafios. Cap. 7.** 1Publicado no ERCEMAPI 2009. Todos os direitos reservados a EDUFPI. 2ª. versão. Setembro de 2010.

STRACQUALURSI, Verônica. **Ataque cibernético provoca fechamento de um dos principais oleodutos dos EUA**. Matéria publicada em 08 mai 2021. Disponível em: https://www.cnnbrasil.com.br/internacional/ataque-cibernetico-provoca-fechamento-de-um-dos-principais-oleodutos-dos-eua/; acesso em 13 out 2022.

TD SYNNEX**. Como surgiu a *Cloud Computing*?** 2022. Disponível em: https://digital.br.synnex.com/bid/332223/como-surgiu-a-cloud-computing; acesso em 30 set 2022.

TI INSIDE. ***Cloud Computing*. Em busca de velocidade, 4 em cada 5 bancos planejam ou já estão migrando *mainframes* para a nuvem**. 04 mai 2022. Disponível em: https://tiinside.com.br/04/05/2022/em-busca-de-velocidade-4-em-cada-5-bancos-planejam-ou-ja-estao-migrando-mainframes-para-a-nuvem/]; acesso em 21 set 2022.

TIGRE, Paulo Bastos; NORONHA, Vitor Branco. **Do mainframe à nuvem: inovações, estrutura industrial e modelos de negócios nas tecnologias da informação e da comunicação**. R.Adm., São Paulo, vol.48, n.1, p.114-127, jan./fev./mar. 2013. Disponível em: https://www.revistas.usp.br/rausp/article/view/55835; acesso em 21 set 2022.

TOTVS. **O que é ERP?** Artigo publicado em 20 jul 2022. Disponível em: https://www.totvs.com/blog/erp/o-que-e-erp/; acesso em 27 set 2022.

Enviado: Novembro, 2022.

Aprovado: Novembro, 2022.

[1] Bacharel em Ciências da computação UNIB - Universidade Ibirapuera. Pós-gradução: Especialização - Projetos e Arquiteturas em Cloud Computing - Anhanguera. Pós-gradução: Especialização - Segurança da Informação e Gestão de TI - Laureate – FMU. ORCID: 0000-0002-1645-6358.