

FACIMP WYDEN

LUIS FELIPHI MARINHO SILVA

Matricula: 202208664113

ATIVIDADE PRÁTICA DE PESQUISA: COMPUTAÇÃO EM NUVEM

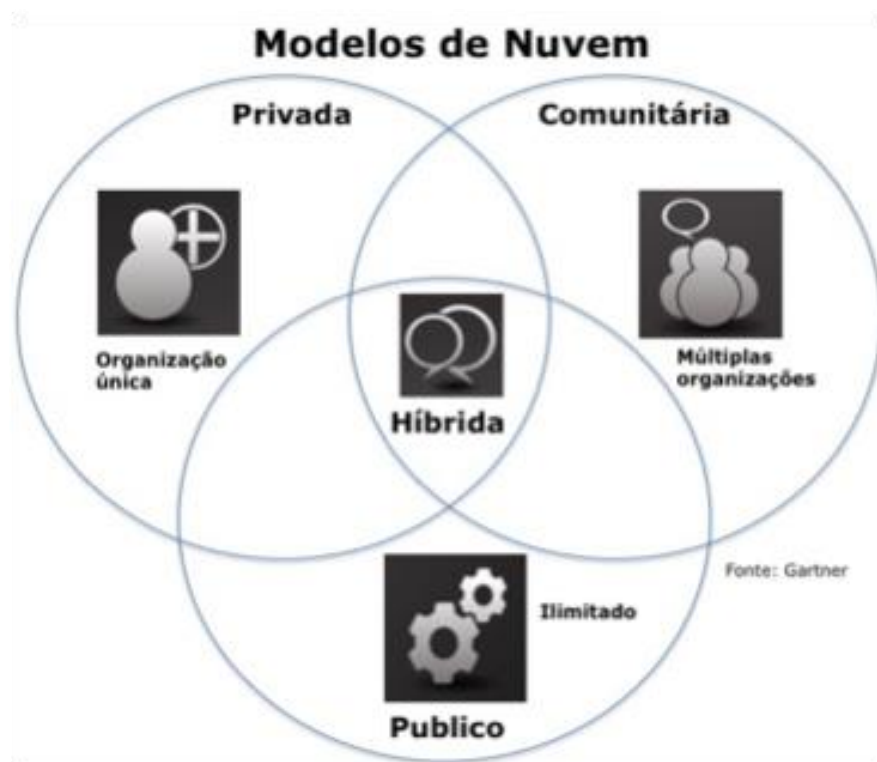
IMPERATRIZ – MA

2023

MODELO DE COMPUTAÇÃO EM NUVEM

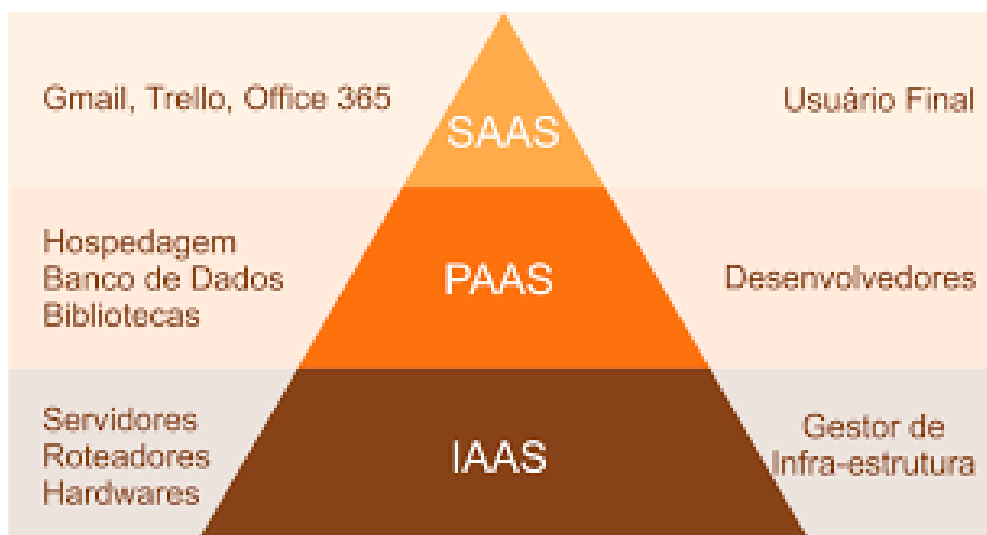
DEFINIÇÃO E TIPOS DE NUVENS:

- **Nuvem pública:** A nuvem pública é um tipo de computação em que os recursos são oferecidos por um provedor terceirizado pela Internet e compartilhados por organizações e indivíduos que querem usá-los ou comprá-los. Alguns recursos de computação em nuvem pública estão disponíveis gratuitamente, e os clientes podem pagar por outros recursos por meio de modelos de preços de assinatura ou pagamento por uso.
- **Nuvem privada:** Uma nuvem privada é um ambiente de computação em nuvem dedicado a uma única organização. Qualquer infraestrutura de nuvem tem recursos de computação subjacentes, como CPU e armazenamento, que você provisiona sob demanda por meio de um portal de autoatendimento. Em uma nuvem privada, todos os recursos estão isolados e sob o controle de uma organização. Assim, a nuvem privada também é chamada de nuvem interna ou corporativa.
- **Nuvem híbrida:** Uma nuvem híbrida é um ambiente de computação misto em que aplicativos são executados usando uma combinação de computação, armazenamento e serviços em diferentes ambientes: nuvens públicas e privadas, incluindo data centers ou locais de "borda". As abordagens de computação em nuvem híbrida são difundidas porque quase ninguém hoje depende totalmente de uma única nuvem pública.
- **Nuvem comunitária:** uma nuvem comunitária é aquela criada por uma federação de nuvens privadas pertencentes a entidades com mesmos fins ou objetivos.



TIPOS DE SERVIÇO

- **IaaS (Infraestrutura como Serviço):** A IaaS (infraestrutura como serviço) é um tipo de serviço de computação em nuvem que oferece recursos fundamentais de computação, armazenamento e rede sob demanda e pagos conforme o uso. Com a IaaS, você não precisa arcar com o custo e a complexidade de comprar e gerenciar os servidores físicos e a infraestrutura do datacenter. Cada recurso é oferecido como um componente de serviço separado e você só paga por um recurso específico durante o tempo em que precisa dele.
- **PaaS (Plataforma como Serviço):** O PaaS (plataforma como serviço) é um ambiente de desenvolvimento e implantação completo na nuvem, com recursos que permitem a você fornecer tudo, desde aplicativos simples baseados em nuvem até sofisticados aplicativos empresariais habilitados para a nuvem. Você adquire os recursos necessários por meio de um provedor de serviços de nuvem com pagamento conforme o uso e os acessa por uma conexão com a Internet segura. Assim como IaaS, PaaS inclui infraestrutura, servidores, armazenamento e rede, além de middleware, ferramentas de desenvolvimento, serviços de BI (business intelligence), sistemas de gerenciamento de banco de dados e muito mais. O PaaS é criado para dar suporte ao ciclo de vida do aplicativo Web completo: compilação, teste, implantação, gerenciamento e atualização.
- **SaaS (Software como Serviço):** O SaaS (Software como Serviço) permite aos usuários se conectar e usar aplicativos baseados em nuvem pela Internet. Exemplos comuns são email, calendário e ferramentas do Office (como Microsoft Office 365). O SaaS fornece uma solução de software completa que você pode comprar em uma base paga conforme o uso por um provedor de serviço de nuvem. Você pode alugar o uso de aplicativo para sua organização e seus usuários se conectarem a ele pela Internet, normalmente por um navegador da Web. Toda a infraestrutura subjacente, middleware, software de aplicativo e dados de aplicativo ficam no datacenter do provedor de serviços. O provedor de serviço gerencia hardware e software e, com o contrato de serviço apropriado, garante a disponibilidade e a segurança do aplicativo e de seus dados. O SaaS permite que sua organização entre em funcionamento rapidamente com um aplicativo por custo inicial mínimo.



FUNDAMENTOS DA COMPUTAÇÃO EM NUVEM

VANTAGENS E DESVANTAGENS:

Benefícios da computação em nuvem:

- **Maior rapidez no tempo de lançamento:** É possível ativar novas instâncias ou desativá-las em segundos, permitindo que os desenvolvedores acelerem o desenvolvimento com implantações rápidas. A computação em nuvem oferece suporte a inovações, facilitando o teste de novas ideias e o desenvolvimento de novos aplicativos sem limitações de hardware ou processos de aquisição lentos.
- **Escalabilidade e flexibilidade:** A computação em nuvem oferece mais flexibilidade para sua empresa. É possível escalar rapidamente recursos e armazenamento horizontalmente para atender às demandas de negócios sem precisar investir em infraestrutura física. As empresas não precisam pagar ou criar a infraestrutura necessária para dar suporte aos níveis mais altos de carga. Da mesma forma, elas podem escalar verticalmente se os recursos não estiverem sendo usados.
- **Ajuda a economizar dinheiro:** Seja qual for o modelo de serviço de nuvem escolhido, você paga apenas pelos recursos que realmente usa. Isso ajuda a evitar o excesso de criação e provisionamento do seu data center, além de permitir que as equipes de TI tenham mais tempo para se concentrar em tarefas mais estratégicas.
- **Melhor colaboração:** O Cloud Storage permite que você disponibilize os dados onde estiver, sempre que precisar. Em vez de estarem vinculados a um local ou dispositivo específico, as pessoas podem acessar dados de qualquer lugar do mundo e de qualquer dispositivo, desde que tenham uma conexão de Internet.
- **Segurança avançada:** Apesar das percepções conhecidas, a computação em nuvem pode fortalecer sua postura de segurança devido à profundidade e amplitude de recursos de segurança, à manutenção automática e ao gerenciamento centralizado. Provedores de nuvem confiáveis também contratam os melhores especialistas em segurança e empregam as soluções mais avançadas, oferecendo uma proteção mais robusta.
- **Prevenção contra perda de dados:** Os provedores de nuvem oferecem recursos de backup e recuperação de desastres. Armazenar dados na nuvem em vez de localmente pode ajudar a evitar a perda de dados em caso de emergência, como mau funcionamento do hardware, ameaças mal-intencionadas ou até mesmo um simples erro do usuário.

Limitações da computação em nuvem

Como qualquer tecnologia, há prós e contras na computação em nuvem.

Por exemplo, uma das desvantagens mais comuns da computação em nuvem é que ela depende de uma conexão de Internet. A computação tradicional usa uma conexão com fio para acessar dados em servidores ou dispositivos de armazenamento. Com a computação em nuvem, uma conexão ruim pode impedir que você acesse as informações ou aplicativos necessários.

Até mesmo os principais provedores de serviços de nuvem podem enfrentar um tempo de inatividade devido a um desastre natural ou um desempenho mais lento devido a um problema técnico inesperado que pode afetar a conectividade. O acesso aos serviços em nuvem pode ser bloqueado até que o problema seja resolvido.

Veja abaixo outras desvantagens da computação em nuvem:

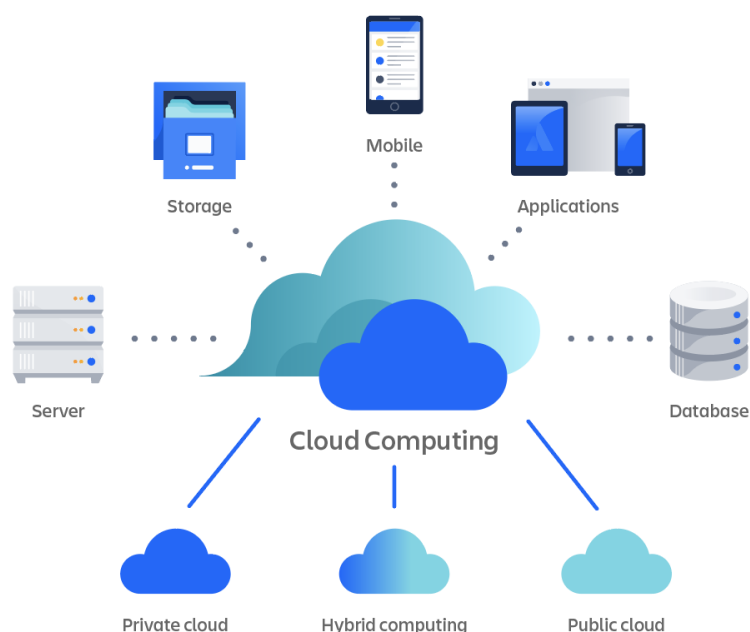
- Risco de dependência do fornecedor;
- Menos controle sobre a infraestrutura em nuvem subjacente;
- Preocupações sobre riscos de segurança, como privacidade de dados e ameaças on-line;
- Complexidade de integração com os sistemas existentes;
- Custos imprevistos e despesas inesperadas.

A boa notícia é que você pode solucionar a maioria dessas desvantagens fazendo uma pesquisa e avaliando cuidadosamente os provedores de serviços de nuvem e os modelos de serviço deles. Muitos dos problemas que surgem durante a migração para a nuvem são resultado de uma falta de compreensão clara sobre o que os provedores oferecem, os modelos de preços e as tarefas de segurança que continuam sendo de responsabilidade do cliente. Além disso, ao escolher uma plataforma de nuvem aberta, você tem mais flexibilidade e liberdade para criar e operar onde necessário. Além disso, é possível fazer a integração perfeita com os serviços que quiser.

ARQUITETURA DE NUVEM:

Projetar uma plataforma de nuvem exige mais do que apenas abstrair os recursos computacionais dos componentes de hardware. É dessa forma que os provedores criam e oferecem a infraestrutura de nuvem aos usuários. A arquitetura também precisa de um grau maior de desenvolvimento para incorporar a containerização, orquestração, interfaces de programação de aplicações (APIs), roteamento, segurança, gerenciamento e software de automação.

A arquitetura de nuvem varia de acordo com o que você quer fazer. No entanto, a maioria das nuvens requer software de automação, gerenciamento, middleware e hardware. A maioria das nuvens também usam a virtualização para abstrair os recursos de hardware em data lakes com gerenciamento central. Já outras nuvens conhecidas como bare-metal conectam os clientes diretamente ao hardware.



Tecnologias para Computação em Nuvem

Provedores de Nuvem:

Google Cloud Platform: A Google Cloud Platform oferece uma ampla variedade de serviços, desde Computação em Nuvem e armazenamento de dados até Inteligência Artificial e Machine Learning.

Atualmente, a GCP conta com mais de 150 produtos em diversas áreas, incluindo:

- Computação em Nuvem: máquinas virtuais, contêineres e funções de Nuvem para atender a diferentes necessidades de computação.
- Armazenamento em Nuvem: Google Cloud Storage e o Google Cloud SQL, que permitem armazenar e gerenciar dados de forma eficiente.
- Banco de dados: Google Cloud Spanner, Google Cloud SQL e o Google Cloud Bigtable.
- Análise de dados: Google Cloud BigQuery, que permite analisar grandes conjuntos de dados em questão de segundos.
- Inteligência Artificial (IA) e Machine Learning: Google Cloud AI Platform, que permite criar, treinar e implantar modelos de aprendizado de máquina.
- Rede e segurança: Google Cloud Load Balancing, Google Cloud CDN e o Google Cloud Armor.
- Ferramentas para desenvolvimento de aplicativos: Google Cloud Functions e o Google Kubernetes Engine, que permitem criar e implantar aplicativos de forma rápida e fácil.
- Internet das Coisas (IoT): Google Cloud IoT Core, que permite conectar e gerenciar dispositivos IoT.
- Gerenciamento de operações: Google Cloud Monitoring e o Google Cloud Logging, que permitem monitorar e gerenciar aplicativos em tempo real.

AWS: A AWS é projetada para permitir que provedores de aplicativos, ISVs e fornecedores hospedem seus aplicativos com rapidez e segurança, tanto aplicativos existentes quanto um novo aplicativo com base em Software como serviço. Você pode usar o AWS Management Console ou APIs de serviços da web bem documentados para acessar a plataforma de hospedagem do aplicativo da AWS.

Seus principais serviços são:

- Computação.
- Armazenamento.
- Banco de dados.
- Redes e entrega de conteúdo.
- Análises.
- Machine learning.
- Segurança, identidade e conformidade.

Azure: O Azure é a plataforma de nuvem pública da Microsoft. O Azure oferece uma ampla coleção de serviços, incluindo PaaS (plataforma como serviço), IaaS (infraestrutura como serviço), DBaaS (banco de dados como serviço) e funcionalidades de serviços de bancos de dados gerenciados.

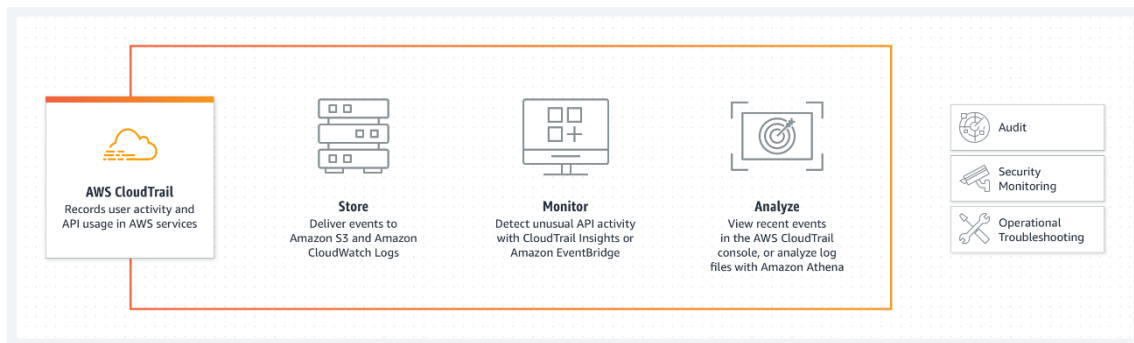
O Azure, como outras plataformas de nuvem, se baseia em uma tecnologia conhecida como virtualização. A maioria dos hardwares de computador pode ser emulada no software.

IBM: IBM Cloud (antiga Bluemix) é a plataforma de nuvem como um serviço (PaaS) da IBM. Oferece funções e serviços fáceis de integrar, permite a criação de novos aplicativos ou a migração daqueles existentes, implementações no local ou fora, tanto para serviços de nuvem IaaS ou PaaS.

ORACLE: A Oracle Cloud Infrastructure (OCI) fornece capacidade de computação rápida, flexível e acessível para atender a qualquer necessidade de carga de trabalho, desde instâncias bare metal de alto desempenho e VMs flexíveis até contêineres leves e computação serverless.

Ferramentas de Gestão:

AWS CloudTrail: O AWS CloudTrail monitora e registra a atividade da conta por toda a infraestrutura da AWS, oferecendo controle sobre o armazenamento, análise e ações de remediação.



Google Analytics: Esse rec



urso é bastante utilizado para acompanhar o tráfego dos sites e aplicativos, então é comum que ele faça parte das estratégias digitais das empresas. Com a ferramenta, você consegue acessar relatórios de dados coletados sobre o comportamento dos usuários durante a navegação.

Azure PowerShell: O Azure PowerShell foi projetado para gerenciar e administrar recursos do Azure na linha de comando. Use o Azure PowerShell quando quiser compilar ferramentas automatizadas que usam o modelo do Azure Resource Manager.



PowerShell
Microsoft Azure

Teste-o em seu navegador com o Azure Cloud Shell ou instale-o em seu computador local.

SEGURANÇA EM NUVEM

DESAFIOS DA SEGURANÇA E ESTRATEGIA DE MISTIGAÇÃO:

1. Segurança

A proteção de dados ainda é uma das principais preocupações das empresas que buscam contratar serviços em nuvem. À medida que as ofertas aumentam, os clientes tornam-se mais dependentes dessa tecnologia, inserindo dados críticos nos inúmeros sistemas oferecidos. É natural que a segurança seja um tópico de discussão — além de um ponto-chave para determinar a assinatura de um contrato ou a perda de um cliente para o seu concorrente.

Para tanto, é importante que uma fornecedora de serviços em cloud computing tenha amplas práticas de segurança, que envolvam uma hierarquia robusta, com as devidas permissões relacionadas aos devidos cargos. Por exemplo, um funcionário do setor financeiro não deve ter o mesmo nível de acesso de um operador da área de TI. São competências diferentes, para departamentos diferentes.

2. Migração

A migração de ambientes (dos servidores físicos para os virtuais) e até mesmo de fornecedores vem se tornando uma preocupação na mente de quem contrata soluções em cloud computing. Isso porque era muito comum a aplicação do termo **vendor lock in** (similar à “carência” dos planos de saúde ou à fidelidade de uma operadora de telecomunicações). Algo que, no final, restringia a inovação e a mobilidade do cliente, que se via preso em cláusulas contratuais por vezes desfavoráveis.

Hoje, torna-se cada vez mais comum a adoção de sistemas mais abertos e universalizados na nuvem. De acordo com informações levantadas pela consultoria de mercado Statistics, o investimento em capacidade de migração deve chegar ao valor de US\$ 20,65 bilhões até 2027 (eram US\$ 3,35 bilhões em 2017). O motivo disso é levar fluidez e flexibilidade para o cliente.

3. Confiabilidade

Um levantamento conduzido pela *RightScale* entrevistou aproximadamente mil executivos de TI, constatando que 96% deles têm negócios na nuvem. Mais além, pouco mais de 50% responderam em nome de empresas multinacionais. Hoje, mesmo que você não saiba, é bem provável que sua empresa faça uso de algum serviço em nuvem de maneira essencial. Por exemplo, o Google Docs ou o Dropbox.

É natural que existam dúvidas quanto à adoção de um serviço que está fora da zona de conforto do seu data center interno. Porém, praticamente toda a indústria de TI está instalada em ambientes virtualizados. O abandono dos sistemas legados não é mais uma tendência, é uma realidade!

Nos servidores e hardwares físicos, as atualizações são menos frequentes, as ameaças encontram brechas facilmente e os custos de manutenção e equipe são astronômicos. Perante um ambiente virtualizado, estamos falando de diminuir custos na sua empresa sem perder a expertise, ao passo que você sempre se manterá atualizado com práticas universais de segurança e se defenderá de ameaças de forma conclusiva.

Ou seja, ao contrário do que muitos gestores podem supor, os serviços alocados em cloud computing são, na realidade, mais confiáveis do que aqueles alocados exclusivamente em servidores físicos.

4. Downtime

Em 2017, o site CRN listou os 10 casos mais impactantes de queda de serviço de empresas que usam ou fornecem cloud computing naquele ano. IBM, Apple e Microsoft tiveram queda brusca em seus serviços, o que gerou impacto direto nos negócios de diversas micro, pequenas e médias empresas. De lá até aqui, as avaliações de downtime (termo aplicado para serviços em queda) são vistas como um fator decisivo na contratação de um novo fornecedor de tecnologia na nuvem.

A isso, dá-se o nome de “SLA”, ou “Service Level Agreement”. No ato da venda, o SLA é uma promessa do fornecedor de que manterá o serviço contratado funcionando por um período majoritário de tempo e, embora ele seja variável, é um detalhe importante: não apenas no valor em si, mas também no que um fornecedor oferece em caso de crise, como recuperação de desastres, tempo de retorno, frequência e velocidade de atendimento.

Por que listamos esse item, mesmo ele sendo uma questão do fornecedor? Porque quando você busca uma empresa que ofereça tecnologia em nuvem, é do seu interesse como contratante se informar sobre os níveis de atendimento e como o seu fornecedor responderá a eventuais downtimes.

Existe redundância de ambientes? Seus sistemas terão algum nível de funcionamento mesmo em queda? Bons fornecedores enfatizam regularmente a sua predileção por ambientes seguros e maleáveis no que tange à sua recuperação. A segurança dos serviços do cliente deve ser prioridade.

5. Gastos

Uma das “lendas” relacionadas à cloud é que a migração dos servidores físicos para ela é onerosa e acaba tornando-se mais cara, tendo em vista a cobrança de mensalidades por parte dos fornecedores de tecnologia em nuvem. Isso se dá porque existe uma crença — infundada — de que um espaço on premise (que depende de hardwares físicos) requer apenas o custeio inicial de instalação.

Entretanto, esse raciocínio falha ao remover da equação os gastos necessários com atualização de software e hardware, as despesas com capacitação e contratação de pessoal para manutenção rotineira dos servidores e outros que, ao final, tornam a opção da nuvem algo financeiramente viável em longo prazo.

Evidentemente, tudo depende do projeto que você busca. A computação em nuvem traz mais flexibilidade na manutenção de todo o ambiente tecnológico. Afinal, você está delegando a responsabilidade de manutenção ao seu fornecedor, por um preço que contemple isso em contrato. Porém, bons fornecedores não trazem soluções prontas, mas sim avaliam a sua atual situação e desenham um projeto especialmente feito para as suas demandas.

O site Enterprisers Project, que reúne depoimentos de CIOs de diversas multinacionais, concorda com essa percepção: “Se a alta resiliência ou bom volume de uptime são as suas prioridades, então, financeiramente, faz sentido migrar para a nuvem”, diz o veículo.

ESTUDO DE CASO:

Cerca de duas em cada cinco (39%) empresas sofreram uma violação de dados em seu ambiente de nuvem em 2022, o que representa um aumento de 4% na comparação com 2021, segundo o Estudo Global de Segurança em Nuvem da Thales, que entrevistou quase 3 mil profissionais de TI e segurança em 18 países.

O estudo também revelou um aumento dramático nos dados confidenciais armazenados na nuvem no ano passado na comparação com o ano anterior. Três quartos (75%) dos entrevistados disseram que mais de 40% dos dados armazenados nos ambientes de nuvem de suas organizações eram “confidenciais”, ante 39% das empresas em 2021.

A principal causa de violações de dados na nuvem foi erro humano (55%), de acordo com o relatório. Isso foi significativamente acima do fator mais alto identificado pelos entrevistados (21%), que foi a exploração de vulnerabilidades.

O relatório destacou também um aumento de 41% no uso de software como serviço (SaaS) de 2021 a 2023, com esses aplicativos substituindo cada vez mais a funcionalidade de aplicativos locais (on premises). Mais da metade dos profissionais de segurança cibernética (55%) disse que essa expansão tornou mais complexa a proteção de dados na nuvem. Além disso, os entrevistados classificaram os aplicativos SaaS como a área mais visada pelos ataques (38%) em 2022, seguidos pelo armazenamento em nuvem (36%).

Outra tendência identificada no estudo foi o aumento contínuo da adoção de várias nuvens, com 79% das organizações pesquisadas tendo mais de um provedor de nuvem em 2022.

O vice-presidente associado técnico da EMEA e segurança de dados da Thales, Chris Harris, disse que os ambientes multicloud criaram mais dificuldades de segurança cibernética para as organizações, pois significa que existem vários controles de segurança e modelos de proteção de dados para entender e implementar.

“Discrepâncias na configuração e compatibilidade podem significar o surgimento de lacunas, aumentando o risco de uma violação ou invasão por um ator mal-intencionado”, destacou. “Isso torna ainda mais importante reconsiderar as medidas de segurança cibernética que estão em vigor quando uma organização move dados críticos para ambientes multicloud, pois as soluções que poderiam ter funcionado em um mundo onde tudo era mantido em ambientes locais provavelmente não são mais suficientes.”

De acordo com a pesquisa, apenas 22% dos entrevistados no estudo relataram que 60% ou mais de seus dados na nuvem são criptografados. Além disso, em média, apenas 45% dos dados confidenciais armazenados na nuvem são criptografados.

REFERÊNCIAS

<https://www.cisoadvisor.com.br/erro-humano-e-a-principal-caoa-de-violacoes-de-dados-na-nuvem/>

<https://docs.aws.amazon.com/>

<https://cloud.google.com/docs>

<https://docs.microsoft.com/pt-br/azure/>