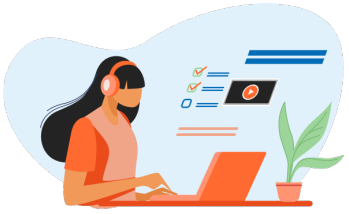
Gestão de datacenter

UNIDADE 1 - CONCEITOS E PROCESSOS BÁSICOS EM DATA CENTER (DC)

Autoria: Melquezedech De Lyra Moura – Revisão técnica: Diógenes Carvalho Matias

Introdução



Em um passado recente, as empresas utilizavam apenas os próprios dados. Com o advento da internet, as fronteiras que separavam os países e, consequentemente, as empresas foram derrubadas. A quantidade de dados limitada de uma empresa passou a ser ilimitada e entre empresas. A necessidade de processamento desses dados antes limitada a um data center local de uma empresa passou a ser terceirizada para outras empresas, que disponibilizam essa solução de forma ilimitada e na nuvem.

Entender os conceitos que amparam o funcionamento de um data center pode ser o ponto de partida para o mundo corporativo responder à necessidade de processamento da quantidade crescente de dados. Alguns assuntos se destacam como base para o estudo da solução em data center, como monitoramento, segurança da informação e *cloud computing.*

A utilização dessa tecnologia vem atrelada à necessidade de monitoramento. O entendimento desses mecanismos possibilita a uma empresa agir de forma eficiente com seus recursos.

A segurança dos dados transitados pelo data center é outro assunto que se destaca para entendimento dessa solução. A segurança está associada às tendências e aos serviços de segurança disponibilizados em data center.

Por fim, uma das principais tecnologias empregadas em data center é a *cloud computing.* Uma ferramenta que possui características essenciais, serviços e implantação, que norteiam a solução em data center.

Dessa forma, nesta unidade, iremos permear esses assuntos para despertar a curiosidade de aprofundamento do tema, a fim de

responder aos seguintes questionamentos: o que é data center? Quais os principais serviços ofertados por essa solução? Em que consiste o monitoramento de data center? O que são prática para integridade desses serviços? Como são caracterizados os serviços de *cloud computing* ou computação em nuvem?

A partir dessas descobertas, conseguiremos vislumbrar as áreas de aplicação dos data centers, que acompanhará as tendências do mundo corporativo. Vamos começar? Acompanhe com atenção!

1.1 Conceitos e infraestrutura de data centers visão geral sobre os itens de data center

O data center é o componente de um conjunto de recursos de tecnologia em serviços de processamento e armazenamento de dados e de informações (VERAS, 2015). No mundo corporativo, as empresas necessitam de um data center para organizar o acesso de usuários, trocar informações com outras empresas e obter locais maiores para armazenar seus dados e suas informações.

Os data centers podem ser segmentados em: data centers empresariais (eDC), que utilizam as instalações da própria empresa, e data centers de internet (iDC), que oferecem serviços na nuvem para outras empresas (VERAS, 2015).

Você o conhece?

David Gauthier é o um dos principais nomes em data center no mundo. Ele é diretor de arquitetura e gerenciamento de design de data center da Microsoft, com mais de 13 anos no setor de data center. Antes ele queria ser cinegrafista. Veja o que ele fala sobre data center no vídeo a seguir:

Acesse (https://www.youtube.com/watch?v=Di2ibzorCm0)

Já os componentes do data center podem ser divididos em blocos: instalações físicas, gerenciamento e Tecnologia da Informação (TI) (VERAS, 2015). As instalações físicas precisam considerar as condições de fornecimento de energia e o clima. O fornecimento de energia tem como objetivo permitir o aumento do consumo da rede de telecomunicações para atender a demanda crescente de processamento e de armazenamento de dados e de informações. Essa mesma demanda impulsiona o gerenciamento voltado para o planejamento e exige uma arquitetura voltada para suportar o planejado, buscando ganhos de escala e busca de eficiência energética.

1.1.1 Principais serviços em data centers

A demanda crescente por armazenamento e processamento em larga escala tem moldado os serviços prestados pelos data centers. Os principais serviços de TI ofertados nos novos níveis de demandas são serviços de: rede, segurança, processamento, armazenamento, virtualização, aplicações, alta disponibilidade e monitoramento, gerenciamento e automação (VERAS, 2015).

Os serviços de rede disponibilizados pelo data center são as conexões realizadas entre os serviços ofertados e os usuários das empresas contratantes. Essas conexões ocorrem por meio dos *switches,* equipamentos que permitem a conexão entre computadores de uma rede. Os *switches* são a evolução dos *hubs*, que retransmitiam os dados e as informações imputadas em uma rede local para todas as estações conectadas àquela rede. Já nos *switches*, os dados e as informações transitam apenas entre os identificados como origem e destino, sem a replicação para todos.

Figura 1 - Conjunto de servidores.
Fonte: iStock (2020).

#PraCegoVer: a imagem traz um conjunto de servidores físicos onde são acoplados os *switches*.

Os serviços de segurança também são ofertados em data centers. Esses serviços são, basicamente, serviços de *firewall*, que são programa de filtragem de acesso. A função do *firewall* é controlar a entrada de usuários, bem como fazer o acompanhamento de sua trilha no data center, e o acesso a dados e informações na rede do data center de indivíduos não autorizados. Hoje, o mercado divide os *firewalls* em três tipos: filtragem de pacotes, aplicações e inspeção de estado (VERAS, 2015).

No serviço de *firewall* de filtragem de pacotes ou *packet filtering*, os acessos de usuários a dados/informações são controlados por critérios pré-estabelecidos – como endereço IP, por exemplo (VERAS, 2015). Esse serviço, geralmente, é ofertado para empresas de pequeno porte.

O *firewall* de aplicações, ou *proxy services,* possibilita a análise de segurança e reconhecimento de protocolos (VERAS, 2015). Isso melhora experiência na internet e de desempenho do data center.

Outro tipo é o *firewall* de inspeção de estado, ou ainda *stateful inspection* (VERAS, 2015). Esse tipo examina o tráfego de dados/informações do data

center para evitar fluxo não autorizado, analisando os pacotes de dados e inspecionando seu estado. Os *firewalls* funcionam como camadas de proteção do data center, garantindo a segurança para a melhoria do tráfego e correto acesso pelos usuários autorizados às informações permitidas ao seu perfil.

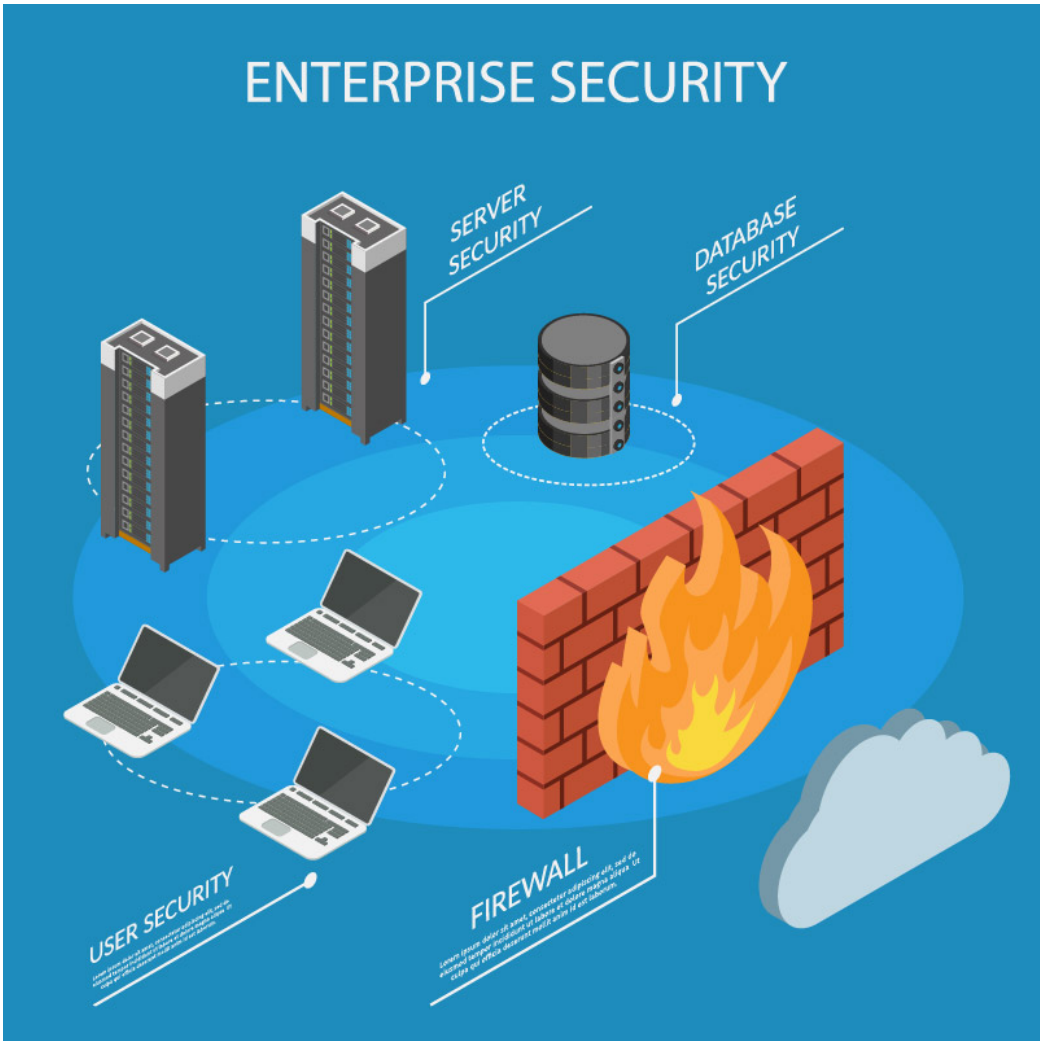


Figura 2 - Central de segurança cibernética.
Fonte: Shutterstock (2020).

#PraCegoVer: a imagem traz o esquema de segurança cujo *firewall* da empresa impede que o servidor de segurança, a base e o usuário sejam atacados por meio da nuvem.

O terceiro tipo de serviços ofertado em data center é o serviço de processamento. É composto por servidores, sistemas operacionais e processadores (VERAS, 2015). Esses dispositivos estão diretamente relacionados ao desempenho (velocidade, por exemplo) dos data centers.
Os servidores são os responsáveis por grande parte do trabalho em um data center (VERAS, 2015). A configuração desses dispositivos pode possibilitar a

disponibilização de aplicações e acelerar o seu funcionamento. Essas configurações classificam os servidores em três principais tipos: servidor de aplicação, servidor de web e servidor de banco de dados (VERAS, 2015).

Num *application server* (servidor de aplicação) ou *middleware*, a configuração é voltada para uma aplicação específica disponibilizada num ambiente com objetivo de aproveitar o processamento desse data center, otimizando a performance (VERAS, 2015).

Já o objetivo do servidor de web é a transferência de dados por protocolo usado na internet para os usuários, hospedagem de arquivos e websites em geral, otimizando os dados dentro dos data centers (VERAS, 2015).

O último tipo de configuração é o servidor de banco de dados. O objetivo dessa configuração é permitir a transferência dos dados entre os componentes do data center, trazendo mais eficiência para os processos que envolvem banco de dados em data centers (VERAS, 2015).

Os sistemas operacionais em data center possuem a capacidade de virtualização desses servidores, gerenciamento de servidores, serviços integrados, *cluster de failover* e DirectAccess (VERAS, 2015). A virtualização permite criar e gerenciar um ambiente de computação de servidor virtualizado. O gerenciamento fornece um ambiente mínimo para executar funções do servidor. Os serviços integrados fornecem uma plataforma unificada na web de acesso ao servidor. O *cluster de failover* minimiza a interrupções nos serviços do data center, criando um ambiente de redundância. Por fim, o DirectAccess permite o acesso à rede do data center a partir de qualquer dispositivo móvel.

O papel dos processadores em data center é melhorar o desempenho dos componentes que compõem o data center. O desempenho, geralmente, está associado à velocidade e à quantidade de dados processados (VERAS, 2015).

Figura 3 - Central de processamento em nuvem.
Fonte: Shutterstock (2020).

#PraCegoVer: a imagem traz blocos de automação, escritórios e servidores com dados processados por um conjunto de servidores externos para processamento central.

Os serviços de armazenamento são o quarto tipo de serviços ofertados em data center. A arquitetura desses serviços é composta por redes de armazenamento e dispositivos de conexão em armazenamento. A disponibilidade e a segurança dos serviços são características desses serviços em data centers.

Outro serviço oferecido por data center é denominado serviços de virtualização, sendo o quinto elencado. Esse serviço permite que os usuários do data center utilizem aplicações em diversos servidores sem a necessidade de conexão no local das aplicações, ou seja, apenas virtualmente. Isso possibilita otimizar a utilização da memória e do processamento.

Os serviços de aplicações – sexto serviço – são outros identificados em data center. Esses serviços envolvem *load balancing, secure socket layer* (SSL), *offloading* e *caching.*

O *load balancing* é o mecanismo que busca equilibrar a carga de aplicações neste serviço. A ligação entre o usuário e o servidor, que equilibra a carga por meio da distribuição do tráfego em diversas zonas de disponibilidade para acesso aos aplicativos, é o *load balancer*.

Para que todas as zonas de disponibilidades estejam seguras, há necessidade de protocolos de segurança projetados para confiabilidade nas comunicações em um data center, permitindo que aplicativos do data center troquem informações em total segurança. Esse protocolo é o SSL. Ele

possibilita o tráfego seguro por meio da proteção adicional de criptografia (usuário e servidor) em transmissão sigilosa e anônima.

O tráfego de dados pode necessitar ser transferido para uma plataforma externa, devido a limitações físicas (hardwares) e gastos de energia nos dispositivos móveis. Essa transferência recebeu o nome de *offloading* e pode utilizar mecanismos como inteligência artificial, *big data*, entre outros.

Para acessar os dados no data center, os usuários compartilham uma conexão, chamada de *proxy*, que tem por função rotear as requisições à rede em que se encontra. Esses *proxys* têm capacidade de armazenar o conteúdo de páginas web, minimizam o consumo de largura de banda e agilizam a navegação. Essa capacidade é denominada *caching* e pode ser aplicada a data center.

O sétimo tipo de serviço são os serviços de alta disponibilidade ou recuperação de desastres. São denominados *high availability* (HA) e *disaster recovery* (DR), que estão amparados em políticas e dispositivos de backup, *restore* e replicação.

As políticas orientam as diretrizes e as estratégias para disponibilidade ou recuperação de desastres. A principal política que viabiliza essas diretrizes e estratégicas é a política de segurança, incluindo as políticas governamentais.

Você quer ver?

A Lei Geral de Proteção de Dados (LGPD) – Lei nº 13.709/2018 – é a legislação brasileira que regula as atividades de processamento de dados pessoais (BRASIL, 2018).

Acesse (http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm)

Um data center pode ser definido por softwares, a sua infraestrutura é virtualizada por abstração, conjunto de recursos e automação. Isso possibilita otimização do gerenciamento, entrega mais rápida dos serviços, redução de custos e ganho de velocidade.

A velocidade como os dados são processados no data center traz a necessidade de dispositivos de backup, *restore* e replicação. O backup possibilita o armazenamento dos dados num local no data center para possibilitar retorná-los para um ponto determinado do armazenamento. Para retornar os dados, é necessário realizar o *restore*. E, para segurança do data

center, muitos dados passam pelo processo de replicação em outro local, além do original. Todos esses processos garantem a segurança e a integridade dos dados.

Por fim, o serviço de monitoramento, gerenciamento e automação é o oitavo serviço ofertado em data center. O monitoramento observa o fluxo de dados e de informação para a identificação do usuário e a verificação do fluxo. O gerenciamento visa à disponibilidade 24 horas por dia e 7 dias por semana, mesmo que remotamente. A automação viabiliza as correções (*patches*) para o perfeito funcionamento do data center.

1.2 Monitoramento de data center (prática): backup eficiente e testes de *restore*

Os serviços de backup e *restore* visam garantir a disponibilidade da infraestrutura de TI e a continuidade dos negócios.

Esses serviços permitem não só a continuidade dos negócios, como também a sustentabilidade empresarial, que objetiva a continuidade de aspectos sociais, econômicos e ambientais (POLETINI, 2016). Os aspectos sociais são aqueles que interferem nas relações sociais que envolvem a empresa utilizadora desses serviços. Os aspectos econômicos envolvem a sustentabilidade do negócio ao longo do tempo. E os ambientais referem-se ao impacto do negócio no ambiente que envolve o negócio.

O backup é uma cópia dos dados de produção com o propósito de recuperar dados apagados ou violados. O *restore* é a recuperação dos dados em si (VERAS, 2015).

Esses processos necessitam ser realizados por várias razões: requisitos de negócio, requisitos legais, proteção contra falhas de hardware, da aplicação ou erro dos usuários, recuperação de desastres e atingimento de níveis de serviços específicos.

A natureza dos dados a serem armazenados desenha a forma do backup. Essa forma passa a exigir uma estratégia de recuperação de dados e uma sequência de testes prevendo a realidade. Dentre os dispositivos mais utilizados no mercado estão fita e disco (VERAS, 2015).

As empresas utilizam a fita como uma escolha natural em virtude do custo-benefício mais baixo em relação aos outros tipos de backups. Nesse tipo de

backup, as empresas devem considerar a rotação das fitas permitidas pelas políticas específicas e o tempo que ficarão armazenadas. Quando utilizada, a encriptação para backup em fita prejudica o desempenho do armazenamento e do *restore*.

A outra forma de backup mais rápida que as fitas é o disco, considerando o tempo de montagem e busca dos dados. O backup em disco permite o acesso aleatório aos dados armazenados, o que otimiza a busca (VERAS, 2016).

Caso

O Superior Tribunal de Justiça (STJ) sofreu um ataque de hackers no dia 3 de novembro de 2020, o que interrompeu o funcionamento das turmas desse tribunal. O tribunal informou que o backup dos sistemas de tecnologia da corte está totalmente íntegro. Contudo, o processo de *restore* ainda não foi realizado, o que fez com que os seus usuários não conseguissem acessar seus próprios arquivos e e-mails. (VALENTE, F. STJ diz ter backup e garante retomada; advogados consideram que episódio é grave. **Conjur**, 6 nov. 2020. Disponível em: **https://www.conjur.com.br/2020-nov-06/stj-backup-advogados-consideram-episodio-grave (https://www.conjur.com.br/2020-nov-06/stj-backup-advogados-consideram-episodio-grave)**. Acesso em: 14 nov. 2020.).

A virtualização planejada, como estratégica de backup e *restore*, chama a atenção para os tipos de backup, bem como para suas respectivas utilidades, a serem realizados na máquina virtual. Esses tipos podem ser segmentados em: desduplicação, arquivamento, replicação, além de considerar os cenários de recuperação de desastres (VERAS, 2016).

1.2.1 Desduplicação

A desduplicação se aplica ao gerenciamento de dados com crescimento exponencial e ao fornecimento de proteção (VERAS, 2016). Essa técnica salva uma cópia de dados e substitui todas as outras cópias por referências que apontam para essa cópia. A desduplicação busca as redundâncias dos dados que vão para o backup, permitindo economia com dados, otimização da capacidade do data center, menor dependência dos backups e recuperação mais ágil após pane. Essa solução pode ser integrada aos backups, aumentando sua eficiência.

1.2.2 Arquivamento

O arquivamento trata da cópia principal dos dados ou das informações de uma empresa (VERAS, 2016). Em geral, esse processo trata dados/informações em sua forma final para conservação por longos períodos. No arquivamento, o acesso e a recuperação têm como objetivo trechos, em vez do backup integral. O crescimento dos números dos dados utilizados pelas empresas em escala global torna o arquivamento muito oneroso. Essa alternativa de tratamento de dados passa a ser improvável para os dias de hoje.

1.2.3 Replicação

A replicação é a tecnologia para proteção de dados e recuperação de desastres (VERAS, 2016), não implicando mobilidade de dados ou espelhamento. A replicação é a cópia de um sistema para outro sistema independente. A distinção entre replicação, mobilidade de dados e espelhamento se dá porque na mobilidade os dados são transferidos de um sistema para outro. Já no espelhamento, há uma replicação, contudo dentro de um único sistema.

A replicação pode ser classificada em replicação síncrona e assíncrona. Na primeira, os dados são escritos na fonte e replicados para um destino remoto. Em geral, esse tipo de replicação ocorre da origem para um ou dois destinos com mais de 200 quilômetros de distância. Na segunda, os dados são escritos na fonte para periodicamente serem transmitidos para o destino de replicação por meio de uma rotina periódica (VERAS, 2016).

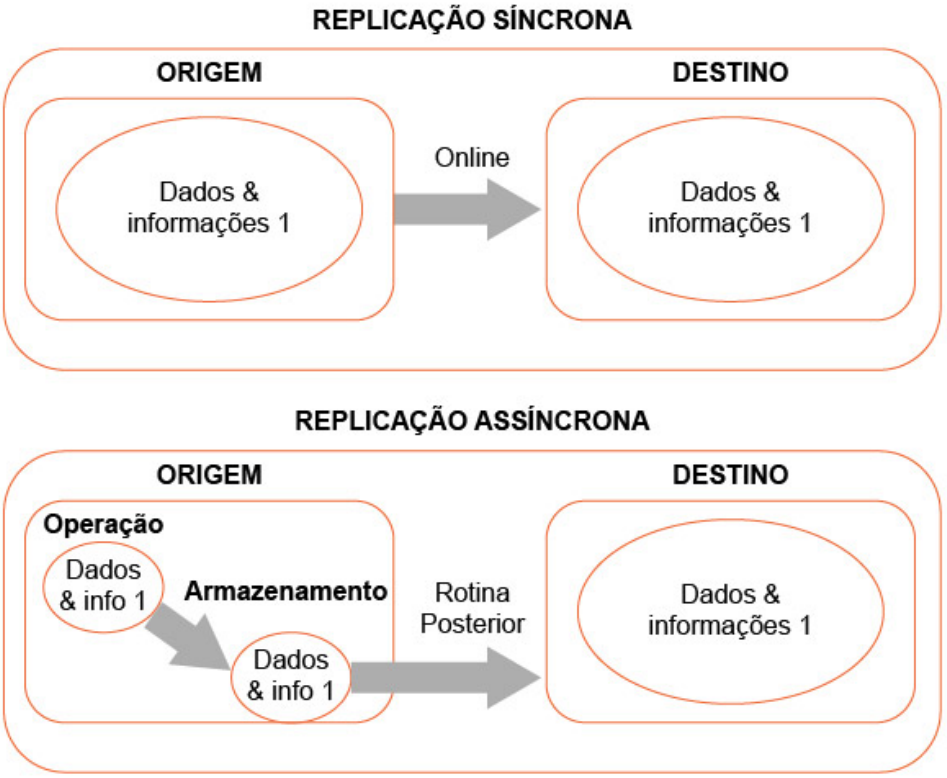


Figura 4 - Replicação síncrona e assíncrona.
Fonte: Elaborada pelo autor, 2020.

#PraCegoVer: a imagem traz um comparativo da réplica síncrona e assíncrona, ilustrando que na primeira os dados transitam entre origem e destino de forma on-line, enquanto na segunda os dados transitam entre origem e destino por meio do armazenamento dos dados na origem em local diferente no sistema para transmissão posterior por rotina para o destino.

1.2.4 Cenários de recuperação de desastres

A recuperação de desastres, associada a alta disponibilidade, constitui parte essencial da continuidade de negócios (*business continuity*). Esses processos associados devem ser pensados em termos de impactos nos serviços prestados pelo data center. A recuperação de desastres é a capacidade de uma empresa, seja ela terceirizada ou não, de reagir à interrupção dos serviços, restaurando as funções essenciais à continuidade de negócios. Já a disponibilidade diz respeito ao tempo em que um sistema está acessível para o seu usuário (VERAS, 2016). Isso pode ocorrer em nível de sistema operacional, para suportar as aplicações do data center, ou em nível de aplicação, para acessar as suas funcionalidades.

Partindo desses dois conceitos, é possível desenhar alguns cenários preliminares. Para se ter alta disponibilidade, faz-se necessário mecanismos

de backup e de *restore* associados a uma alta capacidade de processamento do data center. Quando a capacidade de processamento está abaixo do exigido pela necessidade de alta disponibilidade, os mecanismos de backup e de *restore* ficam comprometidos, retornando uma disponibilidade que pode não atender às necessidades dos usuários do data center. Essa limitação pode ser compensada por outras estratégias, como a desduplicação, contudo pode não garantir a mesma efetividade e eficácia. A alta capacidade de processamento pode ser a chave para uma alta disponibilidade e para mecanismos de backup e de *restore* eficazes (VERAS, 2016).

1.3 Segurança da informação em DC (prática) práticas para integridade dos serviços

As tendências de segurança em data center e os serviços decorrentes dessa necessidade podem ser determinantes na capacidade futura de utilização de ferramentas de segurança nas operações de data center. Dentre os serviços mais utilizados estão autenticação, controle de acesso, confidencialidade de dados, integridade de dados e irretratabilidade. Esses serviços almejam integridade dos dados e verificação dos usuários. Todo esse processo aponta para a segurança da informação como processo voltado para as melhores práticas de mercado nesse segmento (VERAS, 2016).

1.3.1 Tendências de segurança

O Internet Architecture Boad (IAB) elaborou um relatório sobre segurança na arquitetura da internet, que apontava para a necessidade crescente de segurança e levantava as áreas mais sensíveis para mecanismos de segurança (VERAS, 2016). Dentre as áreas levantadas estava a área de proteção de infraestrutura da rede contra monitoração e controle não autorizado do tráfego da rede e de proteção de tráfego entre usuários finais usando mecanismos de autenticação e de criptografia.

Essa necessidade de proteção se deve à vulnerabilidade de segurança dos sistemas operacionais utilizados pelos usuários finais, além das vulnerabilidades nos roteadores de internet e outros dispositivos de rede (VERAS, 2016). Tudo isso compromete a integridade dos dados, bem como dos serviços prestados pelos data centers.

1.3.2 Serviços de segurança

Para fazer frente às vulnerabilidades dos sistemas, surgem os sistemas que procuram garantir a segurança de outros sistemas ou das transferências de dados. Esses sistemas são potencializados quando associados a serviços de segurança alinhados com diretrizes ou políticas de segurança da informação. Os serviços de segurança podem ser divididos em cinco categorias: autenticação, controle de acesso, confidencialidade de dados, integridade de dados e irretratabilidade (CAMELO, 2017).

1.3.3 Autenticação

O foco da autenticação é, como o próprio nome já diz, a autenticidade ou a legitimidade da comunicação em acessos ao data center. Envolve a autenticação das duas pontas da comunicação no data center, origem e destino. Além disso, a autenticação não poderá permitir a interferência no caminho entre as duas pontas da comunicação. A autenticação ocorre de duas formas: autenticação da entidade par e autenticação da origem de dados. A primeira confirma a identidade de uma entidade par associada (origem e destino). A segunda, por sua vez, confirma a origem dos dados (VERAS, 2016).

Outra forma de autenticação muito utilizada no mercado é a autenticação da mensagem. Para autenticar a origem dos dados em uma mensagem, faz-se necessário incluir no processo um segredo compartilhado entre origem e destino. Em outras palavras, o Código de Autenticação de Mensagem ou *message authentication code* (MAC) (FOROUZAN, 2016).

1.3.4 Controle de acesso

O controle de acesso limita e controla o acesso aos sistemas e a suas aplicações. Essa forma de segurança impede o uso não autorizado de recursos do data center (VERAS, 2016). O acesso é concedido de acordo com o perfil estabelecido para cada usuário final. Esses perfis obedecem a diretrizes e políticas de segurança da informação de cada empresa. Via de regra, os perfis obedecem às especificidades dos trabalhos realizados pelos usuários finais.

1.3.5 Confidencialidade de dados

Outra forma de segurança de dados e informações é a confidencialidade, ou seja, a proteção dos dados contra divulgação não autorizada (VERAS, 2016). No mercado, a confidencialidade está atrelada ao público de divulgação dos dados ou das informações. Em tecnologia da informação, a confidencialidade

busca proteger dados de uma conexão, bloco de dados sem conexão, dados por campo selecionado em uma conexão ou bloco de dados, e dados originados em um fluxo de tráfego.

1.3.6 Integridade de dados

A integridade dos dados é a garantia de que os dados recebidos estão como foram enviados pela origem autorizada, sem modificações, inserções, exclusão ou repetição. Pode ser aplicada a um fluxo de mensagens (VERAS, 2016). Esse tipo de serviço de segurança de dados pode ocorrer com ou sem recuperação de dados. A técnica mais efetiva se dá pela proteção do fluxo total da comunicação dos dados, considerando que a origem e o destino estão autenticados.

1.3.7 Irretratabilidade de dados

A irretratabilidade de dados protege contra a negativa de uma parte ter participado de toda ou de parte da comunicação de dados (VERAS, 2016). Pode ocorrer na origem, com a prova de que os dados foram enviados pela parte especificada, ou no destino, quando prova que os dados foram recebidos pela parte especificada.

1.4 *Cloud computing*: introdução e serviços

Inicialmente, as empresas armazenavam e trafegavam apenas os seus próprios dados, que eram limitados em quantidade. Partilhar dados com outras empresas era algo complexo e caro. Via de regra, essa interligação entre empresas era realizada por uma terceira empresa com padrões estabelecidos por nicho de mercado. A internet veio e estabeleceu novos padrões que poderiam ser compartilhados entre empresas, além de reduzir os custos de interligação dessas empresas (VERAS, 2016).

Assim, a internet rompeu as barreiras entre as empresas, aumentando vertiginosamente a quantidade de dados que necessitavam ser armazenados. A TI passou a ser a ferramenta que centraliza o armazenamento e o processamento por meio dos data centers. Para essa nova quantidade de dados, o armazenamento e o processamento físicos passaram a ser o

paradigma de padrões a serem compartilhados entre empresas, dado seu alto custo e sua complexidade. A alternativa para superar esse paradigma foi a *cloud computing* ou computação na nuvem, que é um conjunto de pontos de armazenamento e processamento de dados e informações conhecidos como data centers, interligados pela internet (VERAS, 2016).

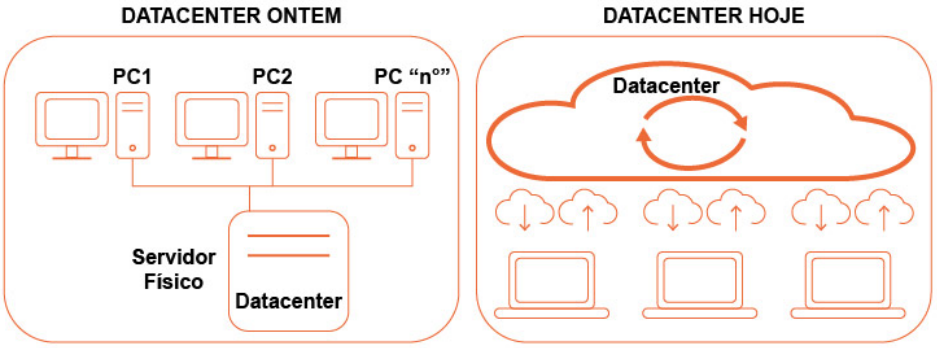


Figura 5 - Modelo data center ontem e hoje.
Fonte: Elaborada pelo autor, 2020.

#PraCegoVer: a imagem traz um comparativo entre o modelo de data center que era utilizado no início da adoção da ferramenta com as interconexões entre os computadores físicos e o servidor de data center, e o modelo que é utilizado hoje na nuvem, com interconexões de forma virtual.

A compreensão do fenômeno de *cloud computing* ou computação na nuvem passa pela resposta às perguntas: qual o conceito de computação em nuvem? Quais as características essenciais da computação em nuvem? Quais os modelos de serviço para computação em nuvem? Quais os modelos de implantação para computação em nuvem? É o que vamos responder nos próximos itens.

1.4.1 Conceito de computação em nuvem

A computação na nuvem é o estágio seguinte do data center, mudando a forma da operação da TI de aquisição de hardwares para aquisição de serviços em TI. Hoje, esses serviços são oferecidos por gigantes da tecnologia, como Amazon, Google e IBM (VERAS, 2016).

Você sabia?

Computação em nuvem crescerá 35,5% no Brasil até o final do ano. Para saber mais, leia a matéria em: **https://diariodocomercio.com.br/inovacao/computacao-em-nuvem-crescera-355-no-brasil-ate-o-final-do-ano (https://diariodocomercio.com.br/inovacao/computacao-em-nuvem-crescera-355-no-brasil-ate-o-final-do-ano)**.

Essa solução de TI é delineada por recursos virtuais acessíveis (hardwares, softwares, plataformas de desenvolvimentos, serviços, entre outros recursos). Por serem virtuais, esses recursos podem ser configurados e reconfigurados de acordo com o acordo de nível de serviços realizado entre a empresa que contratou a computação na nuvem e a empresa ofertante desses serviços (VERAS, 2016).

As configurações realizadas podem utilizar tecnologias como virtualização, arquiteturas de aplicação e infraestrutura orientadas a serviços e tecnologias baseadas na internet para redução dos custos e da complexidade do armazenamento e do processamento de dados e de informações. A empresa contratante pode realizar essa configuração de qualquer lugar do mundo com o mínimo de esforço em gerenciamento e interação com o provedor da empresa contratada (VERAS, 2016).

Na nuvem, o consumidor é o usuário que realiza a configuração (VERAS, 2016). Quem oferta o serviço contratado é o provedor. A ligação entre o usuário e o provedor é realizada pelo integrador. Este gerencia o desempenho e a entrega do serviço pelo provedor. Já o operador é o intermediário que fornece conectividade, ou seja, aquele que fornece o serviço de internet. Esses três papéis podem ser realizados por uma única empresa, embora sejam distintos.

1.4.2 Características essenciais da computação em nuvem

A operação da computação em nuvem possui características essenciais que a distingue das demais operações realizadas na internet, tais como: serviço sob demanda, acesso aos serviços de rede, conjunto de serviços, elasticidade

rápida e medição de serviços (VERAS, 2016).

Primeira característica essencial

A primeira característica essencial, o serviço sob demanda (VERAS, 2016), disponibiliza as funcionalidades da nuvem sem a necessidade de interação humana. Como um serviço de armazenamento e de processamento físico, os data centers são programados pelo ser humano por meio de intervenções diretas.

Segunda característica essencial

O acesso aos serviços de rede, como segunda característica essencial, indica que, quando a empresa contratante necessita dos recursos da nuvem, ela pode acessar o provedor da contratada por meio dos seus usuários autorizados a utilizar os serviços (VERAS, 2016). Esse acesso ocorre por meio de dispositivos móveis (smartphones, tablets, computadores pessoais) remotamente. Já o acesso ao serviço em rede física pressupõe a presença do usuário no local do serviço utilizado.

Terceira característica essencial

O conjunto de serviços utilizados pelos usuários autorizados é outra característica essencial da computação em nuvem (VERAS, 2016). Esses recursos são alocados de acordo com cada nova demanda dos serviços realizada pelos usuários. Numa rede física, haveria necessidade de instalações físicas para atender novas demandas.

A alocação de recursos nos leva à elasticidade rápida dos serviços. Isso significa atender ao crescimento da demanda desse serviço (VERAS, 2016). Na computação em nuvem, quando o usuário necessita acessar uma demanda maior de serviço, deve ter acesso imediato, o que implica uma percepção de serviços ilimitados a qualquer momento. Já no serviço físico, a necessidade de deslocar equipamentos pode tornar inviável o acesso a uma demanda maior do serviço.

Você quer ler?

O livro *Computação em Nuvem (Cloud Computing): tecnologias e estratégias*, de Brian J. S. Chee e Curtis Franklin Jr., oferece uma visão prática sobre serviços em *cloud computing*, destacando a função do provedor de serviços. Os autores traçam um comparativo entre a infraestrutura de TI antes e depois da computação na nuvem, e expõem como essa tecnologia afeta as empresas que a adotam.

Como há possibilidade de acesso a novas e maiores demandas de serviços, a medição de serviços precisa ser em tempo real (VERAS, 2016). Isso traz à tona o imperativo de transparência dos custos de armazenamento e de processamento em nuvem, tanto para o contratante quanto para o contratado.

1.4.3 Modelos de serviços para computação em nuvem

A computação em nuvem pode ser viabilizada em três modelos: infraestrutura como um serviço ou *infrastructure as a service* (IaaS), software como um serviço ou *software as a service* (SaaS) e plataforma como um serviço ou *platform as a service* (PaaS) (VERAS, 2016).

O primeiro modelo fornece infraestrutura de processamento e de armazenamento virtualmente (VERAS, 2016). Há um gerenciamento sobre sistemas operacionais, armazenamento, aplicações instaladas e recursos de redes limitados.

O segundo modelo é recomendado para empresas com grande quantidade de usuários, como substituição ao processamento interno (VERAS, 2016). A nuvem funciona como provedor de serviço de controle e gerenciamento da rede, sistema operacional e servidores de armazenamento e de

processamento, acessados por browser. Um exemplo de SaaS é o Google Apps.

O terceiro modelo busca suportar o desenvolvimento de aplicações para a nuvem, visando oferecer uma operação computacional de forma lógica por regras práticas preestabelecidas (VERAS, 2016).

1.4.4 Modelos de implantação para computação em nuvem

Para implantação dos serviços IaaS, SaaS e PaaS na nuvem, há modelos que permitem a implantação, como a nuvem privada, a nuvem pública e a nuvem híbrida (VERAS, 2016).

A nuvem privada (*private cloud*) ocorre quando a infraestrutura de nuvem de serviços pertence a uma empresa, sendo utilizada pela mesma empresa (VERAS, 2016). Embora não esteja disponível para outras empresas, pode ser gerenciada por uma terceira empresa.

Já a nuvem pública (*public cloud*) pode ser disponibilizada por um ente público ou uma empresa de tecnologia de grande porte com alta capacidade operacional (VERAS, 2016). Essas empresas cobram pelo uso dos serviços.

Teste seus conhecimentos

(Atividade não pontuada)

Para alavancar suas vendas e fazer com que esses clientes realizem mais compras em suas 293 lojas, a empresa deseja realizar um trabalho de *analytics*. Hoje, a empresa não possui capacidade de processamento para analisar a sua base.

Conclui-se que, para realizar essa operação, a empresa de departamentos necessita contratar um data center na nuvem para aumentar a sua capacidade de processamento.

Vamos Praticar!

Uma empresa de departamentos conta com 293 lojas. Cerca de 60% dos seus clientes realizam mais compras em outras empresas do mesmo segmento. Além disso, essa

empresa possui dez anos de registros de atendimento desses clientes.

As informações desses clientes compartilhadas com outras empresas são escassas na sua base.

Por fim, na nuvem híbrida (*hibrid cloud*), há nuvens públicas e privadas conectadas por tecnologias que viabilizam a transmissão de dados e a utilização de aplicações (VERAS, 2016).

Teste seus conhecimentos

(Atividade não pontuada)

Conclusão

Chegamos ao fim da primeira unidade desta disciplina, que abordou a definição de data center, uma ferramenta que auxilia as empresas a realizar o processamento e o armazenamento dos dados e das informações de uma empresa nas suas interações com outras.

Além disso, pudemos compreender os contextos organizacional e mercadológico em que ocorre a utilização da ferramenta data center.

Nesta unidade, você teve a oportunidade de:

- conhecer o conceito de data center e seus principais serviços;
- observar como se dá o monitoramento em data center;
- identificar as tendências de segurança da informação e de serviços de segurança que garantam a integridade dos serviços em data

center;

tomar consciência do fenômeno mercadológico da *cloud computing.*

Referências

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2020]. Disponível em: **http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm (http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm)**. Acesso em: 6 dez. 2020.

CAMELO, S. H. H. (org.). **Gestão de serviços de tecnologia hospitalar**. São Paulo: Pearson Education do Brasil, 2017.

FOROUZAN, B. A. **Redes de computadores**: uma abordagem top-down. São Paulo: McGraw Hill, 2013.

POLETINI, R. A. **Data center**. São Paulo: Viena, 2016.

VERAS, M. **Virtualização**: tecnologia central do data center. 2. ed. São Paulo: Brasport, 2016.

VERAS, M. **Computação em nuvem**: nova arquitetura de TI. São Paulo: Brasport, 2015.