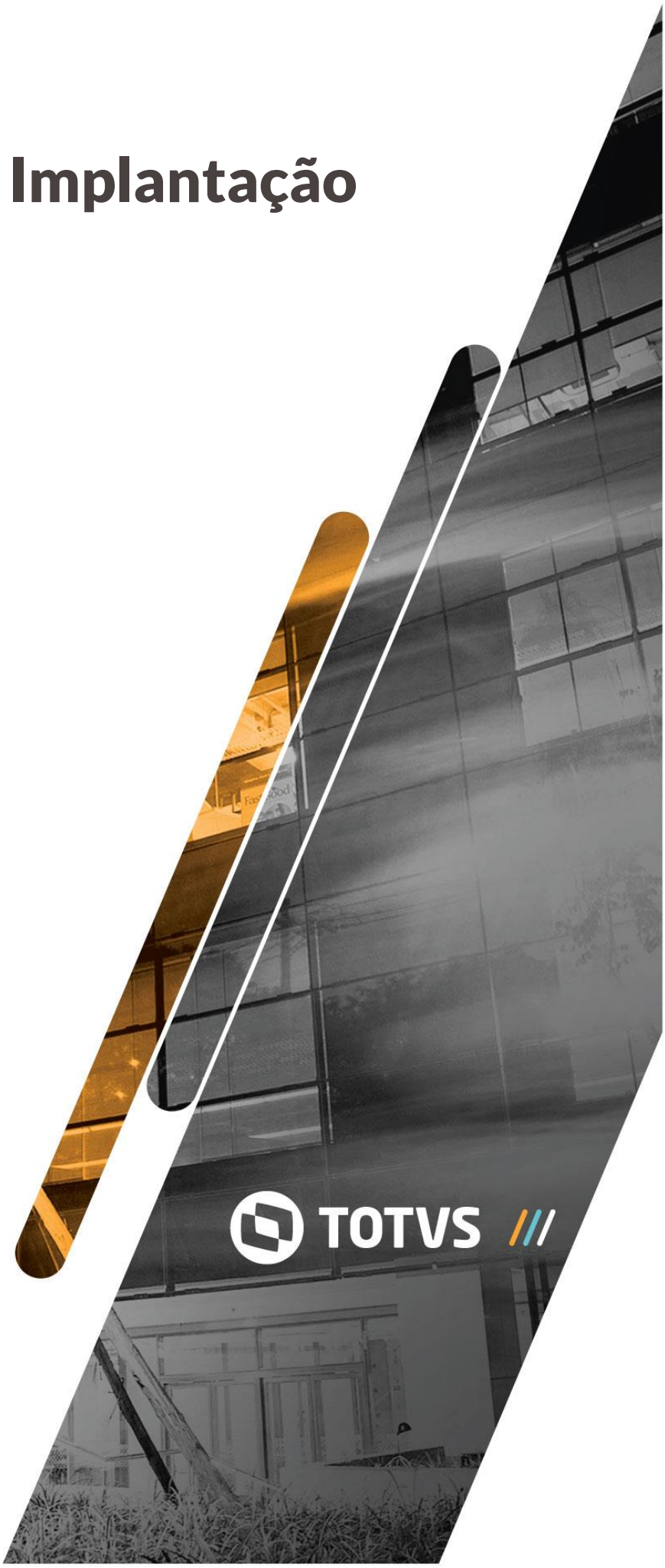
Requisitos de Implantação

Soluções Digitais



Sumário

Este documento é propriedade da TOTVS. Todos os direitos reservados. ©
Este documento é propriedade da TOTVS. Todos os direitos reservados. ©

1. Dados Gerais

Este documento busca descrever todos os requisitos necessários para implantação da Plataforma digital, juntamente com sistemas integradores.

2. Pré-requisitos - Obrigatórios.

2.1. Infraestrutura.

- Disponibilizar acesso aos ambientes, onde se consiga realizar troubleshooting de instalação, caso necessário;
- Disponibilizar servidores distintos para ambiente de homologação e produção;
- Recomenda-se servidores segregados de acordo com a criticidade de cada sistema envolvido, porém pode haver coexistência com outras aplicações TOTVS, desde que respeite os requisitos mínimos de cada aplicação;
- Todas as versões de sistema operacional podem ser evoluídas conforme orientação da TOTVS. Os avisos de modificação de infraestrutura são enviados com até seis meses de antecedência;

2.2. Contas de Desenvolvedor e Publicações nas Lojas.

A Plataforma digital necessita da criação de uma conta de desenvolvedor que possibilita a publicação dos aplicativos nas lojas.

As manutenções dessas contas devem ser realizadas periodicamente **pelo responsável da infraestrutura do "cliente**", pois conforme normativas do Google e Apple os dados de segurança e outras políticas devem ser constantemente atualizados trazendo mais tranquilidade para os usuários das aplicações.

- Apple: A conta de desenvolvimento da Apple tem um custo anual de US$99,00.
- Google: A conta de desenvolvimento do Google tem um custo único de US$25,00.

As manutenções das contas são realizadas periodicamente, pois conforme normativas do Google e Apple os dados de segurança e outras políticas devem ser constantemente atualizados trazendo mais tranquilidade para os usuários das aplicações.

2.3. Certificado Digital.

No projeto de Plataforma digital a informação do cliente é um ativo inviolável e, portanto, ele deve estar protegido do risco de incidentes, acessos indevidos ou mesmo adulteração de dados.

A Plataforma digital deve adotar padrões de segurança que permite exposição e consumo seguro de APIs, assim como padrões rígidos de segurança no processo de comunicação e transmissão da informação (validação de certificado digital, criptografia, etc).

Isso ajuda garantir o sigilo da informação, desde o aplicativo do cliente até o sistema transacional ou “legado” do banco.

Este documento é propriedade da TOTVS. Todos os direitos reservados. ©
Este documento é propriedade da TOTVS. Todos os direitos reservados. ©

Um requisito indispensável é disponbilizar Certificado de Aplicação SSL/TLS na camada de publicação de endereços e na publicação de aplicativos Mobile (IOS/Android).

A Tabela abaixo apresenta como sugestão, entidades que emitem certificados digitais. Ficando da escolha do cliente à escolha da entidade para compra e sua posterior manutenção/renovação.

EMPRESA	CERTIFICADORA	NOME PRODUTO	PERÍODO	VALOR
UOL	Geotrust	OV AVANÇADA SUBDOMÍNIOS	12 meses	R$ 1.7990,90
DigitalSign	Thawte	Thawte SSL WildCard	12 meses 24 meses	R$ 1.495,00 R$ 2.650,00
RapidSSL	Geotrust	GeoTrust True BusinessID WildCard	12 meses 24 meses	R$ 1.980,00 R$ 3.762,00
GoDaddy	GoDaddy	OV SSL Deluxe	12 meses 24 meses	R$ 1.599,00 R$ 2.879,98

3. Arquitetura da Infraestrutura e das Aplicações

O modelo de de arquitetura envolve diversos mecanismos relacionados a segurança de software, mas muitas das recomendações estão diretamente ligadas à infraestrutura. Entre outras coisas, recomenda-se que o tráfego de informações entre a aplicação e o servidor de banco de dados seja criptografado e autenticado com certificado digital.

As características de segurança da informação e segurança de infraestrutura são responsabilidade da instituição usuária e são transparentes para o software aplicativo.

Porém deve ser considerado os seguintes componentes:

- Possuir o serviço de WAF que seja a primeira linha de defesa contra esses tipos de ataques aaplicação e ataques de DDoS.
- Possuir ferramentas de detecção e prevenção de intrusão para que esta seja a segunda linha de defesa, contra esses tipos de ataques aplicação e ataques de DDoS.
- Possuir ferramenta de endpoint protection que tenha função de IDS/IPS, firewall e anti malware e ser a terceira linha de defesa.
- Possuir um DB Firewall, para dessa forma detectar acessos indevidos ao Banco de Dados ou ataques do tipo SQL Injection.

A figura 1 demonstra todas as tecnologias envolvidas no fluxo dos produtos mencionados neste documento.

Este documento é propriedade da TOTVS. Todos os direitos reservados. ©
Este documento é propriedade da TOTVS. Todos os direitos reservados. ©

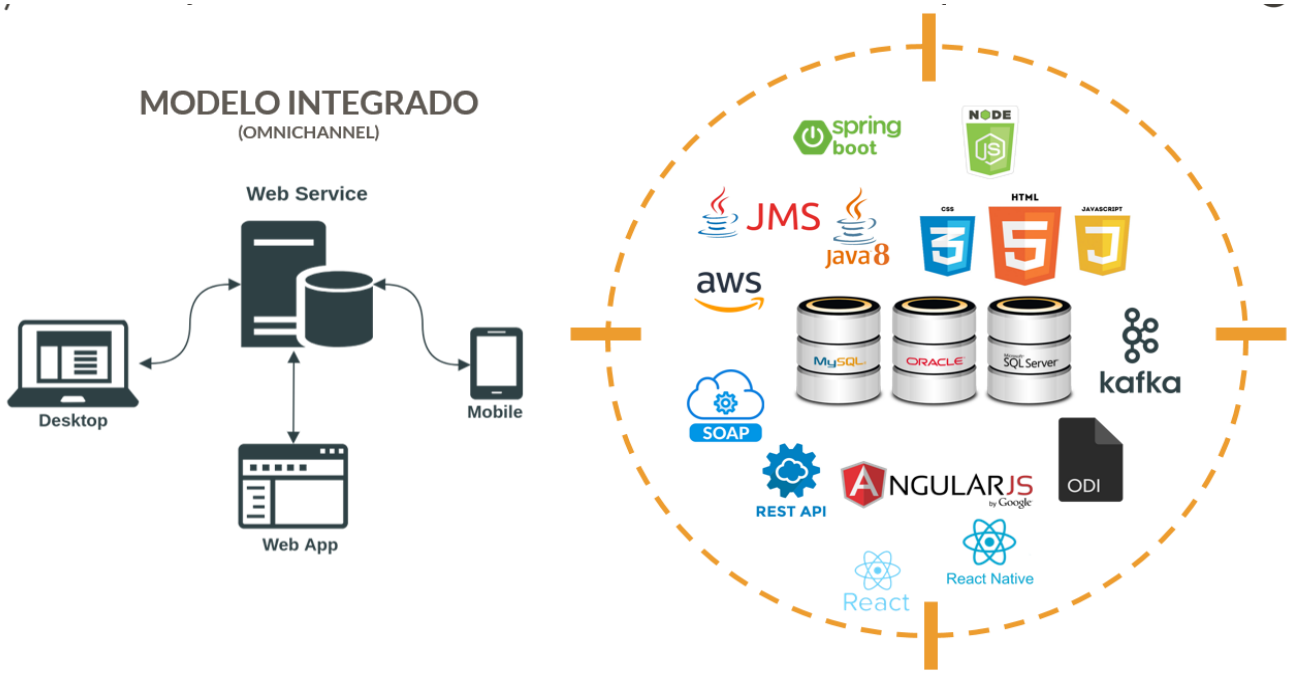


Figura 1– Parque Tecnológico dos Produtos.

3.1. Arquitetura On Premise

Na Figura consta um diagrama macro do ambiente sugerido para a implantação da plataforma digital, bem como suas integrações com serviços externos e os outros sistemas do cliente.

No modelo On Premise importante ressaltar que na arquitetura de servidores e aplicação que ficam armazenados localmente. Nesse modelo questão como diponibilidade, escalabilidade além de outros requisitos de TI precisam ser contemplados.

Este documento é propriedade da TOTVS. Todos os direitos reservados. ©
Este documento é propriedade da TOTVS. Todos os direitos reservados. ©

ARQUITETURA SOLUÇÕES DIGITAIS

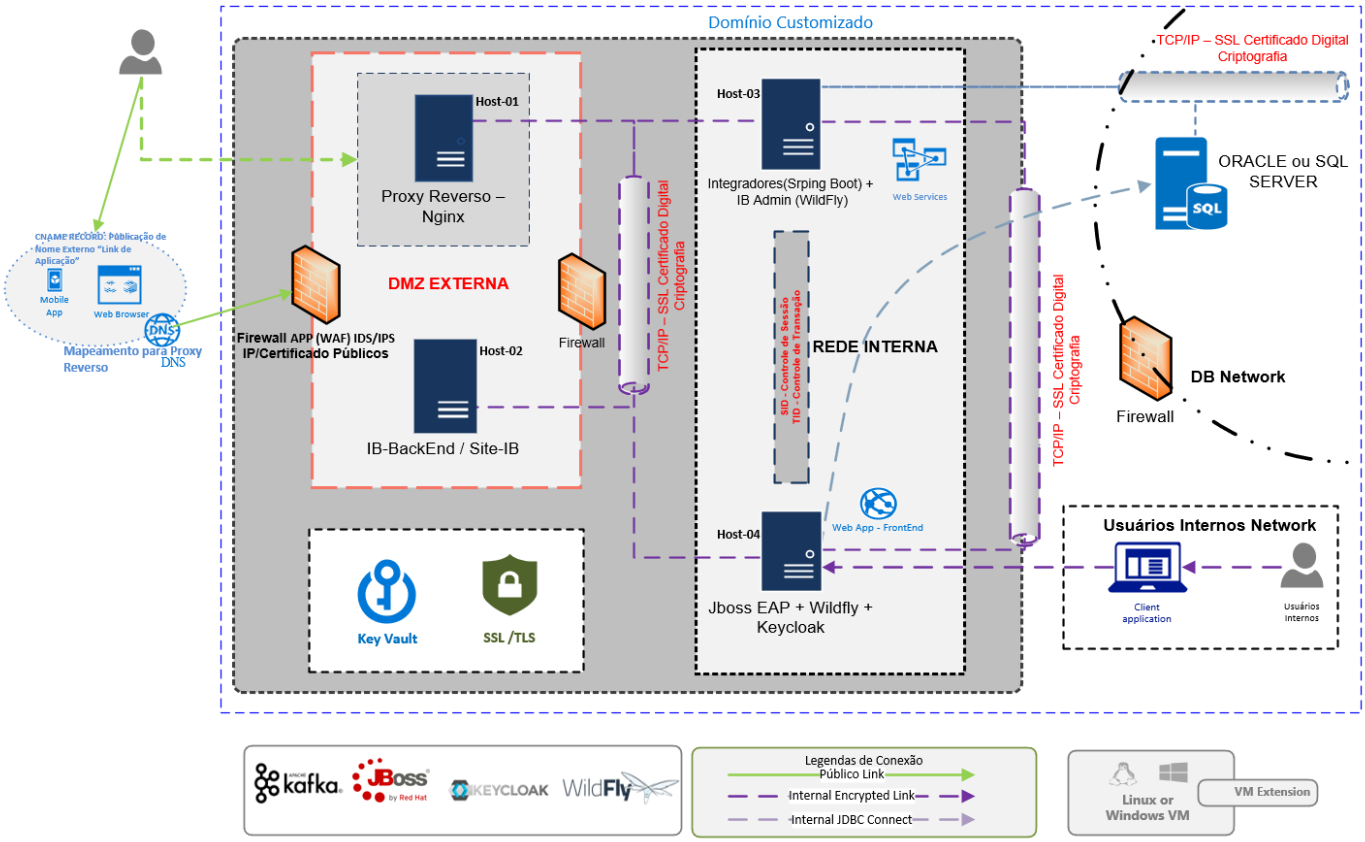


Figura 2 - Visão macro da arquitetura do ecossistema.

3.2. Arquitetura Amazon AWS.

Amazon Web Services, também conhecido como AWS, é uma plataforma de serviços de computação em nuvem, que formam uma plataforma de computação na nuvem oferecida pela Amazon.com. Os serviços são oferecidos em várias geográficas distribuídas pelo mundo.

O diagrama da figura 3, presenta o modelo de responsabilidade compartilhada que AWS disponibiliza a seus clientes, quando esses adquirem alguns dos serviços.

Nesse modelo aspectos de segurança e conformidade são o foco central dessa forma é entendido que mesmo é uma responsabilidade compartilhada entre a AWS e o cliente. Esse modelo Segurança e conformidade é uma responsabilidade compartilhada entre a AWS e o cliente.

Esse modelo compartilhado pode ajudar a aliviar a carga operacional do cliente à medida que a AWS opera, gerencia e controla os componentes do sistema operacional host e da camada de virtualização até a segurança física das instalações nas quais o serviço opera.

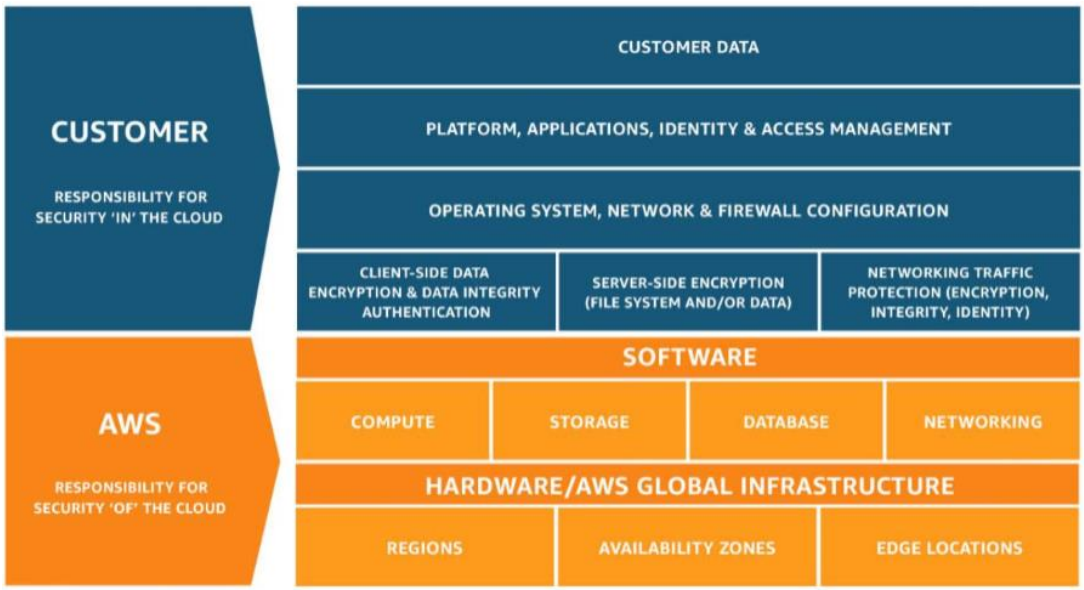


Figura 3 - Modelo de Responsabilidade Compartilhada AWS

A descrição completa desse modelo pode ser obtida junto ao site da AWS:

- https://aws.amazon.com/pt/compliance/shared-responsibility-model/

3.2.1. Diagrama da Aplicação e Fluxo de Dados AWS

Nesse tópico importante detalhar o diagrama da aplicação e fluxo de dados para aplicação provisionadas na AWS, buscando demonstrar que o processo de construção dessa arquitetura precisar ser completa e precisa. A figura

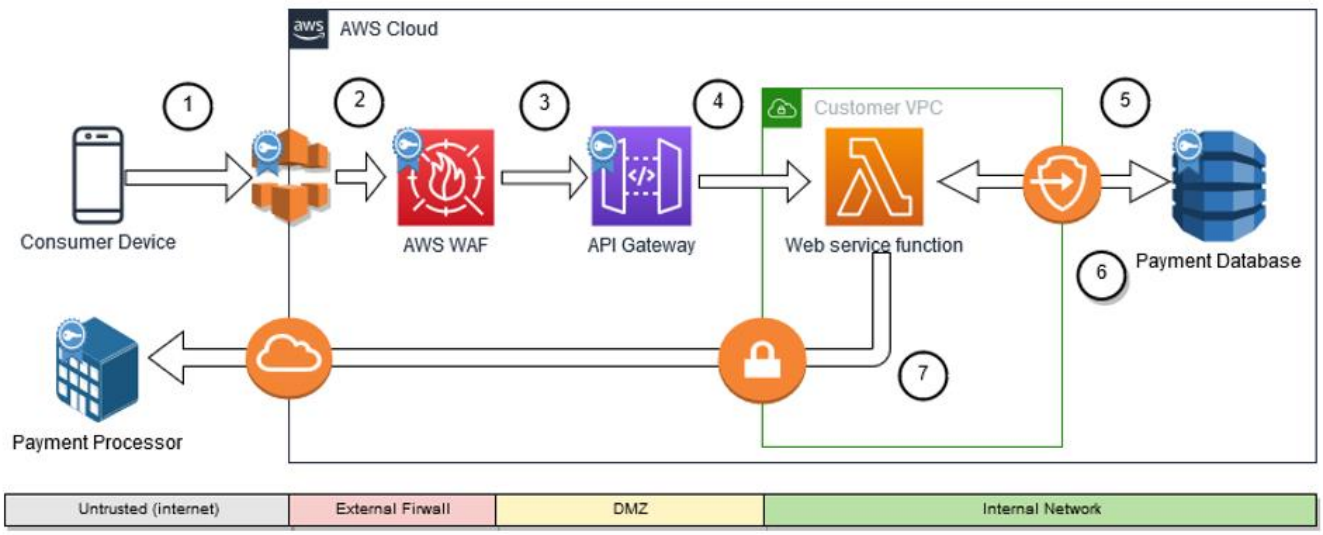


Figura 4 – Diagrama de Aplicação AWS

Este documento é propriedade da TOTVS. Todos os direitos reservados. ©
Este documento é propriedade da TOTVS. Todos os direitos reservados. ©

3.3. Arquitetura Microsoft Azure.

O Microsoft Azure é uma plataforma destinada à execução de aplicativos e serviços, baseada nos conceitos da computação em nuvem.

O diagrama da figura 4, presenta o modelo de responsabilidade compartilhada que Azure plataforma de cloud da Microsoft disponibiliza a seus clientes, quando esses adquirem alguns dos serviços.

Figura 5 - Modelo de Responsabilidade Compartilhada Microsoft Azure

A descrição completa desse modelo pode ser obtida junto ao site da Microsoft

- https://docs.microsoft.com/pt-br/azure/security/fundamentals/shared-responsibility

3.3.1. Diagrama da Aplicação e Fluxo de Dados Azure.

Nesse tópico importante detalhar o diagrama da aplicação e fluxo de dados para aplicação provisionadas na Azure, buscando demonstrar que o processo de construção dessa arquitetura precisar ser completa e precisa.

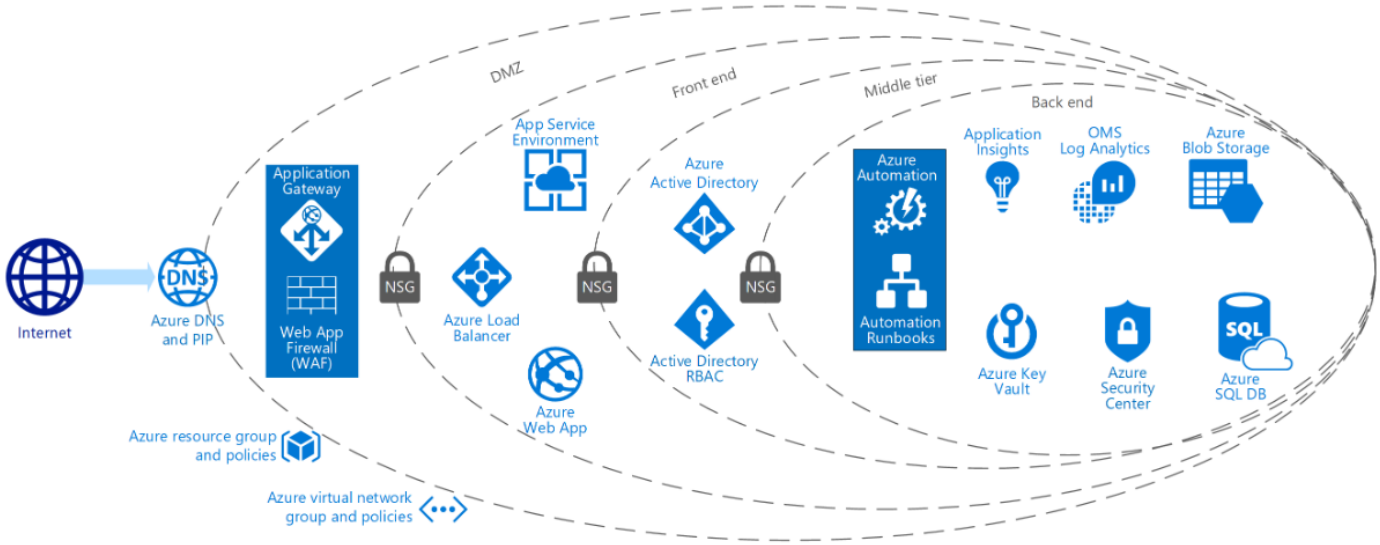


Figura 6 – Diagrama de Aplicação AWS

4. Distribuição das Aplicações por camadas.

Nesse tópico apresentamos a distribuição das aplicações e uma breve descrição.

Figura 7 – Distribuição por Camadas.

Este documento é propriedade da TOTVS. Todos os direitos reservados. ©
Este documento é propriedade da TOTVS. Todos os direitos reservados. ©

Camada de Sistema Operacional, necessário para executar os sistemas.

Oracle JVM (JDK8) é um componente de desenvolvimento para construir e publicar aplicativos, applets e componentes usando a linguagem de programação Java.

Camada de Application Servers, utilizada para publicar as aplicações de Serviços (backend) e Frontend.

Camada de Integração utilizada pelo sistema de frontend da aplicação.

Camada de Serviço que é utilizada para sistema de frontend de aplicação.

Camada de frontend que é publicada para utilização do usuário final..

A figura 8 apresenta a distribuição para componente da arquitetura, considerando a função de componete da aplicação criada.

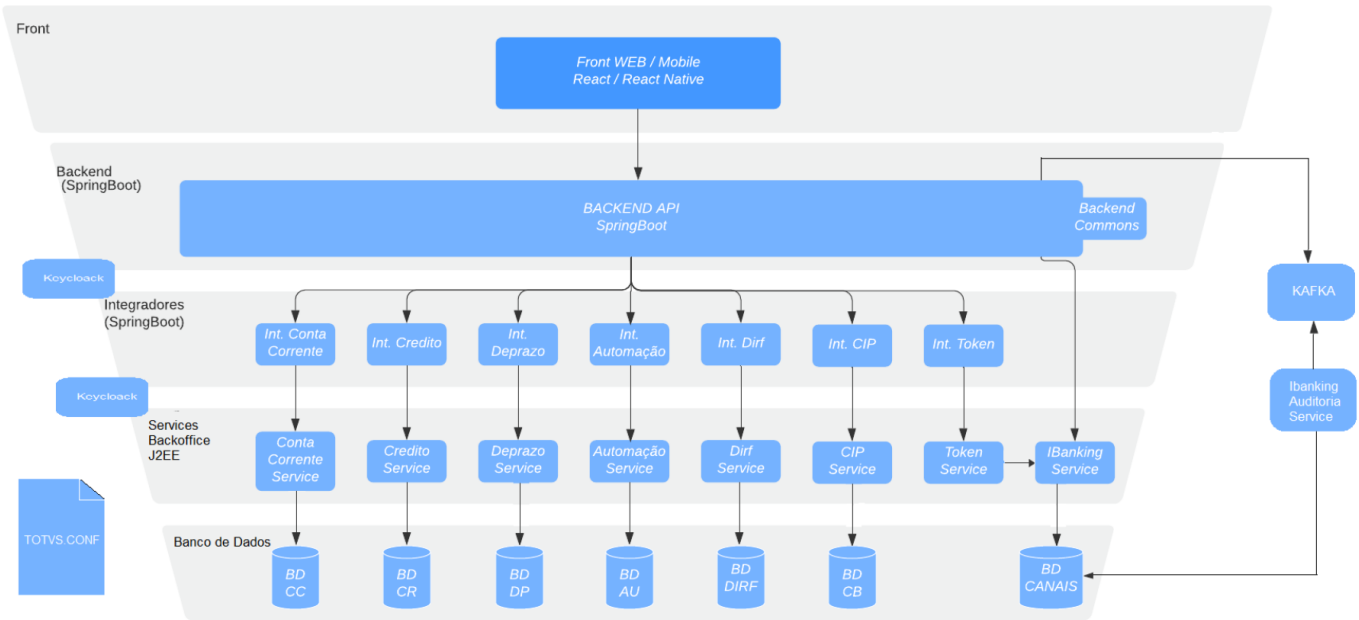


Figura 8 – Distribuição da Aplicação por camada.

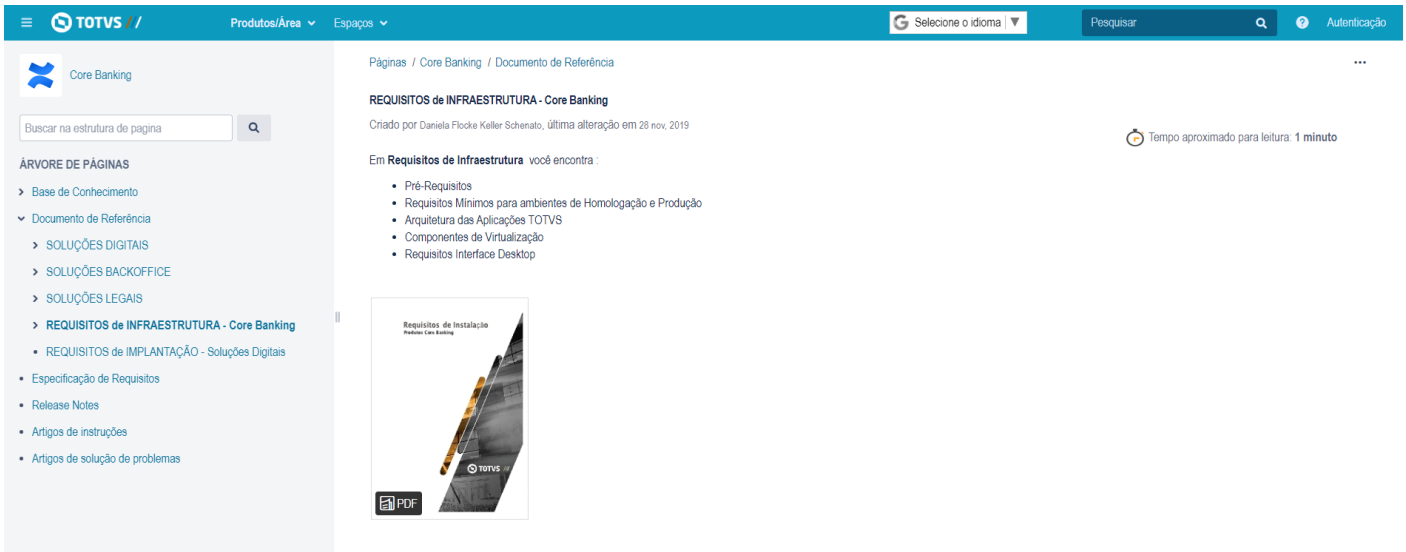
Este documento é propriedade da TOTVS. Todos os direitos reservados. ©
Este documento é propriedade da TOTVS. Todos os direitos reservados. ©

5. Requisitos de Infraestrutura para Servidores.

Esse tópico refere-se aos requisitos de infraestrutura, recomendados para implantação em ambiente de Produção e homologação.

Estes requisitos podem variar conforme a estratégia de implantação em Produção e deve ser discutido em conjunto das equipes de Infraestrutura / Arquitetura do cliente e da Totvs.

As informações podem ser obtidas através do link publico disponibilizado junto ao de documentação TDN: http://tdn.totvs.com.br/display/public/TBC/Requisitos+de+Infraestrutura



6. Referências.

- http://tdn.totvs.com.br/display/public/TBC/Requisitos+de+Infraestrutura
- https://aws.amazon.com/pt/compliance/shared-responsibility-model/
- https://docs.microsoft.com/pt-br/azure/security/fundamentals/shared-responsibility

Este documento é propriedade da TOTVS. Todos os direitos reservados. ©
Este documento é propriedade da TOTVS. Todos os direitos reservados. ©