



Guia de segurança e operações do Autonomous Driving Data Framework (ADDF)

# AWS Orientação prescritiva



# AWS Orientação prescritiva: Guia de segurança e operações do Autonomous Driving Data Framework (ADDF)

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens de marcas da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestige a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

---

# Table of Contents

Introdução .....	1
Público-alvo .....	1
Resultados de negócios desejados .....	2
Arquitetura e terminologia .....	3
Terminologia do ADDF .....	3
Arquitetura do ADDF .....	5
Modelo de responsabilidade compartilhada .....	10
AWS responsabilidade .....	11
Responsabilidade da equipe principal do ADDF .....	12
Responsabilidade do usuário do ADDF .....	12
Conta da AWS Responsabilidades gerais .....	13
Responsabilidades específicas do ADDF .....	13
Processo de revisão de segurança .....	15
Análises regulares de segurança feitas por AWS .....	15
Revisões e contribuições de segurança de código aberto .....	15
Recursos de segurança incorporados .....	17
Privilegio mínimo para o código do módulo ADDF .....	17
Infraestrutura como código .....	18
Verificações de segurança automatizadas para IaC .....	18
Política personalizada de privilégios mínimos para a função de implantação AWS CDK .....	18
Política de privilégios mínimos para o arquivo deployspec do módulo .....	19
Criptografia de dados .....	20
Armazenamento de credenciais usando Secrets Manager .....	20
Análises de segurança de SeedFarmer e CodeSeeder .....	20
Suporte de limite de permissões para a AWS CodeBuild função de CodeSeeder .....	20
AWS arquitetura de várias contas .....	21
Permissões com privilégios mínimos para implantações em várias contas .....	22
Configuração e operação seguras .....	25
Definindo sua arquitetura ADDF .....	25
Executar o ADDF em um ambiente PoC .....	25
Executar o ADDF em um ambiente de produção .....	26
Configuração inicial do .....	30
Personalizar o código da estrutura de implantação do ADDF .....	31
Escrever módulos personalizados no ADDF .....	32

---

Implantações do ADDF recorrentes .....	32
Auditorias de segurança recorrentes .....	32
Atualizações do ADDF .....	32
Descomissionamento .....	33
Próximas etapas .....	34
Recursos .....	35
AWS documentação .....	35
Recursos de código aberto .....	35
Avisos .....	36
Histórico do documento .....	37
Glossário .....	38
# .....	38
A .....	39
B .....	42
C .....	44
D .....	47
E .....	52
F .....	54
G .....	56
H .....	57
eu .....	58
L .....	61
M .....	62
O .....	66
P .....	69
Q .....	72
R .....	72
S .....	75
T .....	79
U .....	81
V .....	81
W .....	82
Z .....	83
.....	lxxxiv

# Guia de segurança e operações do Autonomous Driving Data Framework (ADDF)

Andreas Falkenberg, Junjie Tang, Torsten Reitemeyer e Srinivas Reddy Cheruku, da Amazon Web Services

Novembro de 2022 ([histórico do documento](#))

O Autonomous Driving Data Framework (ADDF) é um projeto de código aberto projetado para fornecer artefatos de código modulares e reutilizáveis para equipes automotivas que desejam implementar tarefas comuns para sistemas avançados de assistência ao motorista (ADAS), como configurar armazenamento centralizado de dados, pipelines de processamento de dados, mecanismos de visualização, interfaces de pesquisa, workloads de simulação, interfaces de análise e painéis pré-criados. Usando o ADDF, você pode compartilhar, modificar ou criar módulos totalmente personalizáveis que reduzem o esforço necessário para criar e implantar essas soluções.

Este guia tem como objetivo ajudar você a entender as práticas recomendadas para implantar e operar o ADDF com segurança na Nuvem AWS. Ele aborda os seguintes tópicos:

- [Arquitetura e terminologia](#): revise a arquitetura geral, os fluxos de trabalho e os termos importantes.
- [Modelo de responsabilidade compartilhada](#)— Entenda sua função e a função de AWS proteger sua implantação do ADDF e seus recursos de nuvem.
- [Processo de revisão de segurança](#)— Como o ADDF é um projeto de código aberto, analise como AWS e os colaboradores concluem as análises de segurança.
- [Recursos de segurança incorporados](#): revise como as práticas recomendadas e os recursos de segurança são incorporados ao projeto de código aberto do ADDF e sua estrutura de implantação.
- [Configuração e operação seguras](#): saiba como implantar e operar o ADDF na Nuvem AWS.

## Público-alvo

Este guia é destinado a equipes de operações de desenvolvimento (DevOps), engenheiros de infraestrutura, administradores, equipe de segurança de TI e equipes de resposta a incidentes encarregadas de avaliar, implantar, personalizar e operar o ADDF. Você pode aplicar as recomendações deste guia para proof-of-concept nossos ambientes de produção.

Este guia pressupõe que você não tenha nenhum conhecimento prévio do ADDF. No entanto, recomendamos que você leia o [readme \(GitHub\) do ADDF](#) antes de continuar.

## Resultados de negócios desejados

Este guia foi desenvolvido para ajudar você a configurar e operar o ADDF em ambientes de desenvolvimento e produção.

# Arquitetura e terminologia do ADDF

Antes de entender os tópicos operacionais e de segurança deste guia, é importante ter uma compreensão de alto nível da terminologia, dos componentes e da arquitetura do Autonomous Driving Data Framework (ADDF). Esta seção contém os seguintes tópicos:

- [Terminologia do ADDF](#)
- [Arquitetura do ADDF](#)

## Terminologia do ADDF

A terminologia importante do ADDF é:

- **Módulo do ADDF:** um módulo é uma infraestrutura como código (IaC) que implementa uma tarefa comum em um sistema avançado de assistência ao motorista (ADAS). As tarefas comuns incluem a configuração de armazenamento de dados centralizado, pipelines de processamento de dados, mecanismos de visualização, interfaces de pesquisa, workloads de simulação, interfaces de análise e painéis pré-criados. Você pode criar um módulo com base em seus requisitos ou pode reutilizar ou personalizar um módulo existente.

Você pode usar o AWS Cloud Development Kit (AWS CDK) para definir módulos ADDF ou usar qualquer estrutura IaC comum, como o Hashicorp Terraform ou AWS CloudFormation, para implementar os módulos ADDF. Um módulo tem um conjunto de parâmetros de entrada. Os parâmetros de entrada podem depender dos valores de saída de outros módulos. Um módulo ADDF é a menor unidade de implantação para uma Conta da AWS de destino do ADDF.

- **Arquivo de manifesto de implantação do ADDF:** esse arquivo define uma orquestração de módulos ADDF autônomos. Orquestração refere-se à ordem de implantação dos módulos. No arquivo de manifesto de implantação do ADDF, você pode usar grupos do ADDF para agrupar módulos relacionados. Nesse arquivo, você também define a cadeia de ferramentas ADDF Conta da AWS, o destino ADDF e o destino Contas da AWS. Regiões da AWS
- **Estrutura de implantação do ADDF** — Essa estrutura implanta módulos do ADDF no destino do ADDF Contas da AWS com base na orquestração definida no arquivo de manifesto de implantação do ADDF. A estrutura de implantação do ADDF é implementada usando os seguintes projetos de AWS código aberto:

- [SeedFarmer](#)(GitHub) — SeedFarmer é a ferramenta CLI usada para implantações de ADDF. Ele gerencia cada estado do módulo, prepara e empacota o código do módulo, cria as políticas de privilégios mínimos para as funções de implantação do ADDF e fornece instruções semânticas que são usadas para implantação. CodeSeeder Você pode interagir diretamente com SeedFarmer o ADDF para executar implantações ou integrá-lo em um pipeline de integração contínua e implantação contínua (CI/CD).
- [CodeSeeder](#)(GitHub) — CodeSeeder implanta infraestrutura arbitrária como pacotes de código por meio de um AWS CodeBuild trabalho. SeedFarmerorquestra e executa automaticamente. CodeSeeder Só interage SeedFarmer diretamente com CodeSeeder.

A estrutura de implantação do ADDF foi projetada para oferecer suporte a implantações em arquiteturas de conta única e de várias contas. Com base nos requisitos da sua organização, você decide se uma arquitetura de conta única ou de várias contas é necessária.

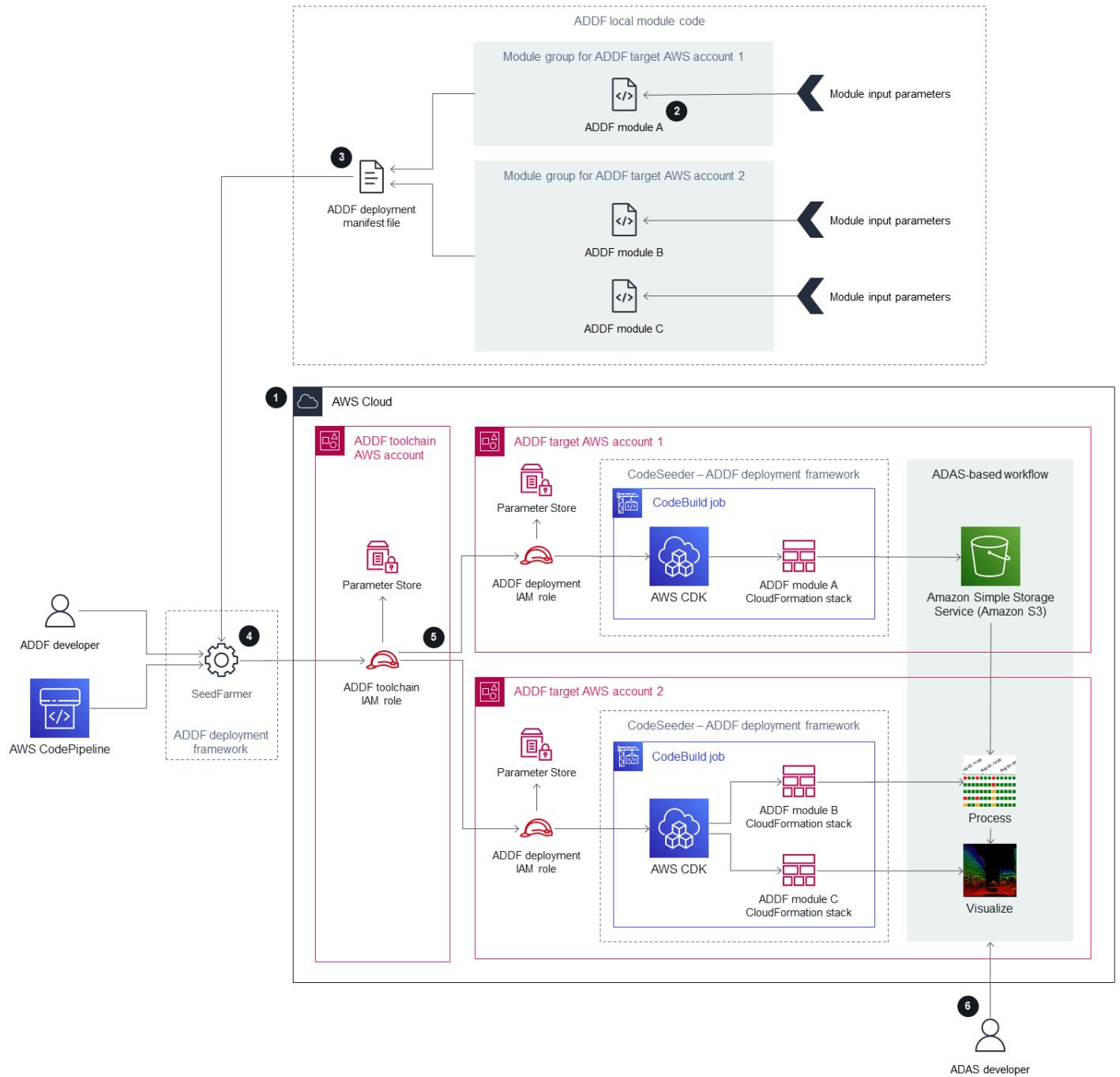
- Conjunto de ferramentas ADDF Conta da AWS — Essa conta orquestra e gerencia a implantação de módulos no destino do ADDF Contas da AWS, com base nas definições do arquivo de manifesto de implantação do ADDF. Uma implantação do ADDF só pode ter uma Conta da AWS de cadeia de ferramentas do ADDF. Em uma arquitetura de conta única, a Conta da AWS da cadeia de ferramentas do ADDF também é a Conta da AWS de destino do ADDF.” Essa conta contém uma função AWS Identity and Access Management (IAM), chamada função IAM da cadeia de ferramentas ADDF, que é assumida SeedFarmer durante o processo de implantação do ADDF. Neste guia, nos referimos a uma cadeia de ferramentas ADDF Conta da AWS como uma conta da cadeia de ferramentas.
- Destino ADDF Contas da AWS — Essas são as contas de destino nas quais você está implantando módulos ADDF. Você pode ter uma ou mais contas de destino. Essas contas contêm os recursos e a lógica da aplicação descritos no arquivo de manifesto de implantação do ADDF e seus módulos mapeados. Em uma arquitetura de conta única, o alvo do ADDF também Conta da AWS é o conjunto de ferramentas do ADDF. Conta da AWS Cada conta de destino do ADDF contém uma função do IAM, chamada função do IAM de implantação do ADDF, que é assumida CodeSeeder durante o processo de implantação. Neste guia, nos referimos a um alvo ADDF Conta da AWS como uma conta de destino.
- Instância do ADDF: quando você implanta o ADDF e seus módulos na nuvem, conforme definido em seu arquivo de manifesto de implantação do ADDF, isso se torna uma instância do ADDF. Uma instância do ADDF pode ter uma arquitetura de conta única ou de várias contas, e você pode implantar várias instâncias do ADDF. Para obter mais informações sobre como escolher o número

---

de instâncias e projetar uma arquitetura de conta para seu caso de uso, consulte [Definindo sua arquitetura ADDF](#).

## Arquitetura do ADDF


O diagrama a seguir mostra uma arquitetura de alto nível para uma instância do ADDF na Nuvem AWS. Ele mostra uma arquitetura de várias contas, incluindo uma conta de cadeia de ferramentas dedicada e duas contas de destino. Este guia discute o end-to-end processo de uso do ADDF para implantar recursos nas contas de destino.



### 1. Crie e inicialize as Contas da AWS do ADDF.

Para funcionar corretamente, cada conta deve ser inicializada para o ADDF e para o AWS CDK. Se isso for uma nova implantação do ADDF ou se você estiver adicionando novas contas de destino, faça o seguinte:

- a. Inicialize AWS CDK na conta do conjunto de ferramentas e em cada conta de destino. Para obter instruções, consulte [Fazer bootstrap](#) (documentação do AWS CDK ). O ADDF usa AWS CDK para implantar sua infraestrutura.
- b. Faça bootstrap do ADDF na conta de cadeia de ferramentas e em cada conta de destino. Para obter instruções, consulte [Bootstrap Conta da AWS\(s\)](#) no Guia de [implantação do ADDF](#). Isso configura todas as funções do IAM específicas do ADDF exigidas por e. SeedFarmer CodeSeeder

 Note

Você deverá realizar essa etapa somente se estiver implantando inicialmente o ADDF ou adicionando novas contas de destino. Essa etapa não faz parte das implantações recorrentes do ADDF em instâncias do ADDF já estabelecidas.

2. Crie ou personalize os módulos do ADDF.

Crie ou personalize módulos do ADDF com base no problema específico que você está tentando resolver. Seu módulo deve representar uma tarefa isolada ou um grupo de tarefas. Defina os parâmetros de entrada para o módulo conforme necessário e use os valores de saída do módulo como parâmetros de entrada para outros módulos.

3. Defina a orquestração do módulo no arquivo de manifesto de implantação do ADDF.

No arquivo de manifesto do ADDF, organize os módulos em grupos e defina a ordem de implantação e as dependências entre eles. Nesse arquivo, você também especifica a conta única do conjunto de ferramentas e as contas de destino (inclusive Regiões da AWS) para cada grupo ADDF e seus módulos.

4. Avalie o arquivo de manifesto de implantação do ADDF e estabeleça o escopo da implantação.

O desenvolvedor do ADDF ou um pipeline de CI/CD, como AWS CodePipeline, inicia uma avaliação do arquivo de manifesto de implantação do ADDF chamando a ferramenta CLI, SeedFarmer Para iniciar a avaliação:

- SeedFarmer usa o arquivo de manifesto de implantação do ADDF como um parâmetro de entrada para a avaliação.
- Para assumir a função IAM da cadeia de ferramentas ADDF, SeedFarmer espera a mesma função IAM válida ou credenciais de usuário que foram definidas durante o processo de bootstrap do ADDF, na etapa 1.

Se SeedFarmer não tiver as credenciais corretas para assumir a função IAM da cadeia de ferramentas ADDF ou não puder acessar o arquivo de manifesto de implantação do ADDF, a avaliação não será iniciada.

Se SeedFarmer puder iniciar a avaliação, ele assume a função IAM da cadeia de ferramentas ADDF na conta da cadeia de ferramentas. A partir daí, SeedFarmer pode acessar qualquer conta de destino, assumindo a função do IAM de implantação do ADDF nessa conta. SeedFarmer em seguida, tenta ler qualquer metadado ADDF na conta do conjunto de ferramentas e nas contas de destino. Uma das seguintes situações acontece:

- Se não houver metadados do ADDF para ler, isso indica que essa é uma nova instância do ADDF. SeedFarmer determina que o escopo de implantação é todo o arquivo de manifesto de implantação do ADDF e seu conteúdo.
- Se existirem metadados do ADDF, SeedFarmer compara o arquivo de manifesto de implantação do ADDF e seu conteúdo com os MD5 hashes dos artefatos implantados existentes nas contas de destino. Se forem detectadas alterações implantáveis, esse processo continuará. Se nenhuma alteração implantável for detectada, o processo será concluído.

#### 5. Implante os módulos ADDF dentro do escopo nas contas de destino.

CodeSeeder agora tem uma lista ordenada de implantações a serem executadas, de acordo com o arquivo de manifesto de implantação do ADDF e os resultados da avaliação da etapa anterior. Com base nessa lista ordenada, CodeSeeder assume a função do IAM de implantação do ADDF em cada conta de destino associada. Em seguida, ele é executado CodeSeeder em uma AWS CodeBuild tarefa para criar ou atualizar as implantações individuais do IaC, como AWS CDK aplicativos, para o módulo ADDF. Por padrão, o ADDF usa AWS CDK como estrutura IaC, mas outras estruturas comuns de IaC também são suportadas. Depois que o processo for concluído para cada conta de destino, você terá um fluxo de trabalho totalmente implantado, entre contas e end-to-end baseado em ADAS, conforme definido no arquivo de manifesto de implantação do ADDF.

Se você usa uma arquitetura de conta única, a conta da cadeia de ferramentas e as contas de destino são a mesma conta, e a conta única tem todos os recursos descritos.

#### 6. Use a infraestrutura implantada pelo ADDF.

Um desenvolvedor do ADAS pode usar o fluxo de trabalho baseado em ADAS implantado, conforme definido pelo seu caso de uso.

Esse fluxo de trabalho descreve a arquitetura de uma única instância de um ambiente com várias contas do ADDF. Dependendo do seu modelo de desenvolvimento, implantação e operações, recomendamos que você execute várias instâncias do ADDF em um ambiente de vários estágios. Uma configuração típica pode incluir uma instância ADDF dedicada Contas da AWS para cada estágio de implantação, como filiais para desenvolvimento, teste e produção. Você também pode executar várias instâncias do ADDF no mesmo ambiente de conta única ou de várias contas Região da AWS, supondo que você tenha criado um namespace de recurso exclusivo para cada instância do ADDF. Para obter mais informações, consulte [Definindo sua arquitetura ADDF](#).

## Modelo de responsabilidade compartilhada do ADDF

O [modelo de responsabilidade compartilhada](#) que se aplica Serviços da AWS também se aplica ao Autonomous Driving Data Framework (ADDF). As seguintes entidades compartilham a responsabilidade de proteger o ADDF, conforme estabelecido no diagrama a seguir:

- AWS— A oferta do provedor de infraestrutura em nuvem Serviços da AWS.
- Equipe principal do ADDF — A equipe principal do ADDF é a entidade que publica as versões do ADDF no repositório do [ADDF](#) (). GitHub
- Usuário do ADDF: os usuários do ADDF incluem, mas não estão limitados a:
  - Desenvolvedor do ADDF: qualquer pessoa que altere, personalize ou crie um novo código do módulo do ADDF.
  - Operador do ADDF: qualquer pessoa que configure e opere uma instância do ADDF.
  - Desenvolvedor do ADAS: o usuário final ou o consumidor dos recursos implantados pelo ADDF. Por exemplo, um desenvolvedor do ADAS pode consultar um front-end de visualização que foi criado como parte da implantação do ADDF.

O diagrama a seguir resume a responsabilidade compartilhada entre AWS a equipe principal do ADDF e o usuário do ADDF.

**AWS responsibility***"Security of the AWS Cloud"*

- Software security, including compute, storage, database, and networking
- Hardware security for the AWS global infrastructure, including AWS Regions, Availability Zones, and edge locations

**ADDF core team responsibility***"Security-hardened framework on an as-is basis, as stated in Apache License 2.0"*

- Periodic security reviews of releases
- Baseline security features
- Security-hardened default modules\*
- Security-hardened deployment and orchestration framework

**ADDF user responsibility***"Secure setup, development, customization, and operation"*

- General AWS account responsibilities:
  - Security controls and checks (directive, detective, preventive, and responsive)
  - Multi-account architecture
  - Networking design
  - Identity and access management
- ADDF responsibilities:
  - ADDF setup
  - ADDF customization
  - ADDF module development
  - ADDF operations
  - ADDF updates

\* Excluding any modules in the ADDF `/modules/demo-only/` folder. Those modules exist only for proof-of-concept purposes and didn't receive security hardening.

## AWS responsabilidade

AWS é responsável por proteger a infraestrutura que executa todos os serviços oferecidos no Nuvem AWS, conforme definido no [modelo de responsabilidade AWS compartilhada](#). Essa infraestrutura é composta pelo hardware, software, rede e instalações que executam Nuvem AWS os serviços.

## Responsabilidade da equipe principal do ADDF

A equipe principal do ADDF fornece uma estrutura segura por si só, com base no melhor esforço, de acordo com a [Licença Apache 2.0](#) (). GitHub A equipe principal do ADDF é responsável pelo seguinte:

- Revisões periódicas de segurança dos lançamentos
- Recursos de segurança de linha de base
- Módulos padrão com segurança reforçada (Isso exclui todos os módulos na pasta. `/modules/demo-only/` Esses módulos são apenas para proof-of-concept fins específicos e não recebem reforço de segurança.)
- Estrutura de implantação e orquestração reforçada com segurança

Essas responsabilidades de segurança se estendem somente à estrutura, conforme fornecido no GitHub repositório, sem nenhuma modificação ou personalização. Isso inclui todos os módulos ADDF, exceto os módulos ADDF na pasta `modules/demo-only/`. Os módulos ADDF nessa pasta não têm segurança reforçada e não devem ser implantados em ambientes de produção ou em qualquer ambiente com dados confidenciais ou protegidos. Esses módulos estão incluídos para mostrar os recursos do sistema, e você pode usá-los como base para criar seus próprios módulos personalizados e com segurança reforçada.

### Note

O ADDF como estrutura é fornecido no estado em que se encontra. Ele não vem com nenhuma responsabilidade e garantia, conforme declarado na [Licença Apache 2.0](#) (GitHub). Você deve conduzir sua própria avaliação de segurança do ADDF e verificar se ele está em conformidade com os requisitos de segurança específicos da sua organização.

## Responsabilidade do usuário do ADDF

O ADDF e seus módulos serão seguros somente se o ADDF for configurado, personalizado e operado de maneira segura. O usuário do ADDF é totalmente responsável pela segurança do seguinte:

- Conta da AWS Responsabilidades gerais:

- Controles e verificações de segurança (diretivos, detectivos, preventivos e responsivos)
- Arquitetura de várias contas
- Design de rede
- Gerenciamento de identidade e acesso
- Responsabilidades específicas do ADDF:
  - Configuração do ADDF
  - Personalização do Java
  - Desenvolvimento do módulo ADDF
  - Operações do ADDF
  - Atualizações do ADDF

## Conta da AWS Responsabilidades gerais

[Antes de implantar qualquer recurso relacionado ao ADDF Contas da AWS, você Contas da AWS deve ser configurado de acordo com as melhores práticas do Well-Architected AWS Framework.](#)

Isso inclui controles de segurança diretivos, detectivos, preventivos e responsivos. Você deve ter processos detalhados de mitigação em vigor, no caso de quaisquer violações ou incidentes de segurança. A política da sua organização deve incluir requisitos para gerenciar centralmente a identidade, o acesso e a rede. Normalmente, esses requisitos e serviços são atendidos por uma equipe dedicada de zona de destino.

## Responsabilidades específicas do ADDF

### Configuração segura do ADDF

A responsabilidade do usuário do ADDF começa com a configuração segura do ADDF de acordo com a documentação do ADDF. É altamente recomendável que você siga as instruções no [Guia de implantação do ADDF](#) (GitHub). Para obter mais informações sobre como configurar de forma segura o ADDF, consulte [Definindo sua arquitetura ADDF](#) e [Configuração inicial do](#).

### Personalização segura do ADDF

No caso de qualquer personalização da funcionalidade principal do ADDF, como CodeSeeder, SeedFarmer e dos módulos principais do ADDF, o usuário do ADDF assume total responsabilidade por essas alterações. Para obter mais informações, consulte [Personalizar o código da estrutura de implantação do ADDF](#).

## Desenvolvimento seguro de módulo ADDF

O usuário do ADDF é totalmente responsável por qualquer módulo personalizado implantado usando o ADDF. Além disso, o usuário do ADDF é responsável por qualquer alteração de código nos módulos fornecidos pelo ADDF. Para obter mais informações, consulte [Escrever módulos personalizados no ADDF](#).

## Atualizações e operações seguras do ADDF

Conforme a estrutura evolui, o ADDF recebe atualizações de recursos e segurança. É responsabilidade do usuário do ADDF verificar regularmente as atualizações publicadas no GitHub repositório e operar o ADDF com segurança a longo prazo. Para ter mais informações, consulte [Implantações do ADDF recorrentes](#), [Auditorias de segurança recorrentes](#), [Atualizações do ADDF](#) e [Descomissionamento](#).

## Processo de revisão de segurança do ADDF

O Autonomous Driving Data Framework (ADDF) foi desenvolvido com a segurança em mente. Antes do lançamento para o público, a AWS realizou uma revisão inicial de segurança interna do ADDF e resolveu todos os problemas de segurança identificados. Tanto a comunidade de código aberto quanto a comunidade de código fechado contribuem para análises contínuas de segurança da estrutura.

## Análises regulares de segurança feitas por AWS

O ADDF é publicado sob a GitHub organização awslabs, de propriedade da AWS. A AWS realiza revisões regulares de segurança automáticas e manuais do código nessa organização, para verificar a segurança da melhor maneira possível. De acordo com a política da AWS, a AWS não divulga informações sobre a frequência de revisão de segurança, a abordagem ou as ferramentas usadas. Além disso, a AWS não publica nenhum relatório de auditoria interna sobre o ADDF. No entanto, todas as descobertas de segurança identificadas são corrigidas e publicadas por meio de pull request, com alta urgência.

### Note

O ADDF como estrutura é fornecido “NO ESTADO EM QUE SE ENCONTRA”, SEM GARANTIAS OU CONDIÇÕES DE QUALQUER TIPO, expressas ou implícitas, incluindo, sem limitação, quaisquer garantias ou condições de título, não violação, comerciabilidade ou adequação a uma finalidade específica, conforme declarado na Licença Apache 2.0 ().

Você deve conduzir sua própria avaliação de segurança do ADDF e verificar se ele está em conformidade com os requisitos de segurança específicos da sua organização e, conforme estabelecido no Apache License 2.0, você é o único responsável por determinar a adequação do uso ou redistribuição do ADDF e assumir quaisquer riscos associados ao seu exercício ou permissões sob tal licença.

## Revisões e contribuições de segurança de código aberto

O ADDF é um projeto de código aberto que aceita contribuições. Convidamos todos os usuários a realizarem suas próprias revisões de segurança da estrutura e contribuir relatando quaisquer

---

descobertas relacionadas à segurança. Se você encontrar um problema no código, siga as diretrizes em [Notificações de problemas de segurança](#) (documentação do ADDF).

# Recursos de segurança incorporados do ADDF

O Autonomous Driving Data Framework (ADDF) tem vários recursos de segurança incorporados. Por padrão, esses recursos são projetados para ajudar você a configurar uma estrutura segura e ajudar sua organização a atender aos requisitos de segurança corporativa comuns.

A seguir estão os recursos de segurança incorporados:

- [Privilégio mínimo para o código do módulo ADDF](#)
- [Infraestrutura como código](#)
- [Verificações de segurança automatizadas para IaC](#)
- [Política personalizada de privilégios mínimos para a função de implantação AWS CDK](#)
- [Política de privilégios mínimos para o arquivo deployspec do módulo](#)
- [Criptografia de dados](#)
- [Armazenamento de credenciais usando Secrets Manager](#)
- [Análises de segurança de SeedFarmer e CodeSeeder](#)
- [Suporte de limite de permissões para a AWS CodeBuild função de CodeSeeder](#)
- [AWS arquitetura de várias contas](#)
- [Permissões com privilégios mínimos para implantações em várias contas](#)

## Privilégio mínimo para o código do módulo ADDF

Privilégio mínimo é a prática recomendada de segurança para conceder as permissões mínimas necessárias para executar uma tarefa. Para obter mais informações, consulte [Aplicar permissões de privilégios mínimos](#). Os módulos fornecidos pelo ADDF seguem rigorosamente o princípio de privilégios mínimos em seus códigos e recursos implantados, da seguinte forma:

- Todas as políticas AWS Identity and Access Management (IAM) geradas para um módulo ADDF têm as permissões mínimas necessárias para o caso de uso.
- Serviços da AWS são configurados e implantados de acordo com o princípio do menor privilégio. Os módulos fornecidos pelo ADDF usam somente os serviços e os recursos de serviço necessários para o caso de uso específico.

## Infraestrutura como código

O ADDF, como estrutura, foi projetado para implantar módulos ADDF como infraestrutura como código (IaC). O IaC elimina os processos de implantação manual e ajuda a evitar erros e configurações incorretas, que podem resultar de processos manuais.

O ADDF foi projetado para orquestrar e implantar módulos usando qualquer estrutura comum de IaC. Isso inclui, mas não está limitado a:

- [AWS Cloud Development Kit \(AWS CDK\)](#)
- [AWS CloudFormation](#)
- [Hashicorp Terraform](#)

Você pode usar diferentes estruturas de IaC para escrever módulos diferentes e, em seguida, usar o ADDF para implantá-los.

A estrutura IaC padrão usada pelos módulos ADDF é. AWS CDK AWS CDK é uma abstração orientada a objetos de alto nível que você pode usar para definir recursos de forma imperativa. AWS AWS CDK já aplica as melhores práticas de segurança por padrão para vários serviços e cenários. Com o uso AWS CDK, o risco de configurações incorretas de segurança é reduzido.

## Verificações de segurança automatizadas para IaC

O utilitário [cdk-nag](#) de código aberto (GitHub) está integrado ao ADDF. Esse utilitário verifica automaticamente os módulos ADDF baseados em quanto AWS CDK à adesão às melhores práticas gerais e de segurança. O utilitário cdk-nag usa regras e pacotes de regras para detectar e denunciar códigos que violam as práticas recomendadas. Para obter mais informações sobre as regras e uma lista abrangente, consulte [cdk-nag rules \(\)](#). GitHub

## Política personalizada de privilégios mínimos para a função de implantação AWS CDK

O ADDF faz uso extensivo da AWS CDK v2. É necessário que você inicialize todo o ADDF Contas da AWS para. AWS CDK Para obter mais informações, consulte [Fazer bootstrapping](#) (documentação do AWS CDK ).

Por padrão, AWS CDK atribui a política [AdministratorAccess](#) AWS gerenciada permissiva à função de AWS CDK implantação criada em contas inicializadas. O nome completo dessa função é `cdk-[CDK_QUALIFIER]-cfn-exec-role-[AWS_ACCOUNT_ID]-[REGION]`. AWS CDK usa essa função para implantar recursos no bootstrap Conta da AWS como parte do processo de implantação. AWS CDK

Dependendo dos requisitos de segurança da sua organização, a política `AdministratorAccess` pode ser muito permissiva. Como parte do processo de bootstrap do AWS CDK, você pode personalizar a política e as permissões de acordo com suas necessidades. Você pode alterar a política ao refazer bootstrap da conta com uma política recém-definida usando o parâmetro `--cloudformation-execution-policies`. Para obter mais informações, consulte [Personalizando a inicialização](#) (documentação).AWS CDK

#### Note

Embora esse recurso de segurança não seja específico do ADDF, ele está listado nesta seção porque pode aumentar a segurança geral da sua implantação do ADDF.

## Política de privilégios mínimos para o arquivo `deployspec` do módulo

Cada módulo contém um arquivo de especificações de implantação chamado `deployspec.yaml`. Esse arquivo define as instruções de implantação do módulo. CodeSeeder o usa para implantar o módulo definido na conta de destino usando AWS CodeBuild. CodeSeeder atribui uma função de serviço padrão para CodeBuild implantar os recursos, conforme instruído no arquivo de especificações de implantação. Esse perfil de serviço foi projetado de acordo com o princípio de privilégios mínimos. Ele inclui todas as permissões necessárias para implantar AWS CDK aplicativos, porque todos os módulos fornecidos pelo ADDF são criados como AWS CDK aplicativos.

No entanto, se você precisar executar qualquer comando de estágio fora do AWS CDK, precisará criar uma política personalizada do IAM em vez de usar a função de serviço padrão para CodeBuild. Por exemplo, se você estiver usando uma estrutura de implantação de IaC diferente de AWS CDK, como o Terraform, precisará criar uma política do IAM que conceda permissões suficientes para que essa estrutura específica funcione. Outro cenário que exige uma política de IAM dedicada é quando você inclui chamadas direct AWS Command Line Interface (AWS CLI) para outras pessoas Serviços da AWS nos comandos `install pre_buildbuild`, ou `post_build` stage. Por exemplo, você

precisará de uma política personalizada se o módulo incluir um comando do Amazon Simple Storage Service (Amazon S3) para fazer upload de arquivos em um bucket do S3. A política personalizada do IAM fornece controle refinado para qualquer AWS comando fora da implantação. AWS CDK Ao criar uma política de IAM personalizada para seu módulo ADDF, certifique-se de aplicar permissões de privilégios mínimos.

## Criptografia de dados

O ADDF armazena e processa dados possivelmente confidenciais. Para ajudar a proteger esses dados,, SeedFarmer CodeSeeder, e os módulos fornecidos pelo ADDF criptografam dados em repouso e em trânsito para todos os usados Serviços da AWS (a menos que seja explicitamente declarado o contrário para os módulos na pasta). `demo-only`

## Armazenamento de credenciais usando Secrets Manager

O ADDF lida com vários segredos para diferentes serviços, como Docker Hub e JupyterHub Amazon [Redshift](#). O ADDF usa [AWS Secrets Manager](#) para armazenar quaisquer segredos relacionados ao ADDF. Isso ajuda a remover dados confidenciais do código-fonte.

Os segredos do Secrets Manager são armazenados somente nas contas de destino, conforme necessário para que a conta funcione corretamente. Por padrão, a conta da cadeia de ferramentas não contém segredos.

## Análises de segurança de SeedFarmer e CodeSeeder

[SeedFarmer](#) e [CodeSeeder](#)(GitHubrepositórios) são usados para implantar o ADDF e seus módulos ADDF. Esses projetos de código aberto passam pelo mesmo processo regular de revisão de segurança AWS interna do ADDF, conforme descrito em. [Processo de revisão de segurança do ADDF](#)

## Suporte de limite de permissões para a AWS CodeBuild função de CodeSeeder

Os limites de permissões do IAM são um mecanismo de segurança comum que define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM. SeedFarmer e CodeSeeder oferece suporte a um anexo de limite de permissões do IAM para cada conta de destino. O limite de permissões limita o máximo de permissões de qualquer função de

serviço usada CodeBuild quando CodeSeeder implementa módulos. Os limites de permissões do IAM devem ser criados fora do ADDF por uma equipe de segurança. Os anexos da política de limite de permissões do IAM são aceitos como um atributo no arquivo de manifesto de implantação do ADDF, `deployment.yaml`. Para obter mais informações, consulte [Limites de permissões](#) (SeedFarmer documentação).

O fluxo de trabalho é o seguinte:

1. Sua equipe de segurança define e cria um limite de permissões do IAM de acordo com seus requisitos de segurança. O limite de permissões do IAM deve ser criado individualmente em cada Conta da AWS ADDF. O resultado é uma lista de Amazon Resource Name (ARN) da política de limite de permissões.
2. A equipe de segurança compartilha a lista de ARN da política com sua equipe de desenvolvedores do ADDF.
3. A equipe de desenvolvedores do ADDF integra a lista de ARN da política ao arquivo de manifesto. Para ver um exemplo dessa integração, consulte [sample-permissionboundary.yaml](#) (). GitHub
4. Após a implantação bem-sucedida, o limite de permissões é anexado a todas as funções de serviço CodeBuild usadas para implantar módulos.
5. A equipe de segurança monitora se os limites das permissões são aplicados conforme necessário.

## AWS arquitetura de várias contas

Conforme definido no pilar de segurança do AWS Well-Architected Framework, é considerada a melhor prática separar recursos e cargas de trabalho em Contas da AWS vários, com base nos requisitos da sua organização. Isso ocorre porque um Conta da AWS atua como um limite de isolamento. Para obter mais informações, consulte [gerenciamento e separação da Conta da AWS](#). A implementação desse conceito é chamada de arquitetura de várias contas. Uma arquitetura de várias contas da AWS projetada corretamente fornece categorização da workload e reduz o escopo do impacto no caso de uma violação de segurança, em comparação com uma arquitetura de conta única.

O ADDF oferece suporte nativo a arquiteturas de AWS várias contas. Você pode distribuir seus módulos ADDF em Contas da AWS quantos forem necessários para a segurança e separation-of-duties os requisitos de sua organização. Você pode implantar o ADDF em uma única Conta da AWS, combinando as funções da cadeia de ferramentas e da conta de destino. Como alternativa, você pode criar contas de destino individuais para módulos ADDF ou grupos de módulos.

A única restrição que você precisa considerar é que um módulo ADDF representa a menor unidade de implantação de cada um. Conta da AWS

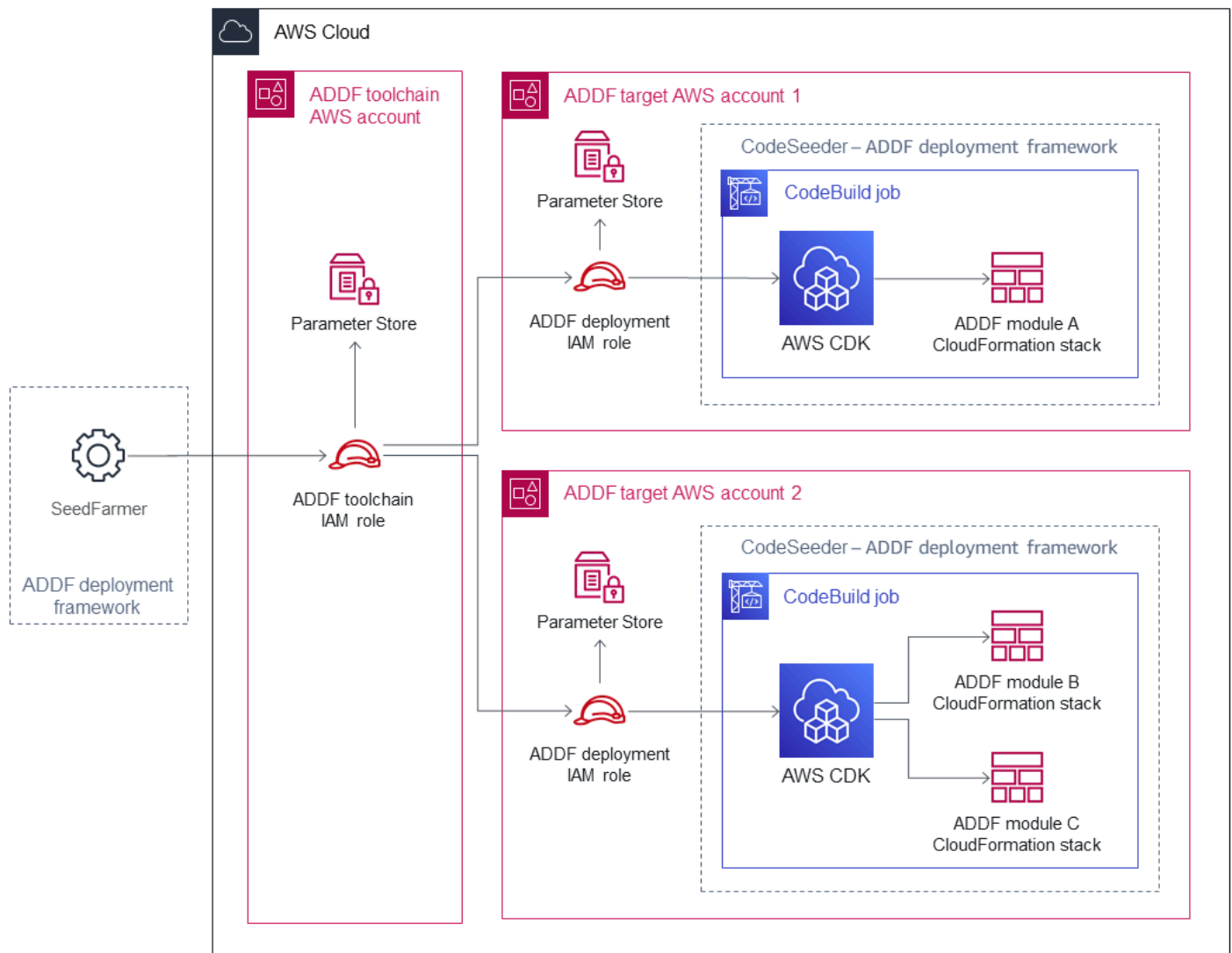
Para ambientes de produção, é recomendável usar uma arquitetura de várias contas que consista em uma conta da cadeia de ferramentas e pelo menos uma conta de destino. Para obter mais informações, consulte [Arquitetura do ADDF](#).

## Permissões com privilégios mínimos para implantações em várias contas

Se você usa uma arquitetura de várias contas, SeedFarmer precisa acessar as contas de destino para realizar as três ações a seguir:

1. Grave os metadados do módulo ADDF nas contas da cadeia de ferramentas e nas contas de destino.
2. Leia os metadados do módulo ADDF atuais da conta da cadeia de ferramentas e das contas de destino.
3. Inicie AWS CodeBuild trabalhos nas contas de destino, com a finalidade de implantar ou atualizar módulos.

A figura a seguir mostra os relacionamentos entre contas, incluindo operações para assumir funções específicas do ADDF AWS Identity and Access Management (IAM).



Essas ações entre contas são alcançadas por meio do uso de operações de assumir perfis bem definidos.

- A função do IAM da cadeia de ferramentas ADDF é implantada na conta da cadeia de ferramentas. SeedFarmer assume esse papel. Esse perfil tem permissões para realizar uma ação `iam:AssumeRole` e pode assumir o perfil do IAM de implantação do ADDF em cada conta de destino. Além disso, a função IAM da cadeia de ferramentas ADDF pode executar operações locais do AWS Systems Manager Parameter Store.
- O perfil do IAM de implantação do ADDF é implantado em cada conta de destino. Esse perfil só pode ser assumido a partir da conta da cadeia de ferramentas usando o perfil do IAM da cadeia de ferramentas do ADDF. Essa função tem permissões para executar operações locais do AWS

---

Systems Manager Parameter Store e tem permissões para executar AWS CodeBuild ações que iniciam e descrevem CodeBuild trabalhos por meio CodeSeeder deles.

Esses perfis do IAM específicos do ADDF são criados como parte do processo de bootstrapping do ADDF. Para obter mais informações, consulte Bootstrap Conta da AWS(s) no [Guia de implantação do ADDF](#) (GitHub).

Todas as permissões entre contas são configuradas de acordo com o princípio de privilégios mínimos. Se uma conta de destino for comprometida, haverá um impacto mínimo ou nenhum impacto nas outras Contas da AWS do ADDF.

No caso de uma arquitetura de conta única para ADDF, os relacionamentos de perfil permanecem os mesmos. Eles simplesmente se transformam em uma única Conta da AWS.

# Configuração e operação seguras do ADDF

O Autonomous Driving Data Framework (ADDF) deve ser tratado como um software personalizado que requer manutenção e cuidados contínuos de uma equipe dedicada DevOps e de segurança em sua organização. Esta seção descreve tarefas comuns relacionadas à segurança que ajudam você a configurar e operar o ADDF em todo o seu ciclo de vida.

Esta seção inclui as seguintes tarefas:

- [Definindo sua arquitetura ADDF](#)
- [Configuração inicial do](#)
- [Personalizar o código da estrutura de implantação do ADDF](#)
- [Escrever módulos personalizados no ADDF](#)
- [Implantações do ADDF recorrentes](#)
- [Auditorias de segurança recorrentes](#)
- [Atualizações do ADDF](#)
- [Descomissionamento](#)

## Definindo sua arquitetura ADDF

Uma instância ADDF é tão segura quanto o Conta da AWS ambiente em que está implantada. Esse Conta da AWS ambiente deve ser projetado para atender às necessidades operacionais e de segurança de seu caso de uso específico. Por exemplo, as tarefas e considerações relacionadas à segurança e às operações para configurar uma instância do ADDF em um ambiente proof-of-concept (PoC) são diferentes daquelas para configurar o ADDF em um ambiente de produção.

## Executar o ADDF em um ambiente PoC

Se você pretende usar o ADDF em um ambiente PoC, recomendamos criar um dedicado Conta da AWS para o ADDF que não contenha nenhuma outra carga de trabalho. Isso ajuda a manter sua conta segura enquanto você explora o ADDF e seus recursos. Estes são os benefícios desta abordagem:

- No caso de uma configuração incorreta grave do ADDF, nenhuma outra workload seria afetada adversamente.

- Não há risco de qualquer outra configuração incorreta da workload que possa afetar adversamente a configuração do ADDF.

Mesmo para um ambiente de PoC, ainda recomendamos que você siga todas as práticas recomendadas listadas em [Executar o ADDF em um ambiente de produção](#) quanto possível.

## Executar o ADDF em um ambiente de produção

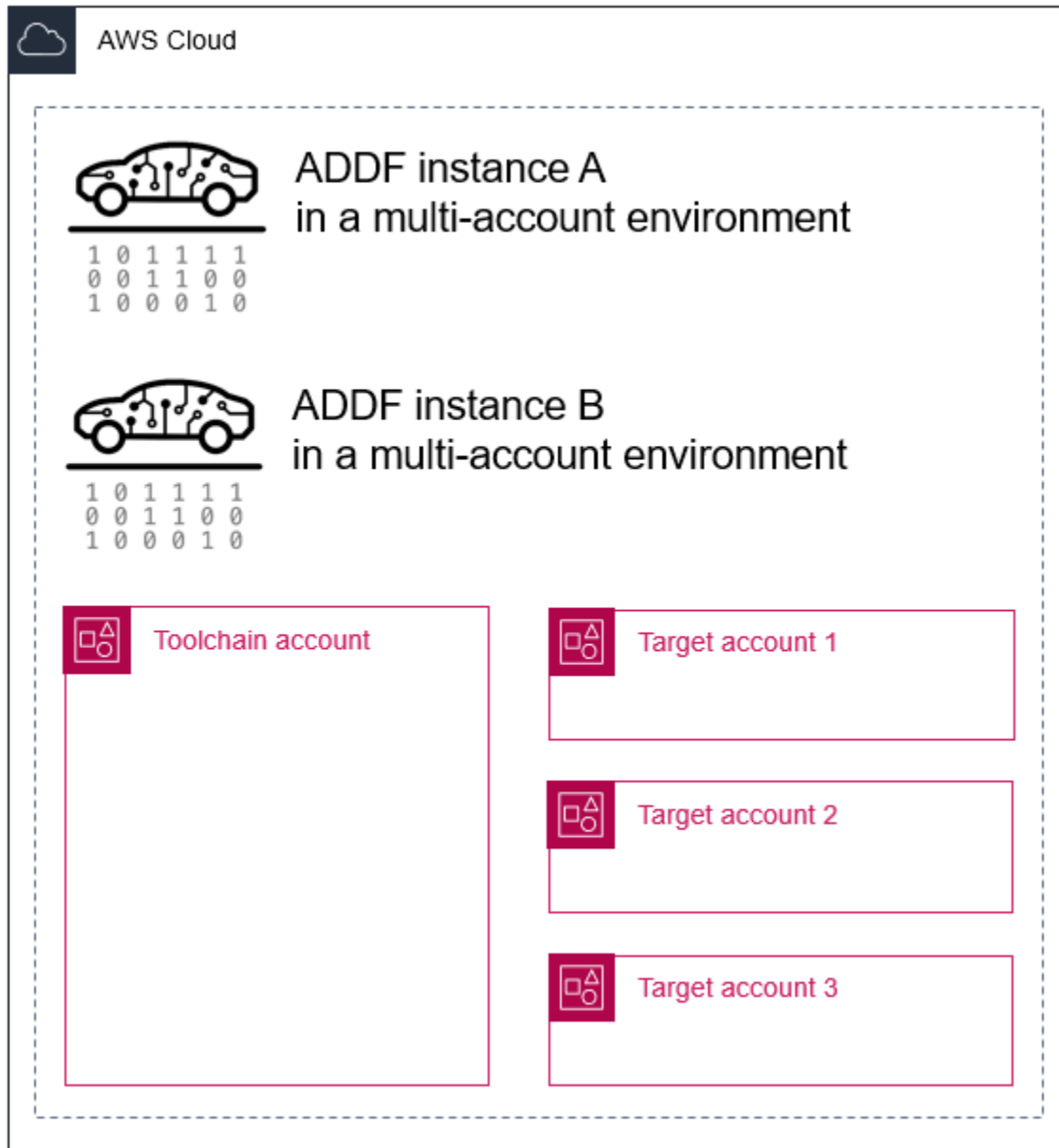
Se você pretende usar o ADDF em um ambiente de produção corporativo, é altamente recomendável que você considere as práticas recomendadas de segurança da sua organização e implemente o ADDF adequadamente. Além das práticas recomendadas de segurança da sua organização, recomendamos que você implemente o seguinte:

- Crie uma DevOps equipe ADDF comprometida e de longo prazo — o ADDF precisa ser tratado como um software personalizado. Ela exige manutenção e cuidados contínuos de uma DevOps equipe dedicada. Antes de começar a executar o ADDF em um ambiente de produção, uma DevOps equipe de tamanho e capacidades suficientes deve ser definida com um compromisso total de recursos, até a implantação end-of-life do ADDF.
- Use uma arquitetura de várias contas: cada instância do ADDF deve ser implantada em seu próprio ambiente dedicado de várias contas da AWS, sem nenhuma outra workload não relacionada. Conforme definido no [gerenciamento e separação de AWS contas](#) (AWS Well-Architected Framework), é considerada a melhor prática separar recursos e cargas de trabalho em Contas da AWS vários, com base nos requisitos da sua organização. Isso ocorre porque um Conta da AWS atua como um limite de isolamento. Uma arquitetura de várias contas da AWS projetada corretamente fornece categorização da workload e reduz o escopo do impacto no caso de uma violação de segurança, em comparação com uma arquitetura de conta única. Usar uma arquitetura de várias contas também ajuda suas contas a permanecerem dentro de suas [cotas do AWS service \(Serviço da AWS\)](#). Distribua seus módulos ADDF em Contas da AWS quantos forem necessários para atender aos separation-of-duties requisitos e segurança da sua organização.
- Implemente várias instâncias do ADDF: configure quantas instâncias separadas do ADDF forem necessárias para desenvolver, testar e implantar adequadamente os módulos do ADDF de acordo com os processos de desenvolvimento de software da sua organização. Ao configurar várias instâncias do ADDF, é possível usar uma das abordagens a seguir:
  - Várias instâncias do ADDF em diferentes ambientes de AWS várias contas — Você pode usar diferentes instâncias do ADDF Contas da AWS para isolar diferentes instâncias do ADDF. Por exemplo, se sua organização tem estágios dedicados de desenvolvimento, teste e produção,

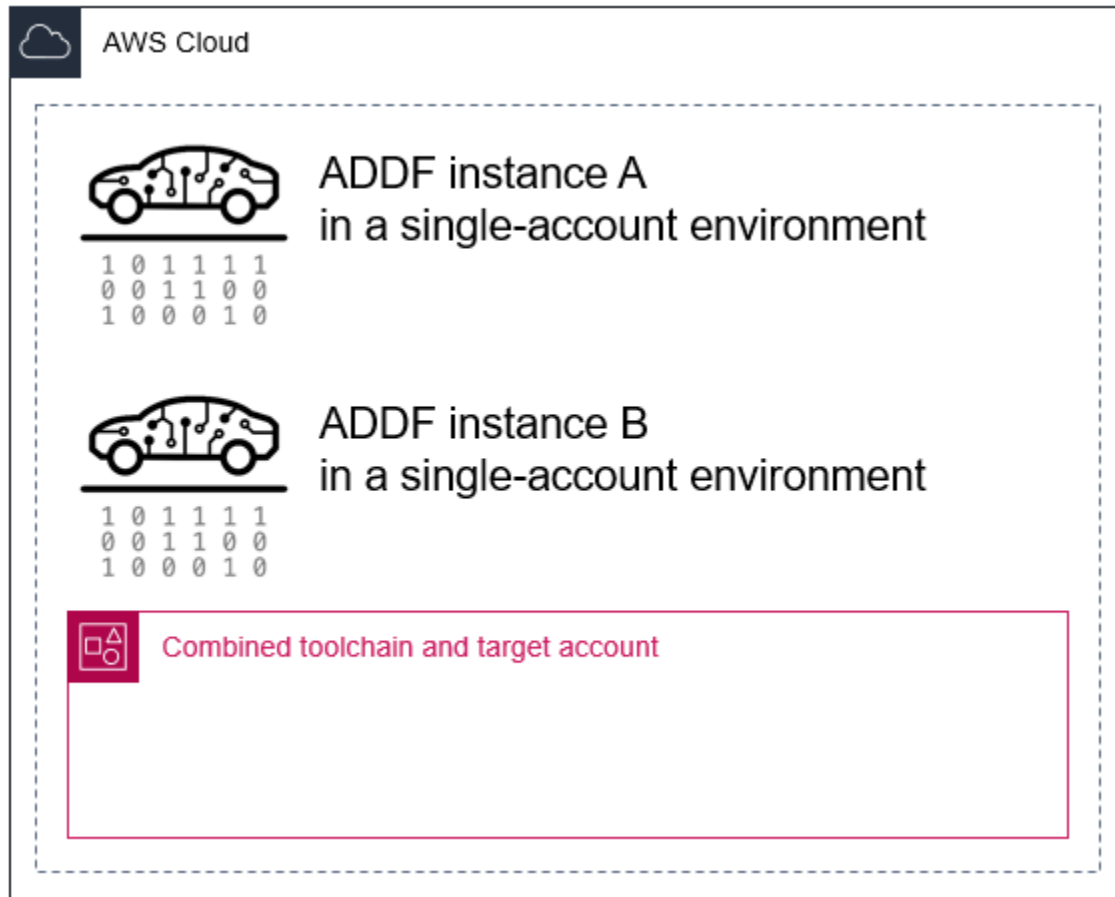
você pode criar instâncias do ADDF separadas e contas dedicadas para cada estágio. Isso oferece muitos benefícios, como reduzir o risco de propagação de qualquer erro entre os estágios, ajudar você a implementar um processo de aprovação e restringir o acesso do usuário somente a determinados ambientes. A imagem a seguir mostra duas instâncias do ADDF implantadas em ambientes separados com várias contas.



- Várias instâncias do ADDF no mesmo ambiente de AWS várias contas — Você pode criar várias instâncias do ADDF que compartilham o mesmo AWS ambiente de várias contas. Isso cria efetivamente ramificações isoladas nas mesmas Contas da AWS. Por exemplo, se diferentes desenvolvedores estiverem trabalhando em paralelo, um desenvolvedor poderá criar uma instância dedicada do ADDF nas mesmas Contas da AWS. Isso ajuda os desenvolvedores a trabalharem em ramificações isoladas para fins de desenvolvimento e teste. Se você usar essa abordagem, para cada instância do ADDF, seus recursos do ADDF deverão ter nomes de recursos exclusivos. Por padrão, isso é compatível com módulos pré-fornecidos pelo ADDF. Você pode usar essa abordagem, desde que não exceda as [cotas do AWS service \(Serviço da AWS\)](#). A imagem a seguir mostra duas instâncias do ADDF implantadas em ambientes com várias contas compartilhadas.



- Várias instâncias do ADDF no mesmo ambiente de conta única da AWS : essa arquitetura é muito semelhante ao exemplo anterior. A diferença é que as várias instâncias do ADDF são implantadas em um ambiente de conta única em vez de em um ambiente de várias contas. Essa arquitetura pode se adequar a casos de uso de ADDF muito simples que têm um escopo muito limitado e vários desenvolvedores trabalhando em diferentes ramificações ao mesmo tempo.



Como SeedFarmer é a única ferramenta que controla as implantações de uma instância ADDF, você pode criar qualquer ambiente e arquitetura de conta que se adapte à estratégia e CI/CD aos processos de implantação da sua organização.

- Personalize o processo de AWS Cloud Development Kit (AWS CDK) bootstrap de acordo com os requisitos de segurança da sua organização — Por padrão, AWS CDK atribui a política [AdministratorAccess](#) AWS gerenciada durante o processo de inicialização. Essa política concede privilégios administrativos completos. Se a política for muito permissiva para os requisitos de segurança da organização, você poderá personalizar quais políticas serão aplicadas. Para obter mais informações, consulte [Política personalizada de privilégios mínimos para a função de implantação AWS CDK](#).
- Siga as melhores práticas ao configurar o acesso no IAM — Estabeleça uma solução de acesso estruturada AWS Identity and Access Management (IAM) que permita que seus usuários acessem o ADDF Contas da AWS. A estrutura do ADDF foi projetada para aderir ao princípio de privilégio mínimo. Seu padrão de acesso do IAM também deve seguir o princípio de privilégio mínimo,

deve estar em conformidade com os requisitos da sua organização e deve aderir às [práticas recomendadas de segurança no IAM](#) (documentação do IAM).

- Configure a rede de acordo com as práticas recomendadas da sua organização: o ADDF inclui uma pilha do AWS CloudFormation de rede opcional que cria uma nuvem privada virtual (VPC) pública ou privada básica. Dependendo da configuração da sua organização, essa VPC pode expor recursos diretamente na Internet. Recomendamos que você siga as práticas recomendadas de rede da sua organização e crie um módulo de rede personalizado com segurança reforçada.
- Implemente medidas de prevenção, detecção e mitigação de segurança em Conta da AWS nível — AWS oferece vários serviços de segurança, como Amazon GuardDuty, AWS Security Hub CSPM Amazon Detective e. AWS Config Habilite esses serviços em seu ADDF Conta da AWS e integre os processos de prevenção, detecção, mitigação e tratamento de incidentes de segurança de sua organização. Recomendamos que você siga as [Práticas recomendadas de segurança, identidade e conformidade](#) (AWS Architecture Center) e quaisquer recomendações específicas do serviço contidas na documentação desse serviço. Para obter mais informações, consulte [Documentação de segurança da AWS](#).

O ADDF não aborda nenhum desses tópicos porque os detalhes de implementação e configuração dependem muito dos requisitos e processos específicos da sua organização. Em vez disso, é uma responsabilidade crucial da sua organização abordar esses tópicos. Normalmente, a equipe que gerencia sua [zona de destino da AWS](#) ajuda você a planejar e implementar seu ambiente do ADDF.

## Configuração inicial do

Configure o ADDF de acordo com o [Guia de implantação do ADDF](#) ( )GitHub. O ponto de partida para qualquer implantação é a `/manifest` pasta no repositório do [autonomous-driving-data-framework](#)Git Hub. A pasta `/manifest/example-dev` contém um exemplo de implantação para fins de demonstração. Use esse exemplo como ponto de partida para projetar sua própria implantação. Nesse diretório, há um arquivo de manifesto de implantação do ADDF chamado `deployment.yaml`. Ele contém todas as informações SeedFarmer para gerenciar, implantar ou excluir o ADDF e seus recursos no Nuvem AWS. Você pode criar grupos de módulos do ADDF em arquivos dedicados. O `core-modules.yaml` é um exemplo de grupo de módulos principais e inclui todos os módulos principais fornecidos pelo ADDF. Para resumir, o arquivo `deployment.yaml` contém todas as referências aos grupos e módulos que serão implantados em suas contas de destino e especifica a ordem de implantação.

Para uma configuração segura e compatível, especialmente em um ambiente que não serve para prova de conceito, recomendamos que você revise o código-fonte de cada módulo que você pretende implantar. De acordo com as práticas recomendadas de fortalecimento de segurança, você deve implantar somente os módulos necessários para o caso de uso pretendido.

#### Note

Os módulos do ADDF na pasta `modules/demo-only/` não têm segurança reforçada e não devem ser implantados em ambientes de produção ou em qualquer ambiente com dados confidenciais ou protegidos. Esses módulos estão incluídos para mostrar os recursos do sistema, e você pode usá-los como base para criar seus próprios módulos personalizados e com segurança reforçada.

## Personalizar o código da estrutura de implantação do ADDF

A estrutura de implantação do ADDF e sua lógica de orquestração e implantação podem ser totalmente personalizadas para atender a quaisquer requisitos. No entanto, sugerimos que você evite personalizar ou minimizar suas alterações pelos seguintes motivos:

- **Mantenha compatibilidade upstream:** a compatibilidade upstream facilita atualizar o ADDF com os recursos e atualizações de segurança mais recentes. A alteração da estrutura quebra a compatibilidade nativa com versões anteriores com SeedFarmer CodeSeeder, e com qualquer módulo principal do ADDF.
- **Consequências de segurança:** alterar a estrutura de implantação do ADDF pode ser uma tarefa complexa que pode ter consequências de segurança não intencionais. No pior cenário, mudanças na estrutura podem criar vulnerabilidades de segurança.

Quando possível, crie e personalize seu próprio código de módulo em vez de modificar a estrutura de implantação do ADDF e o código do módulo principal do ADDF.

#### Note

Se você acha que partes específicas da estrutura de implantação do ADDF precisam ter a segurança aprimorada ou reforçada, contribua com suas alterações para o repositório

do ADDF por meio de uma pull request. Para obter mais informações, consulte [Revisões e contribuições de segurança de código aberto](#).

## Escrever módulos personalizados no ADDF

Criar um novo módulo do ADDF ou estender um módulo existente é um conceito central do ADDF. Ao criar ou personalizar módulos, sugerimos que você siga as práticas recomendadas de segurança gerais da AWS e as práticas recomendadas de codificação segura da sua organização. Além disso, recomendamos que você realize revisões técnicas de segurança internas ou externas iniciais e periódicas, com base nos requisitos de segurança da sua organização, para reduzir ainda mais o risco de problemas de segurança.

## Implantações do ADDF recorrentes

Implante o ADDF e seus módulos conforme descrito no [Guia de implantação do ADDF](#) (GitHub). Para oferecer suporte a implantações recorrentes de ADDF que adicionam, atualizam ou removem recursos em suas contas de destino, SeedFarmer use MD5 hashes, armazenados no Parameter Store de sua cadeia de ferramentas e contas de destino, para comparar a infraestrutura atualmente implantada com a infraestrutura definida nos arquivos de manifesto em sua base de código local.

Essa abordagem segue o GitOps paradigma, em que seu repositório de origem (a base de código local em que você opera SeedFarmer) é a fonte da verdade e a infraestrutura declarada explicitamente nele é o resultado desejado de sua implantação. Para obter mais informações sobre GitOps, consulte [O que é GitOps](#) (GitLab site).

## Auditorias de segurança recorrentes

Assim como qualquer outro software em sua organização, integre o ADDF e seu código do módulo ADDF personalizado em seu ciclo de gerenciamento de riscos de segurança, análise de segurança e auditoria de segurança.

## Atualizações do ADDF

O ADDF recebe atualizações regulares como parte de seu esforço contínuo de desenvolvimento. Isso inclui atualizações de recursos e melhorias e correções relacionadas à segurança.

Recomendamos que você verifique regularmente as novas versões da estrutura e aplique as atualizações em tempo hábil. Para obter mais informações, consulte [Etapas para atualizar o ADDF](#) (documentação do ADDF).

## Descomissionamento

Se o ADDF não for mais necessário, exclua o ADDF e todos os recursos relacionados de suas Contas da AWS. Qualquer infraestrutura autônoma e não utilizada incorre em custos desnecessários e representa um possível risco de segurança. Para obter mais informações, consulte [Etapas para destruir o ADDF](#) (documentação do ADDF).

## Próximas etapas

Este guia analisou as melhores práticas e considerações de segurança e operações ao implantar o Autonomous Driving Data Framework (ADDF) em seu ambiente. Nuvem AWS Este guia analisa o modelo de responsabilidade compartilhada entre o usuário do ADDF e a equipe principal do ADDF AWS para que você entenda sua função e responsabilidades de configurar e operar o ADDF com segurança. Também inclui recomendações para operar o ADDF de forma segura durante todo o seu ciclo de vida, incluindo recomendações específicas do ambiente.

Recomendamos que você se familiarize com os recursos na seção [Recursos](#). Quando estiver pronto, você pode configurar o ADDF de acordo com as instruções no [Guia de implantação do ADDF](#) (GitHub).

À medida que configurar e operar o ADDF, se você achar que a estrutura de implantação precisa de aprimoramento ou de reforço de segurança, contribua com suas alterações para o repositório do ADDF por meio de uma pull request. Para obter mais informações, consulte [Revisões e contribuições de segurança de código aberto](#).

# Recursos

## AWS documentação

- [Desenvolva e implante um fluxo de trabalho personalizado usando o ADDF em AWS](#) (postagem AWS do blog)
- [AWS documentação do serviço de segurança](#)
- [Práticas recomendadas de segurança no IAM](#)
- [AWS gerenciamento e separação de contas](#)
- [Bootstrapping para AWS CDK](#)
- [Modelo de responsabilidade compartilhada da AWS](#)
- [AWS Well-Architected Framework](#)

## Recursos de código aberto

- [Repositório ADDF](#) () GitHub
- [Guia de implantação do ADDF](#) () GitHub
- [CodeSeederrepositório](#) () GitHub
- [SeedFarmerrepositório](#) () GitHub

# Avisos

Os clientes são responsáveis por fazer sua própria avaliação independente das informações contidas neste documento. Este documento: (a) é apenas para fins informativos, (b) representa ofertas e práticas atuais de AWS produtos, que estão sujeitas a alterações sem aviso prévio, e (c) não cria nenhum compromisso ou garantia de AWS suas afiliadas, fornecedores ou licenciadores. AWS os produtos ou serviços são fornecidos “como estão” sem garantias, representações ou condições de qualquer tipo, expressas ou implícitas.

As responsabilidades e obrigações de AWS seus clientes são controladas por AWS contratos, e este documento não faz parte nem modifica nenhum contrato entre AWS e seus clientes.

© 2022 Amazon Web Services, Inc. ou suas afiliadas. Todos os direitos reservados.

## Histórico do documento

A tabela a seguir descreve alterações significativas feitas neste guia. Se desejar receber notificações sobre futuras atualizações, inscreva-se em um [feed RSS](#).

Alteração	Descrição	Data
<a href="#">Publicação inicial</a>	—	15 de novembro de 2022

# AWS Glossário de orientação prescritiva

A seguir estão os termos comumente usados em estratégias, guias e padrões fornecidos pela Orientação AWS Prescritiva. Para sugerir entradas, use o link Fornecer feedback no final do glossário.

## Números

### 7 Rs

Sete estratégias comuns de migração para mover aplicações para a nuvem. Essas estratégias baseiam-se nos 5 Rs identificados pela Gartner em 2011 e consistem em:

- Refatorar/rearquitetar: mova uma aplicação e modifique sua arquitetura aproveitando ao máximo os recursos nativos de nuvem para melhorar a agilidade, a performance e a escalabilidade. Isso normalmente envolve a portabilidade do sistema operacional e do banco de dados. Exemplo: migrar seu banco de dados Oracle on-premises para o Amazon Aurora Edição Compatível com PostgreSQL.
- Redefinir a plataforma (mover e redefinir [mover e redefinir (lift-and-reshape)]): mova uma aplicação para a nuvem e introduza algum nível de otimização a fim de aproveitar os recursos da nuvem. Exemplo: migrar seu banco de dados Oracle on-premises para o Amazon Relational Database Service (Amazon RDS) para Oracle na Nuvem AWS.
- Recomprar (drop and shop): mude para um produto diferente, normalmente migrando de uma licença tradicional para um modelo SaaS. Exemplo: migrar seu sistema de gerenciamento de relacionamento com o cliente (CRM) para o Salesforce.com.
- Redefinir a hospedagem (mover sem alterações [lift-and-shift]) mover uma aplicação para a nuvem sem fazer nenhuma alteração a fim de aproveitar os recursos da nuvem. Exemplo: migrar seu banco de dados Oracle on-premises para o Oracle em uma instância do EC2 na Nuvem AWS.
- Realocar (mover o hipervisor sem alterações [hypervisor-level lift-and-shift]): mover a infraestrutura para a nuvem sem comprar novo hardware, reescrever aplicações ou modificar suas operações existentes. Você migra servidores de uma plataforma on-premises para um serviço de nuvem para a mesma plataforma. Exemplo: Migrar um Microsoft Hyper-V aplicativo para o AWS
- Reter (revisitar): mantenha as aplicações em seu ambiente de origem. Isso pode incluir aplicações que exigem grande refatoração, e você deseja adiar esse trabalho para um

momento posterior, e aplicações antigas que você deseja manter porque não há justificativa comercial para migrá-las.

- Retirar: desative ou remova aplicações que não são mais necessárias em seu ambiente de origem.

## A

### ABAC

Consulte [controle de acesso baseado em atributo](#).

serviços abstraídos

Veja [serviços gerenciados](#).

### ACID

Veja [atomicidade, consistência, isolamento, durabilidade](#).

migração ativa-ativa

Um método de migração de banco de dados no qual os bancos de dados de origem e de destino são mantidos em sincronia (por meio de uma ferramenta de replicação bidirecional ou operações de gravação dupla), e ambos os bancos de dados lidam com transações de aplicações conectadas durante a migração. Esse método oferece suporte à migração em lotes pequenos e controlados, em vez de exigir uma substituição única. É mais flexível, mas exige mais trabalho do que a [migração ativa-passiva](#).

migração ativa-passiva

Um método de migração de banco de dados em que os bancos de dados de origem e de destino são mantidos em sincronia, mas somente o banco de dados de origem manipula as transações das aplicações conectadas, enquanto os dados são replicados no banco de dados de destino. O banco de dados de destino não aceita nenhuma transação durante a migração.

### AGGREGATE FUNCTION

Uma função SQL que opera em um grupo de linhas e calcula um único valor de retorno para o grupo. Exemplos de funções agregadas incluem SUM e MAX.

## AI

Veja [inteligência artificial](#).

## AIOps

Veja [operações de inteligência artificial](#).

### anonimização

O processo de excluir permanentemente informações pessoais em um conjunto de dados. A anonimização pode ajudar a proteger a privacidade pessoal. Dados anônimos não são mais considerados dados pessoais.

### antipadrões

Uma solução frequentemente usada para um problema recorrente em que a solução é contraproducente, ineficaz ou menos eficaz do que uma alternativa.

### controle de aplicações

Uma abordagem de segurança que permite o uso somente de aplicações aprovadas para ajudar a proteger um sistema contra malware.

### portfólio de aplicações

Uma coleção de informações detalhadas sobre cada aplicação usada por uma organização, incluindo o custo para criar e manter a aplicação e seu valor comercial. Essas informações são fundamentais para [o processo de descoberta e análise de portfólio](#) e ajudam a identificar e priorizar as aplicações a serem migradas, modernizadas e otimizadas.

### inteligência artificial (IA)

O campo da ciência da computação que se dedica ao uso de tecnologias de computação para desempenhar funções cognitivas normalmente associadas aos humanos, como aprender, resolver problemas e reconhecer padrões. Para obter mais informações, consulte [O que é inteligência artificial?](#)

### operações de inteligência artificial (AIOps)

O processo de usar técnicas de machine learning para resolver problemas operacionais, reduzir incidentes operacionais e intervenção humana e aumentar a qualidade do serviço. Para obter mais informações sobre como AIOps é usado na estratégia de AWS migração, consulte o [guia de integração de operações](#).

## criptografia assimétrica

Um algoritmo de criptografia que usa um par de chaves, uma chave pública para criptografia e uma chave privada para descryptografia. É possível compartilhar a chave pública porque ela não é usada na descryptografia, mas o acesso à chave privada deve ser altamente restrito.

## atomicidade, consistência, isolamento, durabilidade (ACID)

Um conjunto de propriedades de software que garantem a validade dos dados e a confiabilidade operacional de um banco de dados, mesmo no caso de erros, falhas de energia ou outros problemas.

## controle de acesso por atributo (ABAC)

A prática de criar permissões minuciosas com base nos atributos do usuário, como departamento, cargo e nome da equipe. Para obter mais informações, consulte [ABAC AWS](#) na documentação AWS Identity and Access Management (IAM).

## fonte de dados autorizada

Um local onde você armazena a versão principal dos dados, que é considerada a fonte de informações mais confiável. Você pode copiar dados da fonte de dados autorizada para outros locais com o objetivo de processar ou modificar os dados, como anonimizá-los, redigi-los ou pseudonimizá-los.

## Zona de disponibilidade

Um local distinto dentro de um Região da AWS que está isolado de falhas em outras zonas de disponibilidade e fornece conectividade de rede barata e de baixa latência a outras zonas de disponibilidade na mesma região.

## AWS Estrutura de adoção da nuvem (AWS CAF)

Uma estrutura de diretrizes e melhores práticas AWS para ajudar as organizações a desenvolver um plano eficiente e eficaz para migrar com sucesso para a nuvem. AWS O CAF organiza a orientação em seis áreas de foco chamadas perspectivas: negócios, pessoas, governança, plataforma, segurança e operações. As perspectivas de negócios, pessoas e governança têm como foco habilidades e processos de negócios; as perspectivas de plataforma, segurança e operações concentram-se em habilidades e processos técnicos. Por exemplo, a perspectiva das pessoas tem como alvo as partes interessadas que lidam com recursos humanos (RH), funções de pessoal e gerenciamento de pessoal. Nessa perspectiva, o AWS CAF fornece orientação para desenvolvimento, treinamento e comunicação de pessoas para ajudar a preparar a organização

para a adoção bem-sucedida da nuvem. Para obter mais informações, consulte o [site da AWS CAF](#) e o [whitepaper da AWS CAF](#).

## AWS Estrutura de qualificação da carga de trabalho (AWS WQF)

Uma ferramenta que avalia as cargas de trabalho de migração do banco de dados, recomenda estratégias de migração e fornece estimativas de trabalho. AWS O WQF está incluído com AWS Schema Conversion Tool (AWS SCT). Ela analisa esquemas de banco de dados e objetos de código, código de aplicações, dependências e características de performance, além de fornecer relatórios de avaliação.

## B

### bot malicioso

Um [bot](#) destinado a causar disrupção ou danos a indivíduos ou organizações.

### BCP

Veja [planejamento de continuidade de negócios](#)

### gráfico de comportamento

Uma visualização unificada e interativa do comportamento e das interações de recursos ao longo do tempo. É possível usar um gráfico de comportamento com o Amazon Detective para examinar tentativas de login malsucedidas, chamadas de API suspeitas e ações similares. Para obter mais informações, consulte [Dados em um gráfico de comportamento](#) na documentação do Detective.

### sistema big-endian

Um sistema que armazena o byte mais significativo antes. Veja também [endianness](#).

### classificação binária

Um processo que prevê um resultado binário (uma de duas classes possíveis). Por exemplo, seu modelo de ML pode precisar prever problemas como “Este e-mail é ou não é spam?” ou “Este produto é um livro ou um carro?”

### filtro de bloom

Uma estrutura de dados probabilística e eficiente em termos de memória que é usada para testar se um elemento é membro de um conjunto.

## blue/green deployment (implantação azul/verde)

Uma estratégia de implantação em que você cria dois ambientes separados, mas idênticos. Você executa a versão atual da aplicação em um ambiente (azul) e a nova versão da aplicação no outro ambiente (verde). Essa estratégia ajuda você a reverter rapidamente com o mínimo de impacto.

## bot

Uma aplicação de software que executa tarefas automatizadas na internet e simula a atividade ou interação humana. Alguns bots são úteis ou benéficos, como crawlers da web que indexam informações na internet. Outros bots, conhecidos como bots maliciosos, têm como objetivo causar interrupção ou danos a indivíduos ou organizações.

## botnet

Redes de [bots](#) infectadas por [malware](#) e sob o controle de uma única parte, conhecidas como bot herder ou operador de bots. Os botnets são o mecanismo mais conhecido para escalar bots e seu impacto.

## ramo

Uma área contida de um repositório de código. A primeira ramificação criada em um repositório é a ramificação principal. Você pode criar uma nova ramificação a partir de uma ramificação existente e, em seguida, desenvolver recursos ou corrigir bugs na nova ramificação. Uma ramificação que você cria para gerar um recurso é comumente chamada de ramificação de recurso. Quando o recurso estiver pronto para lançamento, você mesclará a ramificação do recurso de volta com a ramificação principal. Para obter mais informações, consulte [Sobre filiais](#) (GitHub documentação).

## Acesso de emergência

Em circunstâncias excepcionais e por meio de um processo aprovado, um meio rápido para um usuário obter acesso a um Conta da AWS que ele normalmente não tem permissão para acessar. Para obter mais informações, consulte o indicador [Implement break-glass procedures](#) nas orientações do AWS Well-Architected.

## estratégia brownfield

A infraestrutura existente em seu ambiente. Ao adotar uma estratégia brownfield para uma arquitetura de sistema, você desenvolve a arquitetura de acordo com as restrições dos sistemas e da infraestrutura atuais. Se estiver expandindo a infraestrutura existente, poderá combinar as estratégias brownfield e [greenfield](#).

## cache do buffer

A área da memória em que os dados acessados com mais frequência são armazenados.

## capacidade de negócios

O que uma empresa faz para gerar valor (por exemplo, vendas, atendimento ao cliente ou marketing). As arquiteturas de microsserviços e as decisões de desenvolvimento podem ser orientadas por recursos de negócios. Para obter mais informações, consulte a seção [Organizados de acordo com as capacidades de negócios](#) do whitepaper [Executar microsserviços containerizados na AWS](#).

## planejamento de continuidade de negócios (BCP)

Um plano que aborda o impacto potencial de um evento disruptivo, como uma migração em grande escala, nas operações e permite que uma empresa retome as operações rapidamente.

# C

## CAF

Veja [AWS Cloud Adoption Framework](#).

## implantação canário

O lançamento lento e incremental de uma versão para usuários finais. Quando estiver confiante, você implanta a nova versão e substitui a versão atual por completo.

## CCoE

Veja [Centro de Excelência da Nuvem](#).

## CDC

Veja [captura de dados de alteração](#).

## captura de dados de alterações (CDC)

O processo de rastrear alterações em uma fonte de dados, como uma tabela de banco de dados, e registrar metadados sobre a alteração. É possível usar o CDC para várias finalidades, como auditar ou replicar alterações em um sistema de destino para manter a sincronização.

## engenharia do caos

Introduzir intencionalmente falhas ou eventos disruptivos para testar a resiliência de um sistema. Você pode usar [AWS Fault Injection Service \(AWS FIS\)](#) para realizar experimentos que estressam suas AWS cargas de trabalho e avaliar sua resposta.

## CI/CD

Veja [integração e entrega contínuas](#).

## classificação

Um processo de categorização que ajuda a gerar previsões. Os modelos de ML para problemas de classificação predizem um valor discreto. Os valores discretos são sempre diferentes uns dos outros. Por exemplo, um modelo pode precisar avaliar se há ou não um carro em uma imagem.

## criptografia no lado do cliente

Criptografia de dados localmente, antes que o alvo os AWS service (Serviço da AWS) receba.

## Centro de excelência em nuvem (CCoE)

Uma equipe multidisciplinar que impulsiona os esforços de adoção da nuvem em toda a organização, incluindo o desenvolvimento de práticas recomendadas de nuvem, a mobilização de recursos, o estabelecimento de cronogramas de migração e a liderança da organização em transformações em grande escala. Para obter mais informações, consulte as [publicações CCoE](#) no blog de estratégia Nuvem AWS corporativa.

## computação em nuvem

A tecnologia de nuvem normalmente usada para armazenamento de dados remoto e gerenciamento de dispositivos de IoT. A computação em nuvem é normalmente conectada à tecnologia de [computação de borda](#).

## modelo operacional em nuvem

Em uma organização de TI, o modelo operacional usado para criar, amadurecer e otimizar um ou mais ambientes de nuvem. Para obter mais informações, consulte [Criar seu modelo operacional de nuvem](#).

## estágios de adoção da nuvem

As quatro fases pelas quais as organizações normalmente passam ao migrar para a Nuvem AWS:

- Projeto: executar alguns projetos relacionados à nuvem para fins de prova de conceito e aprendizado
- Fundação — Fazer investimentos fundamentais para escalar sua adoção da nuvem (por exemplo, criar uma landing zone, definir um CCo E, estabelecer um modelo de operações)
- Migração: migrar aplicações individuais
- Reinvenção: otimizar produtos e serviços e inovar na nuvem

Esses estágios foram definidos por Stephen Orban na postagem do blog [The Journey Toward Cloud-First & the Stages of Adoption](#) no blog de estratégia Nuvem AWS empresarial. Para obter informações sobre como eles se relacionam com a estratégia de AWS migração, consulte o [guia de preparação para migração](#).

## CMDB

Veja [banco de dados de gerenciamento de configuração](#).

## repositório de código

Um local onde o código-fonte e outros ativos, como documentação, amostras e scripts, são armazenados e atualizados por meio de processos de controle de versão. Os repositórios de nuvem comuns incluem o GitHub ou o Bitbucket Cloud. Cada versão do código é chamada de ramificação. Em uma estrutura de microsserviços, cada repositório é dedicado a uma única peça de funcionalidade. Um único pipeline de CI/CD pode usar vários repositórios.

## cache frio

Um cache de buffer que está vazio, não está bem preenchido ou contém dados obsoletos ou irrelevantes. Isso afeta a performance porque a instância do banco de dados deve ler da memória principal ou do disco, um processo que é mais lento do que a leitura do cache do buffer.

## dados frios

Dados que raramente são acessados e geralmente são históricos. Ao consultar esse tipo de dados, consultas lentas geralmente são aceitáveis. Mover esses dados para níveis ou classes de armazenamento de baixo desempenho e menos caros pode reduzir os custos.

## visão computacional (CV)

Um campo de [IA](#) que usa machine learning para analisar e extrair informações de formatos visuais, como vídeos e imagens digitais. Por exemplo, a Amazon SageMaker AI fornece algoritmos de processamento de imagem para CV.

## desvio de configuração

Em uma workload, uma alteração de configuração em relação ao estado esperado. Isso pode fazer com que a workload se torne incompatível e, normalmente, é gradual e não intencional.

## banco de dados de gerenciamento de configuração (CMDB)

Um repositório que armazena e gerencia informações sobre um banco de dados e seu ambiente de TI, incluindo componentes de hardware e software e suas configurações. Normalmente, os dados de um CMDB são usados no estágio de descoberta e análise do portfólio da migração.

## pacote de conformidade

Um conjunto de AWS Config regras e ações de remediação que você pode montar para personalizar suas verificações de conformidade e segurança. Você pode implantar um pacote de conformidade como uma entidade única em uma Conta da AWS região ou em uma organização usando um modelo YAML. Para obter mais informações, consulte [Pacotes de conformidade na documentação](#). AWS Config

## integração contínua e entrega contínua (CI/CD)

O processo de automatizar os estágios de origem, criação, teste, preparação e produção do processo de lançamento do software. CI/CD é comumente descrito como um pipeline. CI/CD pode ajudá-lo a automatizar processos, melhorar a produtividade, melhorar a qualidade do código e entregar com mais rapidez. Para obter mais informações, consulte [Benefícios da entrega contínua](#). CD também pode significar implantação contínua. Para obter mais informações, consulte [Entrega contínua versus implantação contínua](#).

## CV

Veja [visão computacional](#).

## D

### dados em repouso

Dados estacionários em sua rede, por exemplo, dados que estão em um armazenamento.

### classificação de dados

Um processo para identificar e categorizar os dados em sua rede com base em criticalidade e confidencialidade. É um componente crítico de qualquer estratégia de gerenciamento de riscos de

segurança cibernética, pois ajuda a determinar os controles adequados de proteção e retenção para os dados. A classificação de dados é um componente do pilar de segurança no AWS Well-Architected Framework. Para obter mais informações, consulte [Classificação de dados](#).

#### desvio de dados

Uma variação significativa entre os dados de produção e os dados usados para treinar um modelo de ML ou uma alteração significativa nos dados de entrada ao longo do tempo. O desvio de dados pode reduzir a qualidade geral, a precisão e a imparcialidade das previsões do modelo de ML.

#### dados em trânsito

Dados que estão se movendo ativamente pela sua rede, como entre os recursos da rede.

#### data mesh

Um framework de arquitetura que fornece propriedade de dados distribuída e descentralizada com gerenciamento e governança centralizados.

#### minimização de dados

O princípio de coletar e processar apenas os dados estritamente necessários. Praticar a minimização de dados no Nuvem AWS pode reduzir os riscos de privacidade, os custos e a pegada de carbono de sua análise.

#### perímetro de dados

Um conjunto de proteções preventivas em seu AWS ambiente que ajudam a garantir que somente identidades confiáveis acessem recursos confiáveis das redes esperadas. Para obter mais informações, consulte [Construindo um perímetro de dados em AWS](#)

#### pré-processamento de dados

A transformação de dados brutos em um formato que seja facilmente analisado por seu modelo de ML. O pré-processamento de dados pode significar a remoção de determinadas colunas ou linhas e o tratamento de valores ausentes, inconsistentes ou duplicados.

#### proveniência dos dados

O processo de rastrear a origem e o histórico dos dados ao longo de seu ciclo de vida, por exemplo, como os dados foram gerados, transmitidos e armazenados.

#### titular dos dados

Um indivíduo cujos dados estão sendo coletados e processados.

## data warehouse

Um sistema de gerenciamento de dados compatível com business intelligence, como analytics. Os data warehouses geralmente contêm grandes quantidades de dados históricos e geralmente são usados para consultas e análises.

## linguagem de definição de dados (DDL)

Instruções ou comandos para criar ou modificar a estrutura de tabelas e objetos em um banco de dados.

## linguagem de manipulação de dados (DML)

Instruções ou comandos para modificar (inserir, atualizar e excluir) informações em um banco de dados.

## DDL

Veja [linguagem de definição de banco de dados](#).

## deep ensemble

A combinação de vários modelos de aprendizado profundo para gerar previsões. Os deep ensembles podem ser usados para produzir uma previsão mais precisa ou para estimar a incerteza nas previsões.

## Aprendizado profundo

Um subcampo do ML que usa várias camadas de redes neurais artificiais para identificar o mapeamento entre os dados de entrada e as variáveis-alvo de interesse.

## defense-in-depth

Uma abordagem de segurança da informação na qual uma série de mecanismos e controles de segurança são cuidadosamente distribuídos por toda a rede de computadores para proteger a confidencialidade, a integridade e a disponibilidade da rede e dos dados nela contidos. Ao adotar essa estratégia AWS, você adiciona vários controles em diferentes camadas da AWS Organizations estrutura para ajudar a proteger os recursos. Por exemplo, uma defense-in-depth abordagem pode combinar autenticação multifatorial, segmentação de rede e criptografia.

## administrador delegado

Em AWS Organizations, um serviço compatível pode registrar uma conta de AWS membro para administrar as contas da organização e gerenciar as permissões desse serviço. Essa conta

é chamada de administrador delegado para esse serviço Para obter mais informações e uma lista de serviços compatíveis, consulte [Serviços que funcionam com o AWS Organizations](#) na documentação do AWS Organizations .

## implantação

O processo de criar uma aplicação, novos recursos ou correções de código disponíveis no ambiente de destino. A implantação envolve a implementação de mudanças em uma base de código e, em seguida, a criação e execução dessa base de código nos ambientes da aplicação

## ambiente de desenvolvimento

Veja [ambiente](#).

## controle detectivo

Um controle de segurança projetado para detectar, registrar e alertar após a ocorrência de um evento. Esses controles são uma segunda linha de defesa, alertando você sobre eventos de segurança que contornaram os controles preventivos em vigor. Para obter mais informações, consulte [Controles detectivos](#) em Como implementar controles de segurança na AWS.

## mapeamento do fluxo de valor de desenvolvimento (DVSM)

Um processo usado para identificar e priorizar restrições que afetam negativamente a velocidade e a qualidade em um ciclo de vida de desenvolvimento de software. O DVSM estende o processo de mapeamento do fluxo de valor originalmente projetado para práticas de manufatura enxuta. Ele se concentra nas etapas e equipes necessárias para criar e movimentar valor por meio do processo de desenvolvimento de software.

## gêmeo digital

Uma representação virtual de um sistema real, como um prédio, fábrica, equipamento industrial ou linha de produção. Os gêmeos digitais oferecem suporte à manutenção preditiva, ao monitoramento remoto e à otimização da produção.

## tabela de dimensões

Em um [esquema em estrela](#), uma tabela menor que contém atributos de dados sobre dados quantitativos em uma tabela de fatos. Os atributos da tabela de dimensões geralmente são campos de texto ou números discretos que se comportam como texto. Esses atributos normalmente são usados para restringir consultas, filtrar e rotular conjuntos de resultados.

## desastre

Um evento que impede que uma workload ou sistema cumpra seus objetivos de negócios em seu local principal de implantação. Esses eventos podem ser desastres naturais, falhas técnicas ou o resultado de ações humanas, como configuração incorreta não intencional ou ataque de malware.

### Recuperação de desastres (RD)

A estratégia e o processo que você usa para minimizar o tempo de inatividade e a perda de dados causados por um [desastre](#). Para obter mais informações, consulte [Recuperação de desastres de cargas de trabalho em AWS: Recuperação na nuvem no AWS Well-Architected Framework](#).

## DML

Veja [linguagem de manipulação de banco de dados](#).

## design orientado por domínio

Uma abordagem ao desenvolvimento de um sistema de software complexo conectando seus componentes aos domínios em evolução, ou principais metas de negócios, atendidos por cada componente. Esse conceito foi introduzido por Eric Evans em seu livro, Design orientado por domínio: lidando com a complexidade no coração do software (Boston: Addison-Wesley Professional, 2003). Para obter informações sobre como usar o design orientado por domínio com o padrão strangler fig, consulte [Modernizar incrementalmente os serviços web herdados do Microsoft ASP.NET \(ASMX\) usando contêineres e o Amazon API Gateway](#).

## DR

Veja [recuperação de desastres](#).

## Deteção da oscilação

Rastreamento de desvios de uma configuração de linha de base. Por exemplo, você pode usar AWS CloudFormation para [detectar desvios nos recursos do sistema](#) ou AWS Control Tower para [detectar mudanças em seu landing zone](#) que possam afetar a conformidade com os requisitos de governança.

## DVSM

Veja [mapeamento do fluxo de valor de desenvolvimento](#).

## E

### EDA

Veja [análise exploratória de dados](#).

### EDI

Veja [intercâmbio eletrônico de dados](#).

### computação de borda

A tecnologia que aumenta o poder computacional de dispositivos inteligentes nas bordas de uma rede de IoT. Quando comparada com a [computação em nuvem](#), a computação de borda pode reduzir a latência da comunicação e melhorar o tempo de resposta.

### intercâmbio eletrônico de dados (EDI)

A troca automatizada de documentos comerciais entre organizações. Para obter mais informações, consulte [O que é EDI \(Intercâmbio eletrônico de dados\)?](#).

### criptografia

Um processo de computação que transforma dados de texto simples, legíveis por humanos, em texto cifrado.

### chave de criptografia

Uma sequência criptográfica de bits aleatórios que é gerada por um algoritmo de criptografia. As chaves podem variar em tamanho, e cada chave foi projetada para ser imprevisível e exclusiva.

### endianismo

A ordem na qual os bytes são armazenados na memória do computador. Os sistemas big-endian armazenam o byte mais significativo antes. Os sistemas little-endian armazenam o byte menos significativo antes.

### endpoint

Veja [endpoint de serviço](#).

### serviço de endpoint

Um serviço que pode ser hospedado em uma nuvem privada virtual (VPC) para ser compartilhado com outros usuários. Você pode criar um serviço de endpoint com AWS PrivateLink e conceder permissões a outros diretores Contas da AWS ou a AWS Identity and Access Management (IAM).

Essas contas ou entidades principais podem se conectar ao serviço de endpoint de maneira privada criando endpoints da VPC de interface. Para obter mais informações, consulte [Criar um serviço de endpoint](#) na documentação do Amazon Virtual Private Cloud (Amazon VPC).

## planejamento de recursos empresariais (ERP)

Um sistema que automatiza e gerencia os principais processos de negócios (como contabilidade, [MES](#) e gerenciamento de projetos) para uma empresa.

## criptografia envelopada

O processo de criptografar uma chave de criptografia com outra chave de criptografia. Para obter mais informações, consulte [Criptografia de envelope](#) na documentação AWS Key Management Service (AWS KMS).

## ambiente

Uma instância de uma aplicação em execução. Estes são tipos comuns de ambientes na computação em nuvem:

- ambiente de desenvolvimento: uma instância de uma aplicação em execução que está disponível somente para a equipe principal responsável pela manutenção da aplicação. Ambientes de desenvolvimento são usados para testar mudanças antes de promovê-las para ambientes superiores. Esse tipo de ambiente às vezes é chamado de ambiente de teste.
- ambientes inferiores: todos os ambientes de desenvolvimento para uma aplicação, como aqueles usados para compilações e testes iniciais.
- ambiente de produção: uma instância de uma aplicação em execução que os usuários finais podem acessar. Em um CI/CD pipeline, o ambiente de produção é o último ambiente de implantação.
- ambientes superiores: todos os ambientes que podem ser acessados por usuários que não sejam a equipe principal de desenvolvimento. Isso pode incluir um ambiente de produção, ambientes de pré-produção e ambientes para testes de aceitação do usuário.

## epic

Em metodologias ágeis, categorias funcionais que ajudam a organizar e priorizar seu trabalho. Os epics fornecem uma descrição de alto nível dos requisitos e das tarefas de implementação. Por exemplo, os épicos de segurança AWS da CAF incluem gerenciamento de identidade e acesso, controles de detetive, segurança de infraestrutura, proteção de dados e resposta a incidentes. Para obter mais informações sobre epics na estratégia de migração da AWS, consulte o [guia de implementação do programa](#).

## ERP

Veja [planejamento de recursos empresariais](#).

### análise exploratória de dados (EDA)

O processo de analisar um conjunto de dados para entender suas principais características. Você coleta ou agrega dados e, em seguida, realiza investigações iniciais para encontrar padrões, detectar anomalias e verificar suposições. O EDA é realizado por meio do cálculo de estatísticas resumidas e da criação de visualizações de dados.

## F

### tabela de fatos

A tabela central em um [esquema em estrela](#). Ela armazena dados quantitativos sobre as operações comerciais. Normalmente, uma tabela de fatos contém dois tipos de colunas: as que contêm medidas e as que contêm uma chave externa para uma tabela de dimensões.

### Antecipar-se à falha

Uma filosofia que usa testes frequentes e incrementais para reduzir o ciclo de vida do desenvolvimento. É uma parte essencial de uma abordagem ágil.

### delimitação de isolamento contra falhas

No Nuvem AWS, um limite, como uma zona de disponibilidade, Região da AWS um plano de controle ou um plano de dados, que limita o efeito de uma falha e ajuda a melhorar a resiliência das cargas de trabalho. Para obter mais informações, consulte [AWS Fault Isolation Boundaries](#).

### ramificação de recursos

Veja [ramificação](#).

### recursos

Os dados de entrada usados para fazer uma previsão. Por exemplo, em um contexto de manufatura, os recursos podem ser imagens capturadas periodicamente na linha de fabricação.

### importância do recurso

O quanto um recurso é importante para as previsões de um modelo. Isso geralmente é expresso como uma pontuação numérica que pode ser calculada por meio de várias técnicas, como

Shapley Additive Explanations (SHAP) e gradientes integrados. Para obter mais informações, consulte [Interpretabilidade do modelo de aprendizado de máquina com AWS](#).

## transformação de recursos

O processo de otimizar dados para o processo de ML, incluindo enriquecer dados com fontes adicionais, escalar valores ou extrair vários conjuntos de informações de um único campo de dados. Isso permite que o modelo de ML se beneficie dos dados. Por exemplo, se a data “2021-05-27 00:15:37” for dividida em “2021”, “maio”, “quinta” e “15”, isso poderá ajudar o algoritmo de aprendizado a aprender padrões diferenciados associados a diferentes componentes de dados.

## prompt few shot

Fornecer a um [LLM](#) um pequeno número de exemplos que demonstram a tarefa e o resultado desejado antes de solicitar que ele execute uma tarefa semelhante. Essa técnica é uma aplicação do aprendizado em contexto, em que os modelos aprendem com exemplos (shots) incorporados aos prompts. Prompts few-shot podem ser eficazes para tarefas que exigem formatação, raciocínio ou conhecimento de domínio específicos. Veja também [prompts zero-shot](#).

## FGAC

Veja [controle de acesso refinado](#).

## Controle de acesso refinado (FGAC)

O uso de várias condições para permitir ou negar uma solicitação de acesso.

## migração flash-cut

Um método de migração de banco de dados que usa replicação contínua de dados via [captura de dados de alteração](#) para migrar os dados no menor tempo possível, em vez de usar uma abordagem em fases. O objetivo é reduzir ao mínimo o tempo de inatividade.

## FM

Veja [modelo de base](#).

## modelo de base (FM)

Uma grande rede neural de aprendizado profundo que vem treinando em grandes conjuntos de dados generalizados e não rotulados. FMs são capazes de realizar uma ampla variedade de tarefas gerais, como entender a linguagem, gerar texto e imagens e conversar em linguagem natural. Para obter mais informações, consulte [O que são modelos de base?](#).

# G

## IA generativa

Um subconjunto de modelos de [IA](#) que foram treinados em grandes quantidades de dados e que podem usar um simples prompt de texto para criar novos artefatos e conteúdo, como imagens, vídeos, texto e áudio. Para obter mais informações, consulte [O que é IA generativa?](#).

## bloqueio geográfico

Veja [restrições geográficas](#).

## restrições geográficas (bloqueio geográfico)

Na Amazon CloudFront, uma opção para impedir que usuários em países específicos acessem distribuições de conteúdo. É possível usar uma lista de permissões ou uma lista de bloqueios para especificar países aprovados e banidos. Para obter mais informações, consulte [Restringir a distribuição geográfica do seu conteúdo](#) na CloudFront documentação.

## Fluxo de trabalho do GitFlow

Uma abordagem na qual ambientes inferiores e superiores usam ramificações diferentes em um repositório de código-fonte. O fluxo de trabalho do Gitflow é considerado legado, e o [fluxo de trabalho trunk-based](#) é a abordagem moderna e preferencial.

## golden image

Um snapshot de um sistema ou software usado como modelo para implantar novas instâncias desse sistema ou software. Por exemplo, na manufatura, uma golden image pode ser usada para provisionar software em vários dispositivos e ajudar a melhorar a velocidade, a escalabilidade e a produtividade nas operações de fabricação de dispositivos.

## estratégia greenfield

A ausência de infraestrutura existente em um novo ambiente. Ao adotar uma estratégia greenfield para uma arquitetura de sistema, é possível selecionar todas as novas tecnologias sem a restrição da compatibilidade com a infraestrutura existente, também conhecida como [brownfield](#). Se estiver expandindo a infraestrutura existente, poderá combinar as estratégias brownfield e greenfield.

## barreira de proteção

Uma regra de alto nível que ajuda a governar recursos, políticas e conformidade em todas as unidades organizacionais (OUs). Barreiras de proteção preventivas impõem políticas para

garantir o alinhamento a padrões de conformidade. Elas são implementadas usando políticas de controle de serviço e limites de permissões do IAM. Barreiras de proteção detectivas detectam violações de políticas e problemas de conformidade e geram alertas para remediação. Eles são implementados usando AWS Config, AWS Security Hub CSPM, Amazon GuardDuty AWS Trusted Advisor, Amazon Inspector e verificações personalizadas AWS Lambda .

## H

### HA

Veja [alta disponibilidade](#).

#### migração heterogênea de bancos de dados

Migrar seu banco de dados de origem para um banco de dados de destino que usa um mecanismo de banco de dados diferente (por exemplo, Oracle para Amazon Aurora). A migração heterogênea geralmente faz parte de um esforço de redefinição da arquitetura, e converter o esquema pode ser uma tarefa complexa. [O AWS fornece o AWS SCT](#) para ajudar nas conversões de esquemas.

#### alta disponibilidade (HA)

A capacidade de uma workload operar continuamente, sem intervenção, em caso de desafios ou desastres. Os sistemas AH são projetados para realizar o failover automático, oferecer consistentemente desempenho de alta qualidade e lidar com diferentes cargas e falhas com impacto mínimo no desempenho.

#### modernização de historiador

Uma abordagem usada para modernizar e atualizar os sistemas de tecnologia operacional (OT) para melhor atender às necessidades do setor de manufatura. Um historiador é um tipo de banco de dados usado para coletar e armazenar dados de várias fontes em uma fábrica.

#### dados de hold-out

Uma parte dos dados históricos rotulados que são retidos de um conjunto de dados usado para treinar um modelo de [machine learning](#). Você pode usar dados de hold-out para avaliar a performance do modelo comparando as predições do modelo com os dados de retenção.

## migração homogênea de bancos de dados

Migrar seu banco de dados de origem para um banco de dados de destino que compartilha o mesmo mecanismo de banco de dados (por exemplo, Microsoft SQL Server para Amazon RDS para SQL Server). A migração homogênea geralmente faz parte de um esforço de redefinição da hospedagem ou da plataforma. É possível usar utilitários de banco de dados nativos para migrar o esquema.

## dados quentes

Dados acessados com frequência, como dados em tempo real ou dados translacionais recentes. Esses dados normalmente exigem uma camada ou classe de armazenamento de alto desempenho para fornecer respostas rápidas às consultas.

## hotfix

Uma correção urgente para um problema crítico em um ambiente de produção. Devido à sua urgência, um hotfix geralmente é feito fora do fluxo de trabalho normal de DevOps lançamento.

## período de hipercuidados

Imediatamente após a substituição, o período em que uma equipe de migração gerencia e monitora as aplicações migradas na nuvem para resolver quaisquer problemas. Normalmente, a duração desse período é de 1 a 4 dias. No final do período de hipercuidados, a equipe de migração normalmente transfere a responsabilidade pelas aplicações para a equipe de operações de nuvem.

## eu

## laC

Veja [infraestrutura como código](#).

## Política baseada em identidade

Uma política anexada a um ou mais diretores do IAM que define suas permissões no Nuvem AWS ambiente.

## aplicação ociosa

Uma aplicação que tem um uso médio de CPU e memória entre 5 e 20% em um período de 90 dias. Em um projeto de migração, é comum retirar essas aplicações ou retê-las on-premises.

## IloT

Veja [Internet das Coisas Industrial](#).

### infraestrutura imutável

Um modelo que implanta uma nova infraestrutura para workloads de produção em vez de atualizar, aplicar patches ou modificar a infraestrutura existente. Infraestruturas imutáveis são inerentemente mais consistentes, confiáveis e preditivas do que [infraestruturas mutáveis](#). Para obter mais informações, consulte a prática recomendada [Implantar usando infraestrutura imutável](#) no AWS Well-Architected Framework.

### VPC de entrada (admissão)

Em uma arquitetura de AWS várias contas, uma VPC que aceita, inspeciona e roteia conexões de rede de fora de um aplicativo. A [Arquitetura de Referência de AWS Segurança](#) recomenda configurar sua conta de rede com entrada, saída e inspeção VPCs para proteger a interface bidirecional entre seu aplicativo e a Internet em geral.

### migração incremental

Uma estratégia de substituição na qual você migra a aplicação em pequenas partes, em vez de realizar uma única substituição completa. Por exemplo, é possível mover inicialmente apenas alguns microsserviços ou usuários para o novo sistema. Depois de verificar se tudo está funcionando corretamente, mova os microsserviços ou usuários adicionais de forma incremental até poder descomissionar seu sistema herdado. Essa estratégia reduz os riscos associados a migrações de grande porte.

### Indústria 4.0

Um termo que foi introduzido por [Klaus Schwab](#) em 2016 para se referir à modernização dos processos de manufatura por meio de avanços em conectividade, dados em tempo real, automação, analytics e IA/ML.

### infraestrutura

Todos os recursos e ativos contidos no ambiente de uma aplicação.

### Infraestrutura como código (IaC)

O processo de provisionamento e gerenciamento da infraestrutura de uma aplicação por meio de um conjunto de arquivos de configuração. A IaC foi projetada para ajudar você a centralizar o gerenciamento da infraestrutura, padronizar recursos e escalar rapidamente para que novos ambientes sejam reproduzíveis, confiáveis e consistentes.

## Internet industrial das coisas (IIoT)

O uso de sensores e dispositivos conectados à Internet nos setores industriais, como manufatura, energia, automotivo, saúde, ciências biológicas e agricultura. Para obter mais informações, consulte [Criando uma estratégia de transformação digital industrial da Internet das Coisas \(IIoT\)](#).

## VPC de inspeção

Em uma arquitetura de AWS várias contas, uma VPC centralizada que gerencia as inspeções do tráfego de rede entre VPCs (na mesma ou em diferentes Regiões da AWS) a Internet e as redes locais. A [Arquitetura de Referência de AWS Segurança](#) recomenda configurar sua conta de rede com entrada, saída e inspeção VPCs para proteger a interface bidirecional entre seu aplicativo e a Internet em geral.

## Internet das coisas (IoT)

A rede de objetos físicos conectados com sensores ou processadores incorporados que se comunicam com outros dispositivos e sistemas pela Internet ou por uma rede de comunicação local. Para obter mais informações, consulte [O que é IoT?](#)

## interpretabilidade

Uma característica de um modelo de machine learning que descreve o grau em que um ser humano pode entender como as previsões do modelo dependem de suas entradas. Para obter mais informações, consulte [Interpretabilidade do modelo de aprendizado de máquina com AWS](#).

## IoT

Veja [Internet das Coisas](#).

## Biblioteca de informações de TI (ITIL)

Um conjunto de práticas recomendadas para fornecer serviços de TI e alinhar esses serviços a requisitos de negócios. A ITIL fornece a base para o ITSM.

## Gerenciamento de serviços de TI (ITSM)

Atividades associadas a design, implementação, gerenciamento e suporte de serviços de TI para uma organização. Para obter informações sobre a integração de operações em nuvem com ferramentas de ITSM, consulte o [guia de integração de operações](#).

## ITIL

Veja [biblioteca de informações de TI](#).

## ITSM

Veja [gerenciamento de serviços de TI](#).

## L

### controle de acesso baseado em etiqueta (LBAC)

Uma implementação do controle de acesso obrigatório (MAC) em que os usuários e os dados em si recebem explicitamente um valor de etiqueta de segurança. A interseção entre a etiqueta de segurança do usuário e a etiqueta de segurança dos dados determina quais linhas e colunas podem ser vistas pelo usuário.

### zona de pouso

Uma landing zone é um AWS ambiente bem arquitetado, com várias contas, escalável e seguro. Um ponto a partir do qual suas organizações podem iniciar e implantar rapidamente workloads e aplicações com confiança em seu ambiente de segurança e infraestrutura. Para obter mais informações sobre zonas de pouso, consulte [Configurar um ambiente da AWS com várias contas seguro e escalável](#).

### grande modelo de linguagem (LLM)

Um modelo de [IA](#) de aprendizado profundo pré-treinado em uma grande quantidade de dados. Um LLM pode realizar várias tarefas, como responder a perguntas, resumir documentos, traduzir texto para outros idiomas e completar frases. Para obter mais informações, consulte [O que são LLMs](#).

### migração de grande porte

Uma migração de 300 servidores ou mais.

### LBAC

Veja [controle de acesso baseado em rótulo](#).

### privilégio mínimo

A prática recomendada de segurança de conceder as permissões mínimas necessárias para executar uma tarefa. Para obter mais informações, consulte [Aplicar permissões de privilégios mínimos](#) na documentação do IAM.

mover sem alterações (lift-and-shift)

Veja [7 Rs](#).

sistema little-endian

Um sistema que armazena o byte menos significativo antes. Veja também [endianness](#).

LLM

Veja [grande modelo de linguagem](#).

ambientes inferiores

Veja [ambiente](#).

## M

machine learning (ML)

Um tipo de inteligência artificial que usa algoritmos e técnicas para reconhecimento e aprendizado de padrões. O ML analisa e aprende com dados gravados, por exemplo, dados da Internet das Coisas (IoT), para gerar um modelo estatístico baseado em padrões. Para obter mais informações, consulte [Machine learning](#).

ramificação principal

Veja [ramificação](#).

Malware

Software projetado para comprometer a segurança ou a privacidade do computador. O malware pode interromper os sistemas do computador, vaziar informações sensíveis ou obter acesso não autorizado. Exemplos de malware incluem vírus, worms, ransomware, cavalos de Troia, spyware e keyloggers.

Serviços gerenciados

Serviços da AWS para o qual AWS opera a camada de infraestrutura, o sistema operacional e as plataformas, e você acessa os endpoints para armazenar e recuperar dados. O Amazon Simple Storage Service (Amazon S3) e o Amazon DynamoDB são exemplos de serviços gerenciados. Eles também são conhecidos como serviços abstraídos.

## sistema de execução de manufatura (MES)

Um sistema de software para rastrear, monitorar, documentar e controlar processos de produção que convertem matérias-primas em produtos acabados no chão de fábrica.

## MAP

Veja [Programa de Aceleração da Migração](#).

## mecanismo

Um processo completo em que você cria uma ferramenta, impulsiona a adoção da ferramenta e, em seguida, inspeciona os resultados para fazer ajustes. Um mecanismo é um ciclo que se reforça e se aprimora à medida que opera. Para obter mais informações, consulte [Construindo mecanismos](#) no AWS Well-Architected Framework.

## conta de membro

Todos, Contas da AWS exceto a conta de gerenciamento, que fazem parte de uma organização em AWS Organizations. Uma conta só pode ser membro de uma organização de cada vez.

## MES

Veja [sistema de execução de manufatura](#).

## Transporte de Telemetria de Enfileiramento de Mensagens (MQTT)

[Um protocolo de comunicação leve machine-to-machine \(M2M\), baseado no padrão de publicação/assinatura, para dispositivos de IoT com recursos limitados.](#)

## microsserviço

Um serviço pequeno e independente que se comunica de forma bem definida APIs e normalmente é de propriedade de equipes pequenas e independentes. Por exemplo, um sistema de seguradora pode incluir microsserviços que mapeiam as capacidades comerciais, como vendas ou marketing, ou subdomínios, como compras, reclamações ou análises. Os benefícios dos microsserviços incluem agilidade, escalabilidade flexível, fácil implantação, código reutilizável e resiliência. Para obter mais informações, consulte [Integração de microsserviços usando serviços sem AWS servidor](#).

## arquitetura de microsserviços

Uma abordagem à criação de aplicações com componentes independentes que executam cada processo de aplicação como um microsserviço. Esses microsserviços se comunicam por meio

de uma interface bem definida usando leveza. APIs Cada microserviço nessa arquitetura pode ser atualizado, implantado e escalado para atender à demanda por funções específicas de uma aplicação. Para obter mais informações, consulte [Implementação de microserviços em. AWS](#)

## Programa de Aceleração da Migração (MAP)

Um AWS programa que fornece suporte de consultoria, treinamento e serviços para ajudar as organizações a criar uma base operacional sólida para migrar para a nuvem e ajudar a compensar o custo inicial das migrações. O MAP inclui uma metodologia de migração para executar migrações legadas de forma metódica e um conjunto de ferramentas para automatizar e acelerar cenários comuns de migração.

## migração em escala

O processo de mover a maior parte do portfólio de aplicações para a nuvem em ondas, com mais aplicações sendo movidas em um ritmo mais rápido a cada onda. Essa fase usa as práticas recomendadas e lições aprendidas nas fases anteriores para implementar uma fábrica de migração de equipes, ferramentas e processos para agilizar a migração de workloads por meio de automação e entrega ágeis. Esta é a terceira fase da [estratégia de migração para a AWS](#).

## fábrica de migração

Equipes multifuncionais que simplificam a migração de workloads por meio de abordagens automatizadas e ágeis. As equipes da fábrica de migração geralmente incluem operações, analistas e proprietários de negócios, engenheiros de migração, desenvolvedores e DevOps profissionais que trabalham em sprints. Entre 20 e 50% de um portfólio de aplicações corporativas consiste em padrões repetidos que podem ser otimizados por meio de uma abordagem de fábrica. Para obter mais informações, consulte [discussão sobre fábricas de migração](#) e o [guia do Cloud Migration Factory](#) neste conjunto de conteúdo.

## metadados de migração

As informações sobre a aplicação e o servidor necessárias para concluir a migração. Cada padrão de migração exige um conjunto de metadados de migração diferente. Exemplos de metadados de migração incluem a sub-rede, o grupo de segurança e AWS a conta de destino.

## padrão de migração

Uma tarefa de migração repetível que detalha a estratégia de migração, o destino da migração e a aplicação ou o serviço de migração usado. Exemplo: rehoste a migração para o Amazon EC2 AWS com o Application Migration Service.

## Avaliação de Portfólio para Migração (MPA)

Uma ferramenta on-line que fornece informações para validar o caso de negócios para migrar para a Nuvem AWS. O MPA fornece avaliação detalhada do portfólio (dimensionamento correto do servidor, preços, comparações de TCO, análise de custos de migração), bem como planejamento de migração (análise e coleta de dados de aplicações, agrupamento de aplicações, priorização de migração e planejamento de ondas). A [ferramenta MPA](#) (requer login) está disponível gratuitamente para todos os AWS consultores e consultores parceiros da APN.

## Avaliação de Preparação para Migração (MRA)

O processo de obter insights sobre o status de prontidão de uma organização para a nuvem, identificar pontos fortes e fracos e criar um plano de ação para fechar as lacunas identificadas, usando o CAF. AWS Para mais informações, consulte o [guia de preparação para migração](#). A MRA é a primeira fase da [estratégia de migração para a AWS](#).

## estratégia de migração

A abordagem usada para migrar uma workload para a Nuvem AWS. Para obter mais informações, veja a entrada [7 Rs](#) neste glossário e consulte [Mobilize sua organização para acelerar migrações em grande escala](#).

## ML

Veja [machine learning](#).

## modernização

Transformar uma aplicação desatualizada (herdada ou monolítica) e sua infraestrutura em um sistema ágil, elástico e altamente disponível na nuvem para reduzir custos, ganhar eficiência e aproveitar as inovações. Para obter mais informações, consulte [Strategy for modernizing applications in the Nuvem AWS](#).

## avaliação de preparação para modernização

Uma avaliação que ajuda a determinar a preparação para modernização das aplicações de uma organização. Ela identifica benefícios, riscos e dependências e determina o quão bem a organização pode acomodar o estado futuro dessas aplicações. O resultado da avaliação é um esquema da arquitetura de destino, um roteiro que detalha as fases de desenvolvimento e os marcos do processo de modernização e um plano de ação para abordar as lacunas identificadas. Para obter mais informações, consulte [Evaluating modernization readiness for applications in the Nuvem AWS](#).

## aplicações monolíticas (monólitos)

Aplicações que são executadas como um único serviço com processos fortemente acoplados. As aplicações monolíticas apresentam várias desvantagens. Se um recurso da aplicação apresentar um aumento na demanda, toda a arquitetura deverá ser escalada. Adicionar ou melhorar os recursos de uma aplicação monolítica também se torna mais complexo quando a base de código cresce. Para resolver esses problemas, é possível criar uma arquitetura de microsserviços. Para obter mais informações, consulte [Decompor monólitos em microsserviços](#).

## MPA

Veja [Avaliação do Portfólio para Migração](#).

## MQTT

Veja [Transporte de Telemetria de Enfileiramento de Mensagens](#).

## classificação multiclasse

Um processo que ajuda a gerar previsões para várias classes (prevendo um ou mais de dois resultados). Por exemplo, um modelo de ML pode perguntar “Este produto é um livro, um carro ou um telefone?” ou “Qual categoria de produtos é mais interessante para este cliente?”

## infraestrutura mutável

Um modelo que atualiza e modifica a infraestrutura existente para workloads de produção. Para melhorar a consistência, confiabilidade e previsibilidade, o AWS Well-Architected Framework recomenda o uso de infraestrutura [imutável](#) como uma prática recomendada.

## O

### OAC

Veja [controle de acesso de origem](#).

### OAI

Veja [identidade de acesso de origem](#).

### OCM

Veja [gerenciamento de alterações organizacionais](#).

## migração offline

Um método de migração no qual a workload de origem é desativada durante o processo de migração. Esse método envolve tempo de inatividade prolongado e geralmente é usado para workloads pequenas e não críticas.

OI

Veja [integração de operações](#).

Ola

Veja [acordo de nível operacional](#).

## migração online

Um método de migração no qual a workload de origem é copiada para o sistema de destino sem ser colocada offline. As aplicações conectadas à workload podem continuar funcionando durante a migração. Esse método envolve um tempo de inatividade nulo ou mínimo e normalmente é usado para workloads essenciais para a produção.

OPC-UA

Veja [Open Process Communications - Unified Architecture](#).

Open Process Communications - Unified Architecture (OPC-UA)

Um protocolo de comunicação machine-to-machine (M2M) para automação industrial. O OPC-UA fornece um padrão de interoperabilidade com esquemas de criptografia, autenticação e autorização de dados.

acordo de nível operacional (OLA)

Um acordo que esclarece o que os grupos funcionais de TI prometem oferecer uns aos outros para apoiar um acordo de serviço (SLA).

análise de prontidão operacional (ORR)

Uma lista de verificação de perguntas e práticas recomendadas associadas que ajudam você a entender, avaliar, prevenir ou reduzir o escopo de incidentes e possíveis falhas. Para obter mais informações, consulte [Operational Readiness Reviews \(ORR\)](#) no AWS Well-Architected Framework.

tecnologia operacional (TO)

Sistemas de hardware e software que trabalham com o ambiente físico para controlar operações, equipamentos e infraestrutura industriais. Na manufatura, a integração dos sistemas de

tecnologia da informação (TI) e tecnologia operacional (TO) é o foco principal das transformações da [Indústria 4.0](#).

#### integração de operações (OI)

O processo de modernização das operações na nuvem, que envolve planejamento de preparação, automação e integração. Para obter mais informações, consulte o [guia de integração de operações](#).

#### trilha organizacional

Uma trilha criada por ela AWS CloudTrail registra todos os eventos de todas as Contas da AWS em uma organização em AWS Organizations. Essa trilha é criada em cada Conta da AWS que faz parte da organização e monitora a atividade em cada conta. Para obter mais informações, consulte [Criação de uma trilha para uma organização](#) na CloudTrail documentação.

#### gerenciamento de alterações organizacionais (OCM)

Uma estrutura para gerenciar grandes transformações de negócios disruptivas de uma perspectiva de pessoas, cultura e liderança. O OCM ajuda as organizações a se prepararem e fazerem a transição para novos sistemas e estratégias, acelerando a adoção de alterações, abordando questões de transição e promovendo mudanças culturais e organizacionais. Na estratégia de AWS migração, essa estrutura é chamada de aceleração de pessoas, devido à velocidade de mudança exigida nos projetos de adoção da nuvem. Para obter mais informações, consulte o [guia do OCM](#).

#### controle de acesso de origem (OAC)

Em CloudFront, uma opção aprimorada para restringir o acesso para proteger seu conteúdo do Amazon Simple Storage Service (Amazon S3). O OAC oferece suporte a todos os buckets S3 Regiões da AWS, criptografia do lado do servidor com AWS KMS (SSE-KMS) e solicitações dinâmicas ao bucket S3. PUT DELETE

#### Identidade do acesso de origem (OAI)

Em CloudFront, uma opção para restringir o acesso para proteger seu conteúdo do Amazon S3. Quando você usa o OAI, CloudFront cria um principal com o qual o Amazon S3 pode se autenticar. Os diretores autenticados podem acessar o conteúdo em um bucket do S3 somente por meio de uma distribuição específica. CloudFront Veja também [OAC](#), que fornece um controle de acesso mais granular e aprimorado.

#### ORR

Veja [análise de prontidão operacional](#).

## OT

Veja [tecnologia operacional](#).

### VPC de saída (egresso)

Em uma arquitetura de AWS várias contas, uma VPC que gerencia conexões de rede que são iniciadas de dentro de um aplicativo. A [Arquitetura de Referência de AWS Segurança](#) recomenda configurar sua conta de rede com entrada, saída e inspeção VPCs para proteger a interface bidirecional entre seu aplicativo e a Internet em geral.

## P

### limite de permissões

Uma política de gerenciamento do IAM anexada a entidades principais do IAM para definir as permissões máximas que o usuário ou perfil podem ter. Para obter mais informações, consulte [Limites de permissões](#) na documentação do IAM.

### Informações de identificação pessoal (PII)

Informações que, quando visualizadas diretamente ou combinadas com outros dados relacionados, podem ser usadas para inferir razoavelmente a identidade de um indivíduo. Exemplos de PII incluem nomes, endereços e informações de contato.

## PII

Veja [informações de identificação pessoal](#).

### manual

Um conjunto de etapas predefinidas que capturam o trabalho associado às migrações, como a entrega das principais funções operacionais na nuvem. Um manual pode assumir a forma de scripts, runbooks automatizados ou um resumo dos processos ou etapas necessários para operar seu ambiente modernizado.

## PLC

Veja [controlador lógico programável](#).

## PLM

Veja [gerenciamento do ciclo de vida do produto](#).

## política

Um objeto que pode definir permissões (veja [política baseada em identidade](#)), especificar condições de acesso (veja [política baseada em recurso](#)) ou definir as permissões máximas para todas as contas em uma organização no AWS Organizations (veja [política de controle de serviços](#)).

## persistência poliglota

Escolher de forma independente a tecnologia de armazenamento de dados de um microsserviço com base em padrões de acesso a dados e outros requisitos. Se seus microsserviços tiverem a mesma tecnologia de armazenamento de dados, eles poderão enfrentar desafios de implementação ou apresentar baixa performance. Os microsserviços serão implementados com mais facilidade e alcançarão performance e escalabilidade melhores se usarem o armazenamento de dados mais bem adaptado às suas necessidades.

## avaliação do portfólio

Um processo de descobrir, analisar e priorizar o portfólio de aplicações para planejar a migração. Para obter mais informações, consulte [Avaliar a preparação para a migração](#).

## predicado

Uma condição de consulta que retorna `true` ou `false`, normalmente localizada em uma cláusula `WHERE`.

## pushdown de predicados

Uma técnica de otimização de consultas de banco de dados que filtra os dados na consulta antes da transferência. Isso reduz a quantidade de dados que devem ser recuperados e processados do banco de dados relacional e melhora a performance das consultas.

## controle preventivo

Um controle de segurança projetado para evitar que um evento ocorra. Esses controles são a primeira linha de defesa para ajudar a evitar acesso não autorizado ou alterações indesejadas em sua rede. Para obter mais informações, consulte [Controles preventivos](#) em Como implementar controles de segurança na AWS.

## principal (entidade principal)

Uma entidade AWS que pode realizar ações e acessar recursos. Essa entidade geralmente é um usuário raiz para um Conta da AWS, uma função do IAM ou um usuário. Para obter mais

informações, consulte Entidade principal em [Termos e conceitos de perfis](#) na documentação do IAM.

## Privacidade por design

Uma abordagem em engenharia de sistemas que leva em consideração a privacidade em todo o processo de desenvolvimento.

## zonas hospedadas privadas

Um contêiner que contém informações sobre como você deseja que o Amazon Route 53 responda às consultas de DNS para um domínio e seus subdomínios em um ou mais VPCs. Para obter mais informações, consulte [Como trabalhar com zonas hospedadas privadas](#) na documentação do Route 53.

## controle proativo

Um [controle de segurança](#) desenvolvido para evitar a implantação de recursos não conformes. Esses controles verificam os recursos antes de serem provisionados. Se o recurso não estiver em conformidade com o controle, ele não será provisionado. Para obter mais informações, consulte o [guia de referência de controles](#) na AWS Control Tower documentação e consulte [Controles proativos](#) em Implementação de controles de segurança em AWS.

## gerenciamento do ciclo de vida do produto (PLM)

O gerenciamento de dados e processos de um produto em todo o seu ciclo de vida, desde a concepção, o desenvolvimento e o lançamento, passando pelo crescimento e maturidade, até o declínio e a remoção.

## ambiente de produção

Veja [ambiente](#).

## controlador lógico programável (PLC)

Na manufatura, um computador altamente confiável e adaptável que monitora as máquinas e automatiza os processos de fabricação.

## encadeamento de prompts

Uso da saída de um prompt do [LLM](#) como entrada para o próximo prompt para gerar respostas melhores. Essa técnica é usada para dividir uma tarefa complexa em subtarefas, ou para refinar ou expandir iterativamente uma resposta preliminar. Isso ajuda a melhorar a precisão e a relevância das respostas de um modelo e permite resultados mais granulares e personalizados.

## pseudonimização

O processo de substituir identificadores pessoais em um conjunto de dados por valores de espaço reservado. A pseudonimização pode ajudar a proteger a privacidade pessoal. Os dados pseudonimizados ainda são considerados dados pessoais.

## publish/subscribe (pub/sub)

Um padrão que permite comunicações assíncronas entre microsserviços para melhorar a escalabilidade e a capacidade de resposta. Por exemplo, em um [MES](#) baseado em microsserviços, um microsserviço pode publicar mensagens de eventos em um canal em que outros microsserviços possam assinar. O sistema pode adicionar novos microsserviços sem alterar o serviço de publicação.

## Q

### plano de consulta

Uma série de etapas, como instruções, usadas para acessar os dados em um sistema de banco de dados relacional SQL.

### regressão de planos de consultas

Quando um otimizador de serviço de banco de dados escolhe um plano menos adequado do que escolhia antes de uma determinada alteração no ambiente de banco de dados ocorrer. Isso pode ser causado por alterações em estatísticas, restrições, configurações do ambiente, associações de parâmetros de consulta e atualizações do mecanismo de banco de dados.

## R

### Matriz RACI

Veja [responsável, aprovador, consultado, informado \(RACI\)](#).

### RAG

Veja [geração aumentada via recuperação](#).

### ransomware

Um software mal-intencionado desenvolvido para bloquear o acesso a um sistema ou dados de computador até que um pagamento seja feito.

## Matriz RASCI

Veja [responsável, aprovador, consultado, informado \(RACI\)](#).

## RCAC

Veja [controle de acesso por linha e coluna](#).

## réplica de leitura

Uma cópia de um banco de dados usada somente para leitura. É possível encaminhar consultas para a réplica de leitura e reduzir a carga no banco de dados principal.

## Redefinir arquitetura

Veja [7 Rs](#).

## objetivo de ponto de recuperação (RPO).

O máximo período de tempo aceitável desde o último ponto de recuperação de dados. Isso determina o que é considerado uma perda aceitável de dados entre o último ponto de recuperação e a interrupção do serviço.

## objetivo de tempo de recuperação (RTO)

O máximo atraso aceitável entre a interrupção e a restauração do serviço.

## refatorar

Veja [7 Rs](#).

## Região

Uma coleção de AWS recursos em uma área geográfica. Cada um Região da AWS é isolado e independente dos outros para fornecer tolerância a falhas, estabilidade e resiliência. Para obter informações, consulte [Specify which Regiões da AWS your account can use](#).

## regressão

Uma técnica de ML que prevê um valor numérico. Por exemplo, para resolver o problema de “Por qual preço esta casa será vendida?” um modelo de ML pode usar um modelo de regressão linear para prever o preço de venda de uma casa com base em fatos conhecidos sobre a casa (por exemplo, a metragem quadrada).

## redefinir a hospedagem

Veja [7 Rs](#).

---

## versão

Em um processo de implantação, o ato de promover mudanças em um ambiente de produção.

## realocar

Veja [7 Rs](#).

## redefinir a plataforma

Veja [7 Rs](#).

## recomprar

Veja [7 Rs](#).

## resiliência

A capacidade de uma aplicação de resistir ou se recuperar de interrupções. [Alta disponibilidade](#) e [recuperação de desastres](#) são considerações comuns ao planejar a resiliência na Nuvem AWS. Para obter mais informações, consulte [Nuvem AWS Resilience](#).

## política baseada em recurso

Uma política associada a um recurso, como um bucket do Amazon S3, um endpoint ou uma chave de criptografia. Esse tipo de política especifica quais entidades principais têm acesso permitido, ações válidas e quaisquer outras condições que devem ser atendidas.

## matriz responsável, accountable, consultada, informada (RACI)

Uma matriz que define as funções e responsabilidades de todas as partes envolvidas nas atividades de migração e nas operações de nuvem. O nome da matriz é derivado dos tipos de responsabilidade definidos na matriz: responsável (R), responsabilizável (A), consultado (C) e informado (I). O tipo de suporte (S) é opcional. Se você incluir suporte, a matriz será chamada de matriz RASCI e, se excluir, será chamada de matriz RACI.

## controle responsivo

Um controle de segurança desenvolvido para conduzir a remediação de eventos adversos ou desvios em relação à linha de base de segurança. Para obter mais informações, consulte [Controles responsivos](#) em Como implementar controles de segurança na AWS.

## reter

Veja [7 Rs](#).

## Retirada

Veja [7 Rs](#).

### Geração Aumentada de Recuperação (RAG)

Uma tecnologia de [IA generativa](#) em que um [LLM](#) faz referência a uma fonte de dados autorizada que está fora de suas fontes de dados de treinamento antes de gerar uma resposta. Por exemplo, um modelo RAG pode realizar uma pesquisa semântica na base de conhecimento ou nos dados personalizados de uma organização. Para obter mais informações, consulte [O que é RAG \(geração aumentada via recuperação\)?](#).

### alternância

O processo de atualizar periodicamente um [segredo](#) para dificultar o acesso de um invasor às credenciais.

### controle de acesso por linha e coluna (RCAC)

O uso de expressões SQL básicas e flexíveis que tenham regras de acesso definidas. O RCAC consiste em permissões de linha e máscaras de coluna.

### RPO

Veja [objetivo de ponto de recuperação](#).

### RTO

Veja [objetivo de tempo de recuperação](#).

### runbook

Um conjunto de procedimentos manuais ou automatizados necessários para realizar uma tarefa específica. Eles são normalmente criados para agilizar operações ou procedimentos repetitivos com altas taxas de erro.

## S

### SAML 2.0

Um padrão aberto que muitos provedores de identidade (IdPs) usam. Esse recurso permite o login único federado (SSO), para que os usuários possam fazer login no Console de gerenciamento da AWS ou chamar as operações da AWS API sem que você precise criar um usuário no IAM

para todos em sua organização. Para obter mais informações sobre a federação baseada em SAML 2.0, consulte [Sobre a federação baseada em SAML 2.0](#) na documentação do IAM.

## SCADA

Veja [controle de supervisão e aquisição de dados](#).

## SCP

Veja [política de controle de serviço](#).

## secret

Em AWS Secrets Manager, informações confidenciais ou restritas, como uma senha ou credenciais de usuário, que você armazena de forma criptografada. Consiste no valor secreto e em seus metadados. O valor secreto pode ser binário, uma única string ou várias strings. Para obter mais informações, consulte [What's in a Secrets Manager secret?](#) na documentação do Secrets Manager.

## segurança desde a concepção

Uma abordagem em engenharia de sistemas que leva em consideração a segurança em todo o processo de desenvolvimento.

## controle de segurança

Uma barreira de proteção técnica ou administrativa que impede, detecta ou reduz a capacidade de uma ameaça explorar uma vulnerabilidade de segurança. Existem quatro tipos primários de controles de segurança: [preventivos](#), [detectivos](#), [responsivos](#) e [proativos](#).

## hardening da segurança

O processo de reduzir a superfície de ataque para torná-la mais resistente a ataques. Isso pode incluir ações como remover recursos que não são mais necessários, implementar a prática recomendada de segurança de conceder privilégios mínimos ou desativar recursos desnecessários em arquivos de configuração.

## sistema de gerenciamento de eventos e informações de segurança (SIEM)

Ferramentas e serviços que combinam sistemas de gerenciamento de informações de segurança (SIM) e gerenciamento de eventos de segurança (SEM). Um sistema SIEM coleta, monitora e analisa dados de servidores, redes, dispositivos e outras fontes para detectar ameaças e violações de segurança e gerar alertas.

## automação de resposta de segurança

Uma ação predefinida e programada projetada para responder ou remediar automaticamente um evento de segurança. Essas automações servem como controles de segurança [responsivos](#) ou [detectivos](#) que ajudam você a implementar as melhores práticas AWS de segurança. Exemplos de ações de resposta automatizada incluem a modificação de um grupo de segurança da VPC, a aplicação de patches em uma instância do Amazon EC2 ou a alternância de credenciais.

## Criptografia do lado do servidor

Criptografia dos dados em seu destino, por AWS service (Serviço da AWS) quem os recebe.

## política de controle de serviços (SCP)

Uma política que fornece controle centralizado sobre as permissões de todas as contas em uma organização em AWS Organizations. SCPs defina barreiras ou estabeleça limites nas ações que um administrador pode delegar a usuários ou funções. Você pode usar SCPs como listas de permissão ou listas de negação para especificar quais serviços ou ações são permitidos ou proibidos. Para obter mais informações, consulte [Políticas de controle de serviço](#) na AWS Organizations documentação.

## service endpoint (endpoint de serviço)

O URL do ponto de entrada para um AWS service (Serviço da AWS). Você pode usar o endpoint para se conectar programaticamente ao serviço de destino. Para obter mais informações, consulte [Endpoints do AWS service \(Serviço da AWS\)](#) na Referência geral da AWS.

## acordo de serviço (SLA)

Um acordo que esclarece o que uma equipe de TI promete fornecer aos clientes, como tempo de atividade e performance do serviço.

## indicador de nível de serviço (SLI)

Uma avaliação de um aspecto de performance de um serviço, como taxa de erro, disponibilidade ou throughput.

## objetivo de nível de serviço (SLO)

Uma métrica alvo que representa a integridade de um serviço, conforme avaliado por um [indicador de nível de serviço](#).

## modelo de responsabilidade compartilhada

Um modelo que descreve a responsabilidade com a qual você compartilha AWS pela segurança e conformidade na nuvem. AWS é responsável pela segurança da nuvem, enquanto você é responsável pela segurança na nuvem. Para obter mais informações, consulte o [Modelo de responsabilidade compartilhada](#).

## SIEM

Veja [sistema de gerenciamento de eventos e informações de segurança](#).

## ponto único de falha (SPOF)

Uma falha em um único componente crítico de uma aplicação que pode interromper o sistema.

## SLA

Veja [acordo de serviço](#).

## SLI

Veja [indicador de nível de serviço](#).

## SLO

Veja [objetivo de nível de serviço](#).

## split-and-seed modelo

Um padrão para escalar e acelerar projetos de modernização. À medida que novos recursos e lançamentos de produtos são definidos, a equipe principal se divide para criar novas equipes de produtos. Isso ajuda a escalar os recursos e os serviços da sua organização, melhora a produtividade do desenvolvedor e possibilita inovações rápidas. Para obter mais informações, consulte [Phased approach to modernizing applications in the Nuvem AWS](#).

## SPOF

Veja [ponto único de falha](#).

## esquema em estrela

Uma estrutura organizacional de banco de dados que usa uma grande tabela de fatos para armazenar dados transacionais ou medidos e usa uma ou mais tabelas dimensionais menores para armazenar atributos de dados. Essa estrutura foi projetada para ser usada em um [data warehouse](#) ou para fins de inteligência comercial.

## padrão strangler fig

Uma abordagem à modernização de sistemas monolíticos que consiste em reescrever e substituir incrementalmente a funcionalidade do sistema até que o sistema herdado possa ser desativado. Esse padrão usa a analogia de uma videira que cresce e se torna uma árvore estabelecida e, eventualmente, supera e substitui sua hospedeira. O padrão foi [apresentado por Martin Fowler](#) como forma de gerenciar riscos ao reescrever sistemas monolíticos. Para ver um exemplo de como aplicar esse padrão, consulte [Modernizar incrementalmente os serviços Web herdados do Microsoft ASP.NET \(ASMX\) usando contêineres e o Amazon API Gateway](#).

## sub-rede

Um intervalo de endereços IP na VPC. Cada sub-rede fica alocada em uma única zona de disponibilidade.

## controle supervisor e aquisição de dados (SCADA)

Na manufatura, um sistema que usa hardware e software para monitorar ativos físicos e operações de produção.

## symmetric encryption (criptografia simétrica)

Um algoritmo de criptografia que usa a mesma chave para criptografar e descriptografar dados.

## testes sintéticos

Testar um sistema de forma que simule as interações do usuário para detectar possíveis problemas ou monitorar a performance. Você pode usar o [Amazon CloudWatch Synthetics](#) para criar esses testes.

## prompt do sistema

Uma técnica para fornecer contexto, instruções ou orientações a um [LLM](#) a fim de direcionar seu comportamento. Os prompts do sistema ajudam a definir o contexto e a estabelecer regras para interações com os usuários.

# T

## tags

Pares de valores-chave que atuam como metadados para organizar seus recursos. AWS As tags podem ajudar você a gerenciar, identificar, organizar, pesquisar e filtrar recursos da . Para obter mais informações, consulte [Marcar seus recursos do AWS](#).

## variável-alvo

O valor que você está tentando prever no ML supervisionado. Ela também é conhecida como variável de resultado. Por exemplo, em uma configuração de fabricação, a variável-alvo pode ser um defeito do produto.

## lista de tarefas

Uma ferramenta usada para monitorar o progresso por meio de um runbook. Uma lista de tarefas contém uma visão geral do runbook e uma lista de tarefas gerais a serem concluídas. Para cada tarefa geral, ela inclui o tempo estimado necessário, o proprietário e o progresso.

## ambiente de teste

Veja [ambiente](#).

## treinamento

O processo de fornecer dados para que seu modelo de ML aprenda. Os dados de treinamento devem conter a resposta correta. O algoritmo de aprendizado descobre padrões nos dados de treinamento que mapeiam os atributos dos dados de entrada no destino (a resposta que você deseja prever). Ele gera um modelo de ML que captura esses padrões. Você pode usar o modelo de ML para obter previsões de novos dados cujo destino você não conhece.

## gateway de trânsito

Um hub de trânsito de rede que você pode usar para interconectar sua rede com VPCs a rede local. Para obter mais informações, consulte [O que é um gateway de trânsito](#) na AWS Transit Gateway documentação.

## fluxo de trabalho baseado em troncos

Uma abordagem na qual os desenvolvedores criam e testam recursos localmente em uma ramificação de recursos e, em seguida, mesclam essas alterações na ramificação principal. A ramificação principal é então criada para os ambientes de desenvolvimento, pré-produção e produção, sequencialmente.

## Acesso confiável

Conceder permissões a um serviço que você especifica para realizar tarefas em sua organização AWS Organizations e em suas contas em seu nome. O serviço confiável cria um perfil vinculado ao serviço em cada conta, quando esse perfil é necessário, para realizar tarefas de gerenciamento para você. Para obter mais informações, consulte [Usando AWS Organizations com outros AWS serviços](#) na AWS Organizations documentação.

## tuning (ajustar)

Alterar aspectos do processo de treinamento para melhorar a precisão do modelo de ML. Por exemplo, você pode treinar o modelo de ML gerando um conjunto de rótulos, adicionando rótulos e repetindo essas etapas várias vezes em configurações diferentes para otimizar o modelo.

## equipe de duas pizzas

Uma pequena DevOps equipe que você pode alimentar com duas pizzas. Uma equipe de duas pizzas garante a melhor oportunidade possível de colaboração no desenvolvimento de software.

# U

## incerteza

Um conceito que se refere a informações imprecisas, incompletas ou desconhecidas que podem minar a confiabilidade dos modelos preditivos de ML. Há dois tipos de incertezas: a incerteza epistêmica é causada por dados limitados e incompletos, enquanto a incerteza aleatória é causada pelo ruído e pela aleatoriedade inerentes aos dados.

## tarefas indiferenciadas

Também conhecido como trabalho pesado, trabalho necessário para criar e operar um aplicativo, mas que não fornece valor direto ao usuário final nem oferece vantagem competitiva. Exemplos de tarefas indiferenciadas incluem aquisição, manutenção e planejamento de capacidade.

## ambientes superiores

Veja [ambiente](#).

# V

## aspiração

Uma operação de manutenção de banco de dados que envolve limpeza após atualizações incrementais para recuperar armazenamento e melhorar a performance.

## controle de versões

Processos e ferramentas que rastreiam mudanças, como alterações no código-fonte em um repositório.

## emparelhamento da VPC

Uma conexão entre duas VPCs que permite rotear o tráfego usando endereços IP privados. Para ter mais informações, consulte [O que é emparelhamento de VPC?](#) na documentação da Amazon VPC.

## Vulnerabilidade

Uma falha de software ou hardware que compromete a segurança do sistema.

# W

## cache quente

Um cache de buffer que contém dados atuais e relevantes que são acessados com frequência. A instância do banco de dados pode ler do cache do buffer, o que é mais rápido do que ler da memória principal ou do disco.

## dados mornos

Dados acessados raramente. Ao consultar esse tipo de dados, consultas moderadamente lentas geralmente são aceitáveis.

## função de janela

Uma função SQL que executa um cálculo em um grupo de linhas que se relacionam de alguma forma com o registro atual. As funções de janela são úteis para processar tarefas, como calcular uma média móvel ou acessar o valor das linhas com base na posição relativa da linha atual.

## workload

Uma coleção de códigos e recursos que geram valor empresarial, como uma aplicação voltada para o cliente ou um processo de backend.

## workstreams

Grupos funcionais em um projeto de migração que são responsáveis por um conjunto específico de tarefas. Cada workstream é independente, mas oferece suporte aos outros workstreams do projeto. Por exemplo, o workstream de portfólio é responsável por priorizar aplicações, planejar ondas e coletar metadados de migração. O workstream de portfólio entrega esses ativos ao workstream de migração, que então migra os servidores e as aplicações.

## WORM

Veja [gravação única e várias leituras](#).

## WQF

Veja [AWS Workload Qualification Framework](#).

### gravação única e várias leituras (WORM)

Um modelo de armazenamento que grava dados uma única vez e evita que os dados sejam excluídos ou modificados. Os usuários autorizados podem ler os dados quantas vezes forem necessárias, mas não podem alterá-los. Essa infraestrutura de armazenamento de dados é considerada [imutável](#).

## Z

### exploração de dia zero

Um ataque, normalmente malware, que tira proveito de uma [vulnerabilidade zero-day](#).

### vulnerabilidade de dia zero

Uma falha ou vulnerabilidade não mitigada em um sistema de produção. Os agentes de ameaças podem usar esse tipo de vulnerabilidade para atacar o sistema. Os desenvolvedores frequentemente ficam cientes da vulnerabilidade como resultado do ataque.

### prompt zero shot

Fornecer a um [LLM](#) instruções para realizar uma tarefa, mas sem exemplos (shots) que possam ajudar a orientá-lo. O LLM deve usar seu conhecimento pré-treinado para lidar com a tarefa. A eficácia dos prompts zero-shot depende da complexidade da tarefa e da qualidade do prompt.

Veja também [prompts few-shot](#).

### aplicação zumbi

Uma aplicação que tem um uso médio de CPU e memória inferior a 5%. Em um projeto de migração, é comum retirar essas aplicações.

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.