



# THE DEVELOPER'S CONFERENCE

**Trilha Software Security – Gestão de identidade  
Federada para Soluções Orientadas Serviços**

**Juscélio de Oliveira Reis**  
MTAC

# Juscélio de Oliveira Reis



THE  
DEVELOPER'S  
CONFERENCE

- Pai de 2 anjos!
- MTAC - Multi Platform Audience Contributor
- Profissional com mais de 1 década de experiência de desenvolvimento de software.
- Especialista em Gestão de Segurança da Informação pela UNB.
- Cursando MBA em Gestão de pessoas e Liderança pela FGV.



# Agenda

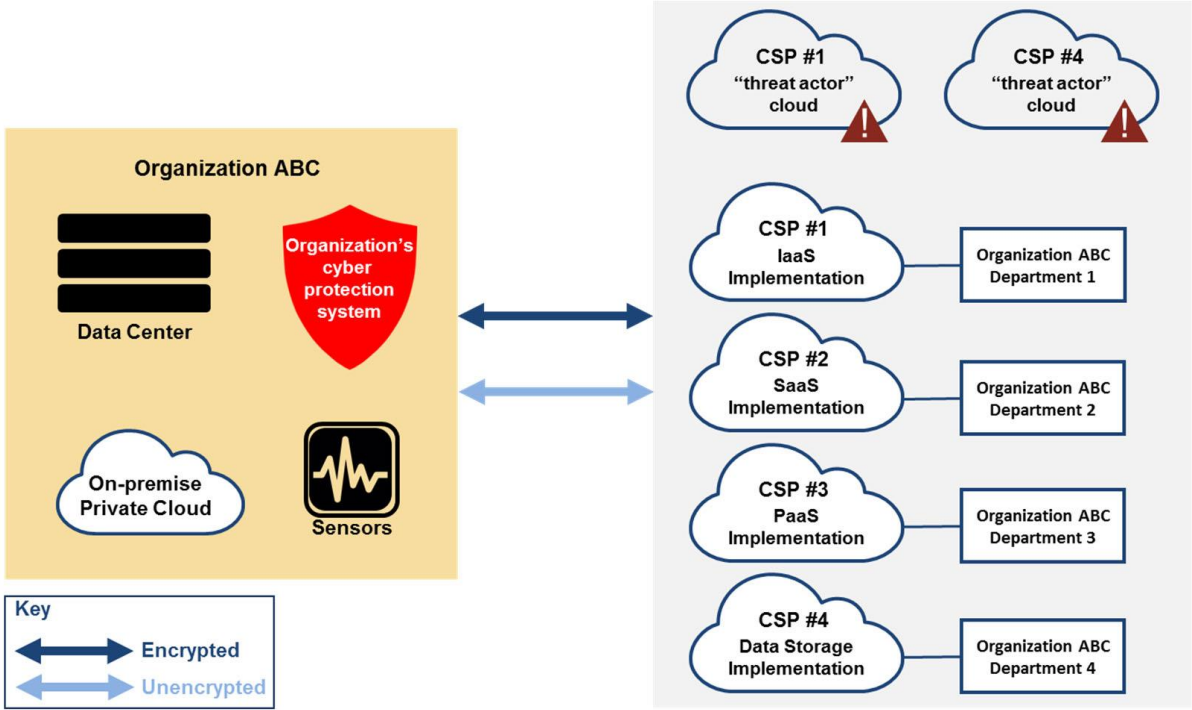


- Modelo atual
  - Exemplo de topologia
  - Exemplo de ataque
- Compartilhamento de responsabilidade
- Ameaças e riscos

# Modelo atual



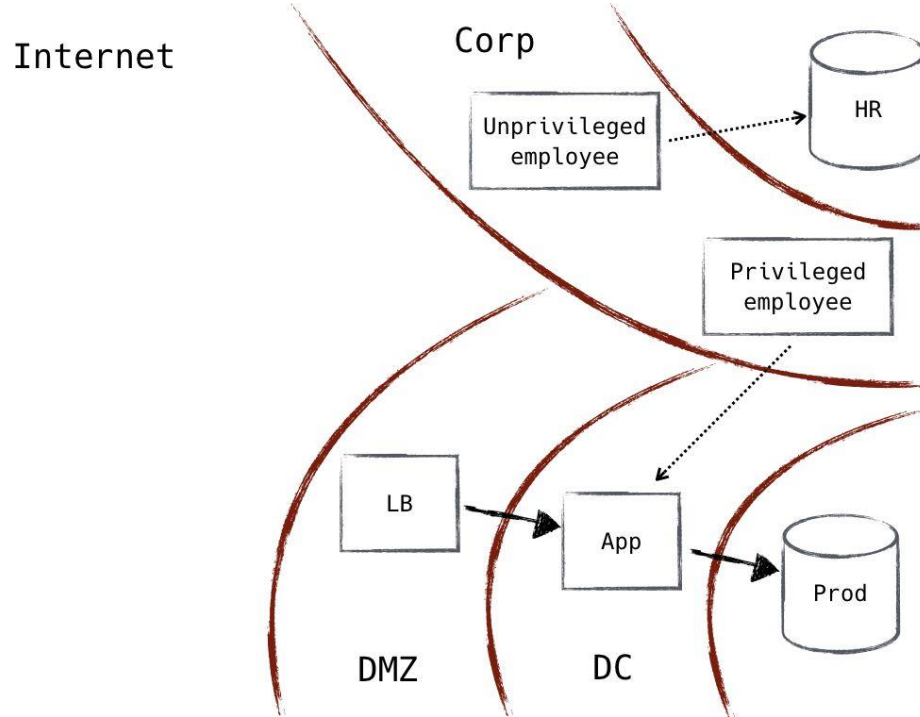
THE  
DEVELOPER'S  
CONFERENCE



# Exemplo de topologia



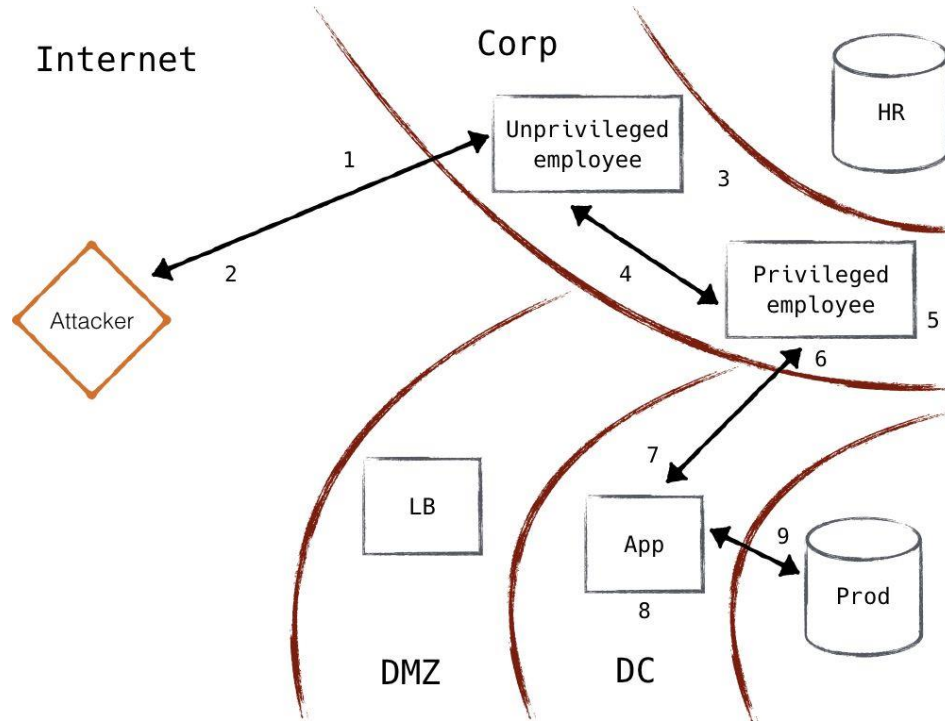
THE  
DEVELOPER'S  
CONFERENCE



# Exemplo de ataque



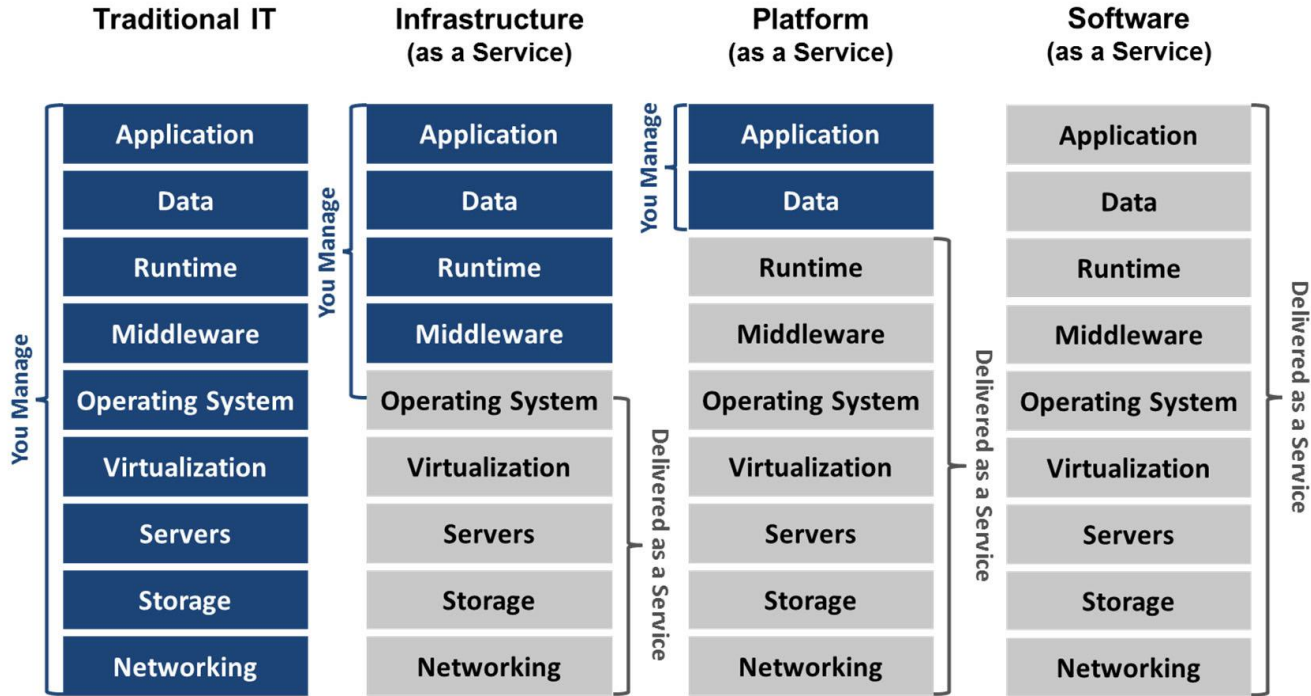
THE  
DEVELOPER'S  
CONFERENCE



# Compartilhamento de responsabilidade



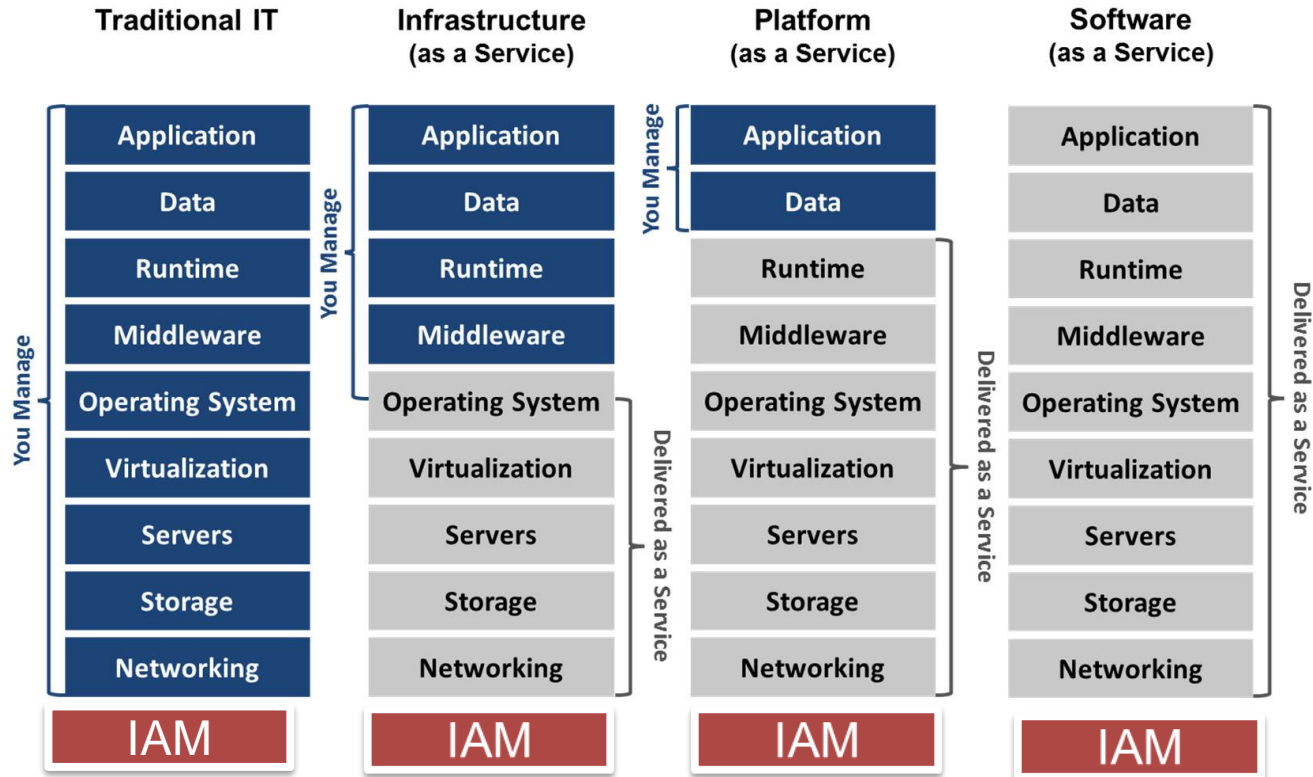
THE  
DEVELOPER'S  
CONFERENCE



# Compartilhamento de responsabilidade



THE  
DEVELOPER'S  
CONFERENCE





# Salesforce



## THE DEVELOPER'S CONFERENCE

Web Cryptography... SJKL demo O envelope de tran... Liderança de Pessoa... DPG - Decanato de... IAM Consensus Zero Trust Aluno Regular | Portal RH - Logon

Identity for Customers > Set Up Social Sign-On ▾

In production, you don't choose yourself. You create a service account instead to avoid problems in the future. If you use yourself and leave the company, the process starts to fail when your Salesforce account is disabled.

- For Icon URL, click **Choose one of our sample icons**, select an icon, copy the URL, and paste it in **Icon URL**.
- Leave the other fields empty, Salesforce supplies the values, including the consumer key and consumer secret, when you use the Salesforce out-of-the-box providers (Facebook, Google, and so on).
- Click **Save**.

### Auth. Provider

**Auth. Provider Edit** Save Save & New Cancel

Provider Type: Facebook

Name: Facebook

URL Suffix: Facebook

Consumer Key:

Consumer Secret:

Authorize Endpoint URL:

Token Endpoint URL:

User Info Endpoint URL:

Default Scopes:

Custom Error URL:

Custom Logout URL:

Registration Handler:

Execute Registration As:

Portal: --None--

Icon URL:

#### Time Estimate

About 15 mins

#### Topics

Learning Objectives

Social Sign-On

[Create an Authentication Provider](#)

Log In with Facebook

Update the Registration Handler

Resources


Challenge

+500 POINTS

[? Question, feedback or help](#)

After defining the auth provider, Salesforce generates several URLs. Use the Test-Only Initialization URL to test your connection with the social network.





## Amazon Cognito

Guia do desenvolvedor

Documentação – este guia

Pesquisar

- + O que é o Amazon Cognito?
- Conceitos básicos do Amazon Cognito
- Cenários comuns do Amazon Cognito
- + Tutoriais
- + Grupos de usuários do Amazon Cognito
- Amazon Cognito Grupos de identidades
  - Conceitos básicos dos grupos de identidades
- + Uso de grupos de identidades
- + Conceitos de grupos de identidades
- Controle de acesso com base em função
- Como obter as credenciais

Documentação da AWS » Amazon Cognito » Guia do desenvolvedor » Grupos de identidades do Amazon Cognito (identidades fed) Provedores OpenID Connect (grupos de identidades)

## Provedores OpenID Connect (grupos de identidades)

OpenID Connect é um padrão aberto para autenticação que é compatível com vários provedores de provedores OpenID Connect que são configuradas por meio do [AWS Identity and Access Man](#).

### Adição de um provedor OpenID Connect

Para obter informações sobre como criar um provedor OpenID Connect, consulte a [documentação](#)

### Associação de um provedor ao Amazon Cognito

Assim que criar um provedor OpenID Connect no console do IAM, você poderá associá-lo a um grupo Edit Identity Pool no console do Amazon Cognito no cabeçalho OpenID Connect Providers.

▼ OpenID Connect providers ⓘ

Amazon Cognito can authenticate users through any OpenID Connect provider. Once a provider has been configured with IAM, you can select the provider from the list below. [Learn more about using OpenID Connect providers.](#)

- accounts.google.com
- login.salesforce.com

# OpenID



THE  
DEVELOPER'S  
CONFERENCE

https://openid.net/developers/certified/

Bookmarks PKJs Web Cryptography... SICL demo O envelope de tran... Liderança de Pesso... DPG - Decanato de... IAM Consensus ZeroTrust Aluno Regular | Portal RH - Logon

OpenID OpenID Foundation Intellectual Property Current Working Groups Specs & Dev Info OpenID® Certification OpenID Connect

## Certified OpenID Provider Libraries

### C#

#### IdentityServer3

- **IdentityServer** is an open source OpenID Connect Provider and OAuth 2.0 Authorization Framework for ASP.NET 4.x/Katana
- *Target Environment:* OWIN/Katana
- *License:* Apache 2.0
- *Certified By:* Dominick Baier & Brock Allen
- *Conformance Profiles:* Basic OP, Implicit OP, Hybrid OP, Config OP

#### IdentityServer4

- **IdentityServer** is an open source OpenID Connect and OAuth 2.0 framework for ASP.NET Core
- *Target Environment:* Middleware for ASP.NET Core
- *License:* Apache 2.0
- *Certified By:* Dominick Baier & Brock Allen
- *Conformance Profiles:* Basic OP, Implicit OP, Hybrid OP, Config OP

#### SimpleIdentityServer V2.0.0

- **SimpleIdentityServer** is an open source implementation of Openid connect, OAUTH2.0, UMA and SCIM2.0 for ASP.NET CORE
- *Target Environment:* SimpleIdentityServer is written in C#. It can be installed on LINUX / WINDOWS environment via Docker or MSI installer.
- *License:* Apache 2.0
- *Certified By:* Thierry Habart
- *Conformance Profiles:* Basic OP, Implicit OP, Hybrid OP, Config OP, Dynamic OP

### Java

#### Connect2id Server 6.1.2a

- **Delivers OpenID Connect and OAuth 2.0 to the enterprise**
- *Target Environment:* Java in Apache Tomcat web server

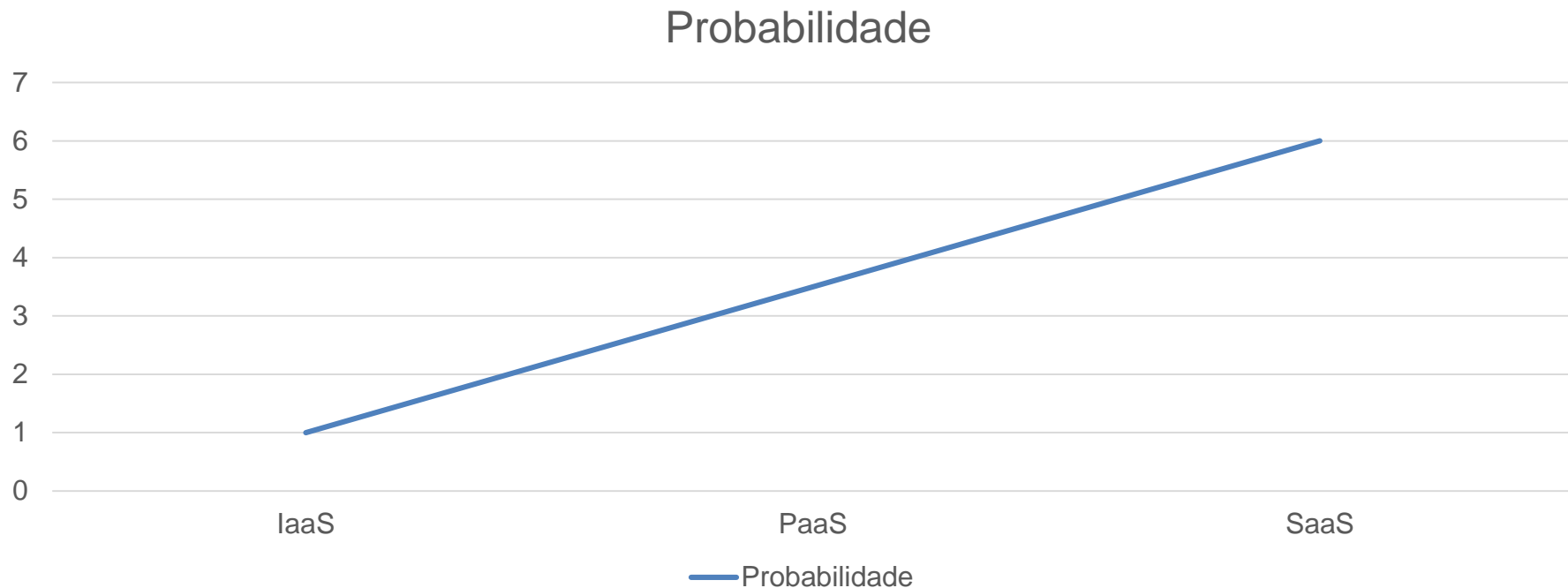


THE  
DEVELOPER'S  
CONFERENCE

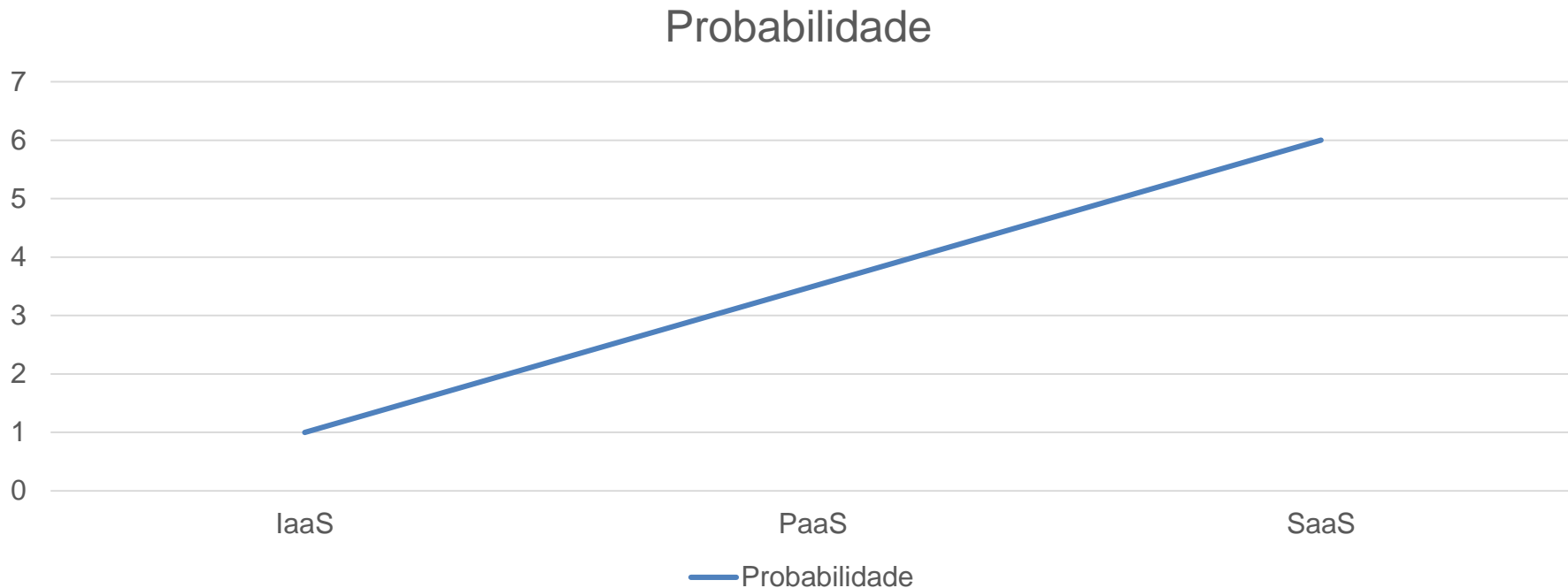
Características da computação em nuvem

# AMEAÇAS E RISCOS

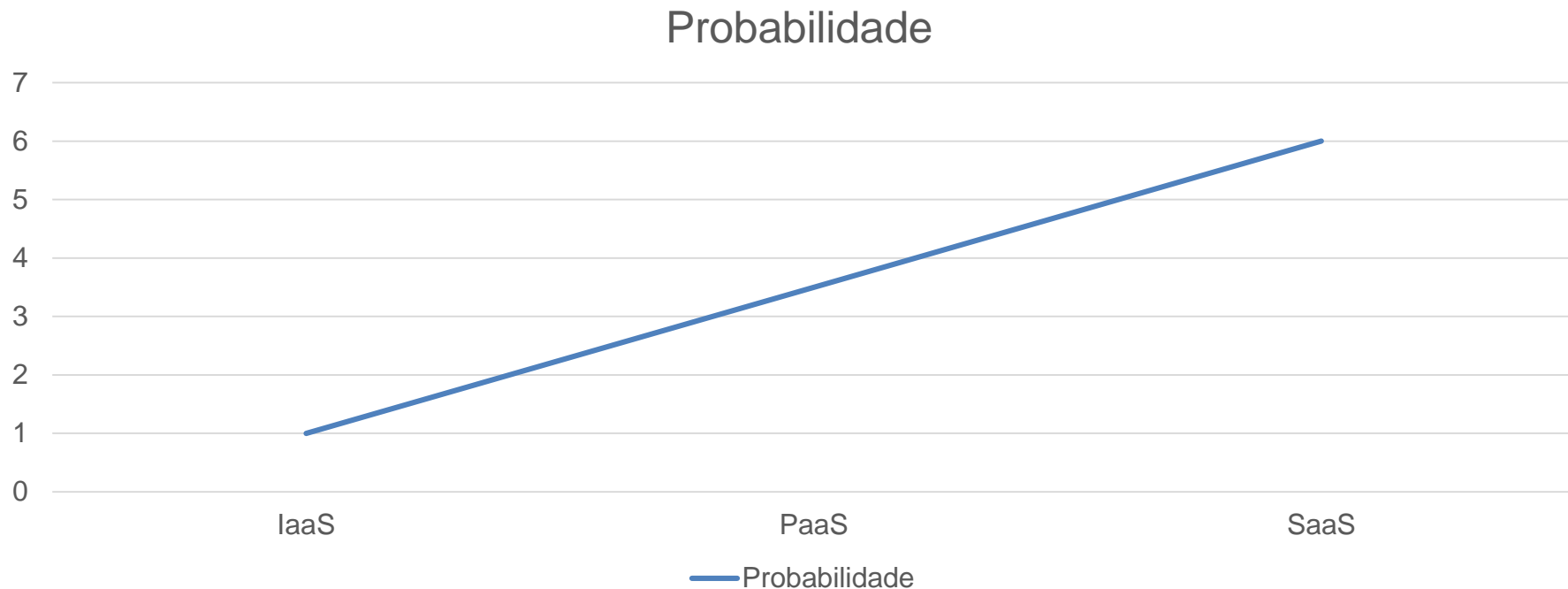
# #1 Redução de visibilidade e controle



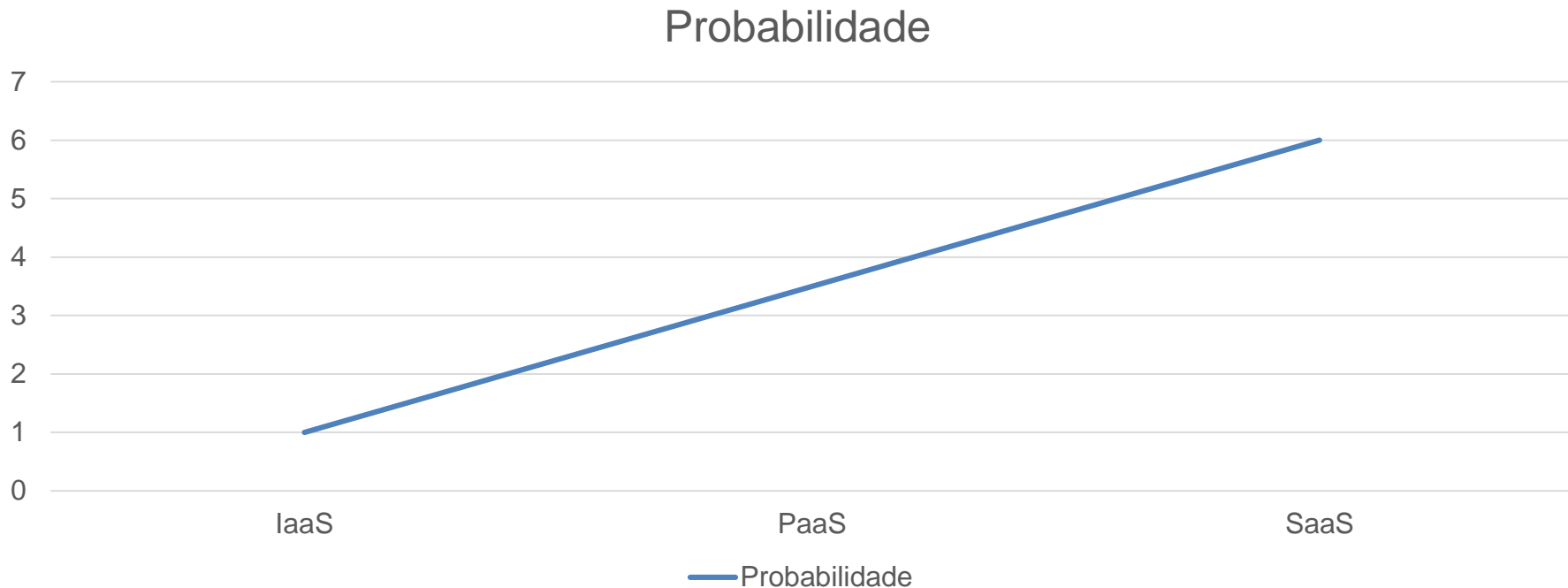
# #2 On-Demand Self Service: Simplifica o uso não autorizado



# #3 Compromisso de Gestão da API

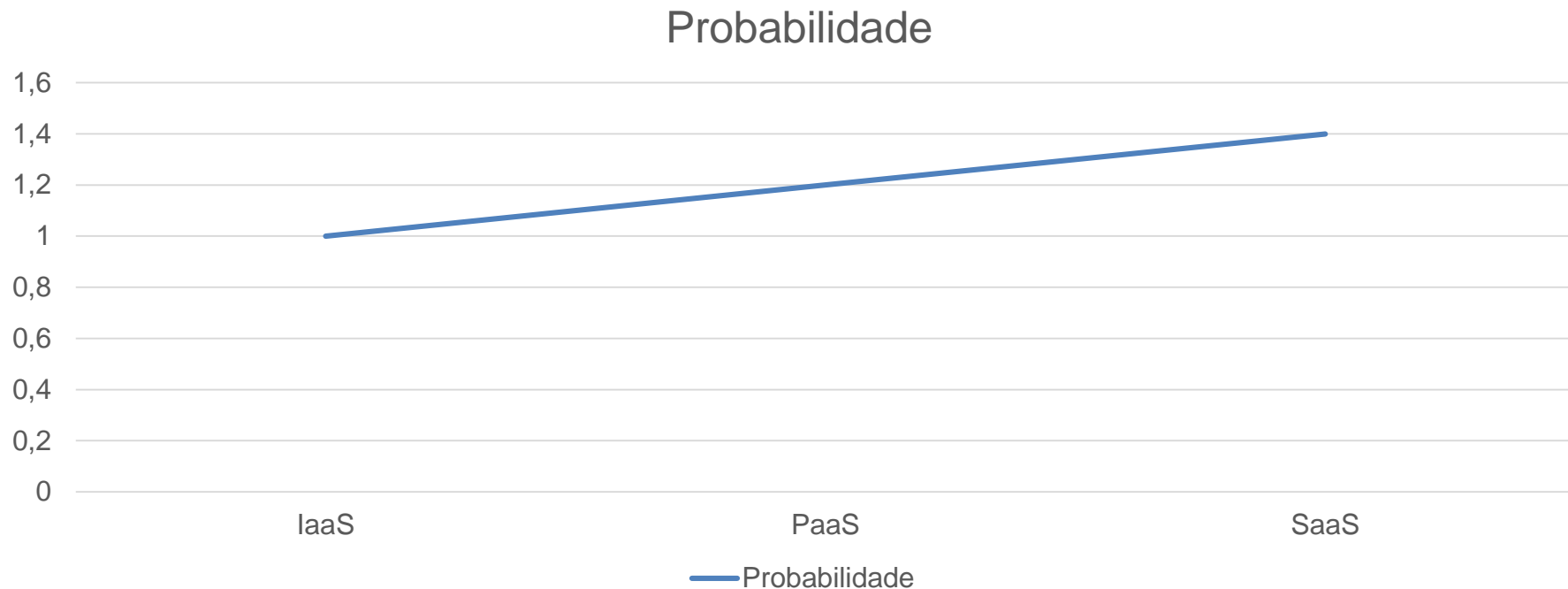


# #4 Separação lógica de falhas entre vários inquilinos

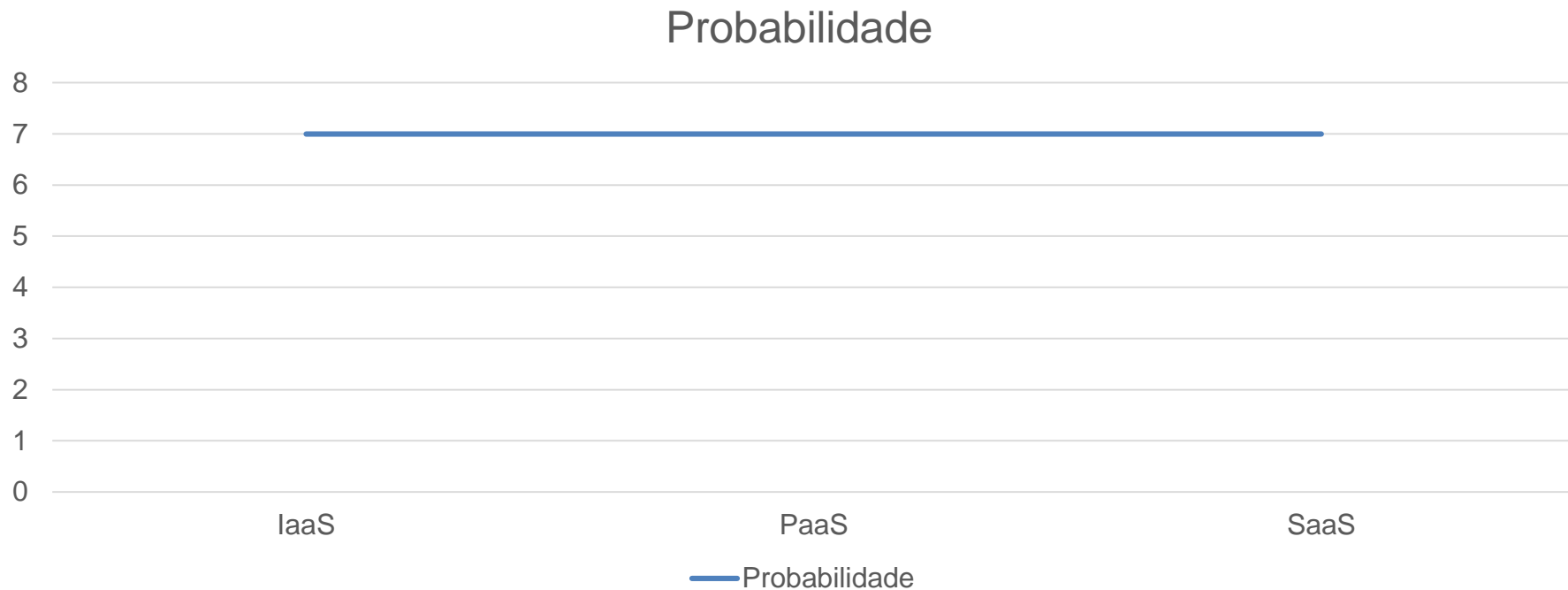




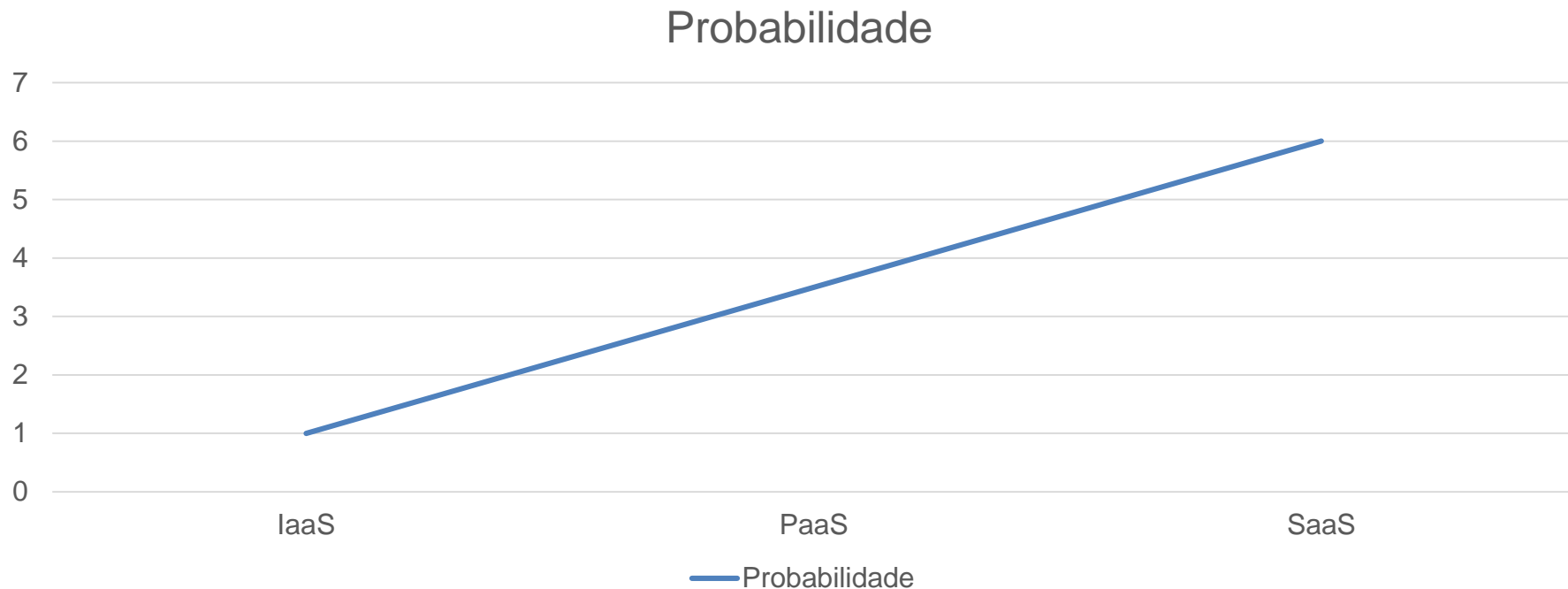
# #5 Exclusão incompleta de dados



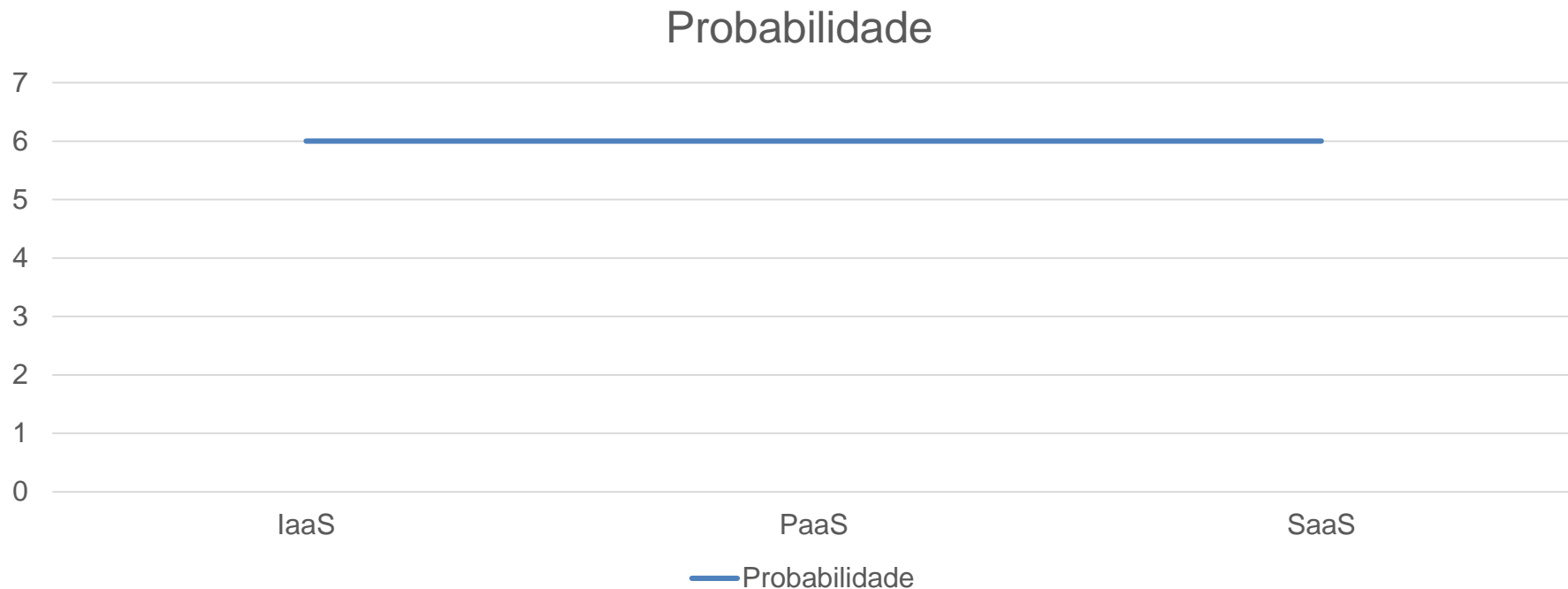
# #6 Credenciais Roubadas



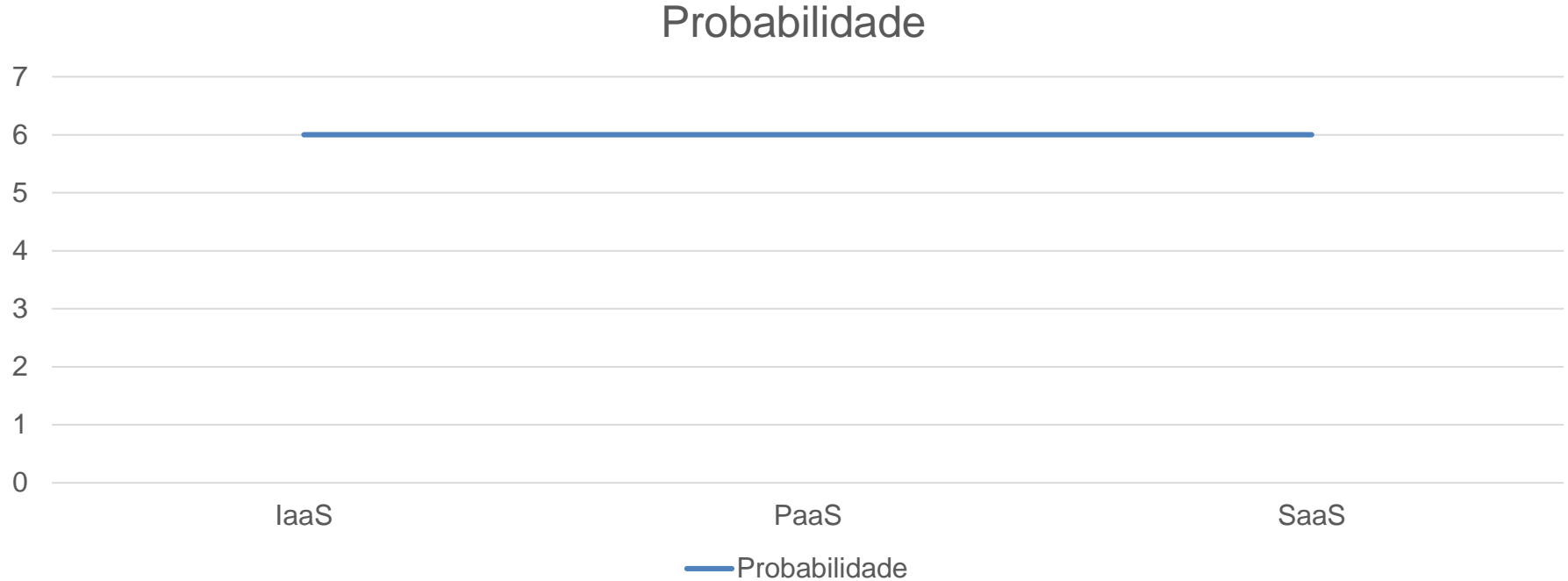
# #7 Vendor lock-in complica a migração para outros CSPs



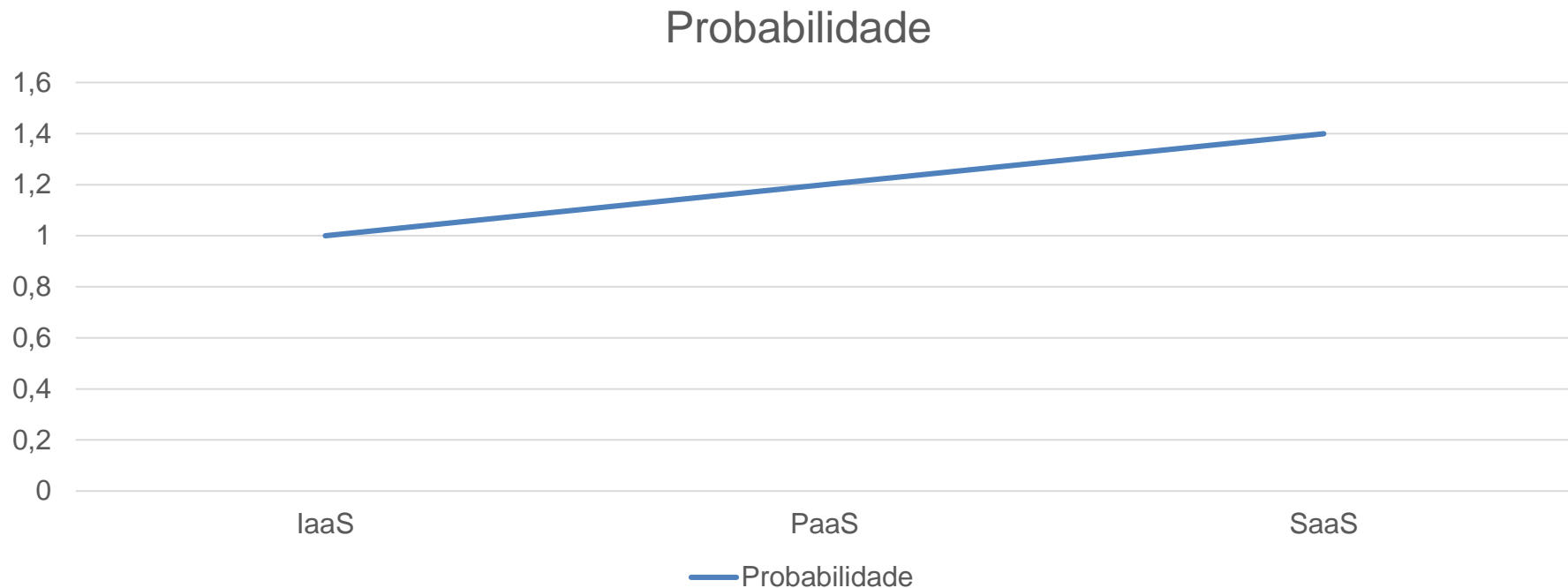
# #8 Maior complexidade que sobrecarrega o pessoal de TI



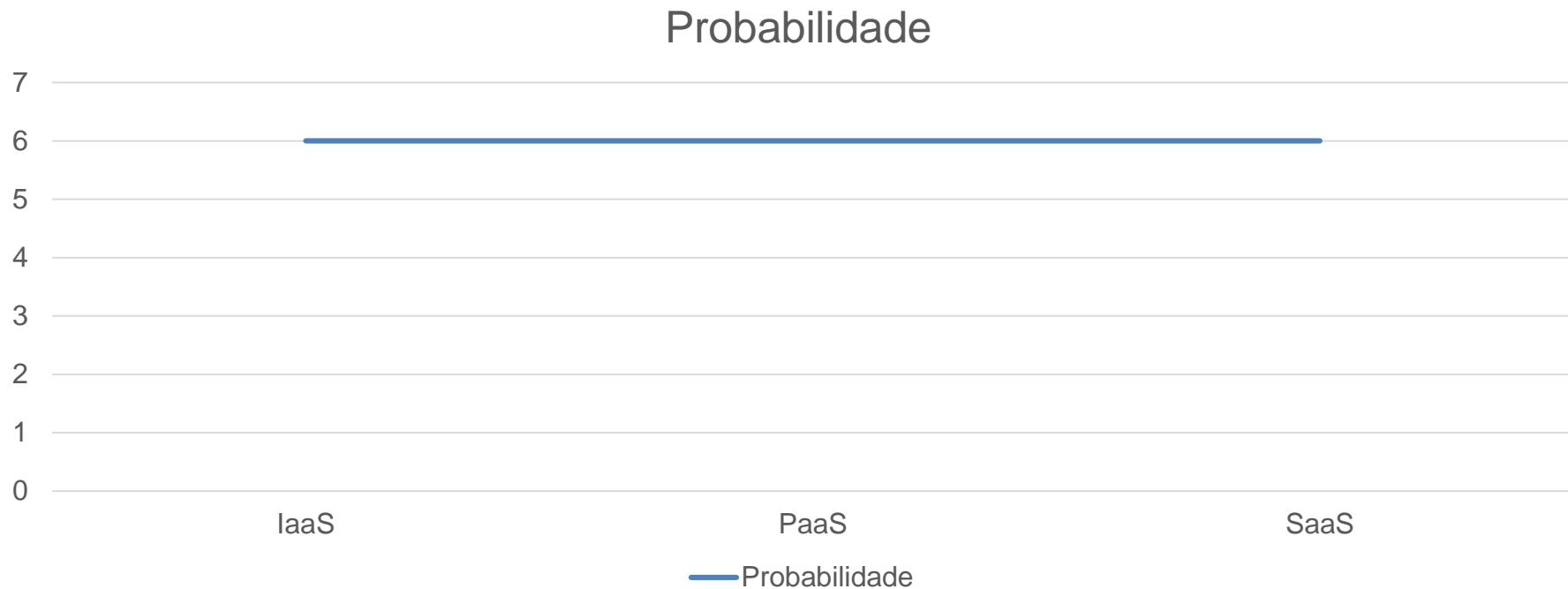
# #9 Ameaça interna



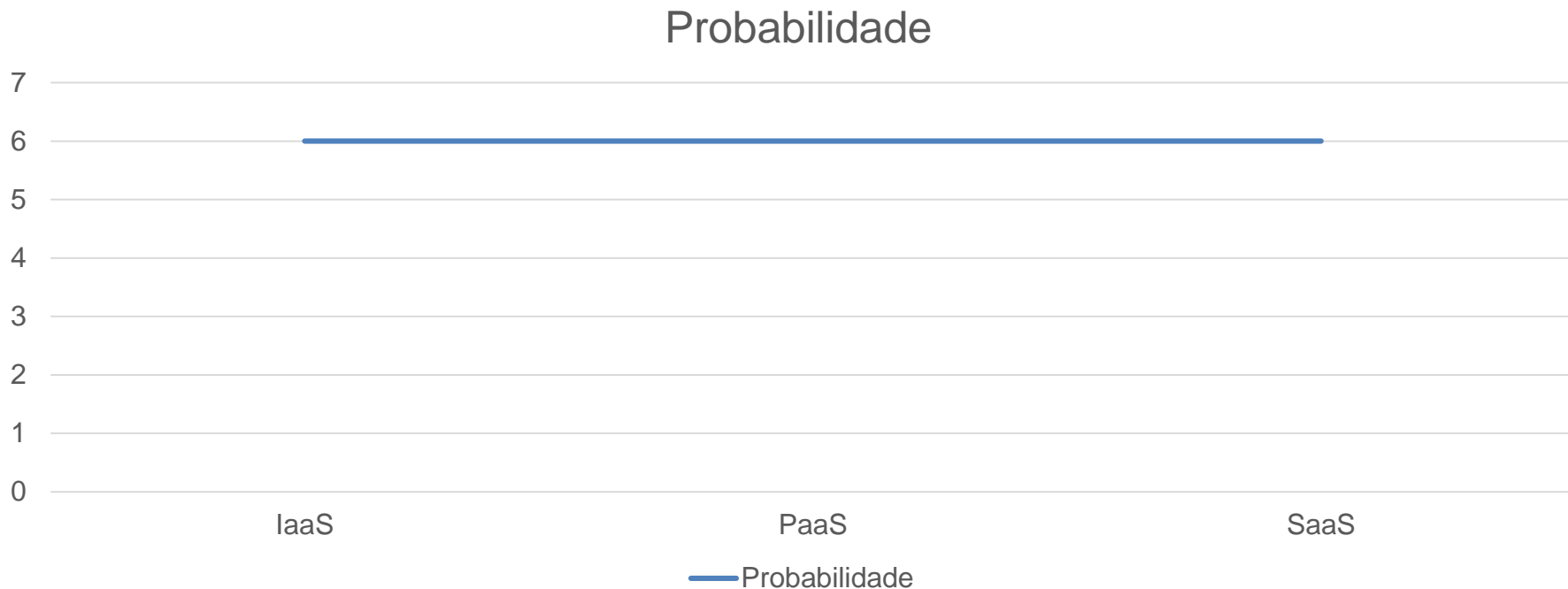
# #10 Perda de dados



# #11 Cadeia de suprimentos comprometida



# #12 Insuficiente Due Diligence aumenta o risco de segurança cibernética







THE  
DEVELOPER'S  
CONFERENCE

gerenciamento de  
identidade e acesso  
(IAM)

gerenciamento de  
configuração

Monitoramento

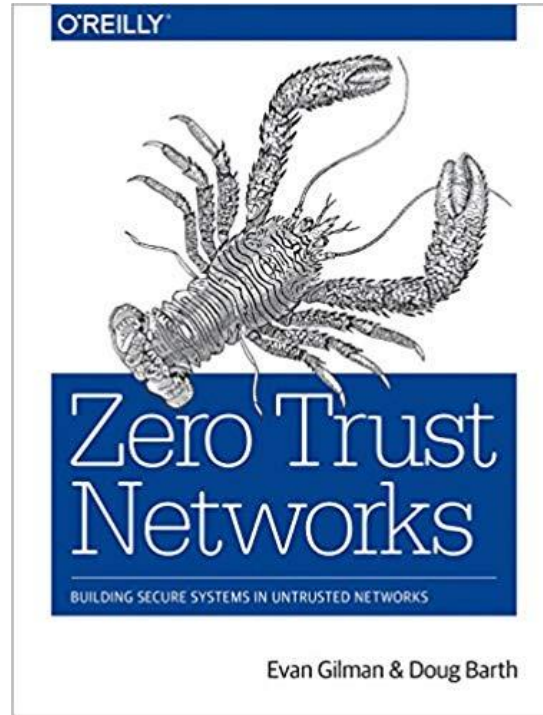
Análise de log

São responsabilidades que as  
organizações devem adotar  
para ajudar a proteger seus  
dados e ativos na nuvem

# Recomendação de leitura



THE  
DEVELOPER'S  
CONFERENCE



# Recomendação de leitura



THE  
DEVELOPER'S  
CONFERENCE





# THE DEVELOPER'S CONFERENCE

Obrigado!



# THE DEVELOPER'S CONFERENCE