FACULDADE DE TECNOLOGIA DE AMERICANA "Ministro Ralph Biasi"
Curso Superior de Tecnologia em Segurança da Informação

Guilherme Henrique Vieira Soares

Maria Clara Juvino de Sousa

Segurança na Nuvem: Gerenciamento de Identidades e Acessos com AWS IAM

Americana, SP

2025

FACULDADE DE TECNOLOGIA DE AMERICANA "Ministro Ralph Biasi"
Curso Superior de Tecnologia em Segurança da Informação

Guilherme Henrique Vieira Soares

Maria Clara Juvino de Sousa

Segurança na Nuvem: Gerenciamento de Identidades e Acessos com AWS IAM

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação sob a orientação do (a) Prof. Henri Alves de Godoy.

Área de concentração: Segurança da informação

Americana, SP

2025

FICHA CATALOGRÀFICA – Biblioteca Fatec Americana Ministro Ralph Biasi-CEETEPS Dados Internacionais de Catalogação-na-fonte

SOARES, Guilherme Henrique Vieira

Segurança em nuvem: gerenciamento de identidades e acessos com AWS IAM. / Guilherme Henrique Vieira Soares, Maria Clara Juvino de Sousa – Americana, 2025.

41f.

Monografia (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana Ministro Ralph Biasi – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Dr. Henri Alves de Godoy

1. Computação em nuvens 2. Segurança em sistemas de informação. I. SOARES, Guilherme Henrique Vieira, II. SOUSA, Maria Clara Juvino de III. GODOY, Henri Alves de IV. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana Ministro Ralph Biasi

CDU: 681518
681.518.5

Elaborada pelo autor por meio de sistema automático gerador de ficha catalográfica da Fatec de Americana Ministro Ralph Biasi.

Guilherme Henrique Vieira Soares

Maria Clara Juvino de Sousa

Segurança na Nuvem: Gerenciamento de Identidades e Acessos com AWS IAM

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Curso Superior de Tecnologia em Segurança da Informação pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana Ministro Ralph Biasi.
Área de concentração: Segurança da Informação

Americana, 24 de junho de 2025.

Banca Examinadora:

Henri Alves de Godoy
Doutor
Fatec Americana "Ministro Ralph Biasi"

Marcus Vinicius Lahr Giraldi
Especialista
Fatec Americana "Ministro Ralph Biasi"

Benedito Aparecido Cruz
Mestre
Fatec Americana "Ministro Ralph Biasi"

Gostaríamos de expressar nosso agradecimento ao nosso orientador, Henri Godoy, cujo apoio foi fundamental para a realização deste trabalho acadêmico.

RESUMO

Este trabalho apresenta uma análise sobre o gerenciamento de identidades e acessos no serviço AWS Identity and Access Management (IAM), destacando a importância de uma segurança corretamente aplicada em ambientes de computação em nuvem com grandes fluxos de informações. O objetivo principal foi identificar os riscos relacionados a configurações inadequadas de permissões e compreender como vulnerabilidades nesse serviço podem comprometer os princípios-chave da segurança da informação, sendo eles a integridade e a confidencialidade dos dados de uma organização. Para isso, foi empregada uma metodologia qualitativa, baseada em revisões bibliográficas e testes em ambientes virtuais simulados na plataforma AWS. Os resultados obtidos demonstraram que permissões excessivas são um dos principais vetores de risco, podendo expor recursos críticos caso não sejam corretamente configuradas. Conclui-se que a aplicação de boas práticas, como o princípio do menor privilégio e a revisão periódica das políticas de acesso, é fundamental para garantir um ambiente seguro. A pesquisa reforça a necessidade e sugere recomendações práticas de segurança para organizações que utilizam a AWS.

Palavras-chave: Segurança na Nuvem; Proteção de Dados; Soluções em Nuvem.

ABSTRACT

This work presents an analysis of identity and access management using the AWS Identity and Access Management (IAM) service, highlighting the importance of properly implemented security in cloud computing environments with large information flows. The main objective was to identify the risks related to improper permission configurations and understand how vulnerabilities in this service can compromise the key principles of information security, namely the integrity and confidentiality of an organization's data. A qualitative methodology was employed, based on literature reviews and testing in virtual environments simulated on the AWS platform. The results showed that excessive permissions are one of the main risk vectors, potentially exposing critical resources if not properly configured. It is concluded that applying best practices, such as the principle of least privilege and periodic review of access policies, is essential to ensure a secure environment. The research reinforces the need for and suggests practical security recommendations for organizations that use AWS.

Keywords: *Cloud Security; Data Protection; Cloud Solutions.*

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AWS: Amazon Web Services

CIDR: Classless Inter-Domain Routing

DLP: Data Loss Prevention

EC2: Elastic Compute Cloud

IAM: Identity and Access Management

IBM: International Business Machines

LISP: List Processing

MFA: Multi-factor Authentication

NAT: Network Address Translation

OUS: Organization Units

SCPs: Políticas de controle de serviço

SIEM: Security Information and Event Management

TI: Tecnologia da Informação

VPC: Virtual Private Cloud

SUMÁRIO

1 INTRODUÇÃO

Com o avanço da tecnologia, novas formas de gerenciar e explorar dados foram se desenvolvendo, e hoje em dia, o ambiente *Cloud* é um dos meios mais utilizados para armazená-los devido a sua escalabilidade e disponibilidade. Sendo assim, é necessário levar em conta a segurança desses dados, tendo que, no cenário corporativo atual, o vazamento de diferentes tipos de dados pode ocasionar uma perda significativa de valor de mercado.

A tecnologia de computação em cloud está sendo pensada desde a década de 50, onde John McCarthy, inventor da linguagem LISP, demonstrou o conceito de "*Time Sharing*", ou seja, esse princípio permitia que um único computador fosse compartilhado entre vários usuários (Pereira Borges, 2022).

Um dos primeiros exemplos desse conceito foi registrado pela IBM, que lançou a primeira máquina virtual capaz de realizar computação simultânea, essa ideia representou a aplicação comercial inicial do conceito de "*Time Sharing*". Com o passar dos anos, à medida que a tecnologia evoluía, a combinação dessas duas abordagens começou a se tornar realidade (Rosa e Canteiro, 2022). Desde então a computação em nuvem vem sendo adotada por muitas empresas, conforme a Gartner, até 2025 mais de 85% das empresas deverão adotar a "*cloud computing*" como parte central de suas operações e não serão capazes de executar suas estratégias digitais sem o uso de tecnologia e arquiteturas em nuvem (Gartner, 2021).

Esse avanço tecnológico proporcionou as empresas uma melhor administração dos recursos de TI necessários, visto que o cliente paga somente o que ele precisa, evitando desperdícios e caso demande mais recursos é possível ampliar conforme necessita-se, trouxe também melhoras na flexibilidade e mobilidade aos usuários, pois a computação em nuvem proporciona acesso a dados e aplicações de qualquer lugar. Esse tipo de estratégia minimiza os riscos relacionados a infraestrutura, dado que não é necessário a empresa investir tanto em equipamentos físicos (Nogueira e Pedrosa, 2011).

Deste modo, a tendência é que as organizações migrem ou já nasçam em um ambiente *cloud*, diminuindo o uso do modelo tradicional de TI. (Rosa e Canteiro, 2022).

A importância do trabalho está diretamente relacionada à segurança, proteção e gerenciamento eficaz de acessos dentro de uma organização. Os benefícios proporcionados pelo projeto incluem a demonstração de uma aplicação chave da segurança na nuvem, evidenciando que, ao explorar novas tecnologias, é possível criar um ambiente digital mais seguro, promovendo a confiança para adoção de um ambiente em *Cloud*.

A viabilidade do trabalho é garantida pela consulta em diversas bibliotecas digitais, artigos científicos disponíveis e relatórios públicos, que fornecerão informações relevantes para o desenvolvimento da pesquisa. Além disso, o estudo demonstrará o de uso de ferramentas úteis para organizações que não possuem a devida supervisão de segurança em seus ambientes.

Os testes serão realizados utilizando ferramentas AWS (Amazon Web Services), com auxílio do nosso orientador, permitindo a introdução de suas aplicações de segurança, que podem ser implementadas para gerenciar, mitigar e prevenir ataques digitais dentro de diferentes organizações. Um cronograma será mantido para simular o uso e exemplificar como as ferramentas oferecem proteção contra diferentes tipos de ameaças. Em cada um dos testes, detalharemos as vulnerabilidades mais críticas para auxiliar no gerenciamento efetivo de acessos e identidades dentro de corporações.

Focando em ambientes que garantem a segurança dos dados, mesmo em trânsito, e que possuem um controle de acesso implementado, esse trabalho mostrará os riscos aos quais um ambiente configurado em computação em nuvem pode estar exposto caso não configurado adequadamente.

O objetivo da pesquisa é identificar riscos recorrentes de ambientes configurados na AWS, muitas vezes suscetíveis a falhas humanas e, por meio de experimentos práticos, destacar as principais falhas que podem comprometer a eficiência operacional, a integridade das informações e aumentar a exposição a ataques cibernéticos.

A hipótese deste trabalho é que as soluções de segurança apresentadas, em particular o serviço da AWS IAM, comprovem sua eficácia no gerenciamento de acesso e identidades dentro de um ambiente em nuvem. O IAM é fundamental para a segurança de organizações que lidam com grandes volumes e complexidade de dados, permitindo controlar acessos e definir políticas de autenticação e autorização.

Com ele, é possível garantir que apenas os usuários específicos ou sistemas autorizados tenham acesso a diferentes tipos de recursos.

O percurso metodológico desta pesquisa consiste em uma investigação exploratória, com revisão bibliográfica sobre o ambiente *Cloud*. Os sujeitos da pesquisa serão laboratórios virtualizados no ambiente da AWS. Os dados levantados serão analisados de forma qualitativa.

O trabalho está estruturado em cinco capítulos, o capítulo 1 é introdutório ao trabalho acadêmico, o capítulo 2 aborda a fundamentação teórica, o capítulo 3 descreve o percurso metodológico, o capítulo 4 apresenta os resultados, análise e discussão dos dados e o capítulo 5, as considerações finais.

2 FUNDAMENTAÇÃO TEÓRICA

No embasamento desta pesquisa, optou-se por organizar este capítulo com uma apresentação dos conceitos chave que referenciam o trabalho, sendo eles: segurança em nuvem, Amazon Web Services, AWS Virtual Private Cloud, AWS Elastic Compute Cloud, gerenciamento de identidade e acesso e as políticas da AWS IAM.

2.1 Segurança em Nuvem

A segurança em nuvem tem como principal objetivo proteger dados e sistemas que operam em um ambiente virtualizado. As organizações vêm, cada vez mais, migrando para a nuvem em busca de eficiência e flexibilidade. Com isso em mente, a segurança torna-se fundamental para a sustentação e a inovação dos ambientes que conhecemos atualmente. (Objective, 2023). A padronização das melhores práticas de segurança costuma ser adotada pelos provedores, pois há a necessidade de proteger a integridade de seus sistemas. No entanto, cada operação demanda configurações específicas, de acordo com suas particularidades. Um dos principais diferenciais da computação em nuvem é a flexibilidade no gerenciamento da segurança, uma vez que há diversas soluções disponíveis, as quais serão abordadas ao longo desta pesquisa. Diante disso, consideramos o fator de exposição a riscos significativos de conformidade, que podem surgir ao lidar com dados de clientes. (IBM, 2023). Esses são alguns exemplos de soluções de segurança na nuvem que estão disponíveis:

- **Prevenção contra perda de dados (DLP):** Trata-se de um serviço amplamente usado em todo o mundo, que oferece um conjunto de ferramentas voltadas à prevenção de perda de informações e a garantia da segurança dos dados na nuvem. É reconhecido por empregar criptografia de dados, emitir alertas e adotar diversas medidas preventivas que asseguram a proteção das informações. (IBM, 2023).

- **Gerenciamento de informações de segurança e eventos (SIEM)**: Amplamente utilizado para monitorar e identificar ameaças em ambientes de computação em nuvem, esse recurso permite a aplicação ativa de

protocolos de rede e segurança, possibilitando respostas rápidas a eventuais riscos e incidentes. (IBM, 2023).

- **Continuidade dos negócios e recuperação de desastres:** Mesmo com a implementação de diversos recursos de segurança na nuvem, uma organização ainda está sujeita a sofrer algum tipo de incidente, seja causado por desastres naturais ou por ataques deliberados. Diante dessa realidade, é essencial que as empresas sejam capazes de responder rapidamente a vulnerabilidades identificadas, garantindo a continuidade das operações sem interrupções significativas. A continuidade de negócios tem exatamente esse propósito: fornecer as estratégias, ferramentas e serviços necessários para assegurar a manutenção das atividades. Trata-se de um aspecto fundamental da segurança em nuvem, pois viabiliza a recuperação e a retomada dos processos corporativos de forma eficiente. (IBM, 2023).

2.2 Amazon Web Services (AWS)

A AWS é uma plataforma em nuvem com uma ótima reputação no mercado atual. O serviço entrega funcionalidades como armazenamento de dados, infraestrutura de redes, servidores, virtualização, e diversos outros. A AWS surgiu com o foco inicial em ofertar um sistema para dar suporte as operações de vendas online da própria, Amazon. A empresa identificou a necessidade de uma gigantesca infraestrutura de TI para fazer as operações funcionarem de forma ágil e segura. Considerando esse cenário, a Amazon optou por automatizar e manter o máximo de atividades e processo de TI possíveis, ao invés de contratar serviços terceiros para suporte (ALURA, 2024). A nuvem tem algumas características essenciais (Mell e Grance, 2011):

- **Autoatendimento sob demanda:** O consumidor pode, de forma unilateral, provisionar recursos computacionais, como tempo de processamento em servidores e armazenamento em rede, conforme a necessidade, de maneira automatizada e sem a exigência de interação humana direta com cada provedor de serviço.

- **Acesso amplo a rede:** As capacidades estão disponíveis por meio da rede e são acessadas através de mecanismos padrão, promovendo a utilização por diferentes plataformas cliente, sejam estes dispositivos móveis, tablets, laptops ou estações de trabalho.
- **Agrupamento de recursos:** Os recursos computacionais do provedor são agrupados para atender múltiplos consumidores, utilizando um modelo de multi inquilino (*multi-tenant*). Os recursos físicos e virtuais são dinamicamente alocados e realocados de acordo com a demanda. Há um senso de independência da localização, uma vez que o cliente geralmente não tem controle ou conhecimento sobre o local exato onde os recursos estão hospedados, embora possa ser possível especificar uma localização em nível mais abstrato (por exemplo, país, estado ou data center). Exemplos de recursos incluem armazenamento, processamento, memória e largura de banda.
- **Elasticidade rápida:** As capacidades podem ser provisionadas e liberadas de forma elástica, em alguns casos de maneira automática, permitindo escalabilidade rápida conforme a demanda. Para o consumidor, os recursos disponíveis aparentam ser ilimitados e podem ser utilizados em qualquer quantidade, a qualquer momento.
- **Serviço mensurado:** Os sistemas de computação em nuvem controlam e otimizam automaticamente o uso dos recursos, por meio de capacidades de medição apropriadas ao tipo de serviço (como armazenamento, processamento, largura de banda e contas de usuários ativas). O uso dos recursos pode ser monitorado, controlado e reportado, proporcionando transparência tanto para o provedor quanto para o consumidor.

2.3 AWS Virtual Private Cloud (VPC)

Os serviços de rede desempenham um papel fundamental na computação em nuvem, oferecendo a infraestrutura essencial para que as organizações construam ambientes seguros, escaláveis e bem conectados para suas aplicações e dados. A Amazon Web Services disponibiliza um conjunto abrangente de ferramentas de rede que permitem aos usuários implementar e gerenciar arquiteturas de rede na nuvem,

a principal é a VPC que permite criar um ambiente isolado de redes dentro da AWS, com isso podemos gerir um ambiente seguro aplicando configurações de redes disponíveis dentro desse serviço (MIRYALA, 2024). Os principais recursos da Amazon Virtual Private Cloud (VPC) são:

- **Nuvens privadas virtuais (VPCs):** Uma VPC é uma rede virtual que simula uma rede tradicional que seria operado em um data center local.
- **Sub-redes (subnets):** Uma sub-rede representa um intervalo de endereços IP dentro da VPC. Cada sub-rede deve estar localizada em uma única Zona de Disponibilidade, que são data centers isolados ou localizados em regiões específicas nas quais os serviços de nuvem pública se originam e operam.
- **Endereçamento IP:** A AWS permite a utilização de endereços IPv4 e IPv6 em VPCs e sub-redes. Além disso, o usuário pode importar seus próprios endereços públicos e alocá-los a recursos como instâncias EC2, *gateways* NAT etc.
- **Gateways e Endpoints:** *Gateways* são utilizados para conectar a VPC a outras redes. Por exemplo, um Internet *Gateway* conecta a VPC a internet. Já os *endpoints*, permitem a conexão privada com serviços da AWS, sem a necessidade de um *gateway* de internet ou dispositivo NAT.
- **Espelhamento de tráfego:** Permite copiar o tráfego de rede de interfaces específicas e enviá-lo para ferramentas de monitoramento ou inspeção profunda de pacotes, contribuindo para a segurança e auditoria de rede (AWS, 2024a).

2.4 AWS Elastic Compute Cloud (EC2)

Esse serviço disponível na AWS é um dos mais importantes e usados, onde ele disponibiliza servidores virtuais que podem ser ajustados de acordo com a demanda do cliente. Os usuários têm à disposição diversos tipos de instâncias, escolhendo a melhor para o propósito definido, sendo possível configurar o desempenho, escolher o sistema operacional, o espaço de armazenamento e os recursos de redes necessários para executar o projeto (MIRYALA, 2024).

2.5 Gerenciamento de identidade e acesso (IAM)

É o processo de controle de acesso a quem possui privilégios a informações críticas. É essencial para controlar quem tem acesso a dados protegidos e manter boas práticas de Segurança da Informação, mesmo que a informação esteja armazenada na nuvem. É um dos componentes mais importantes para manter a segurança de dados na nuvem (Mohammed Ishaq, 2019). O IAM garante a distribuição de acessos de acordo com a necessidade da função sendo exercida.

Com o IAM, uma organização pode realizar a verificação da identidade de uma pessoa e suas permissões para utilização de recursos (Microsoft, 2024).

O IAM é um serviço em ambientes de nuvem que permite autenticar, autorizar e gerenciar usuários com base nos recursos e funções de acesso atribuídas. Essa funcionalidade é extremamente importante em uma organização para manter o controle de acesso de dados que podem estar acessíveis para uma pessoa, mas inacessível para outros, definindo acessos corretamente entre um funcionário e dispositivos. Essas são as duas etapas para concessão de acesso seguro dentro de uma organização (Microsoft, 2024):

- **Gerenciamento de identidade:** É a verificação da identidade de algum usuário dentro de uma organização. Esse processo é essencial para garantir a segurança dos sistemas e dados. Um dos métodos mais utilizados para essa finalidade é a autenticação multifator, na qual o usuário precisa comprovar sua identidade por meio de dois ou mais fatores distintos. Entre os meios mais comuns estão o uso de números de celular, endereços de e-mail e códigos temporários que expiram após um curto período, aumentando a confiabilidade do processo de autenticação.

- **Gerenciamento de acesso:** Trata-se de um controle sobre quais recursos um usuário tem permissão para acessar dentro da data-base de uma organização. Podem existir diversos níveis de acesso, os fatores determinantes são cargos, projetos, tempo de trabalho e diversos outros. Um dos objetivos do IAM é garantir que a tentativa de autenticação e a autorização a recursos ocorra de maneira efetiva em todas as tentativas de acesso.

2.6 Políticas do AWS IAM

Dentro do console do AWS IAM, existem diferentes tipos de políticas que podem ser atribuídas a usuários, grupos e roles. Essas políticas oferecem ampla flexibilidade, permitindo a definição de permissões de forma restrita e bem distribuída, de acordo com as responsabilidades de cada entidade. Por meio do gerenciamento adequado, é possível autorizar ou negar uma variedade de solicitações, configurando essas permissões por meio do vínculo das políticas às entidades do IAM durante a implementação do ambiente. Existem os seguintes tipos de políticas (AWS, 2023b):

- **Políticas baseadas em identidade:** Essas políticas podem ser anexadas a um usuário, grupo ou role, permitindo o controle das ações de uma entidade principal ao analisar quais recursos são necessários e sob quais condições a política pode ser aplicada. Existem três tipos de políticas de identidade: as políticas gerenciadas pela própria AWS, as políticas gerenciadas pelos clientes — que podem ser reutilizadas e anexadas a diversas identidades — e as políticas em linha (*inline policies*), que também são baseadas em identidades, mas só podem ser aplicadas a uma única entidade principal. Dessa forma, trata-se de um recurso com grande potencial de exploração.
- **Políticas de controle de serviço (SCPs):** São políticas responsáveis por definir permissões no contexto de uma organização e suas unidades organizacionais (OUs). As políticas de controle de serviço permitem a aplicação de invariantes de segurança — controles que podem ser aplicados de forma centralizada a múltiplas contas ou OUs dentro da AWS — com o objetivo de restringir permissões, inclusive para entidades privilegiadas, como o usuário raiz. O propósito das SCPs é estabelecer barreiras de segurança, de modo que o acesso não seja concedido diretamente, mas sim controlado por meio da aplicação dessas políticas em contas ou unidades organizacionais específicas.
- **Políticas de limite de permissões:** Esse recurso é parecido com as políticas de controle de serviço (SCPs), pois ele impõe uma camada extra de controle, que ajuda a restringir o que as entidades podem ou não fazer,

mesmo que tenham permissões em suas políticas. O limite de permissões é um recurso avançado do IAM, ele define o máximo de permissões que um usuário, grupo ou role pode ter, possibilitando o controle de ações baseado em permissões já atribuídas a entidade, ou seja, só poderá fazer o que for permitido pela política de permissões e pelo limite de permissões, definindo até onde o acesso pode ir.

- **Políticas baseadas em recursos:** As políticas baseadas em recursos são documentos que podem ser anexados diretamente a um recurso e podem ser configuradas como políticas em linha, o que permite a especificação detalhada de ações específicas a serem executadas sobre os recursos da AWS. Por exemplo, um bucket do serviço S3, onde é possível controlar o acesso aos objetos, definindo quem pode ler, escrever ou apagar os itens dentro do bucket.
- **Políticas de sessão:** Têm o objetivo de estabelecer um conjunto de regras para o gerenciamento seguro das sessões de usuários em sistemas de computação. Elas são essenciais para prevenir acessos não autorizados, além de garantir que as sessões sejam mantidas de forma controlada e de acordo com os requisitos de segurança organizacionais.
- **Lista de controle de acesso:** É um mecanismo de segurança que especifica quais usuários ou grupos têm permissão para acessar determinados recursos em um sistema, e quais ações podem ser realizadas sobre esses recursos. Esse tipo de controle é crucial para limitar o acesso aos dados e recursos dentro de um sistema, baseando-se em permissões de leitura, escrita e execução.

3 CENÁRIO ORGANIZACIONAL AWS

Nesse capítulo, um plano de execução de teste prático será detalhado. O objetivo é simular configurações inadequadas no serviço AWS IAM (*Identity and Access Management*). O IAM da Amazon Web Services é uma ferramenta essencial e crucial para o controle de acessos, gerenciamento de identidades e a segurança de operações na nuvem. Conforme conceitos apresentados anteriormente, esse teste visa explorar vulnerabilidades comuns que podem ser exploradas por indivíduos mal-intencionados, onde configurações erradas, como permissões excessivas, políticas mal configuradas e falta de segmentação de privilégios, podem resultar na exploração de um ambiente. Nesse teste será feito uma análise qualitativa da segurança da AWS IAM.

Esse capítulo será estruturado da seguinte maneira: na seção 3.1, serão definidos os objetivos e cronograma do teste prático; na seção 3.2, será descrito o ambiente de testes e as configurações e ferramentas necessárias para sua preparação; na seção 3.3, os requerimentos para a análise de dados, com o foco em ambientes mal configuradas dentro da AWS IAM.

3.1 Objetivo e Pesquisa;

Desenvolveremos uma pesquisa explicativa com o propósito de compreender como a segurança, quando falamos de IAM, é importante para o ambiente. Segundo Tumelero (2019), o principal objetivo da pesquisa explicativa é estabelecer uma conexão de ideias, permitindo uma compreensão das relações de causa e efeito dentro de um determinado contexto buscando esclarecer e justificar os eventos estudados.

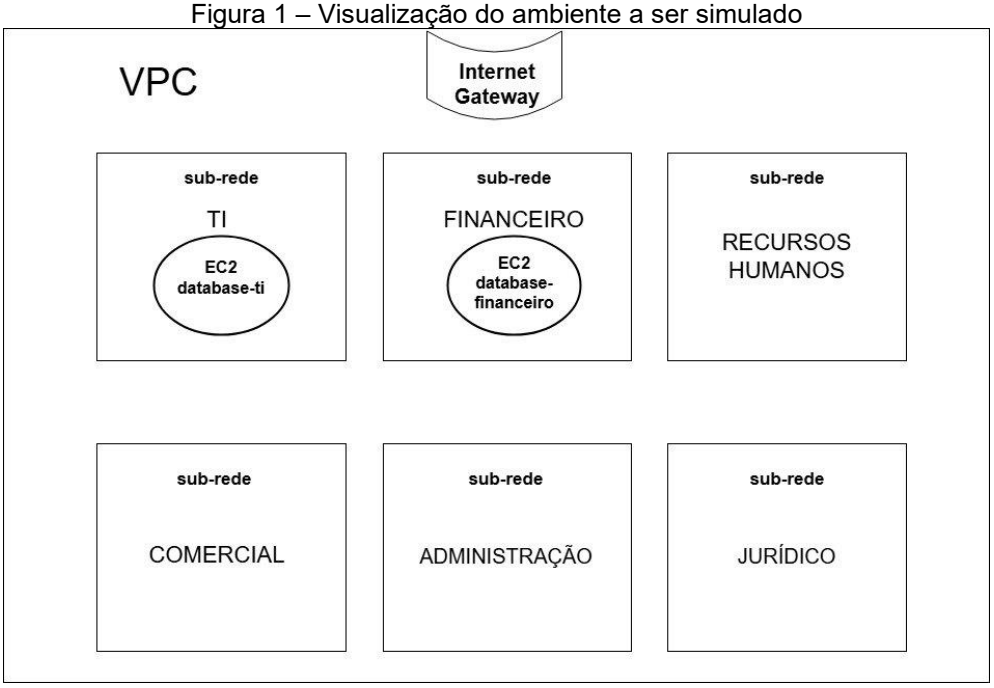
Como objetivo, iremos demonstrar como um ambiente organizacional pode ser explorado caso tenha as configurações inadequadas no serviço AWS IAM. O IAM da Amazon Web Services é uma ferramenta essencial e crucial para o controle de acessos, gerenciamento de identidades e a segurança de operações na nuvem. Conforme conceitos apresentados anteriormente, esse teste visa explorar vulnerabilidades comuns que podem ser exploradas por indivíduos mal-intencionados,

onde configurações erradas, como permissões excessivas, políticas mal configuradas e falta de segmentação de privilégios, podem resultar na exploração de um ambiente.

Uma simulação de ambiente organizacional será realizada na AWS, onde uma estrutura de departamentos que representam áreas chave da empresa, como Jurídico, Financeiro, Recursos Humanos, Tecnologia da Informação serão criados. Cada departamento será configurado com usuários e grupos específicos no AWS *Identity and Access Management*, de modo que as permissões sejam atribuídas de acordo com as responsabilidades de cada função. Buscaremos, não apenas segmentar as permissões de forma eficiente, mas também explorar e corrigir configurações malfeitas e demonstrar como elas podem ser uma brecha de exploração nas organizações.

Na figura 1, temos um exemplo da visualização da organização a ser simulada para melhor entendimento.

Figura 1 – Visualização do ambiente a ser simulado



Fonte: autoria própria (2025).

Na tabela 1, temos um cronograma que foi desenvolvido para exemplificar a desenvoltura do projeto.

Tabela 1 – Cronograma de desenvolvimento do TCC.

CRONOGRAMA DO TCC						
ETAPAS	**Janeiro 2025**	**Fevereiro 2025**	**Março 2025**	**Abril 2025**	**Maio 2025**	**Junho 2025**
Elaboração do projeto	X	X				
Revisão de Estrutura Organizacional			X			
Configuração do Ambiente Organizacional			X			
Testes no Ambiente Organizacional			X	X		
Elaboração e revisão do projeto acadêmico				X	X	X
Apresentação						X

Fonte: autoria própria (2024).

3.1.1 Quanto ao delineamento

Segundo Yin (2001), o estudo de caso é um método de pesquisa que utiliza, geralmente, dados qualitativos, coletados a partir de eventos reais, com o objetivo de explicar, explorar ou descrever fenômenos atuais inseridos em seu próprio contexto.

A presente pesquisa caracteriza-se, predominantemente, como um estudo de caso, por analisar em profundidade um cenário específico e delimitado: a estrutura de permissões e identidade em um ambiente simulado da AWS, aplicado a uma empresa fictícia composta por diversos departamentos organizacionais. O estudo de caso permite compreender, de forma prática e detalhada, os impactos decorrentes da má configuração de políticas de acesso no serviço AWS IAM utilizando experimentações controladas.

Adicionalmente, a pesquisa possui caráter bibliográfico, por basear-se em livros, artigos científicos, manuais técnicos da AWS e diretrizes reconhecidas de

segurança da informação, os quais fundamentam teoricamente os conceitos aplicados e as análises realizadas.

A investigação também assume, em menor grau, aspectos de uma abordagem experimental, à medida que são realizadas simulações reais dentro do ambiente da AWS (*Free Tier*), com a finalidade de provocar e observar comportamentos e vulnerabilidades típicas em ambientes de produção mal configurados.

Esse conjunto metodológico foi escolhido por permitir a análise técnica dos riscos de segurança, combinando a observação prática de um ambiente real, ainda que simulado, com os fundamentos teóricos da área de segurança da informação.

3.2 Ambiente AWS Academy

Foi feita uma pesquisa de laboratório experimental que, de acordo com Gonçalves (2021), é um tipo de pesquisa onde é elaborado um experimento para demonstração de algo e com isso em mente foi realizada a criação de um ambiente organizacional onde o uso da AWS IAM será exemplificado. Em uma empresa fictícia, existem os seguintes departamentos: Administração, Recursos Humanos, Financeiro, Jurídico, TI e Comercial, onde cada departamento contém 1 usuário efetivo na empresa. A decisão de realizar uma simulação de empresa e seus departamentos deu-se dada necessidade de configurar incorretamente políticas da AWS IAM.

3.2.1 Criação da VPC

Para dar início à construção do ambiente fictício proposto neste estudo de caso, a primeira etapa consiste na criação de uma VPC (*Virtual Private Cloud*). A VPC é essencial para o isolamento e controle da rede dentro da infraestrutura em nuvem, proporcionando um ambiente seguro e personalizável para o desenvolvimento dos recursos. Durante essa fase, é necessário definir o bloco CIDR (*Classless Inter-Domain Routing*), que delimita o intervalo de endereços IP disponíveis para uso dentro da VPC. Optou-se pelo bloco 10.0.0.0/16, que oferece um espaço de endereçamento privado, sendo uma faixa suficiente para atender às demandas deste ambiente controlado, permitindo ainda a criação de sub-redes conforme as necessidades do projeto. A Figura 2 representa a apresentação da VPC criada no laboratório da AWS.

Figura 2 - Criação de VPC na AWS

Fonte: AWS Academy, laboratório de testes (2025).

3.2.2 Criação das sub-redes departamentais

Com o objetivo de promover uma melhor organização e segurança dentro da infraestrutura de rede, os diferentes departamentos foram segmentados por meio da criação de sub-redes distintas. Essa abordagem permite isolar logicamente os recursos de cada setor, facilitando a aplicação de políticas de segurança específicas e otimizando o controle de tráfego interno.

Apesar dos testes terem sido configurados utilizando o protocolo IPv4, é importante ressaltar que a AWS oferece total suporte ao IPv6, o que garante maior flexibilidade para aplicações que precisam operar em ambientes modernos e compatíveis com a nova geração de endereçamento IP.

Como requisito técnico, todas as sub-redes devem pertencer ao mesmo bloco CIDR previamente definido para a VPC, uma vez que fazem parte de sua estrutura interna. Isso garante que haja comunicação entre elas, caso permitido pelas regras de roteamento e controle de acesso.

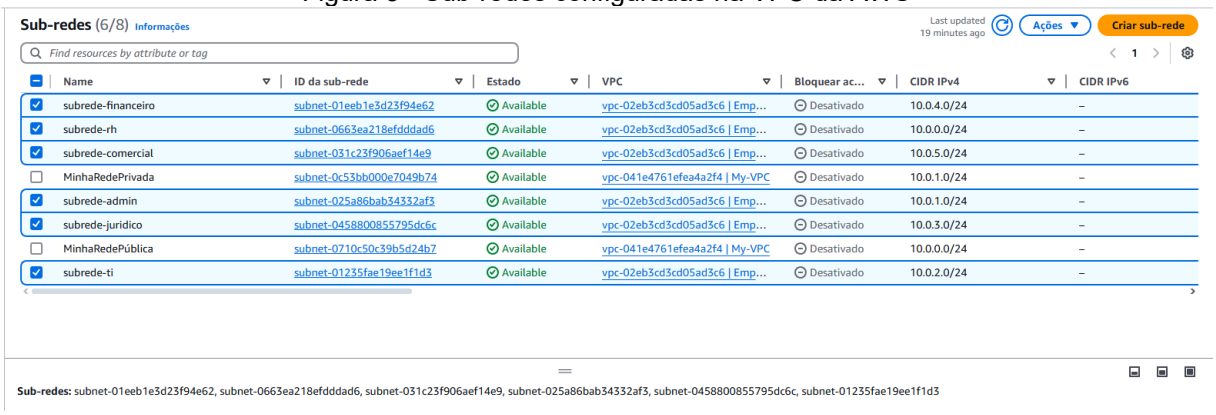
Para facilitar a compreensão, pode-se fazer uma analogia em que a VPC representa uma casa, e as sub-redes, os cômodos dessa casa, todos compartilham o mesmo espaço físico (ou lógico), mas cada um com sua função e delimitação.

Dessa forma, foram criadas as seguintes sub-redes, cada uma com seu respectivo intervalo de endereçamento IP:

- subrede-rh: 10.0.0.0/24;
- subrede-administração: 10.0.1.0/24;
- subrede-ti: 10.0.2.0/24;
- subrede-jurídico: 10.0.3.0/24;
- subrede-financeiro: 10.0.4.0/24;
- subrede-comercial: 10.0.5.0/24;

Essa estrutura modular facilita a administração da rede e permite uma escalabilidade mais eficiente conforme novas necessidades surgirem, foi configurado conforme a Figura 3.

Figura 3 - Sub-redes configuradas na VPC da AWS

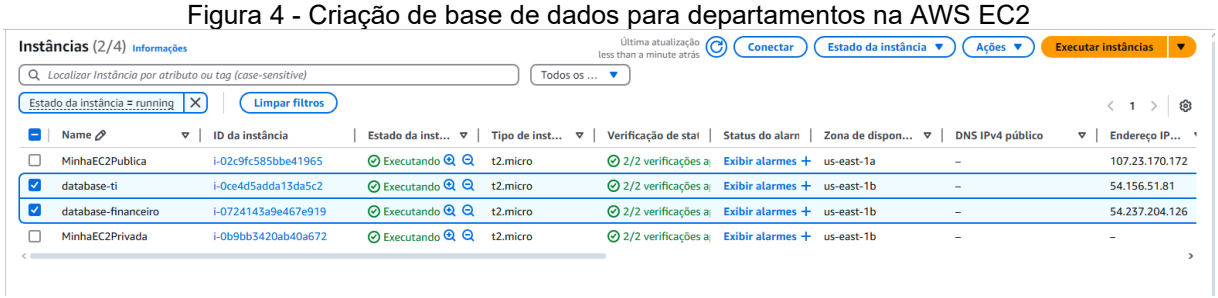


Fonte: AWS Academy, laboratório de testes (2025).

3.2.3 Criação das Instâncias EC2

Alguns serviços na AWS geram custo de acordo com o uso, as instâncias fazem parte desse custo, com isso em mente, decidimos criar somente 2 instâncias para exemplificar no ambiente, sendo elas a **database-ti** e **database-financeiro**. No processo de criação da instância, os primeiros passos são atribuir qual será o sistema operacional do servidor, onde escolhemos a distribuição Linux Ubuntu. Segundamente atribuir a chave privada para acesso SSH, selecionar as regras de segurança da sub-rede e o passo mais importante é atribuir a instância a VPC desejada e a sub-rede que ela fará parte, sendo assim, a **database-ti** foi atribuída a VPC empresa e a subrede-ti, **database-financeiro** delegada a mesma VPC, mas a subrede-financeiro. A Figura 4 apresenta as *databases* criadas para os departamentos de TI e Financeiro.

Figura 4 - Criação de base de dados para departamentos na AWS EC2



Fonte: AWS Academy, laboratório de testes (2025).

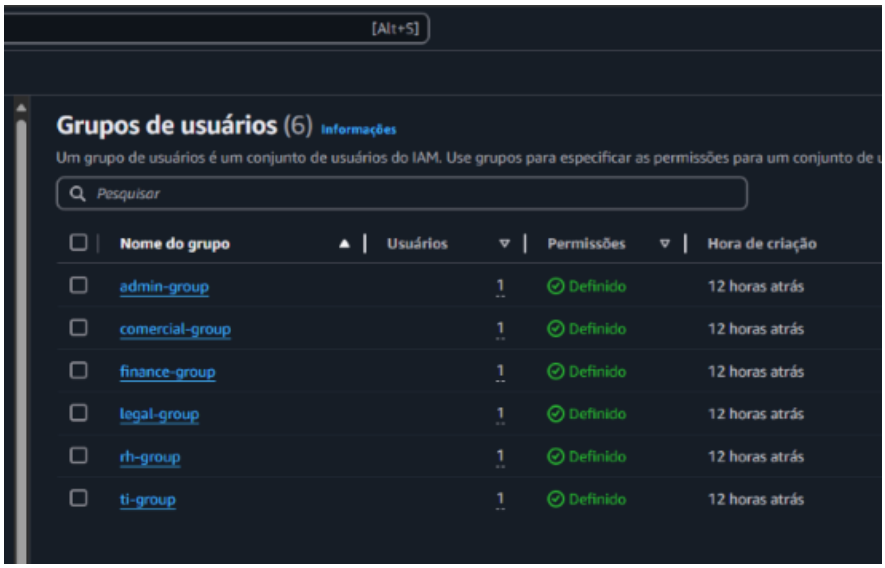
3.3 Requerimentos para a análise de dados.

Após a definição da estrutura organizacional fictícia, foram criados os respectivos grupos no AWS IAM representando cada um dos departamentos mencionados anteriormente. A Figura 5 exibe a criação de todos os grupos departamentais, são eles:

- **Admin-group:** Grupo designado para usuários com perfil de administração geral do ambiente. Esse grupo deve possuir permissões amplas, com possibilidade de criação, modificação e exclusão de diferentes recursos da AWS, sendo responsável pela governança da conta e aplicação de boas práticas de segurança.
- **Comercial-group:** Grupo destinado aos usuários ligados à área de vendas e relacionamento com clientes. Esse grupo deve possuir permissões para acessar dados de clientes, ferramentas de análise de vendas e recursos de comunicação. O acesso deve ser restrito a serviços como S3, DynamoDB e ferramentas de marketing, mas não é permitido acessar dados jurídicos ou financeiros.
- **Finance-group:** Responsável pela gestão financeira e contábil da organização. Os usuários desse grupo devem ter acesso a relatórios financeiros, sistemas de cobrança e demais informações financeiras sensíveis. A política atribuída deve limitar o acesso apenas aos recursos financeiros, garantindo a confidencialidade e integridade.
- **Legal-group:** Designado a gerenciamento de dados e documentos legais da organização. Este grupo deve possuir acessos a serviços que armazenam informações jurídicas, como contratos e documentos normativos, com restrição de acesso conforme o princípio do menor privilégio.
- **RH-group:** Esse grupo é responsável pelo acesso a dados e sistemas relacionados a gestão de pessoas, como informações de colaboradores, folha de pagamento e benefícios. Ele deve possuir acesso restrito a recursos específicos, como *buckets* S3 que contém documentos de RH e serviço de banco de dados que armazenam informações sensíveis de funcionários.

- **TI-group:** É o setor responsável pela infraestrutura de TI. Os usuários deste grupo devem possuir permissões para gerenciar instâncias EC2, banco de dados, serviços de monitoramento (como o CloudWatch) e automações. É indicado a implementação de roles e políticas, pois é um dos principais grupos que necessitam de acesso elevado.

Figura 5 - Grupos departamentais criados na AWS IAM



Fonte: AWS Free Tier, configuração própria (2025).

O procedimento que será adotado para a coleta e análise dos dados vem com o objetivo de identificar e avaliar configurações incorretas realizadas na AWS IAM, no contexto da organização fictícia desenvolvida para este estudo.

A coleta de dados foi realizada por meio da criação e monitoramento de grupos, usuários, funções e políticas criadas na AWS IAM, onde os departamentos especificados têm diferentes tipos de permissões aplicadas a cada um deles, o que inclui propositalmente políticas inadequadas, com o intuito de simular falhas reais de configurações. As permissões foram atribuídas manualmente por meio do console da AWS, criadas com o objetivo de representar práticas inseguras.

3.3.1 Técnicas para coleta de dados

A análise dos dados coletados consistiu na comparação entre as permissões efetivamente concedidas e as permissões esperadas com base na função organizacional de cada grupo. Foram avaliados os seguintes fatores:

- Privilégios excessivos;
- Acesso indevido entre departamentos;
- Falta de autenticação multifator (MFA);
- Uso de políticas genéricas como *:*;
- Assunção de roles administrativas por usuários não autorizados.
- Princípio do menor privilégio.

4 RESULTADOS

Este capítulo apresenta os resultados obtidos a partir da implementação do ambiente simulado na AWS IAM, conforme estrutura organizacional fictícia proposta. O foco da análise está nas configurações incorretas de permissões de acesso e identidade, propositalmente inseridas em diferentes grupos e usuários com o objetivo de simular falha comuns que podem ser encontradas em ambientes corporativos.

A partir da execução dos testes, foram observadas inconsistências em políticas de acesso, atribuições de privilégios excessivos, *trust policies* mal definidas e ausência de medidas básicas de segurança, como autenticação multifator.

Os resultados apresentados serão segmentados por vulnerabilidades identificadas, permitindo clarificar como uma configuração pode afetar diferentes áreas da organização e facilitar o acesso indevido a informações sensíveis. A seguir, são detalhadas as principais falhas detectadas, acompanhadas de suas respectivas implicações de segurança.

4.1 Ausência de autenticação multifator (MFA)

O MFA é um recurso para comprovar a autenticidade do usuário, podendo ser através de códigos temporários enviados para um e-mail, para o celular por SMS ou ligação, aplicativos onde o código muda a cada 30 segundos, ou até biometria.

Usar somente a proteção de senha não é recomendável, pois a aplicação ou conta podem sofrer alguns tipos de ataques que tem facilidade em quebrar senhas, como ataques de *phishing*, vazamento de credenciais e força bruta, principalmente se essas senhas forem de nível baixo, ou seja, fácil descobrimento.

Uma possível configuração que pode ocorrer dentro de uma empresa é justamente a ausência dessa autenticação de multifatores, no cenário fictício que criamos, não temos uma política de uso obrigatório e os usuários não contêm esse método de segurança ativado, podendo comprometer a segurança do ambiente. Conforme a Figura 6, podemos perceber que o recurso MFA não está habilitado para nenhum usuário da organização.

Figura 6 - Configuração de MFA na AWS

Fonte: AWS Free Tier, configuração própria (2025).

A ausência de autenticação multifator (MFA) em um ambiente de nuvem como a AWS representa uma falha crítica de segurança que pode expor a organização a diversos riscos operacionais, financeiros e reputacionais. A seguir, são discutidos alguns dos principais riscos associados à falta desse controle.

- **Elevação de privilégio caso credenciais sejam comprometidas:** sem MFA, um atacante que obtenha o nome de usuário e a senha de um usuário pode acessar a conta como se fosse o próprio usuário legítimo. Isso é especialmente perigoso quando se trata de contas com permissões administrativas ou mal configuradas. Com esse acesso, o invasor pode escalar seus privilégios, explorar falhas de configuração ou modificar políticas para ampliar ainda mais seu controle sobre o ambiente.
- **Acesso a dados sensíveis:** com as credenciais expostas sem a proteção de um segundo fator, dados críticos armazenados nos serviços da AWS podem ser facilmente acessados, levando a vazamento de informações, violação de privacidade e possíveis dados a reputação da empresa.
- **Acesso a conta root AWS:** a conta root na AWS possui controle total dos recursos e serviços disponíveis, caso a conta esteja sem MFA e suas credenciais sejam comprometidas, o invasor poderá alterar configurações importantes, excluir usuários, ou até remover dados, podendo ter uma paralisação total da operação em nuvem da empresa.

4.2 Trust Policies mal configuradas

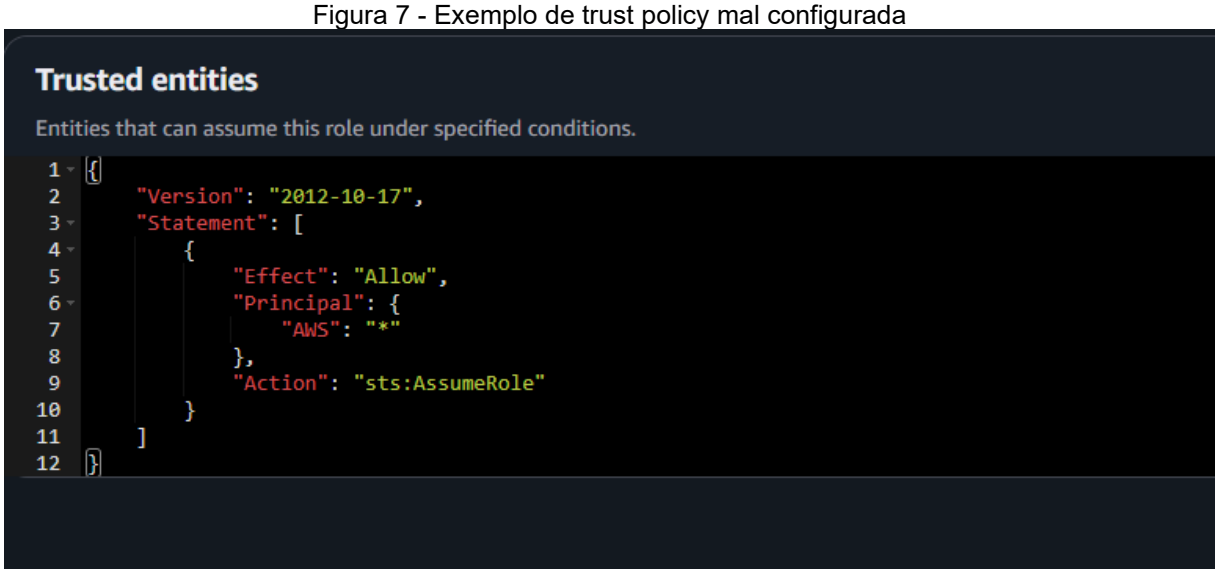
As funções são identidades semelhantes a usuários, porém não são exclusivamente associadas a uma pessoa, elas têm o propósito de serem assumidas dada a necessidade de cada departamento (AWS, 2025c).

Os *roles* podem ter diversos usos, como delegação de acesso a usuários, serviços ou aplicações. Com essa demanda, é estabelecida uma relação de confiança entre duas políticas anexadas.

No ambiente organizacional, foi realizada a configuração de uma trust policy que poderia ser facilmente explorada por um agente malicioso. A parametrização incorreta desse tipo de recurso pode desencadear uma série de vulnerabilidades de segurança, como a concessão indevida de permissões e elevação de privilégios. No contexto do ambiente estudado, as *trust policies* configuradas de forma inadequada podem permitir que identidades externas assumam funções (*roles*) sensíveis dentro da conta, o que acaba comprometendo a integridade de recursos confidenciais e dados críticos.

A *trust policy* apresentou uma brecha de segurança que poderia ser explorada. Ela permite que qualquer identidade AWS assume o *role* ao qual a política está anexada. Isso ocorre porque a política utiliza um valor “*”, que significa, literalmente, “qualquer identidade AWS”. Conforme apresentado na Figura 7, há um *role* atribuído, identificado como **legal-admin-role**. Essa *trust policy* permite que qualquer identidade AWS assume o referido *role*, o que representa um sério risco à segurança do ambiente.

Figura 7 - Exemplo de trust policy mal configurada



Fonte: AWS Free Tier, configuração própria (2025).

A existência de permissionamento excessivo é clara na política acima. Feita a análise, observa-se que o acesso irrestrito aos roles pode ocasionar graves consequências operacionais, legais e financeiras para uma organização. Foram

identificados diversos riscos que essa configuração pode acarretar para uma organização real, são eles:

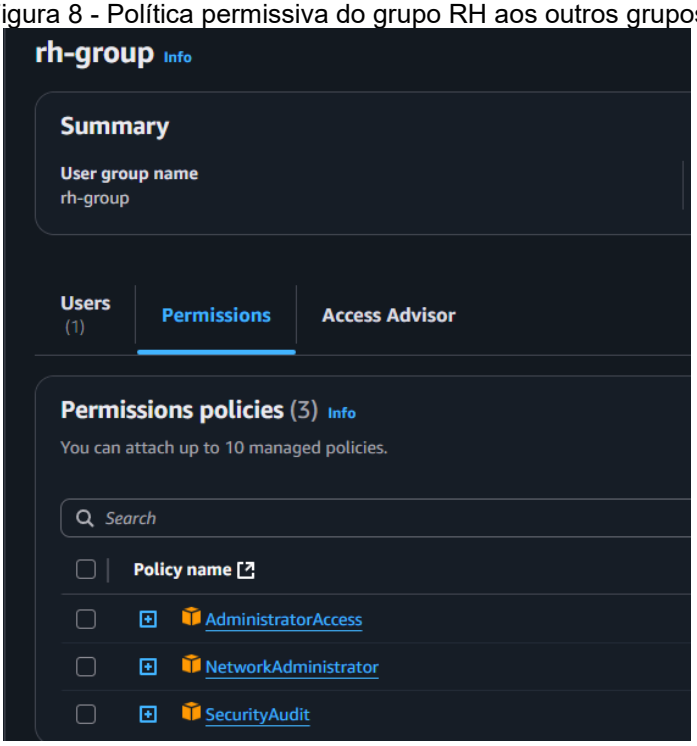
- **Permissão irrestrita no campo “Principal”:** A utilização do asterisco permite que qualquer identidade AWS assuma o role, o que viola o princípio de menor privilégio, abrindo portas para acessos não autorizados e elevação indevida de privilégios.
- **Ausência de restrições adicionais:** Falta evidente de condições específicas que limitam a origem do acesso ou definam entidades confiáveis, o que torna o ambiente vulnerável a ataques externos e internos, além de dificultar a rastreabilidade das ações realizadas.
- **Riscos operacionais e financeiros**: Exposição da organização a riscos significativos, como perda de dados sensíveis, interrupções nos serviços, descumprimento de normas regulatórias, multas e prejuízos financeiros, o que afetaria diretamente a integridade e continuidade de negócios.

4.3 Acesso indevido entre departamentos

Dentro de empresas que utilizam serviços em nuvem, como a AWS, o controle de acesso entre diferentes departamentos é crucial para a segurança das informações. Cada setor da empresa lida com diferentes tipos de dados e sistemas, que muitas das vezes são sensíveis e confidenciais.

Quando não há a configuração adequada para a segregar o acesso desses grupos, pode ocorrer o acesso indevido, permitindo um departamento ter visibilidade e controle sobre os recursos de outro grupo. Segundo a Figura 8, é exemplificado o grupo de RH (Recursos Humanos), contendo políticas permissivas para ter acesso a outros tipos de funções dentro do ambiente.

Figura 8 - Política permissiva do grupo RH aos outros grupos



Fonte: AWS Free Tier, configuração própria (2025).

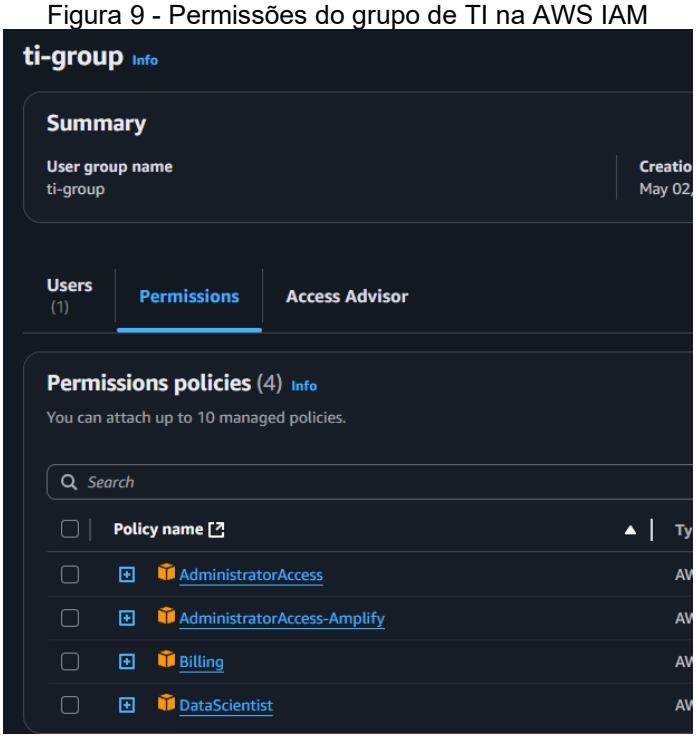
Esse tipo de falha representa não somente um problema técnico, mas também um problema jurídico e organizacional, comprometendo a privacidade e conformidade com as leis como a LGPD (Lei Geral de Proteção de Dados).

4.4 Privilégios excessivos atribuídos aos usuários

Uma vulnerabilidade crítica que é analisada no ambiente simulado é uma preocupante concentração de acessos irrestritos entre um dos grupos da AWS IAM. Esse cenário viola diretamente o princípio do menor privilégio, o qual estabelece que cada identidade deve possuir apenas as permissões estritamente necessárias para a execução de suas funções. Essa prática é fundamental, pois, quanto mais restrito for o acesso, menor será o impacto caso a conta seja comprometida, seja por erro humano ou por ações maliciosas.

Conforme demonstrado na Figura 9, o grupo de TI foi configurado com múltiplas permissões administrativas, o que constitui uma das principais fragilidades de segurança no ambiente analisado, com potencial para gerar impactos severos sobre a confidencialidade, integridade e disponibilidade dos recursos corporativos.

Figura 9 - Permissões do grupo de TI na AWS IAM



Fonte: AWS Free Tier, configuração própria (2025).

Sob a ótica da segurança da informação, é observado que o grupo denominado “ti-group” possui permissões excessivamente amplas, o que foi feito para simular uma configuração inadequada. Essas políticas permissivas representam um risco elevado, uma vez que o usuário pertencente a esse grupo pode, deliberadamente ou acidentalmente, realizar ações críticas, como a exclusão de serviços essenciais, alteração de configurações de segurança ou o comprometimento de dados sensíveis da organização. A seguir, apresenta-se a análise realizada sobre o permissionamento atribuído a este grupo:

- **Privilégios administrativos irrestritos:** O grupo possui as políticas “AdministratorAccess” e “AdministratorAccess-Amplify”, que concedem acesso total a todos os serviços e recursos existentes da AWS, sem qualquer restrição. Essa configuração representa uma falha crítica na segregação de acessos, pois viola o princípio do menor privilégio, expondo a organização a riscos operacionais e de segurança.
- **Acesso a informações financeiras:** A presença da política “Billing” permite que os membros do grupo de TI tenham acesso a informações financeiras e de faturamento da conta AWS. Esse tipo de acesso expõe dados

sensíveis que deveriam estar restritos ao departamento financeiro, o que destaca a importância do controle de acesso nas empresas.

- **Permissões desnecessárias para ciência de dados**: A atribuição da política “DataScientist” ao grupo de TI representa uma excessividade que não condiz com as funções típicas deste setor. Essa política concede acesso a diversos serviços relacionados a análise de dados, que não são imprescindíveis para as atividades administrativas ou operacionais da equipe. Essa permissividade dificulta a rastreabilidade das ações realizadas, uma vez que o escopo de atuação dos usuários não está alinhado a suas atribuições reais.
- **Risco de abuso e comprometimento:** A concentração de múltiplos privilégios elevados em um único grupo aumenta substancialmente o risco de abuso de privilégios ou comprometimento da conta. Em caso de vazamento de credenciais ou um ataque bem-sucedido, um agente malicioso teria a capacidade de manipular recursos críticos, interromper operações, excluir dados e modificar configurações essenciais para o funcionamento interno. Além disso, a possibilidade de ações não intencionais por parte de usuários internos, decorrentes de erros ou desconhecimento, é igualmente preocupante, podendo gerar impactos operacionais severos, como indisponibilidade de sistemas ou perda de integridade de informações estratégicas para a organização.
- **Ausência de segmentação adequada:** A inexistência de uma segmentação granular nas permissões concedidas ao grupo de TI evidencia uma falha na aplicação de boas práticas de gestão de acessos. O ideal seria a criação de perfis distintos, com permissões específicas para diferentes funções dentro do próprio setor, como administração de infraestrutura, suporte técnico ou desenvolvimento. A falta dessa divisão impede o controle preciso sobre quem pode realizar determinadas ações, elevando o risco de acessos não autorizados e dificultando a implementação de políticas de auditoria e compliance.

5 CONSIDERAÇÕES FINAIS

Esse estudo concentrou-se na Segurança em Nuvem, com ênfase na análise no Gerenciamento de Identidades e Acessos (IAM) utilizando os recursos disponibilizados pela Amazon Web Services (AWS). O objetivo principal foi examinar como configurações incorretas no AWS IAM podem comprometer a segurança de ambientes organizacionais reais e identificar como ele poderia ser explorado em um contexto real.

A questão norteadora desta pesquisa foi: “como uma falha de configuração no gerenciamento de acessos pode afetar um ambiente organizacional em nuvem?”.

Durante o desenvolvimento desta pesquisa, o objetivo principal de analisar como as configurações realizadas poderiam afetar a segurança do ambiente foi atingido com sucesso, o que possibilitou a identificação de potenciais vulnerabilidades que muitas empresas tendem a negligenciar.

Diante dos resultados obtidos, recomenda-se a adoção de algumas boas práticas no gerenciamento de identidades e acessos a nuvem, como a implementação do princípio de menor privilégio, a configuração adequada de políticas de confiança (*trust policies*) e a obrigatoriedade do uso de autenticação multifator. Essas medidas são essenciais para mitigar riscos associados a acessos indevidos entre departamentos, privilégios excessivos e configurações inadequadas que podem comprometer seriamente a segurança do ambiente organizacional.

Apesar disso, tivemos algumas dificuldades e aprendizados durante o processo de elaboração do nosso trabalho de conclusão de curso, primeiramente seria um conjunto tanto de dificuldades e aprendizados que seria o conhecimento para estruturarmos e configurarmos um ambiente dentro de uma plataforma de serviços em nuvem, onde tivemos que pesquisar várias fontes e vídeos para o entendimento principalmente da plataforma da AWS e dos conceitos relacionados à segurança e aplicações em nuvem.

Espera-se que este estudo contribua para o fortalecimento das práticas de segurança em nuvem, promovendo maior conscientização sobre a importância do gerenciamento adequado de identidades e acessos por meio do AWS IAM, e incentivando a adoção de políticas mais seguras e bem estruturadas no contexto de ambientes corporativos em nuvem.

Como sugestão para pesquisas futuras, recomenda-se a investigação do uso de ferramentas de automação e auditoria contínua em ambientes de nuvem e soluções de inteligência artificial para detecção de comportamentos anômalos. Além disso, vale aprofundar o estudo sobre os desafios de gerenciamento de identidades nesse cenário, ampliando o debate sobre a segurança em arquiteturas de nuvem.

REFERÊNCIAS

ALURA, AWS: o que é Amazon Web Services e suas Certificações. 2024. Disponível em: https://www.alura.com.br/artigos/aws?srsltid=AfmBOooFEyfsIPVEbH0r85a0vCzuRFhPwQKvvh7KMgai0vFKcFluM5ir. Acesso em: 06 abr. 2025, às 20h23min.

AWS BRASIL. Tipos de política do IAM: Como e quando usá-las. O blog da AWS. 2023b. Disponível em: https://aws.amazon.com/pt/blogs/aws-brasil/tipos-de-politica-do-iam-como-e-quando-usa-las/. Acesso em: 29 mar. 2025, às 19h32min.

AWS BRASIL. Perfis do IAM. 2025c. Disponível em: https://docs.aws.amazon.com/pt_br/IAM/latest/UserGuide/id_roles.html. Acesso em: 23 maio 2025, às 19h54min.

AWS, *What is Amazon VPC?* 2024a. Disponível em: https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html. Acesso em: 06 abr. 2025, às 18h12min.

Gartner. *Gartner Says Cloud Will Be the Centerpiece of New Digital Experiences*. 2021. Disponível em: https://www.gartner.com/en/newsroom/press-releases/2021-11-10-gartner-says-cloud-will-be-the-centerpiece-of-new-digital-experiences. Acesso em: 15 set. 2024, às 17h15min.

Gonçalves, Jonas Rodrigo. MANUAL DE PROJETO DE PESQUISA: (3ª edição). Portal de Livros Abertos da Editora UniProcessus, p. 57, 2021. Disponível em: https://periodicos.processus.com.br/index.php/plaep/article/view/344/429. Acesso em: 03 maio 2025, às 17h23min.

IBM. O que é segurança da nuvem? 2023. Disponível em: https://www.ibm.com/br-pt/topics/cloud-security. Acesso em: 21 out. 2024, às 20h17min.

Mell, Peter e Grance, Timothy. *The NIST Definition of Cloud Computing*. NIST Special Publication. 2011. Disponível em: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf. Acesso em: 06 de abril de 2025, às 18h41min.

MICROSOFT. O que é gerenciamento de identidades e acesso (IAM)? 2024. Disponível em: https://www.microsoft.com/pt-br/security/business/security-101/what-isidentity-access-management-iam. Acesso em: 15 out. 2024, às 20h25min.

Miryala, Naresh Kumar, Cloud Performance: A Comparative Study of Aws vs. Azure. 2024. Disponível em: <https://iaeme.com/MasterAdmin/Journal_uploads/IJCET/VOLUME_15_ISSUE_2/IJCET_15_02_024.pdf>. Acesso em: 05 abril 2025, às 23h11min.

Mohammed, Azhar Ishaq. *Cloud Identity and Access Management – A model proposal Dubai*, UAE. 2019. Disponível em: https://www.researchgate.net/profile/Ishaq-Azhar-Mohammed/publication/353887567_CLOUD_IDENTITY_AND_ACCESS_MANAGEMENT_-_A_MODEL_PROPOSAL/links/61169d070c2bfa282a41f553/CLOUD-

IDENTITY-AND-ACCESS-MANAGEMENT-A-MODEL-PROPOSAL.pdf. Acesso em: 15 out. 2024, às 22h43min.

OBJECTIVE. Segurança em nuvem: conheça as melhoras estratégias e práticas para sua empresa. 2023. Disponível em: https://www.objective.com.br/insights/seguranca-em-nuvem/. Acesso em: 10 out. 2024, às 20h43min.

Borges, Hélder Pereira et al. COMPUTAÇÃO EM NUVEM. [s.l: s.n.]. Disponível em: https://livroaberto.ibict.br/bitstream/123456789/861/1/COMPUTA%c3%87%c3%83O%20EM%20NUVEM.pdf. Acesso em: 20 out. 2024, às 18h35min.

Pedrosa, Paulo H. C., e Nogueira, Tiago. Computação em Nuvem. 2011. Disponível em: https://www.ic.unicamp.br/~ducatte/mo401/1s2011/T2/Artigos/G04-095352-120531-t2.pdf. Acesso em: 11 out. 2024, às 14h55min.

Rosa, Gabriel De Oliveira; Canteiro, Henrique Santos. Desafios na segurança da informação usando virtualização na computação em nuvem. 2023. Disponível em: https://ric.cps.sp.gov.br/bitstream/123456789/14665/1/20231S_Gabriel De Oliveira Rosa_OD1606.pdf. Acesso em: 19 out. 2024, às 19h24min.

Tumelero, Naína. Pesquisa explicativa: conceitos, objetivos, exemplos e comparativos, 2019. Disponível em https://blog.mettzer.com/pesquisa-explicativa/. Acesso em: 24 de abril de 2025, às 15h07min.

Yin, Robert K. Estudo de caso: planejamento e métodos. pg. 21. 2. ed. Porto Alegre: Bookman. 2001. Disponível em http://maratavarespsictics.pbworks.com/w/file/fetch/74304716/3-YIN-planejamento_metodologia.pdf. Acesso em: 24 de abril de 2025, às 16h36min.