

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA POLITÉCNICA E DE ARTES
GRADUAÇÃO EM CIÊNCIA DE COMPUTAÇÃO



**SEGURANÇA NO ARMAZENAMENTO DE ARQUIVOS EM NUVEM: ESTUDO
DE CASO COM O MICROSOFT AZURE**

RAFAEL OLIVEIRA PORFÍRIO

GOIÂNIA
2024

RAFAEL OLIVEIRA PORFÍRIO

**SEGURANÇA NO ARMAZENAMENTO DE ARQUIVOS EM NUVEM: ESTUDO
DE CASO COM O MICROSOFT AZURE**

Trabalho de Conclusão de Curso apresentado à Escola Politécnica e de Artes, da Pontifícia Universidade Católica de Goiás, como parte dos requisitos para a obtenção do título de Bacharel em Ciência da Computação.

Orientadora:

Prof.^a Ma. Angélica da Silva Nunes

Banca examinadora:

Prof. Me. Rafael Leal Martins

Prof. Me. Wilmar Oliveira de Queiroz

GOIÂNIA
2024

RAFAEL OLIVEIRA PORFÍRIO

**SEGURANÇA NO ARMAZENAMENTO DE ARQUIVOS EM NUVEM: ESTUDO
DE CASO COM O MICROSOFT AZURE**

Trabalho de Conclusão de Curso aprovado em sua forma final pela Escola Politécnica e de Artes, da Pontifícia Universidade Católica de Goiás, para obtenção do título de Bacharel em Ciência da Computação, em ____/____/_____.

Orientadora: Prof. Ma. Angélica da Silva Nunes

Prof. Me. Rafael Leal Martins

Prof. Me. Wilmar Oliveira de Queiroz

GOIÂNIA
2024

RESUMO

Apresenta-se a implementação de um sistema de gerenciamento de arquivos em nuvem na plataforma Microsoft Azure, com foco na segurança computacional. Inicialmente, foi feita a escolha do serviço de armazenamento, optando pelo Azure Blob Storage. Esta foi seguida pela primeira fase da autenticação e a configuração de rede virtual. Posteriormente, a segunda fase da autenticação foi realizada, seguida pela reconfiguração do Azure Blob Storage e gerenciamento de chaves. Testou-se o registro de contas, as restrições aplicadas por diferentes tipos de autorização, e a presença das criptografias em trânsito e em repouso. Os resultados indicam uma implementação viável de segurança no armazenamento de arquivos em nuvem.

Palavras-Chave: Azure, Computação em Nuvem, Segurança Computacional, Armazenamento de Arquivos.

ABSTRACT

This study presents the implementation of a cloud-based file management system on the platform Microsoft Azure, with a focus on computer security. First, the selection of a storage service was made, opting for Azure Blob Storage. This was followed by a preliminary implementation of authentication and the configuration of a virtual network. Subsequently, the final implementation of the authentication was carried out, followed by the reconfiguration of Azure Blob Storage and the implementation of key management. Account registration, restrictions applied by different types of authorization, and the presence of encryption were tested. The results indicate a viable implementation of security for cloud-based file storage.

Keywords: *Azure, Cloud Computing, Computer Security, File Storage.*

LISTA DE FIGURAS

Figura 1: Percentagem de dados empresariais armazenados na nuvem em organizações de todo o mundo de 2015 a 2022	13
Figura 2: O uso de funções <i>hash</i> no armazenamento de senhas.....	18
Figura 3: Economia de Escala	23
Figura 4: Tipos de Serviço.....	27
Figura 5: Regiões e Zonas de Disponibilidade.....	28
Figura 6: <i>Market shares</i> dos principais provedores de computação em nuvem.....	29
Figura 7: Diagrama do LRS.....	32
Figura 8: Diagrama do ZRS.....	32
Figura 9: Configuração do Azure Blob <i>Storage</i>	33
Figura 10: Configuração do Azure Blob <i>Storage</i>	34
Figura 11: <i>Upload</i> para o Azure Blob <i>Storage</i>	34
Figura 12: Arquivo Hospedado no Azure Blob <i>Storage</i>	35
Figura 13: Configuração do Azure AD B2C	36
Figura 14: Configuração do Azure AD B2C	37
Figura 15: Configuração de Rede Virtual.....	39
Figura 16: Configuração de Rede Virtual.....	40
Figura 17: Configuração de Rede Virtual.....	41
Figura 18: Rede Virtual Criada Com Sucesso	42
Figura 19: Implementação da Máquina Virtual	43
Figura 20: Configuração do <i>Private Endpoint</i>	44
Figura 21: Configuração do <i>Private Endpoint</i>	44
Figura 22: Configuração do <i>Private Endpoint</i>	45
Figura 23: Configuração do <i>Private Endpoint</i>	46
Figura 24: <i>Endpoint</i> Criado Com Sucesso	46
Figura 25: Topologia da Rede.....	47
Figura 26: Etapas da Autenticação Azure AD B2C	48
Figura 27: Registro de Aplicação	49
Figura 28: Atribuição de Papel RBAC	50
Figura 29: Registro de Fluxo de Usuário	51

Figura 30: Funcionamento do Azure <i>Storage Explorer</i>	52
Figura 31: Configuração do Azure Blob <i>Storage</i>	53
Figura 32: Configuração do Azure Blob <i>Storage</i>	54
Figura 33: Configuração do Azure Blob <i>Storage</i>	55
Figura 34: Configuração do Azure <i>Key Vault</i>	56
Figura 35: Configuração do Azure <i>Key Vault</i>	56
Figura 36: Escolha da Criptografia.....	57
Figura 37: Vinculando Chave.....	58
Figura 38: Vinculando Chave.....	58
Figura 39: Erro do Azure Blob <i>Storage</i>	59
Figura 40: Vinculando Chave.....	59
Figura 41: Vinculando Chave.....	60
Figura 42: Configuração do Microsoft Entra ID.....	61
Figura 43: Registro de Conta no Microsoft Entra ID.....	62
Figura 44: Lista de Usuários.....	62
Figura 45: <i>Login</i> no Azure <i>Storage Explorer</i>	63
Figura 46: <i>Login</i> no Azure <i>Storage Explorer</i>	63
Figura 47: <i>Login</i> no Azure <i>Storage Explorer</i>	64
Figura 48: Registro de Senha.....	64
Figura 49: Solicitação de Autenticação Multifator.....	65
Figura 50: <i>QR Code para autenticação multifator</i>	65
Figura 51: Pedido de Autenticação por Aplicativo.....	66
Figura 52: Autenticação Bem-Sucedida.....	66
Figura 53: Atribuição de Papel RBAC.....	67
Figura 54: Interface do Azure <i>Storage Explorer</i>	67
Figura 55: Seleção de Container.....	68
Figura 56: Arquivos do Azure Blob <i>Storage</i>	68
Figura 57: Leitura de Arquivo.....	69
Figura 58: Teste de <i>Upload</i>	70
Figura 59: Erro de Upload.....	70
Figura 60: Atribuição de Papel RBAC.....	70
Figura 61: <i>Upload</i> Bem-Sucedido.....	71

Figura 62:Lista de Arquivos	71
Figura 63: Leitura de Arquivo Enviado Por Upload.....	71
Figura 64: Pacotes Rastreados no Wireshark	72
Figura 65: Pacotes Rastreados no Wireshark	72
Figura 66: Configurações da Criptografia em Repouso	73

LISTA DE ABREVIATURAS E SIGLAS

AAA	Autenticação, Autorização e Auditoria
AD	<i>Active Directory, Diretório Ativo</i>
AES	<i>Advanced Encryption Standard, Padrão Avançado de Criptografia</i>
API	<i>Application Programming Interface, Interface de Programação de Aplicação</i>
AWS	<i>Amazon Web Services, Serviços de Rede da Amazon</i>
B2C	<i>Business to Customer, Negócio para Cliente (B2C)</i>
BLOB	<i>Binary Large Object, Objeto Binário Grande</i>
CID	Confidencialidade, Integridade e Disponibilidade
CBC	<i>Cipher Block Chaining, Encadeamento de Cifras de Bloco.</i>
CLI	<i>Command Line Interface, Interface de Linha de Comando</i>
CMK	<i>Customer-Managed Keys, Chaves Gerenciadas pelo Cliente</i>
DAC	<i>Discretionary Access Control, Controle de Acesso Discricionário</i>
DDoS	<i>Distributed Denial-of-Service, Negação de Serviço Distribuída</i>
DES	<i>Data Encryption Standard, Padrão de Encriptação de Dados</i>
DTLS	<i>Datagram Transport Layer Security, Segurança da Camada de Transporte de Datagramas</i>
EC	<i>Elliptic Curve, Curva Elíptica</i>
ECC	<i>Elliptic Curve Cryptography, Criptografia de Curva Elíptica</i>
FWaaS	<i>Firewall as a Service, Firewall como Serviço</i>
HTTPS	<i>Hypertext Transfer Protocol Secure, Protocolo de Transferência de Hipertexto Seguro</i>
HTTP	<i>Hypertext Transfer Protocol, Protocolo de Transferência de Hipertexto</i>
IaaS	<i>Infrastructure as a Service, Infraestrutura como um Serviço</i>
ID	<i>Identification, Identificação</i>
IP	<i>Internet Protocol, Protocolo de Internet</i>
LRS	<i>Locally Redundant Storage, Armazenagem Localmente Redundante</i>

MAC	<i>Mandatory Access Control</i> , Controle de Acesso Mandat3rio
MMK	<i>Microsoft-Managed Keys</i> , Chaves Gerenciadas pela Microsoft
PaaS	<i>Platform as a Service</i> , Plataforma como Servi7o
PIN	<i>Personal Identification Number</i> , N3mero de Identifica73o Pessoal
QR	<i>Quick-Response</i> , Resposta R3pida
RAM	<i>Random Access Memory</i> , Mem3ria de Acesso Aleat3rio
RBAC	<i>Role-Based Access Control</i> , Controle de Acesso Baseado em Pap3is
REST	<i>Representational State Transfer</i> , Transfer3ncia de Estado Representacional
RSA	Rivest-Shamir-Adleman
SaaS	<i>Software as a Service</i> , <i>Software como Servi7o</i>
SHA	<i>Secure Hash Algorithm</i> , Algoritmo Seguro de Hash
SHA-256	<i>Secure Hash Algorithm-256</i> , Algoritmo Seguro de Hash-256
SHA-384	<i>Secure Hash Algorithm-384</i> , Algoritmo Seguro de Hash-384
SHA-512	<i>Secure Hash Algorithm-512</i> , Algoritmo Seguro de Hash-512
SSD	<i>Solid State Drive</i> , Unidade de Estado S3lido
SSL	<i>Secure Sockets Layer</i> , Camada de Soquete Seguro
TI	Tecnologia da Informa73o
TLS	<i>Transport Layer Security</i> , Seguran7a da Camada de Transporte
URL	<i>Uniform Resource Locator</i> , Localizador de Recurso Uniforme
vCPU	<i>Virtual Central Processing Unit</i> , Unidade Central de Processamento Virtual
VPN	<i>Virtual Private Network</i> , Rede Virtual Particular
VPC	<i>Virtual Private Cloud</i> , Nuvem Privada Virtual
ZRS	<i>Zone Redundant Storage</i> , Armazenagem Redundante em Zonas

SUMÁRIO

1 INTRODUÇÃO	12
1.1 Justificativa e questão de pesquisa	13
1.2 Objetivo geral	14
1.3 Objetivos específicos	14
1.4 Metodologia.....	14
1.5 Estrutura da monografia	14
2 PRINCÍPIOS DE SEGURANÇA.....	16
2.1 Pilares de Segurança.....	16
2.2 Ferramentas Criptográficas.....	16
2.3 Autenticação	19
2.4 Controle de Acesso	20
3 COMPUTAÇÃO EM NUVEM	22
3.1 Motivação	22
3.2 Dificuldades de Implementação	24
3.3 Tipos de Nuvem.....	25
3.4 Tipos de Serviço	26
3.5 Regiões e Zonas de Disponibilidade	27
3.6 Provedores	28
4 IMPLEMENTAÇÃO DE SISTEMA DE GERENCIAMENTO DE ARQUIVOS	30
4.1 Escolha do Serviço de Armazenamento	30
4.2 Implementação do Azure Blob <i>Storage</i>	31
4.3 Implementação da autenticação (fase 1).....	35
4.4 Implementação de rede virtual	38
4.5 Implementação da autenticação (fase 2).....	47
4.6 Reconfiguração do Azure Blob <i>Storage</i>	52
4.7 Gerenciamento de Chaves	55
5 TESTES REALIZADOS.....	61
5.1 Teste 1: registro da conta	61
5.2 Teste 1: autenticação.....	63
5.3 Teste 2: autorização	66

5.3.1 Acesso ao diretório compartilhado	67
5.3.2 Testes em cada um dos perfis de usuário.....	69
5.4 Teste 3: criptografia	71
5.4.1 Criptografia em trânsito.....	71
5.4.2 Criptografia em repouso	72
6 CONSIDERAÇÕES FINAIS.....	74
6.1 Sugestões de trabalhos futuros	75
REFERÊNCIAS	76

1 INTRODUÇÃO

Na era do *mainframe*, os sistemas computacionais eram controlados de forma centralizada, o que levava a ineficiências na produtividade. Em seguida, o advento do computador pessoal descentralizou as cargas de trabalho, oferecendo agilidade em detrimento da governança e da segurança. Este processo continuou com a ascensão do modelo cliente-servidor, no qual a computação foi distribuída entre clientes (geralmente computadores pessoais), e servidores especializados. Por fim, a *Internet* expandiu o comércio global, também aumentando a complexidade dos sistemas e as vulnerabilidades a ataques (KAVIS, 2014).

A computação em nuvem combina as vantagens dos *mainframes*, sistemas cliente-servidor, e da *Internet*. Quando utilizada de forma correta, pode prover controle centralizado e governança, oferecendo ao mesmo tempo recursos de computação escaláveis com um modelo de pagamento conforme o uso, semelhante à cobrança de serviços públicos (KAVIS, 2014).

Contudo, a computação em nuvem não só beneficia as empresas, mas também oferece oportunidades para criminosos cibernéticos (KAVIS, 2014).

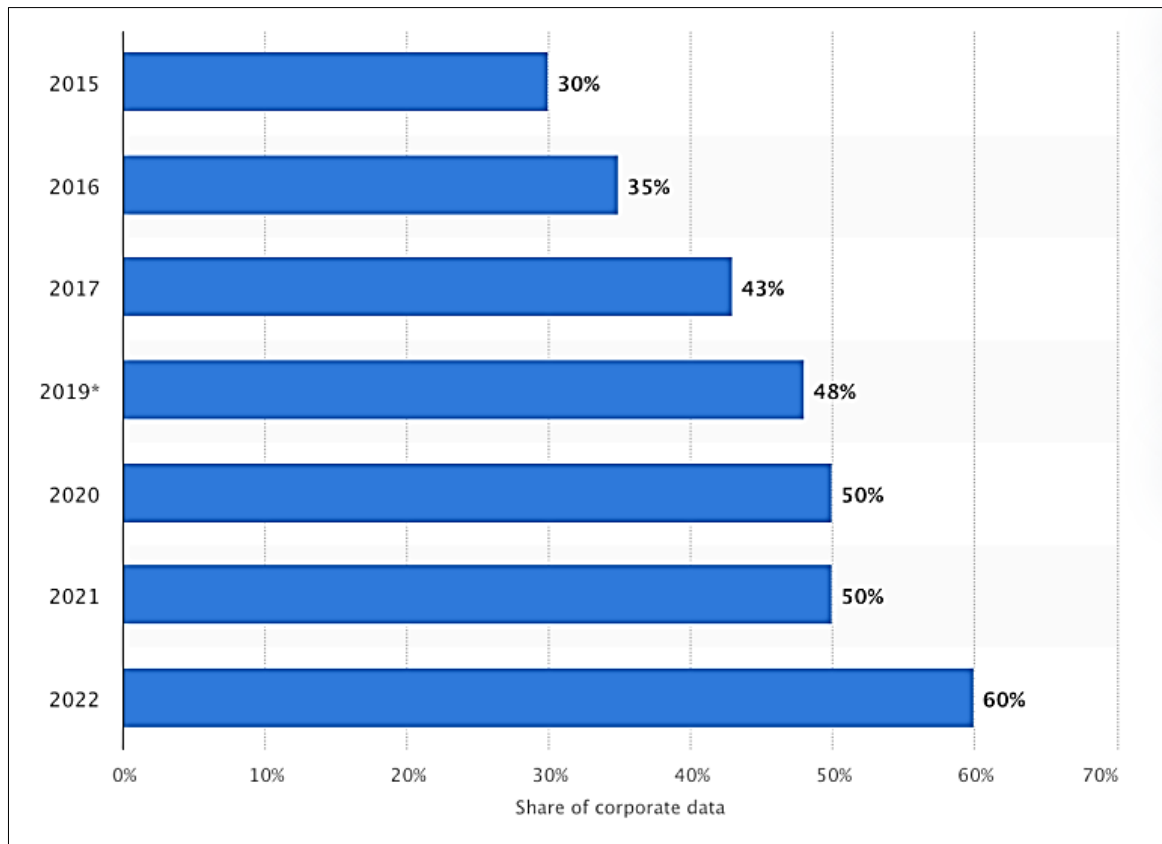
Segundo Kavis (2014), isso se deve a dois motivos principais:

- A tecnologia de nuvem ainda está em estágio inicial de desenvolvimento e carece de padrões estabelecidos. A escassez de engenheiros com experiência prática em segurança de aplicativos na nuvem contribui para a implementação de muitos serviços sem os controles e a segurança necessários;
- Os provedores de nuvem se tornam alvos atraentes, hospedando dados e recursos computacionais de várias empresas. Embora os provedores de nuvem ofereçam segurança de perímetro robusta, cabe às empresas que utilizam esses serviços construir níveis adequados de segurança para seus aplicativos.

Por exemplo, um fornecedor de serviços de *Infrastructure as a Service*, Infraestrutura como Serviço (IaaS) na nuvem, como a *Amazon Web Services*, Serviços de Rede da Amazon (AWS), conta com *data centers* altamente seguros e fornece orientações técnicas para desenvolver serviços com alta segurança em sua plataforma. Além disso, disponibiliza um conjunto de *Application Programming Interfaces*, Interfaces de Programação de Aplicativos (APIs), que simplificam o *design* com foco na segurança. Contudo, a responsabilidade de criptografar os dados, gerenciar chaves, implementar políticas robustas de senhas, dentre outras tarefas, recai sobre os arquitetos que estão construindo o *software* na AWS (KAVIS, 2014).

O problema da segurança de dados na nuvem é considerado cada vez mais relevante: a proporção de dados empresariais armazenados na nuvem aumentou de 30% em 2015 para 60% até 2022, e prevê-se que esta tendência continue a aumentar, como pode ser observado na Figura 1. (STATISTA, 2023).

Figura 1: Percentagem de dados empresariais armazenados na nuvem em organizações de todo o mundo de 2015 a 2022



Fonte: STATISTA, 2023a

1.1 Justificativa e questão de pesquisa

Esta pesquisa justifica-se pela crescente adoção da computação em nuvem e pela necessidade de implementar medidas de segurança eficazes. A questão de pesquisa é: Como implementar medidas de segurança no armazenamento de arquivos em nuvem com o Microsoft Azure?

1.2 Objetivo geral

- Implementar práticas de segurança em sistemas de armazenamento em nuvem

1.3 Objetivos específicos

- Conhecer as tecnologias de segurança mais utilizadas na computação em nuvem;
- Conhecer os recursos de segurança disponíveis na plataforma Azure;
- Implementar um sistema de arquivos com técnicas de criptografia de dados em repouso e em trânsito;
- Hospedar a aplicação dentro do serviço de computação em nuvem Azure;

1.4 Metodologia

Esta pesquisa constitui um resumo de assunto, pois é embasada em materiais pré-existentes para delinear a sistematização da segurança computacional e da computação em nuvem.

Quanto aos seus objetivos, a pesquisa é explicativa, porque seu intuito se restringe a compreender técnicas de segurança.

E quanto aos procedimentos técnicos, a pesquisa é experimental, pois consiste em implementar por conta própria as tecnologias estudadas.

1.5 Estrutura da monografia

No Capítulo 1, são apresentados o contexto e a relevância do tema da monografia, estabelecendo a justificativa e a questão de pesquisa. São definidos o objetivo geral e os objetivos específicos do estudo, além da metodologia utilizada para a realização da pesquisa.

No Capítulo 2, são abordados os princípios fundamentais de segurança na computação. São discutidos os pilares de segurança, as ferramentas criptográficas, os métodos de autenticação e os mecanismos de controle de acesso.

No Capítulo 3, a computação em nuvem é explorada em profundidade. São discutidas as motivações para a adoção da nuvem, as dificuldades de implementação, os diferentes tipos de nuvem e serviços, e as regiões e zonas de disponibilidade.

O Capítulo 4 detalha a implementação de um sistema de gerenciamento de arquivos utilizando a plataforma Azure. A escolha do serviço de armazenamento é explicada, seguida pela implementação do Azure Blob *Storage*.

No Capítulo 5, são apresentados os testes realizados sobre o sistema implementado. O capítulo inclui testes de registro de conta, autenticação, autorização e criptografia.

O Capítulo 6 oferece uma síntese dos resultados alcançados e discute as implicações da pesquisa. São apresentadas sugestões de trabalhos futuros que podem expandir ou aprofundar o estudo realizado.

2 PRINCÍPIOS DE SEGURANÇA

Neste capítulo, são abordados os fundamentos da segurança computacional, começando pelos seus objetivos principais, passando pelas técnicas de criptografia e, por fim, abordando os métodos de autenticação e controle de acesso.

2.1 Pilares de Segurança

A segurança de computadores é considerada essencial no âmbito da computação em nuvem, e é normalmente implementada através da tríade Confidencialidade, Integridade e Disponibilidade (CID). A confidencialidade engloba a não revelação de informações privadas a indivíduos não autorizados, enquanto a integridade garante que informações e programas só sejam alterados de maneira autorizada. A disponibilidade assegura que os sistemas funcionem prontamente, sem negação de serviço a usuários autorizados (STALLINGS, 2014).

Além da tríade CID, são consideradas importantes a autenticidade, garantindo a validade e verificabilidade das informações; e a determinação de responsabilidade, exigindo que as ações sejam rastreadas e atribuídas unicamente a uma entidade (STALLINGS, 2014).

2.2 Ferramentas Criptográficas

A criptografia é uma técnica para proteger a comunicação e o armazenamento de dados por meio da transformação de informações em formato ilegível para aqueles que não possuam a(s) chave(s) adequada(s). Na computação em nuvem, essa técnica é essencial para a segurança de dados sensíveis em trânsito e em repouso (STALLINGS, 2014).

A informação original, não criptografada, é denominada como “texto às claras” antes de qualquer processo de cifração. A transformação desse texto ocorre por meio de um algoritmo de cifração, resultando no texto cifrado. Essa transformação é reversível apenas com o uso da chave secreta adequada (STALLINGS, 2014).

Segundo Stallings (2014), as técnicas de cifração mais comuns são: criptografia simétrica, criptografia assimétrica e funções de *hash*.

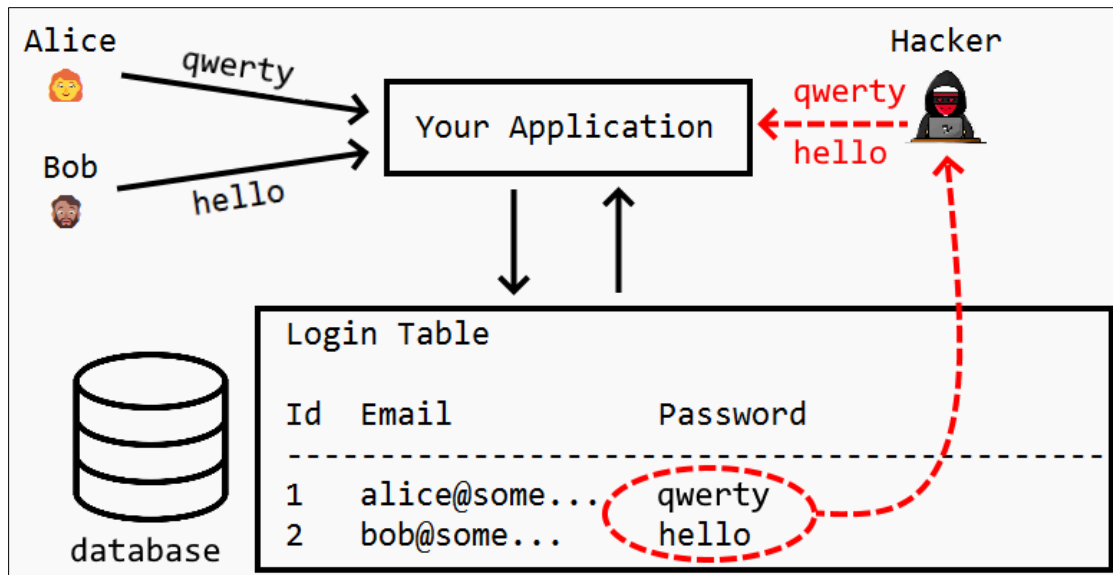
A cifração simétrica é baseada no uso de uma única chave para cifrar e decifrar informações. A simplicidade dessa abordagem é uma de suas principais vantagens, permitindo uma rápida

implementação e eficiência no processamento de grandes volumes de dados. A confidencialidade é mantida pela exclusividade da chave compartilhada entre as entidades autorizadas. Os dois algoritmos de cifração simétrica mais conhecidos são o *Advanced Encryption Standard*, Padrão Avançado de Criptografia (AES), e o *Data Encryption Standard*, Padrão de Encipção de Dados (DES).

A cifração assimétrica utiliza um par de chaves, uma pública e uma privada, para cifrar e decifrar dados, respectivamente. A chave pública é compartilhada amplamente, enquanto a chave privada permanece em posse exclusiva do destinatário. O processo de cifração assimétrica se inicia com a obtenção da chave pública do destinatário. O remetente utiliza essa chave para cifrar a mensagem, gerando um texto cifrado. A decifração é realizada pelo destinatário com sua chave privada correspondente. A vantagem principal deste método é a distribuição segura da chave pública, sem a necessidade de compartilhar a chave privada. Os dois algoritmos de cifração assimétrica mais conhecidos são o Rivest-Shamir-Adleman (RSA), e o *Elliptic Curve Cryptography*, Criptografia de Curva Elíptica (ECC) (STALLINGS, 2014).

Uma função *hash* é um algoritmo que mapeia dados de entrada de comprimento variável para valores de saída de comprimento fixo e de pequeno tamanho, geralmente uma sequência de caracteres alfanuméricos. A saída, conhecida como *hash*, é uma representação determinística (para a mesma entrada, o mesmo *hash* sempre será gerado) e não pode ser revertido novamente para os dados de entrada, diferentemente dos métodos de criptografia supracitados. Assim, funções de *hash* são consideradas úteis para aplicações relacionadas a autenticação, possibilitando o armazenamento do *hash* de uma senha no lugar do seu texto as claras ou de uma cifra reversível. Um usuário é autenticado somente se sua senha digitada for transformada no mesmo *hash* armazenado, conforme a Figura 2.

Figura 2: O uso de funções *hash* no armazenamento de senhas



Fonte: STALLINGS, 2014

O algoritmo de *hash* mais conhecido é o *Secure Hash Algorithm*, Algoritmo Seguro de Hash (SHA), que possui diversas versões aprimoradas em uso no mercado, como o *Secure Hash Algorithm-256*, Algoritmo Seguro de Hash-256 (SHA-256), o *Secure Hash Algorithm-384*, Algoritmo Seguro de Hash-384 (SHA-384), e o *Secure Hash Algorithm-512*, Algoritmo Seguro de Hash-512 (SHA-512) (STALLINGS, 2014).

Segundo Kavis (2014), dois conceitos essenciais sobre a criptografia no contexto da computação em nuvem são:

- a criptografia *at-rest*, em repouso: refere-se à prática de proteger dados enquanto estão sendo armazenados em dispositivos de armazenamento.
- a criptografia *in-transit*, em trânsito: refere-se à prática de proteger os dados enquanto estão em movimento, durante sua transferência entre dispositivos.

Existem diversas formas de implementar as criptografias *at-rest* e *in-transit*. Os dados podem ser criptografados antes da transmissão e armazenados em seu estado criptografado. O sistema de arquivos ou a estrutura de pastas em que os dados são armazenados pode ser criptografada. Quando os arquivos são acessados, eles podem ser protegidos por senha e exigir uma chave para serem descriptografados (KAVIS, 2014).

Também é possível implementar a criptografia *in-transit* através do uso de protocolos como o *Secure Sockets Layer*, Camada de Soquete Seguro (SSL)/ *Transport Layer Security*, Segurança

da Camada de Transporte (TLS), ou utilizando a implementação de criptografia de uma *Virtual Private Network*, Rede Virtual Particular (VPN). (STALLINGS, 2014).

Para a computação em nuvem, também é importante considerar a distribuição de chaves. Chaves associadas a usuários ou dispositivos devem ser trocadas regularmente, e de forma automatizada, para garantir a segurança (KAVIS, 2014).

2.3 Autenticação

A autenticação garante que apenas os usuários com identidade verificada tenham acesso a recursos sensíveis, sendo essencial para a segurança da computação em nuvem e é uma das prioridades. Os métodos de autenticação variam em complexidade e segurança, e a escolha adequada depende da sensibilidade dos dados e dos requisitos específicos de segurança. A abordagem comumente adotada envolve a combinação de diferentes meios para formar um sistema robusto (STALLINGS, 2014).

Para Stallings (2014), os métodos de autenticação mais usados são:

- Autenticação baseada em conhecimento: senhas e *Personal Identification Numbers*, Números de Identificação Pessoal (PINs) são exemplos típicos. No entanto, a fragilidade desse método reside em sua suscetibilidade a ataques de força bruta e a problemas associados à gestão de senhas, como reutilização e esquecimento;
- Autenticação baseada em posse: a autenticação baseada na posse de um objeto físico, como *tokens* de autenticação ou cartões inteligentes acrescenta uma camada adicional de segurança. Esses dispositivos geram códigos temporários ou utilizam chaves criptográficas para autenticar usuários. No entanto, a gestão e a possível perda desses dispositivos podem representar desafios significativos;
- Autenticação biométrica estática: baseia-se em características físicas estáticas do usuário. Impressões digitais, varreduras de retina e reconhecimento facial são exemplos comuns. Embora ofereçam uma forma única e intrínseca de identificação, questões como a privacidade do indivíduo e a possibilidade de falsificação devem ser observadas;
- Autenticação biométrica dinâmica: a biometria dinâmica considera ações específicas do usuário, como a assinatura ou a voz. Esses métodos estão em constante evolução devido à melhoria na tecnologia de reconhecimento. No entanto, as variações individuais podem influenciar na eficácia desses métodos.

A autenticação remota é considerada mais complexa que a local, devido à exposição associada à transmissão de informações sensíveis pela rede. Os protocolos projetados para este propósito devem garantir a confidencialidade, integridade e autenticidade dos dados transmitidos e, ao mesmo tempo resistir a ataques como a interceptação de dados e a tentativa de *login* por força bruta (STALLINGS, 2014).

O protocolo *Hypertext Transfer Protocol Secure*, Protocolo de Transferência de Hipertexto Seguro (HTTPS) é considerado eficiente neste âmbito. Ele é uma extensão do *Hypertext Transfer Protocol*, Protocolo de Transferência de Hipertexto (HTTP), projetado para garantir a segurança da comunicação pela *Internet*. A autenticação remota por senha através de HTTPS possibilita o uso de criptografia SSL/TLS para proteger a transmissão de dados (STALLINGS, 2014).

2.4 Controle de Acesso

O controle de acesso é um componente importante na segurança da computação em nuvem, assegurando que apenas usuários autorizados tenham acesso a recursos e dados sensíveis (STALLINGS, 2014).

Os princípios de controle de acesso na nuvem baseiam-se na tríade: Autenticação, Autorização e Auditoria (AAA). A identidade dos usuários é verificada, os privilégios de acesso são concedidos com base nas necessidades, e as atividades são registradas para análise e monitoramento (STALLINGS, 2014).

Segundo Stallings (2014), as principais políticas de controle de acesso são:

- *Discretionary Access Control*, Controle de Acesso Discricionário (DAC): o DAC atribui aos usuários o controle sobre os objetos que possuem, permitindo a eles determinarem quem pode acessar esses objetos e com que permissões. Este controle é feito através de uma *flag* concedida ao proprietário do objeto. Em ambientes de nuvem, o DAC é frequentemente aplicado a sistemas de arquivos e dados individuais, permitindo que os proprietários decidam sobre o acesso aos seus recursos;
- *Mandatory Access Control*, Controle de Acesso Mandatário (MAC): o MAC impõe políticas definidas pela administração do sistema, limitando o controle que os usuários individuais têm sobre a segurança dos objetos. Em ambientes de nuvem, o MAC é útil para reforçar políticas de segurança consistentes em larga escala, especialmente em organizações com requisitos rigorosos de conformidade;

- *Role-Based Access Control*, Controle de Acesso Baseado em Papéis (RBAC): O RBAC é um modelo que atribui permissões com base nas funções dos usuários dentro da organização. Em ambientes de nuvem, isso simplifica a administração de políticas de acesso, permitindo a designação de funções específicas, como administrador ou usuário final, com conjuntos predefinidos de permissões associadas.

3 COMPUTAÇÃO EM NUVEM

Neste capítulo, são abordados os motivos da migração para a computação em nuvem, as vantagens e desvantagens da computação em nuvem, e o estado atual da indústria.

3.1 Motivação

A computação em nuvem modificou a forma com que empresas e indivíduos lidam com o *hardware*, disponibilizando o acesso a equipamentos de mais alta *performance* para empresas pequenas. Para empresas grandes a computação em nuvem pode levar a uma redução dos custos de manutenção dos equipamentos durante o tempo ocioso. Assim, a migração para a nuvem é considerada inevitável (OPUS SOFTWARE, 2015).

Para Opus Software (2015) os pontos que têm levado as empresas para a migração para a nuvem são:

- Economia de custos: a ausência da necessidade de investimentos significativos em *hardware* é uma das principais razões para a adoção da computação em nuvem. Em vez de adquirir servidores, as empresas podem alugar recursos na nuvem, reduzindo os custos operacionais;
- Escalabilidade e flexibilidade: a capacidade de alocar mais ou menos recursos de acordo com a demanda é uma das maiores vantagens da computação em nuvem. Isso permite que empresas se adaptem rapidamente a mudanças no volume de trabalho, sem a necessidade de investir em recursos permanentes que podem ser subutilizados. Isso também permite que as empresas paguem apenas pelo que usam (modelo “*pay-per-use*”), reduzindo os custos;
- Agilidade e eficiência: a capacidade de acessar o *software* hospedado na nuvem em qualquer lugar, a qualquer momento, aumenta a eficiência operacional. Além disso, a implementação de novos recursos e atualizações é mais ágil na nuvem, permitindo uma vantagem competitiva;
- Alta disponibilidade e confiabilidade: a nuvem possui alto grau de redundância nos servidores e *datacenters*, de modo que dificilmente todos estarão indisponíveis ao mesmo tempo. Isso oferece elevada disponibilidade e confiabilidade;
- Suporte técnico: os maiores provedores de nuvem oferecem suporte técnico robusto;

- Acessível a pequenos negócios: pequenos negócios podem se beneficiar da computação em nuvem devido à ausência de investimentos iniciais em *hardware*; e os baixos custos fixos proporcionados pelo modelo “*pay-per-use*”.

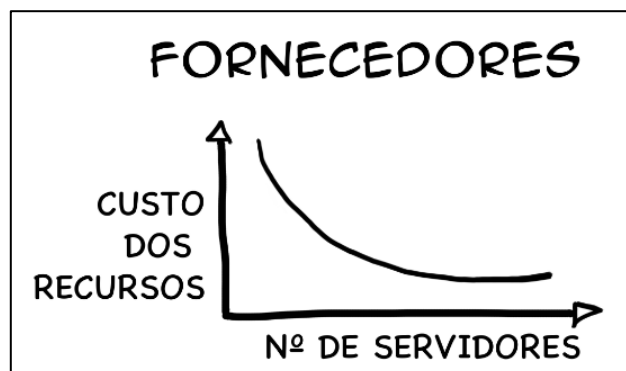
Opus Software (2015) destaca que, a computação em nuvem é considerada inevitável pelos seguintes motivos:

- Favorece a inovação: a computação em nuvem possibilita a experimentação, por permitir que empresas testem e desenvolvam novas ideias e tecnologias sem a necessidade de grandes investimentos iniciais;
- Baixo custo em caso de falha: a computação em nuvem também permite minimizar perdas em casos de falhas ou erros, pois não há investimentos em infraestrutura que não será mais utilizada;
- Alta agilidade em casos de sucesso: quando uma iniciativa é bem-sucedida, a flexibilidade da computação em nuvem permite ampliá-la rapidamente ao alocar mais recursos.

Outro fator relevante é a economia de escala, que descreve a dinâmica da redução de custos quanto maior o número de empresas de computação em nuvem e de clientes (OPUS SOFTWARE, 2015).

Do lado do fornecedor, quanto mais clientes, o fornecedor precisa de mais recursos como energia elétrica e *hardware*. Torna-se possível negociar preços baixos ao comprar uma grande quantidade desses recursos, e a concorrência influencia as empresas a repassarem os preços baixos aos clientes, conforme mostra a Figura 3. Além disso, a concorrência influencia a otimização, que também gera uma redução de custos repassada aos clientes (OPUS SOFTWARE, 2015).

Figura 3: Economia de Escala



Fonte: OPUS SOFTWARE, 2015

3.2 Dificuldades de Implementação

Mesmo com as vantagens supracitadas, a computação em nuvem ainda enfrenta muitas dificuldades de adoção. Para Opus Software (2015), elas incluem:

- **Integração de sistemas:** um dos maiores desafios na migração para a nuvem é a integração de sistemas legados. Muitas empresas possuem infraestruturas de Tecnologia de Informação (TI) antigas e a transição para a nuvem envolve a integração desses sistemas com os novos, o que pode ser altamente complexo;
- **Aspectos legais:** questões relacionadas à conformidade legal, privacidade de dados e regulamentos governamentais são cruciais. Os requisitos legais variam de acordo com a região e o setor, tornando essencial compreender e garantir que a migração para a nuvem esteja em conformidade com todas as normativas aplicáveis;
- **Falta de compreensão do termo “nuvem”:** para muitos indivíduos e até mesmo profissionais de empresas, o conceito de computação em nuvem pode ser abstrato e complexo. Isso pode resultar em resistência ou falta de compreensão sobre os benefícios e desafios da migração para a nuvem;
- **Segurança:** a segurança dos dados é uma preocupação constante ao considerar a nuvem. A confiança na segurança dos dados armazenados e transmitidos na nuvem é um ponto de preocupação, pois a perda de controle físico sobre a infraestrutura pode gerar incertezas sobre a proteção dos dados;
- **Resistência dos gestores:** a resistência dos gestores e líderes de uma organização pode ser um obstáculo na implementação da computação em nuvem. A transição para a nuvem pode em muitas vezes significar perda de poderes para um gestor, o que leva a uma postura conservadora em relação à adoção da nuvem;
- **Banda de comunicação:** A dependência de uma conexão de *Internet* estável e de alta velocidade é vital na computação em nuvem. Limitações na largura de banda podem prejudicar o desempenho e a acessibilidade, especialmente para aplicações que demandem transferência de dados em tempo real;
- **Complexidade:** a migração para a nuvem pode ser um processo complexo. A seleção do tipo de nuvem, a escolha dos serviços, a configuração e a migração de dados requerem

expertise técnica e estratégica, tornando o processo desafiador para muitas organizações;

- Custos enterrados: as organizações que investiram pesadamente em infraestrutura local enfrentam o dilema de abandonar esses recursos para investir na nuvem. Muitas vezes, a transição para a nuvem é vista como um custo adicional em vez de uma economia futura, pois os custos iniciais da migração podem ser consideráveis. Além disso, a interrupção das operações enquanto a transição é realizada é uma preocupação, afetando a continuidade dos negócios.

3.3 Tipos de Nuvem

Há uma variedade de modelos de computação em nuvem para atender às necessidades específicas das organizações. Segundo Opus Software (2015), os principais tipos são:

- Nuvem pública: o modelo no qual os serviços e infraestrutura são fornecidos por provedores de nuvem externos e compartilhados entre várias organizações. Esse modelo oferece escalabilidade, flexibilidade e redução de custos, uma vez que elimina a necessidade de investimentos em infraestrutura local. Os recursos são proporcionados de forma elástica, permitindo que as organizações paguem apenas pelos serviços que consomem;
- Nuvem privada: oferece serviços e infraestrutura dedicados exclusivamente a uma única organização. Dentro do contexto da nuvem privada, duas abordagens comuns são amplamente adotadas:
 - Na rede interna de empresa: a infraestrutura de nuvem é implantada localmente nas instalações da empresa, proporcionando controle total sobre os recursos e dados. Essa abordagem é preferida por organizações que desejam manter total controle sobre sua infraestrutura, especialmente em setores no qual os requisitos de conformidade e regulamentações são rigorosos.
 - *Virtual Private Cloud*, Nuvem Privada Virtual (VPC): é uma implementação de nuvem privada que utiliza a infraestrutura de nuvem pública, mas com isolamento lógico dedicado a uma única organização. Isso combina os benefícios da nuvem privada, como controle e segurança, com a escalabilidade e eficiência operacional da nuvem pública.

- Nuvem híbrida: A nuvem híbrida é uma combinação de nuvem pública e privada, permitindo a movimentação de dados entre esses ambientes. Essa abordagem oferece flexibilidade, permitindo que as organizações mantenham dados sensíveis na nuvem privada, enquanto utilizam a nuvem pública para cargas de trabalho mais dinâmicas e escaláveis.

3.4 Tipos de Serviço

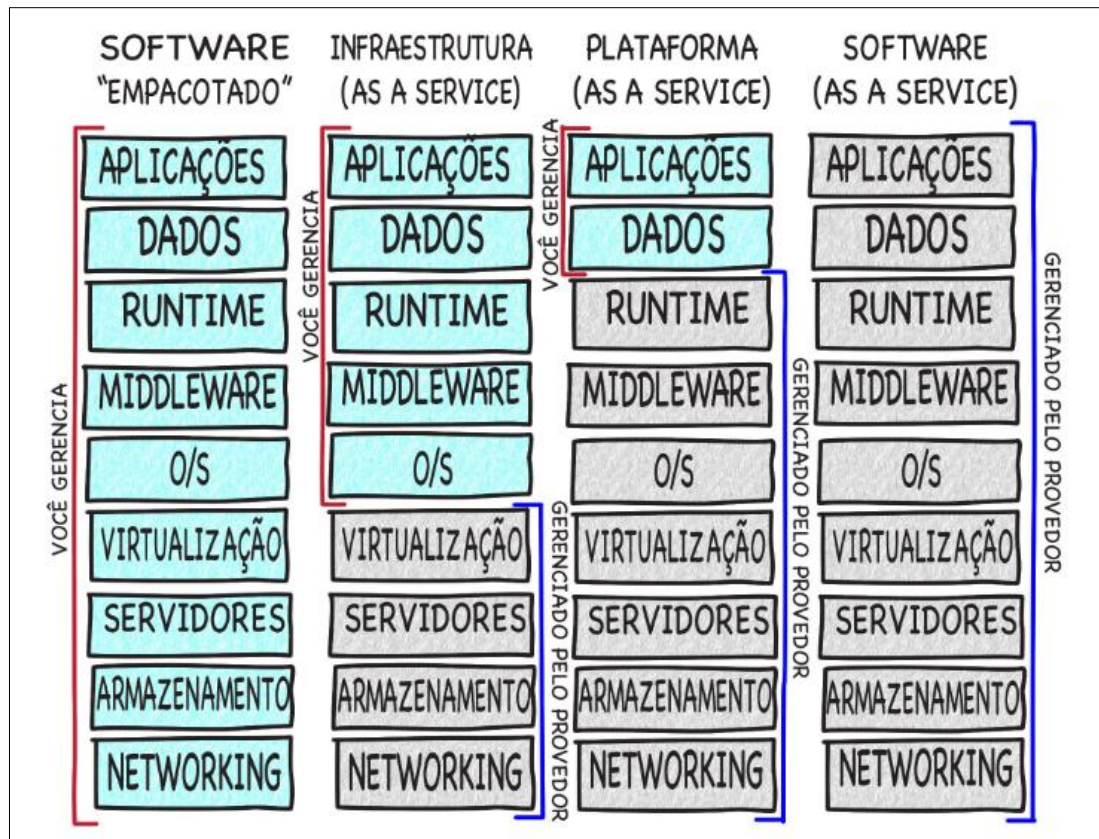
A indústria proporciona diversos tipos de serviço de computação em nuvem, que se diferenciam principalmente pelo grau de controle proporcionado aos usuários sob os componentes virtualizados. Para o usuário, quanto maior for o nível de controle concedido, maiores se tornam as suas responsabilidades, de forma que assumir mais controle que o necessário pode gerar dificuldades evitáveis (OPUS SOFTWARE, 2015).

Para Opus Software (2015), os principais tipos de serviço na computação em nuvem incluem:

- *Infrastructure as a Service*, Infraestrutura como Serviço (IaaS): o usuário gerencia o sistema operacional, o espaço de armazenamento, e as aplicações;
- *Platform as a Service*, Plataforma como Serviço (PaaS): o usuário somente gerencia as aplicações;
- *Software as a Service*, Software como Serviço (SaaS): o usuário acessa um *software* do provedor.

As diferentes responsabilidades do provedor e do usuário para cada tipo de serviço são ilustradas na Figura 4.

Figura 4: Tipos de Serviço



Fonte: OPUS SOFTWARE, 2015

3.5 Regiões e Zonas de Disponibilidade

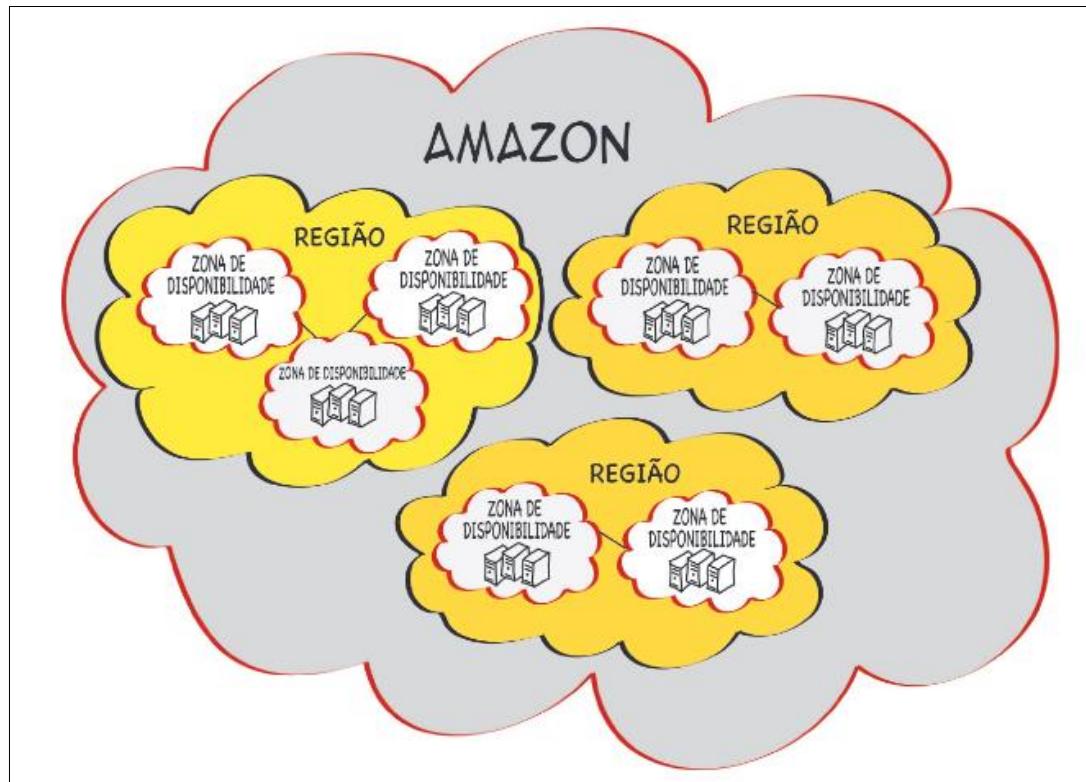
Cada provedor de computação em nuvem possui suas próprias terminologias para descrever a estrutura global dos seus serviços. Devido à similaridade entre essas estruturas, o estudo do modelo do provedor AWS é considerado suficiente para compreender os demais modelos (OPUS SOFTWARE, 2015).

O AWS é organizado em regiões e zonas de disponibilidade, de forma a proporcionar alta disponibilidade, redundância e a capacidade de recuperação de desastres. Uma região refere-se a uma área geográfica específica onde um provedor de nuvem possui *data centers*, e cada região é composta por uma ou mais zonas de disponibilidade. Cada região é projetada para ser independente de outras regiões (OPUS SOFTWARE, 2015).

Dentro de cada região, as zonas de disponibilidade representam locais físicos separados, com infraestrutura própria e fornecendo redundância adicional. Essas zonas são conectadas por

redes de baixa latência, mas são projetadas para serem isoladas umas das outras, conforme pode ser observado na Figura 5 (OPUS SOFTWARE, 2015).

Figura 5: Regiões e Zonas de Disponibilidade



Fonte: OPUS SOFTWARE, 2015

3.6 Provedores

Os três principais provedores de nuvem são: AWS, Microsoft Azure, e Google Cloud Platform (OPUS SOFTWARE, 2015).

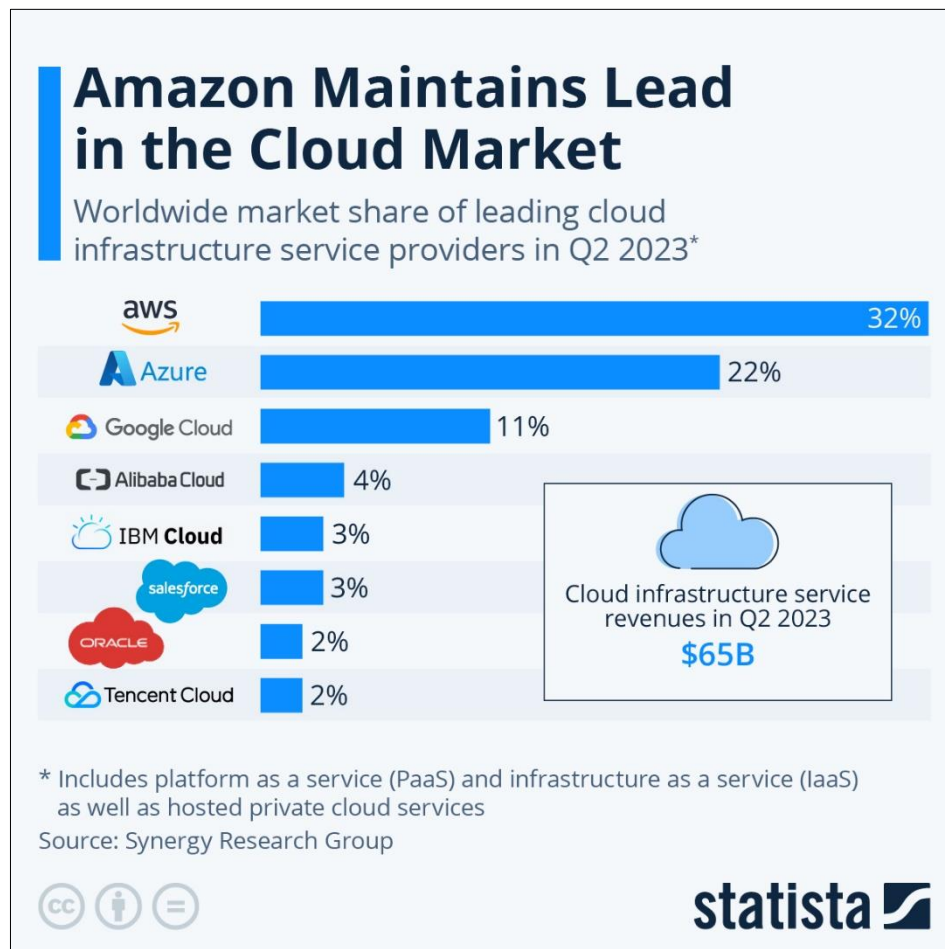
A AWS é pioneira no mercado de computação em nuvem, e oferece serviços como banco de dados, análise de dados, *machine learning*, dentre outros. Está presente globalmente com uma extensa rede de *data centers* (AMAZON, 2023).

O Microsoft Azure é uma plataforma de nuvem da Microsoft que também oferece uma variedade de serviços, como soluções de inteligência artificial. Um dos seus diferenciais é a integração com os produtos Microsoft, como o Windows Server e o Active Directory (MICROSOFT, 2023).

A Google Cloud Platform da Google, destaca-se por sua especialização em serviços de dados e aprendizado de máquina. Oferece uma infraestrutura global e serviços que se alinham à filosofia de inovação da Google (GOOGLE, 2023).

Conforme o ilustrado na Figura 6, a AWS controla a maior parte do mercado, seguida pela Azure, e pelo Google Cloud.

Figura 6: *Market shares* dos principais provedores de computação em nuvem



Fonte: STATISTA, 2023b

4 IMPLEMENTAÇÃO DE SISTEMA DE GERENCIAMENTO DE ARQUIVOS

Para mostrar as tecnologias de segurança em nuvem em uso no mercado, foi escolhida a plataforma Microsoft Azure para a implementação de um sistema de gerenciamento de arquivos. Esta decisão se baseia de que segundo Microsoft (2024a), essa plataforma oferece robustez nos recursos de segurança, além de sua ampla adoção e flexibilidade de implementação.

4.1 Escolha do Serviço de Armazenamento

Segundo Microsoft (2024a), as seguintes soluções para armazenamento de dados em nuvem estão disponíveis no Azure:

- *Azure Blob Storage*: um serviço especializado em armazenar *Binary Large Objects*, Objetos Binários Grandes (BLOBs), que consistem em unidades de armazenamento de dados não estruturados, como vídeos, áudio, imagens, documentos, etc. O navegador pode ser usado para exibir arquivos diretamente, e bibliotecas são disponibilizadas para .NET, Java, Node.js, Python, PHP e Ruby. O serviço pode ser utilizado através de *Uniform Resource Locators*, Localizadores de Recurso Uniforme (URLs), da API *Azure Storage Representational State Transfer*, Transferência de Estado Representacional (REST), e dos *softwares* Azure PowerShell, *Azure Command Line Interface*, Interface de Linha de Comando (CLI), ou *Azure Storage Client Library*;
- *Azure File Storage*: serviço para a transferência de arquivos por meio dos protocolos *Network File System*, Sistema de Arquivos de Rede (NFS) e *Server Message Block*, Blocos de Mensagem de Servidor (SMB), funcionando como se estivessem sendo utilizados em uma rede local;
- *Azure Disk Storage*: oferece máquinas virtuais escalonáveis, com possibilidade de discos *Solid State Drive*, Unidade de Estado Sólido (SSD) e *Hard Disc Drive*, Unidade de Disco Rígido (HDD);
- *Azure Table Storage*: permite que grandes *datasets* sejam salvos como pares de valores-chave no NoSQL;
- *Azure Queue Storage*: Para facilitar a comunicação entre componentes de aplicações executados em *Personal Computers*, Computadores Pessoais (PCs), dispositivos

móveis, servidores em nuvem ou locais, o Azure *Queue Storage* oferece processamento assíncrono de mensagens.

O serviço escolhido nesse trabalho foi Azure *Blob Storage*, pois o sistema de gerenciamento de arquivos deve trabalhar com arquivos como imagens e documentos, que podem ser armazenados como BLOBs.

4.2 Implementação do Azure *Blob Storage*

Segundo Microsoft (2024a), há vários tipos de armazenamento no Azure *Blob Storage*:

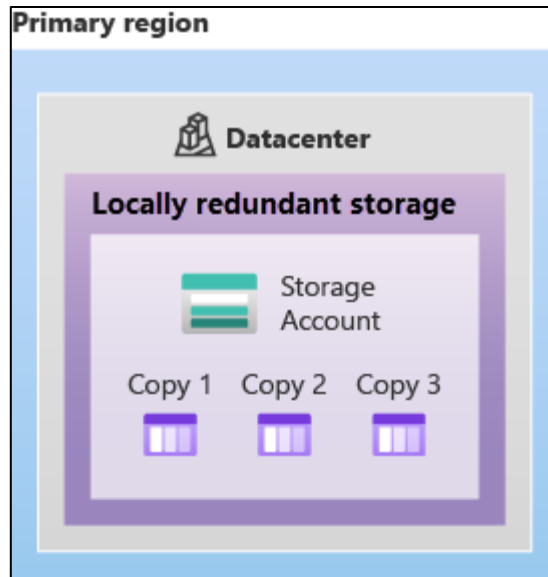
- *Hot*: otimizado para dados que são acessados regularmente. Tem os menores custos de acesso, mas os seus custos de armazenamento são os mais altos, e desta forma possui melhor custo-benefício apenas para dados acessados com frequência, como imagens de um *site*, por exemplo;
- *Cold*: concebido para dados que não são acessados com frequência, e são retidos por um período mínimo de 30 dias, como recibos, por exemplo;
- *Archive*: projetado para *backups* e outros materiais de acesso pouco frequente, mantidos por um período mínimo de 180 dias.

O serviço tipo escolhido nesse trabalho foi *Hot*, pois o sistema deve trabalhar com arquivos diversificados como imagens e documentos.

Segundo Microsoft (2024a), o Azure também permite diferentes tipos de redundância para os dados:

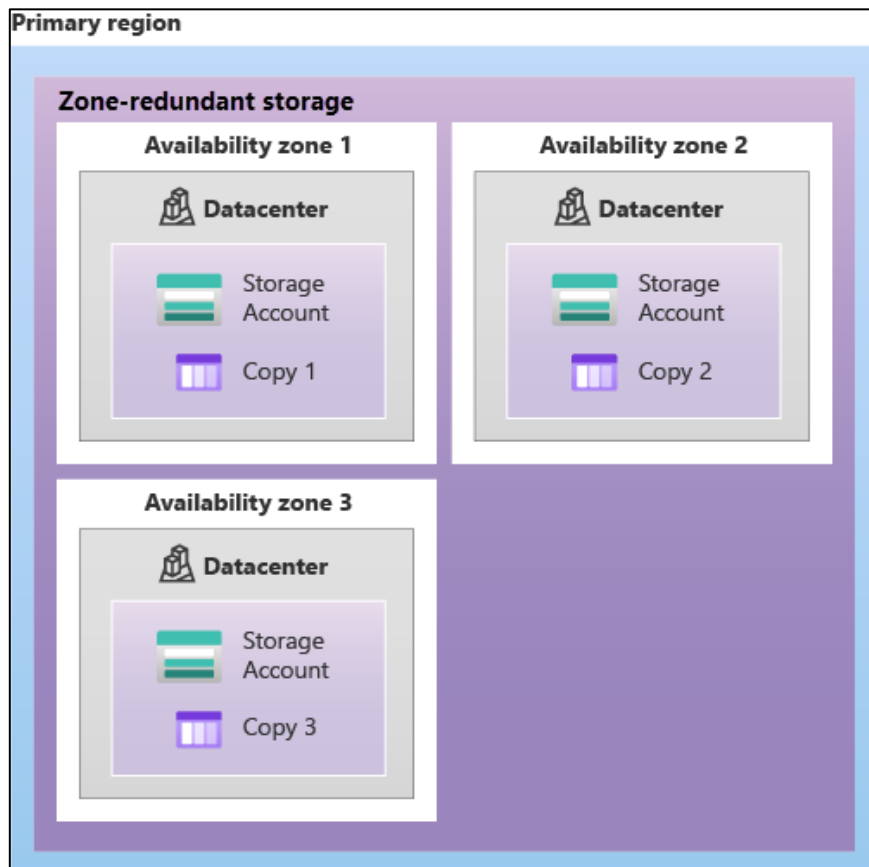
- *Locally Redundant Storage*, Armazenagem Localmente Redundante (LRS): os dados são replicados três vezes em um mesmo *datacenter*, conforme mostrado na Figura 7;
- *Zone Redundant Storage*, Armazenagem Redundante em Zonas (ZRS): os dados são replicados de forma síncrona entre três *data centers*, cada um em uma zona diferente, na região primária, conforme mostrado na Figura 8;
- Redundâncias em zonas secundárias: os dados são replicados em *data centers* de outras regiões.

Figura 7: Diagrama do LRS



Fonte: MICROSOFT, 2024a

Figura 8: Diagrama do ZRS



Fonte: MICROSOFT, 2024a

Por questões de custos, o serviço escolhido nesse trabalho foi o LRS.

As funcionalidades do serviço de armazenamento também dependem do modelo de pagamento, segundo Microsoft (2024a):

- *Standard*: o mais barato, com suporte a todas as opções já mencionadas nesse trabalho, exceto as extras presentes nas outras opções de pagamento;
- *Premium Block Blobs*: opção mais cara disponível apenas para *Blob Storage*, com suporte a baixa latência e elevadas taxas de transmissão de dados;
- *Premium File Shares*: opção mais cara disponível apenas para *Azure Files*, com suporte a alta *performance* e uso conjunto de tanto SMB quanto NFS.

Por questões de custos, o serviço escolhido foi o *Standard*.

Inicialmente, uma instância do Azure *Blob Storage* foi implementada através do *website* Azure Portal com acesso anônimo, sem autenticação, para que fosse verificado o seu funcionamento, conforme mostra as Figura 9 e 10.

Figura 9: Configuração do Azure *Blob Storage*

The screenshot displays the configuration interface for a new Azure Storage account. The 'Basics' tab is active, showing the following settings:

- Project details:**
 - Subscription: Azure subscription 1
 - Resource group: (New) TCC_Rafael
- Instance details:**
 - Storage account name: tccdorafael
 - Region: (South America) Brazil South
 - Performance: Standard (Selected)
 - Redundancy: Locally-redundant storage (LRS)

Navigation buttons at the bottom include 'Review', '< Previous', and 'Next : Advanced >'.

Fonte: Capturado pelo autor desse trabalho a partir de Azure, 2024.

Figura 10: Configuração do Azure Blob Storage

Basics **Advanced** Networking Data protection Encryption Tags Review

Security

Configure security settings that impact your storage account.

Require secure transfer for REST API operations

Allow enabling anonymous access on individual containers

Enable storage account key access

Default to Microsoft Entra authorization in the Azure portal

Minimum TLS version

Permitted scope for copy operations (preview)

Fonte: Capturado pelo autor desse trabalho a partir de Azure, 2024.

Para fim de testes, as outras configurações foram ajustadas para *default*. O Azure Blob Storage foi implementado, um *container* foi criado, e nele foi feito o *upload* de uma imagem através do Azure Portal, como mostra a Figura 11.

Figura 11: Upload para o Azure Blob Storage

Upload Change access level Refresh | Delete Change tier Acquire lease Break lease View snapshots ...

Authentication method: Access key (Switch to Microsoft Entra user account)
Location: rafael01

Search blobs by prefix (case-sensitive) Show deleted blobs

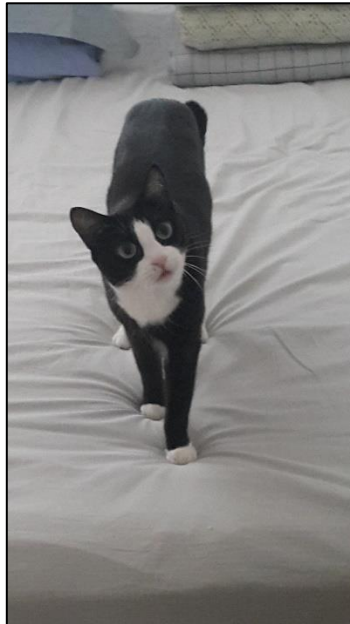
+ Add filter

Name	Modified	Access tier	Archive status	Blob type
<input checked="" type="checkbox"/> imagem.jpg	3/12/2024, 6:53:32 PM	Hot (Inferred)		Block blob

Fonte: Capturado pelo autor desse trabalho a partir de Azure, 2024.

Até então, era exibido no navegador a imagem que está na Figura 12, por meio do *link* <https://tccdorafael.blob.core.windows.net/rafael01/imagem.jpg>, que não está mais disponível, pois o acesso sem autenticação foi desabilitado.

Figura 12: Arquivo Hospedado no Azure Blob *Storage*



Fonte: Capturado pelo autor desse trabalho a partir de Azure, 2024.

4.3 Implementação da autenticação (fase 1)

Dentre os serviços de autenticação disponíveis no Microsoft Azure, foi escolhido o Azure *Active Directory, Diretório Ativo (AD), Business to Customer, Negócio para Cliente (B2C)*, um serviço projetado para que negócios possam autenticar e gerenciar as identidades dos seus clientes. O Azure AD B2C permite construir fluxos de usuário, em que é possível controlar como os clientes se registram, fazem *login*, e gerenciam os seus perfis através de experiências altamente customizáveis (Microsoft, 2024a).

O Azure AD B2C permite coletar atributos como o nome ou data de nascimento do cliente durante o registro. Ele também permite implementar diversos métodos de autenticação, como a autenticação multifator, em que um aplicativo autenticador no *smartphone* do cliente é usado durante o processo de autenticação. Também é possível configurar o Azure AD B2C para que

contas sociais de *websites* como o Facebook, Twitter ou LinkedIn sejam utilizados para a autenticação.

Uma instância do Azure AD B2C foi criada, conforme as Figuras 13 e 14:

Figura 13: Configuração do Azure AD B2C

The screenshot shows the 'Basics' step of the Azure AD B2C configuration wizard. At the top, there are three tabs: '* Basics' (selected), '* Configuration', and 'Review + create'. Below the tabs, a message states: 'Microsoft Entra ID and Azure AD B2C enable users to access applications published'. The main section is titled 'Tenant type'. A light blue information banner contains the text: 'Customers must own a paid license to create Microsoft Entra Workforce tenant.' Below this, the instruction 'Select a tenant type *' is followed by two radio button options: 'Microsoft Entra ID' (unselected) and 'Azure AD B2C' (selected). A link 'Help me choose...' is positioned below the 'Azure AD B2C' option. At the bottom of the wizard, there are three buttons: 'Review + create' (blue), '< Previous' (disabled), and 'Next : Configuration >' (disabled).

Fonte: Capturado pelo autor desse trabalho a partir de Azure, 2024.

Figura 14: Configuração do Azure AD B2C

The screenshot shows the 'Configuration' tab of the Azure AD B2C setup wizard. It includes the following sections and fields:

- Directory details:**
 - Organization name: Organização TCCRafael
 - Initial domain name: dominiotccrafael
 - Location: United States
 - Geographic location - United States (checked)
 - Note: The location selected above will determine the geographic location where Azure AD B2C will store availability and data residency.
- Subscription:**
 - Subscription: Azure for Students
 - Resource group: resource_group_TCCRafael (with a 'Create new' link below it)

Fonte: Capturado pelo autor desse trabalho a partir de Azure, 2024.

Inicialmente, não foi encontrada uma forma de conectar a instância Azure Blob *Storage* à instância Azure AD B2C pelo Azure Portal, impedindo a utilização da instância Azure AD B2C para autenticar usuários para a instância Azure Blob *Storage*. Foi feita uma consulta à documentação do Microsoft Azure, disponibilizada pela Microsoft (2024a), em busca de uma abordagem alternativa.

Como resultado da consulta, verificou-se que, segundo a Microsoft (2024a), tanto instâncias do Azure Blob *Storage*, quanto do Azure AD B2C, podem ser implementados com *endpoints*, pontos de conexão ao tráfego de rede. Eles existem em dois tipos:

- *Endpoint* público: Possui endereço de IP público, e pode ser acessado livremente.
- *Endpoint* privado: Possui endereço de IP privado, e pode ser acessado através de uma rede virtual.

Por questões de segurança, a abordagem escolhida foi conectar as instâncias através de uma rede virtual a partir de *endpoints* privados, e desabilitar o acesso público que foi usado nos testes iniciais desse trabalho.

4.4 Implementação de rede virtual

Foi implementada uma rede virtual conforme as Figuras 15 e 16, com as funcionalidades descritas segundo informações da Microsoft (2024a):

- Criptografia de rede virtual: ao estabelecer um túnel *Datagram Transport Layer Security*, Segurança da Camada de Transporte de Datagramas (DTLS), o serviço possibilita a criptografia e a decifração de dados na rede virtual. O túnel DTLS funciona através da troca de datagramas criptografados por chaves simétricas distribuídas por meio de criptografia assimétrica. Isso significa que, embora a comunicação entre as partes ocorra usando chaves simétricas para garantir eficiência e velocidade, as próprias chaves simétricas são trocadas de maneira segura usando criptografia assimétrica;
- Azure Bastion: um serviço PaaS que fornece acesso seguro via os protocolos *Remote Desktop Protocol*, Protocolo de *Desktop* Remoto (RDP) e *Secure Shell*, Shell Seguro (SSH) para máquinas virtuais diretamente através do portal do Azure. O acesso é feito por um endereço de *Internet Protocol*, Protocolo de Internet (IP) privado, e o Azure Bastion age como um *bastion host*, isolando o tráfego de dados do público e permitindo conexões apenas através de sessões seguras e autenticadas;
- Azure Firewall: um serviço *Firewall as a Service*, Firewall como Serviço (FWaaS). Por ser um *firewall* disponibilizado pela nuvem, possui vantagens em relação a *firewalls* implementados localmente, como a alta escalabilidade em função de demandas da rede. O Azure Firewall é completamente *stateful*, ou seja, mantém os estados das sessões da rede, e é capaz de reconhecer cada sessão de tráfego;
- Azure Distributed Denial-of-Service, Negação de Serviço Distribuída (DDoS) *Network Protection*: um serviço de defesa contra ataques DDoS, que protege as camadas 3 e 4 da rede.

Figura 15: Configuração de Rede Virtual

Home > Virtual networks >

Create virtual network ...

Basics Security IP addresses Tags Review + create

Enhance the security of your virtual network with these additional paid security services. [Learn more](#) ↗

Virtual network encryption

Enable Virtual network encryption to encrypt traffic traveling within the virtual network. Virtual machines must have accelerated networking enabled. Traffic to public IP addresses is not encrypted. [Learn more](#). ↗

Virtual network encryption

Azure Bastion

Azure Bastion is a paid service that provides secure RDP/SSH connectivity to your virtual machines over TLS. When you connect via Azure Bastion, your virtual machines do not need a public IP address. [Learn more](#). ↗

Enable Azure Bastion ⓘ

Azure Bastion host name

Azure Bastion public IP address * ▼
[Create a public IP address](#)

Fonte: Capturado pelo autor desse trabalho a partir de Azure, 2024.

Figura 16: Configuração de Rede Virtual

Azure Firewall

Azure Firewall is a managed cloud-based network security service that protects your Azure Virtual Network resources. [Learn more.](#)

Enable Azure Firewall

Azure Firewall name

Subnet name *

Tier *

Policy *
[Create new](#)

Azure Firewall public IP address *
[Create a public IP address](#)

Azure DDoS Network Protection

Azure DDoS Network Protection is a paid service that offers enhanced DDoS mitigation capabilities via adaptive tuning, attack notification, and telemetry to protect against the impacts of a DDoS attack for all protected resources within this virtual network. [Learn more.](#)

Enable Azure DDoS Network Protection

DDoS protection plan *
[Create a DDoS protection plan](#)

Fonte: Capturado pelo autor desse trabalho a partir de Azure, 2024.

Era desejado criar um espaço de endereços IPv6 para a rede virtual pela segurança, mas o *Azure Firewall* não suporta o IPv6 ainda, segundo Microsoft (2024a). Então, foi criado um espaço IPv4 conforme a Figura 17:

Figura 17: Configuração de Rede Virtual

Create virtual network ...

Basics Security **IP addresses** Tags Review + create

Configure your virtual network address space with the IPv4 and IPv6 addresses and subnets you need. [Learn more](#)

Define the address space of your virtual network with one or more IPv4 or IPv6 address ranges. Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the resource an IP address from the subnet. [Learn more](#)

Add IPv4 address space | ▾

10.0.0.0/16 🗑 Delete address space

10.0.0.0 /16

10.0.0.0 - 10.0.255.255 65.536 addresses

+ Add a subnet

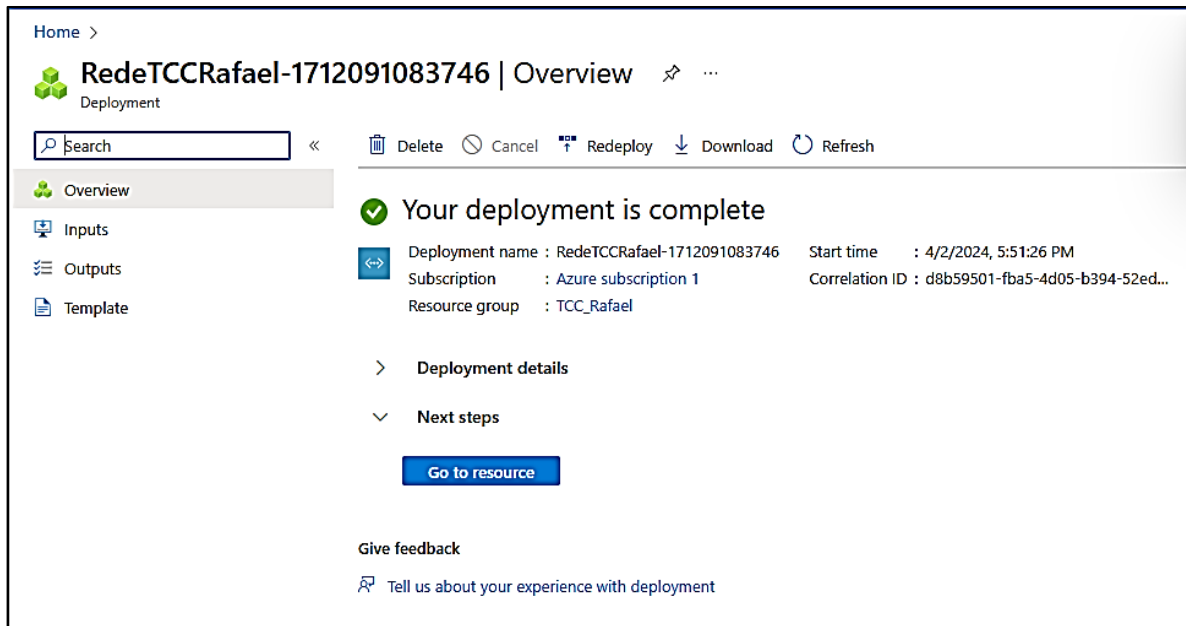
Subnets	IP address range	Size	NAT gateway
default	10.0.0.0 - 10.0.0.255	/24 (256 addresses)	- ✎ 🗑

ⓘ A NAT gateway is recommended for outbound internet access from subnets. Edit the subnet to add a NAT gateway. [Learn more](#)

Fonte: Capturado pelo autor desse trabalho a partir de Azure, 2024.

A rede foi criada com sucesso, conforme a Figura 18.

Figura 18: Rede Virtual Criada Com Sucesso



Fonte: Capturado pelo autor desse trabalho a partir de Azure, 2024.

A rede foi configurada como privada, e uma máquina virtual foi adicionada. Por limitações financeiras, a máquina virtual escolhida foi o modelo *Standard B1s* com o sistema operacional Windows 10, contendo: uma *Virtual Central Processing Unit*, Unidade Central de Processamento Virtual (vCPU); 1 Gigabyte (GB) de *Random Access Memory*, Memória de Acesso Aleatório (RAM); e 4 GB de SSD para armazenamento. A implementação da máquina virtual pode ser verificada na Figura 19.

Figura 19: Implementação da Máquina Virtual

Create a virtual machine ...

Run with Azure Spot discount

Size * [See all sizes](#)

Enable Hibernation

Administrator account

Authentication type SSH public key Password

Username * ✓

Password * ✓

Confirm password * ✓

i Hibernate is not supported by the size that you have selected. Choose a size that is compatible with Hibernation to enable this feature. [Learn more](#)

Fonte: MICROSOFT, 2024a

Foi criado um *endpoint* privado configurado para lidar com arquivos, conforme as Figuras 20 e 21.

Figura 20: Configuração do *Private Endpoint*

Create a private endpoint ...

⚠ Changes you make on this tab may affect any configuration you've done on other tabs. Review all options prior to creating the private endpoint.

✓ Basics ② Resource ③ Virtual Network ④ DNS ⑤ Tags ⑥ Review + create

Use private endpoints to privately connect to a service or resource. Your private endpoint must be in the same region as your virtual network, but can be in a different region from the private link resource that you are connecting to. [Learn more](#)

Project details

Subscription * ⓘ

Resource group * ⓘ [Create new](#)

Instance details

Name * ✓

Network Interface Name * ✓

Region *

Fonte: Capturado pelo autor desse trabalho a partir de Azure, 2024.

Figura 21: Configuração do *Private Endpoint*

Home > tccdorafael | Networking >

Create a private endpoint ...

✓ Basics ✓ Resource ③ Virtual Network ④ DNS ⑤ Tags ⑥ Review + create

Private Link offers options to create private endpoints for different Azure resources, like your private link service, a SQL server, or an Azure storage account. Select which resource you would like to connect to using this private endpoint. [Learn more](#)

Subscription Azure subscription 1 (3e1efd99-7c46-4c6c-8e34-3945696aa733)

Resource type Microsoft.Storage/storageAccounts

Resource tccdorafael

Target sub-resource * ⓘ

Fonte: Capturado pelo autor desse trabalho a partir de Azure, 2024.

A rede virtual já criada foi atrelada ao *endpoint*, conforme a Figura 22.

Figura 22: Configuração do *Private Endpoint*

The screenshot displays the 'Virtual Network' configuration step in the Azure portal. At the top, there are navigation tabs: 'Basics', 'Resource', 'Virtual Network' (selected), 'DNS', 'Tags', and 'Review + create'. Below the tabs, the 'Networking' section is active, with a sub-header 'Networking' and a note: 'To deploy the private endpoint, select a virtual network subnet. [Learn more](#)'. The configuration includes a dropdown for 'Virtual network' set to 'RedeTCCRafael (TCC_Rafael)', a dropdown for 'Subnet *' set to 'default', and a toggle for 'Network policy for private endpoints' set to 'Disabled (edit)'. The 'Private IP configuration' section has two radio buttons: 'Dynamically allocate IP address' (selected) and 'Statically allocate IP address'. The 'Application security group' section includes a description: 'Configure network security as a natural extension of an application's structure. ASG allows you to group virtual machines and define network security policies based on those groups. You can specify an application security group as the source or destination in an NSG security rule. [Learn more](#)'. Below this is a '+ Create' button and an empty dropdown menu for 'Application security group'.

Fonte: Capturado pelo autor desse trabalho a partir de Azure, 2024.

Uma zona DNS foi criada e adicionada ao *endpoint*, conforme a Figura 23.

Figura 23: Configuração do *Private Endpoint*

Home > tccdorafael | Networking >

Create a private endpoint ...

Basics
 Resource
 Virtual Network
 4 DNS
 5 Tags
 6 Review + create

Private DNS integration

To connect privately with your private endpoint, you need a DNS record. We recommend that you integrate your private endpoint with a private DNS zone. You can also utilize your own DNS servers or create DNS records using the host files on your virtual machines. [Learn more](#)

Integrate with private DNS zone Yes No

Configuration name	Subscription	Resource group	Private DNS zone
privatelink-file-core-wind...	Azure subscription 1	TCC_Rafael	(new) privatelink.file.core....

Fonte: Capturado pelo autor desse trabalho a partir de Azure, 2024.

O *endpoint* foi criado com sucesso, conforme a Figura 25.

Figura 24: *Endpoint* Criado Com Sucesso

Home >

Microsoft.PrivateEndpoint-20240402175958 | Overview

Deployment

Delete Cancel Redeploy Download Refresh

- Overview
- Inputs
- Outputs
- Template

✔ Your deployment is complete

Deployment name : Microsoft.PrivateEndpoint-20240... Start time : 4/2/2024, 6:07:35 PM
 Subscription : Azure subscription 1 Correlation ID : f8c2f3e6-bb7c-4ea4-8d9c-7ab34...
 Resource group : TCC_Rafael

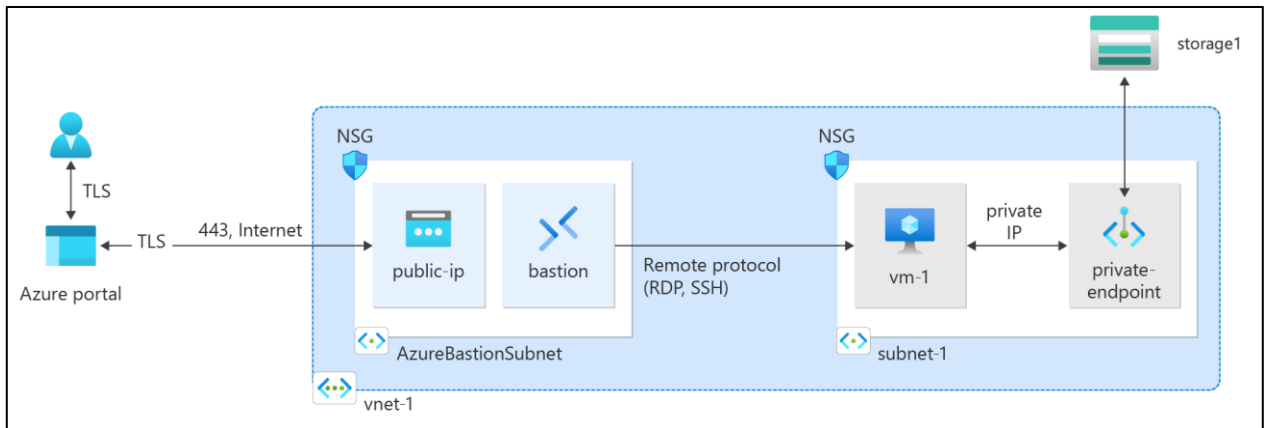
> Deployment details
 ∨ Next steps

[Go to resource](#)

Fonte: Capturado pelo autor desse trabalho a partir de Azure, 2024.

A topologia da rede com todos os componentes implementados pode ser verificada na figura 25. Nela, um usuário utiliza o Azure Bastion para se conectar ao Azure Bastion por IP público, para acessar uma máquina virtual na rede privada. Essa máquina virtual acessa um recurso de armazenamento através de um *endpoint* privado.

Figura 25: Topologia da Rede

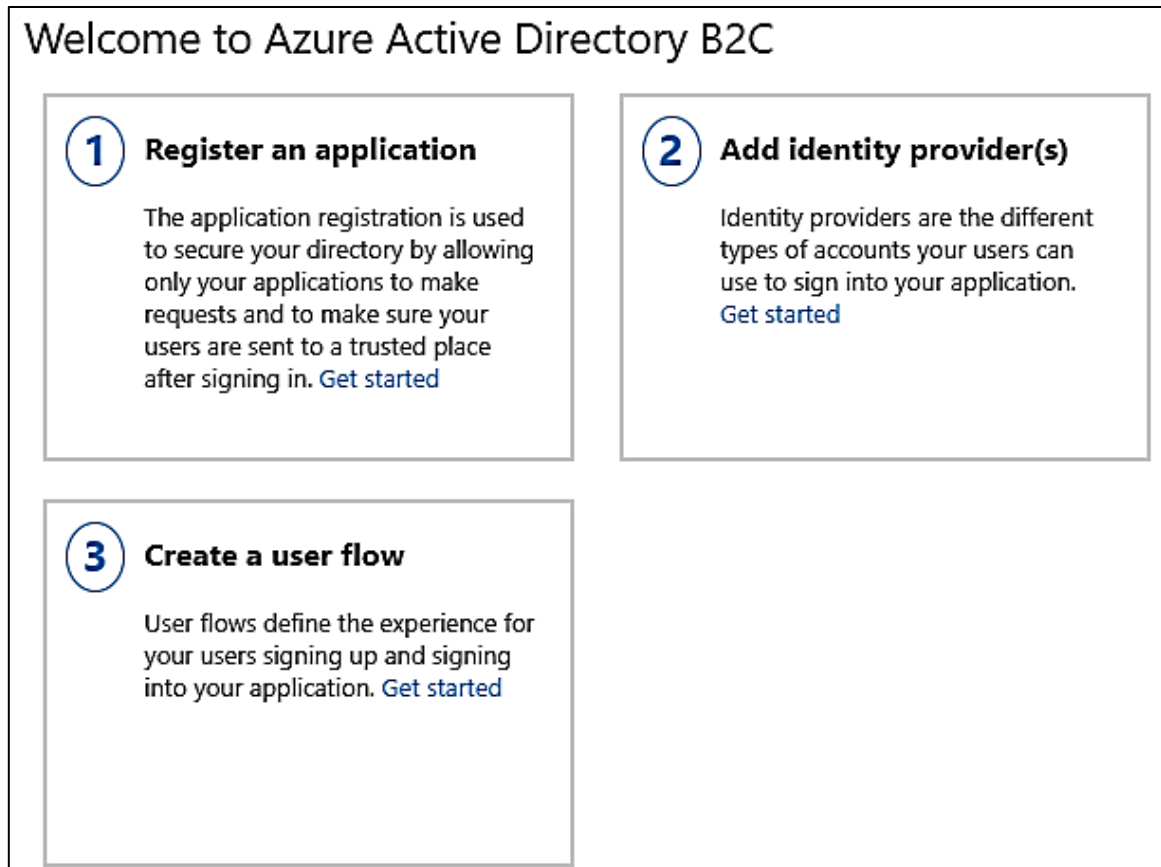


Fonte: MICROSOFT, 2024a

4.5 Implementação da autenticação (fase 2)

Segundo Microsoft (2024a), as etapas para configurar a autenticação no Azure AD B2C são: registrar uma aplicação; adicionar os tipos de conta que os usuários podem utilizar na aplicação; e criar um fluxo de usuário, que descreve a experiência de registro de conta para um usuário.

Figura 26: Etapas da Autenticação Azure AD B2C



Fonte: MICROSOFT, 2024a

Uma aplicação nomeada como “Sistema de Gerenciamento de Arquivos” foi registrada e configurada para aceitar fluxos de usuário, conforme a Figura 27:

Figura 27: Registro de Aplicação

Home > Azure AD B2C | App registrations >

Register an application ...

*** Name**
The display name for this application (this can be changed later).

Sistema de Armazenamento de Arquivos ✓

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (TCC do Rafael only - Single tenant)
- Accounts in any organizational directory (Any Microsoft Entra ID tenant – Multitenant)
- Accounts in any identity provider or organizational directory (for authenticating users with user flows)

[Help me choose...](#)

Fonte: Capturado pelo autor desse trabalho a partir de Azure, 2024.

Na instância do Azure Blob *Storage*, a aplicação foi adicionada, e o papel RBAC *Storage Blob Data Contributor* foi atribuído a ela. Segundo a Microsoft (2024a), este papel atribui direitos de ler, salvar e deletar arquivos no Azure Blob *Storage*. Estas configurações podem ser observadas na Figura 28:

Figura 28: Atribuição de Papel RBAC

Home > storagetccrafael | Access Control (IAM) >

Add role assignment ...

Role **Members** Conditions Review + assign

Selected role Storage Blob Data Contributor

Assign access to

User, group, or service principal

Managed identity

Members + Select members

Name	Object ID	Type
Sistema de Armazenamento de Arquivos	c50e085c-8597-437f-b06f-fa2dc5e0eb15	App

Fonte: Capturado pelo autor desse trabalho a partir de Azure, 2024.

O fluxo de usuário foi configurado conforme a Figura 29, com a opção de aceitar registro de contas com autenticação por *e-mail* e coletando os atributos: nome, sobrenome e *login*.

Figura 29: Registro de Fluxo de Usuário

Home > External Identities | External collaboration settings > External Identities | All identity providers > External Identities | User flows >

Create

Sign up and sign in (Recommended)

i Got a second? We would love your feedback on creating user flows →


Get started with your user flow with a few basic selections. Don't worry about getting everything right here, you can modify your user flow after you've created it.


1. Name
The unique string used to identify this user flow in requests to Microsoft Entra ID. This cannot be changed after a user flow has been created.


B2X_1_*

2. Identity providers *
Identity providers are the different types of accounts your users can use to log into your application. You need to select at least one for a valid user flow and you [about identity providers](#).

Please select at least one identity provider

 Azure Active Directory Sign up

 Microsoft Account

 Email one-time passcode

3. User attributes
User attributes are values collected on sign up. You can create custom attributes for use in your directory. [Learn more about user attributes](#).

Collect attribute

Given Name ⓘ	<input checked="" type="checkbox"/>
Surname ⓘ	<input checked="" type="checkbox"/>
City ⓘ	<input type="checkbox"/>
Country/Region ⓘ	<input type="checkbox"/>
Display Name ⓘ	<input checked="" type="checkbox"/>

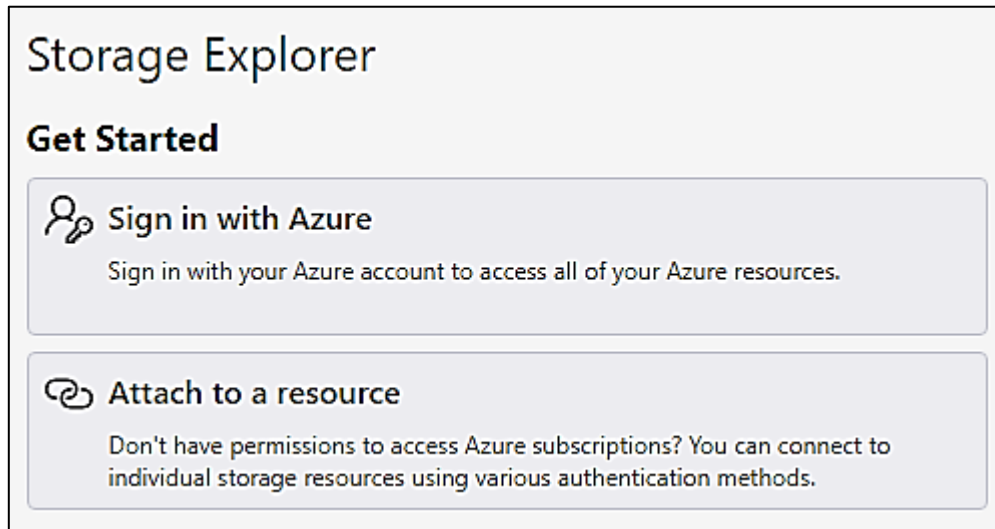
Also selected: Email Address
[Show more...](#)

Fonte: Capturado pelo autor desse trabalho a partir de Azure, 2024.

Planejava-se registrar uma conta para testar as configurações de autenticação, mas um problema foi encontrado. Quando a instância do Azure Blob *Storage* foi implementada inicialmente, o *upload* da imagem para testes foi feito pelo *website* Azure Portal, e assim esperava-se que visitantes pudessem registrar suas contas e realizar operações com arquivos também através do Azure Portal. No entanto, não foi encontrado um método de realizar o registro de contas de visitantes e o *upload* de arquivos dentro do *site*, e uma nova consulta à documentação do Azure *Storage* disponibilizada pela Microsoft (2024a) foi feita em busca de uma abordagem alternativa.

A nova abordagem decidida foi o uso do *software* *Azure Storage Explorer*. Segundo Microsoft (2024a), *Azure Storage Explorer* é um *software* para gerenciar dados de armazenamento *Azure Storage*, e ele permite que contas autenticadas se conectem a instâncias *Azure Storage*, conforme a opção *Attach to a resource* da Figura 30:

Figura 30: Funcionamento do *Azure Storage Explorer*



Fonte: Capturado pelo autor desse trabalho a partir de *Azure Storage Explorer*, 2024.

4.6 Reconfiguração do *Azure Blob Storage*

Quando a instância do *Azure Blob Storage* foi criada, ela havia sido feita com acesso público para visualizar a imagem que foi enviada por *upload*, pois o serviço de autenticação não havia sido implementado ainda. Além disso, muitas das opções foram deixadas como *default*, pois o objetivo era apenas testar se o *Azure Blob Storage* funcionava. Portanto, foi constatada a necessidade de reconfigurar a instância para fechar o acesso público, e implementar opções de criptografia.

Foi desabilitada a opção *Allow enabling anonymous access on individual containers* nas configurações do *Azure Blob Storage*, conforme a Figura 31. Segundo Microsoft (2024a), sua funcionalidade é "*Allow enabling anonymous access on individual containers*" que permite que seja habilitado o acesso anônimo aos arquivos.

Foram habilitadas opções do *Azure Blob Storage* conforme as Figuras 31 e 32. Segundo Microsoft (2024a), suas funcionalidades são:

- *Require secure transfer for tls REST API operations*: requisições para o Azure Blob Storage só serão aceitas em HTTPS;
- *Enable Storage account key access*: permite acesso à conta de armazenamento com uma chave de acesso;
- *Default to Microsoft Entra authorization in the Azure Portal*: a autorização padrão será feita através do Microsoft Entra, que no contexto deste trabalho corresponde ao Azure AD B2C já configurado;
- *Minimum TLS version 1.2*: requisições para o Azure Blob Storage só serão aceitas se utilizarem o protocolo TLS versão 1.2, a versão mais recente disponível no Azure;
- *Disable public access and use private access*: desabilita o acesso público, e usa no seu lugar o acesso privado;
- *Microsoft network routing*: o acesso será feito pela rede global da Microsoft.

Figura 31: Configuração do Azure Blob Storage

Security

Configure security settings that impact your storage account.

Require secure transfer for REST API operations ⓘ	<input checked="" type="checkbox"/>
Allow enabling anonymous access on individual containers ⓘ	<input type="checkbox"/>
Enable storage account key access ⓘ	<input checked="" type="checkbox"/>
Default to Microsoft Entra authorization in the Azure portal ⓘ	<input checked="" type="checkbox"/>
Minimum TLS version ⓘ	Version 1.2 <input type="button" value="v"/>

Fonte: Capturado pelo autor desse trabalho a partir de Azure, 2024.

Figura 32: Configuração do Azure Blob Storage

Network connectivity

You can connect to your storage account either publicly, via public IP addresses or service endpoints, or privately, using a private endpoint.

Network access * Enable public access from all networks
 Enable public access from selected virtual networks and IP addresses
 Disable public access and use private access

Network routing

Determine how to route your traffic as it travels from the source to its Azure endpoint. Microsoft network routing is recommended for most customers.

Routing preference * ⓘ Microsoft network routing
 Internet routing

Fonte: Capturado pelo autor desse trabalho a partir de Azure, 2024.

Segundo Microsoft (2024a), a criptografia em repouso do Azure Blob Storage pode ser implementada como:

- Criptografia a nível de serviço: garante que todos os dados armazenados na nuvem sejam criptografados. Essa criptografia pode ser configurada manualmente pelo cliente com a opção *Customer-Managed Keys*, Chaves Gerenciadas pelo Cliente (CMK), ou pode ser gerenciada automaticamente pela Microsoft através da opção *Microsoft-Managed Keys*, Chaves Gerenciadas pela Microsoft (MMK);
- Criptografia a nível de estrutura: complementa a criptografia a nível de serviço com uma camada extra de criptografia. Desta forma, os dados são criptografados duas vezes: uma vez a nível de serviço, e outra a nível de infraestrutura, com algoritmos e chaves diferentes. Diferentemente da criptografia a nível de serviço, a criptografia a nível de estrutura não pode ser configurada manualmente, e sempre usa o algoritmo AES com chave de 256 bits e *Cipher Block Chaining*, Encadeamento de Cifras de Bloco (CBC).

Foram habilitadas opções de criptografia conforme a Figura 33. Segundo Microsoft (2024a), elas têm como função:

- *Microsoft-Managed Keys*: faz com que a Microsoft gerencie a criptografia em repouso, sem que seja necessário configurá-la por conta própria. Esta opção foi habilitada temporariamente, enquanto o gerenciamento de chaves não foi configurado, e depois disso a opção escolhida seria CMK, que possibilita configurar a criptografia em repouso por conta própria;
- *Enable support for customer-managed keys* configurado para *all service types*: permite utilizar a CMK com todos os tipos de serviço;
- *Enable infrastructure encryption*: habilita a criptografia a nível de estrutura.

Figura 33: Configuração do Azure Blob Storage

The screenshot shows the 'Encryption' tab of the Azure Blob Storage configuration page. The navigation tabs at the top are: Basics, Advanced, Networking, Data protection, **Encryption**, Tags, and Review + create. The 'Encryption' tab is active and underlined.

Under the 'Encryption' tab, there are three main settings:

- Encryption type *** (with an information icon):
 - Microsoft-managed keys (MMK)
 - Customer-managed keys (CMK)
- Enable support for customer-managed keys** (with an information icon):
 - Blobs and files only
 - All service types (blobs, files, tables, and queues)
 - Warning:** This option cannot be changed after this storage account is created.
- Enable infrastructure encryption** (with an information icon):
 -
 - Warning:** This option cannot be changed after this storage account is created.

Fonte: Capturado pelo autor desse trabalho a partir de Azure, 2024.

4.7 Gerenciamento de Chaves

A Microsoft disponibiliza o serviço de gerenciamento de chaves criptográficas *Azure Key Vault*, que é compatível com o *Azure Blob Storage* (MICROSOFT, 2024a).

Foi criada uma instância do *Azure Key Vault* conforme as Figuras 34 e 35, e a opção *Azure role-based access control*, que implementa controle de acesso RBAC para acessar o *Azure Key Vault*, foi habilitada. Desta forma, somente um indivíduo autorizado com o papel específico para isso pode gerenciar as chaves criptográficas.

Figura 34: Configuração do Azure *Key Vault*

Create a key vault ...

to store security information in their code. It allows you to centralize the storage of your application secrets which greatly reduces the chances that secrets may be leaked. Key Vault also allows you to securely store secrets and keys backed by Hardware Security Modules or HSMs. The HSMs used are Federal Information Processing Standards (FIPS) 140-2 Level 2 validated. In addition, key vault provides logs of all access and usage attempts of your secrets so you have a complete audit trail for compliance.

Project details
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * Azure for Students ▼

Resource group * resource_group_TCCRafael ▼
Create new

Instance details

Key vault name * ⓘ keyvaultTCCrafael ✓

Region * Brazil South ▼

Pricing tier * ⓘ Standard ▼

Fonte: Capturado pelo autor desse trabalho a partir de Azure, 2024.

Figura 35: Configuração do Azure *Key Vault*

Basics Access configuration Networking Tags Review + create

Configure data plane access for this key vault

To access a key vault in data plane, all callers (users or applications) must have proper authentication operations the caller can execute. [Learn more](#)

Permission model
Grant data plane access by using a [Azure RBAC](#) or [Key Vault access policy](#)

Azure role-based access control (recommended) ⓘ

Vault access policy ⓘ

Resource access

Azure Virtual Machines for deployment ⓘ

Azure Resource Manager for template deployment ⓘ

Azure Disk Encryption for volume encryption ⓘ

Fonte: Capturado pelo autor desse trabalho a partir de Azure, 2024.

Foi criada uma chave *Elliptic Curve*, Curva Elíptica (EC) utilizando o campo primo P-256, conforme a Figura 36. Esta chave foi escolhida porque segundo Tencent Cloud (2024), a criptografia EC é computacionalmente mais eficiente que a RSA, sem comprometer a segurança mesmo com chaves relativamente pequenas.

Figura 36: Escolha da Criptografia

The screenshot shows the 'Create a key' interface in the Azure portal. The breadcrumb navigation is 'Home > storagegetccrafael | Encryption > Select a key >'. The main heading is 'Create a key' with a key icon. Below this, there are several configuration options:

- Options:** A 'Generate' button.
- Name *:** A text input field containing 'chavetccrafael'.
- Key type:** Radio buttons for 'RSA' and 'EC', with 'EC' selected.
- Elliptic curve name:** Radio buttons for 'P-256', 'P-384', 'P-521', and 'P-256K', with 'P-256' selected.
- Set activation date:** An unchecked checkbox.
- Set expiration date:** An unchecked checkbox.
- Enabled:** A toggle switch with 'Yes' selected and 'No' unselected.

Fonte: Capturado pelo autor desse trabalho a partir de Azure, 2024.

Após o gerenciamento de chaves ter sido configurado, houve a troca da opção MMK pela CMK no Azure Blob *Storage*, como o planejado, e a chave foi vinculada ao Azure Blob *Storage*, conforme as Figuras 37 e 38.

Figura 37: Vinculando Chave

Home > storagetccrafael | Encryption >

Select a key ...

i The key 'chavetccrafael' has been successfully created.

Subscription *

Key store type ⓘ Key vault Managed HSM

Key vault *
[Create new key vault](#)

Key *
[Create new key](#)

Fonte: Capturado pelo autor desse trabalho a partir de Azure, 2024.

Figura 38: Vinculando Chave

Enable support for customer-managed keys ⓘ All service types (blobs, files, tables, and queues)

Infrastructure encryption ⓘ Enabled

Encryption type Microsoft-managed keys Customer-managed keys
i When customer-managed keys are enabled, the selected key vault. Both soft delete and purge disabled. [Learn more](#)

Key selection

Encryption key Select from key vault Enter key URI

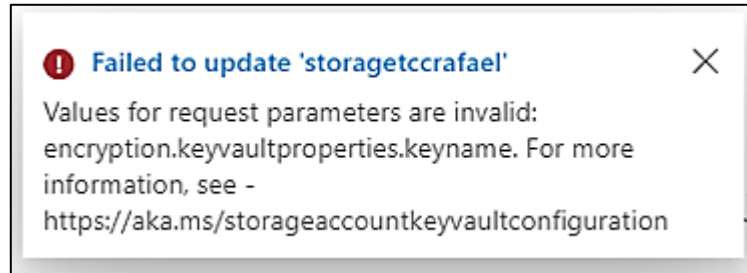
Key vault and key *
 Key vault: keyvaulttcc
 Key: chavetccrafael
[Select a key vault and key](#)

Identity type ⓘ System-assigned User-assigned

Fonte: Capturado pelo autor desse trabalho a partir de Azure, 2024.

Foi observado um erro, conforme a Figura 39:

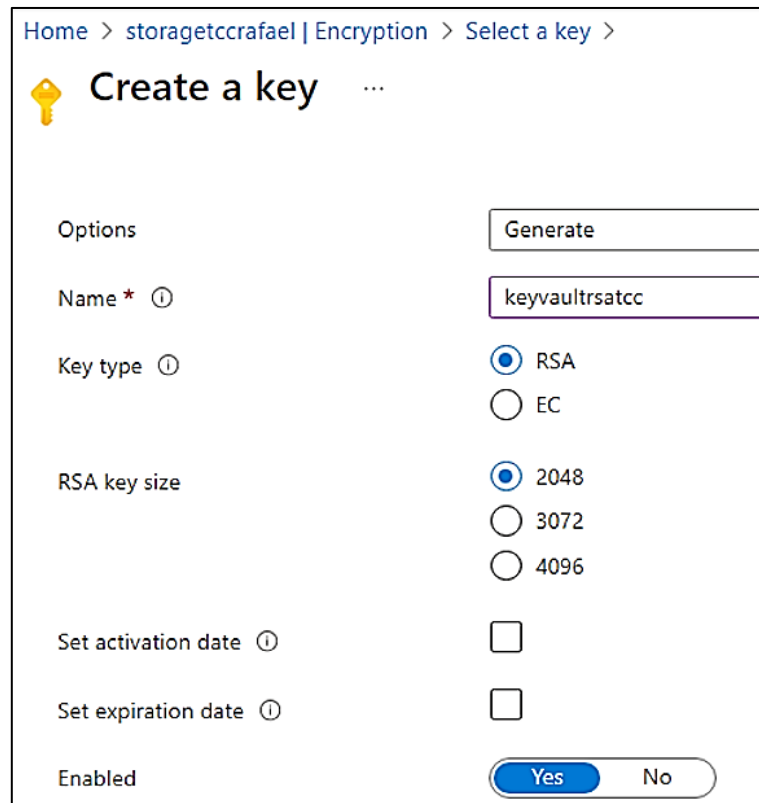
Figura 39: Erro do Azure Blob *Storage*



Fonte: Capturado pelo autor desse trabalho a partir de Azure, 2024.

Após um longo processo de tentativa-e-erro modificando configurações, verificou-se que o erro ocorre apenas quando uma chave EC é utilizada. Assim, foi decidido implementar uma chave RSA no lugar da chave EC, e o erro não apareceu novamente. Foi implementado o menor tamanho de chave para não haver impacto na eficiência de transferência de arquivos, conforme a Figura 40:

Figura 40: Vinculando Chave



Home > storagetccrafael | Encryption > Select a key >

Create a key ...

Options Generate

Name * ⓘ keyvaultrsatcc

Key type ⓘ RSA EC

RSA key size 2048 3072 4096

Set activation date ⓘ

Set expiration date ⓘ

Enabled Yes No

Fonte: Capturado pelo autor desse trabalho a partir de Azure, 2024.

A chave nova foi vinculada ao Azure Blob *Storage*, conforme a Figura 41:

Figura 41: Vinculando Chave

Subscription *	Azure for Students
Key store type ⓘ	<input checked="" type="radio"/> Key vault <input type="radio"/> Managed HSM
Key vault *	keyvaulttcc Create new key vault
Key *	keyvaultrsatcc Create new key

Fonte: Capturado pelo autor desse trabalho a partir de Azure, 2024.

5 TESTES REALIZADOS

5.1 Teste 1: registro da conta

Primeiramente, o administrador do sistema entrou no *site* Azure portal e acessou o Microsoft Entra *identification*, identificação (ID), um serviço que corresponde ao diretório padrão, conforme a Figura 42:

Figura 42: Configuração do Microsoft Entra ID

The screenshot displays the Microsoft Entra ID Overview page. The left-hand navigation pane includes sections for 'Overview', 'Preview features', 'Diagnose and solve problems', and 'Manage' (with sub-items: Users, Groups, External Identities, Roles and administrators, Administrative units, Delegated admin partners, and Enterprise applications). The main content area features a top navigation bar with '+ Add', 'Manage tenants', 'What's new', and 'Preview features'. Below this is a notification banner: 'Azure Active Directory is now Microsoft Entra ID. [Learn more](#)'. The main content is divided into tabs: 'Overview' (selected), 'Monitoring', 'Properties', 'Recommendations', and 'Tutorials'. A search bar labeled 'Search your tenant' is positioned below the tabs. The 'Basic information' section contains the following data:

Basic information	
Name	Diretório Padrão
Tenant ID	20314b82-f843-4d4d-a320-9a4df94ec50f
Primary domain	ropmsgoutlook.onmicrosoft.com
License	Microsoft Entra ID Free

Fonte: Capturado pelo autor desse trabalho a partir de Azure, 2024.

Em seguida, na seção de usuários, foi criada uma conta, conforme a Figura 43.

Segundo Microsoft (2024a), ao desabilitar a opção *Account enabled*, é possível criar uma conta ainda não funcional, e habilitar a conta para uso somente quando todo o seu controle de acesso estiver configurado, para maior segurança. Também é possível gerar uma senha aleatória.

Figura 43: Registro de Conta no Microsoft Entra ID

Home > Users >

Create new user

Create a new internal user in your organization

Basics Properties Assignments Review + create

Create a new user in your organization. This user will have a user name like alice@contoso.com. [Learn more](#)

Identity

User principal name * @ [Domain not listed? Learn more](#)

Mail nickname * Derive from user principal name

Display name *

Password * Auto-generate password

Account enabled

Fonte: Capturado pelo autor desse trabalho a partir de Azure, 2024.

A conta foi adicionada ao diretório padrão, conforme a Figura 44:

Figura 44: Lista de Usuários

Users ...

Diretório Padrão - Microsoft Entra ID

Search + New user Download users Bulk operations Refresh Manage

All users [Azure Active Directory is now Microsoft Entra ID.](#)

Audit logs Search Add




Sign-in logs

Diagnose and solve problems

Manage

Troubleshooting + Support

3 users found (1 user selected)

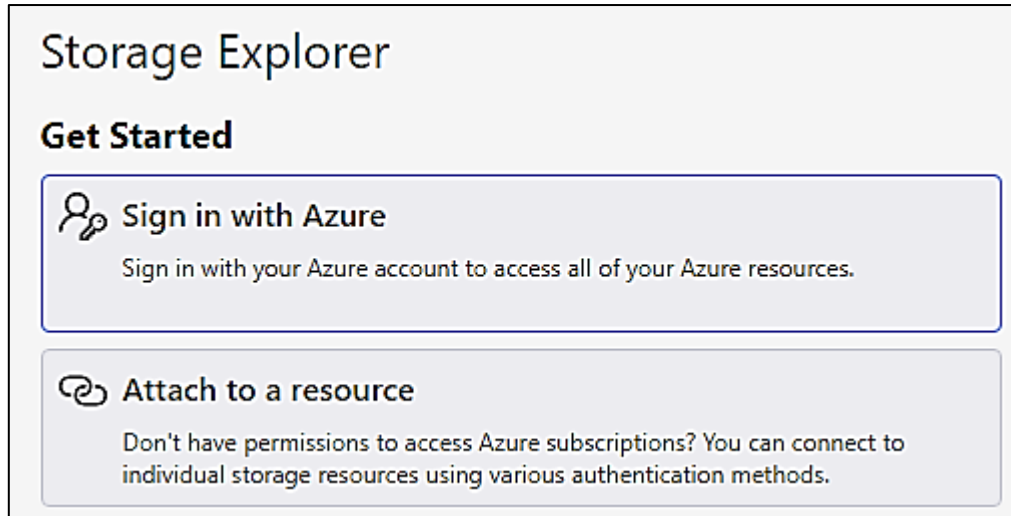
<input type="checkbox"/>	Display name ↑	User principal name ↑	User type
<input type="checkbox"/>	 Angelica	angelica@ropmsgoutlook...	Member
<input type="checkbox"/>	 Rafael Oliveira Porfirio	rop.msg_outlook.com#EX...	Member
<input checked="" type="checkbox"/>	 Usuário Teste	usuario_teste@ropmsgou...	Member

Fonte: Capturado pelo autor desse trabalho a partir de Azure, 2024.

5.2 Teste 1: autenticação

Foi instalado o *software* Microsoft Azure Storage Explorer, e foi feito o *login* na conta criada anteriormente através da opção *Sign in with Azure*, conforme a Figura 45:

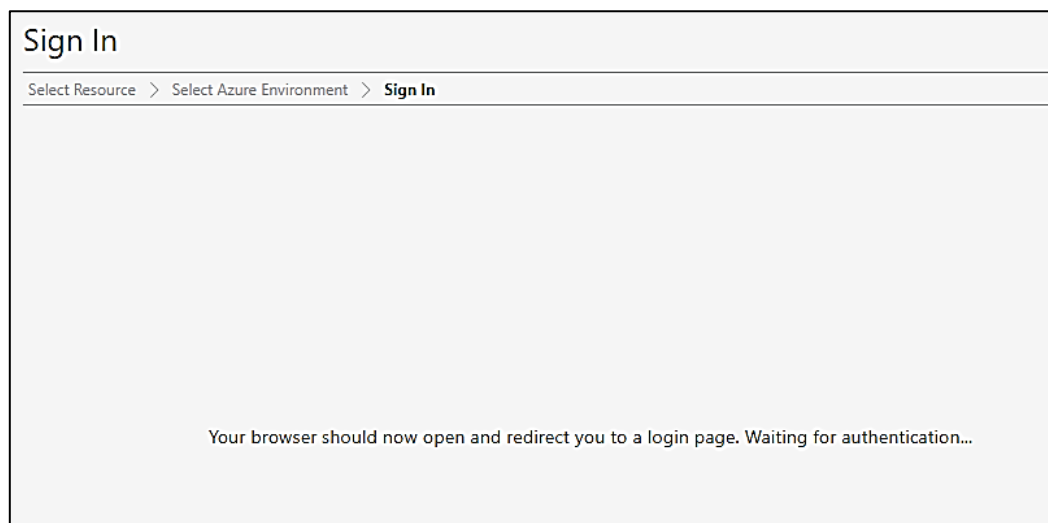
Figura 45: *Login* no Azure Storage Explorer



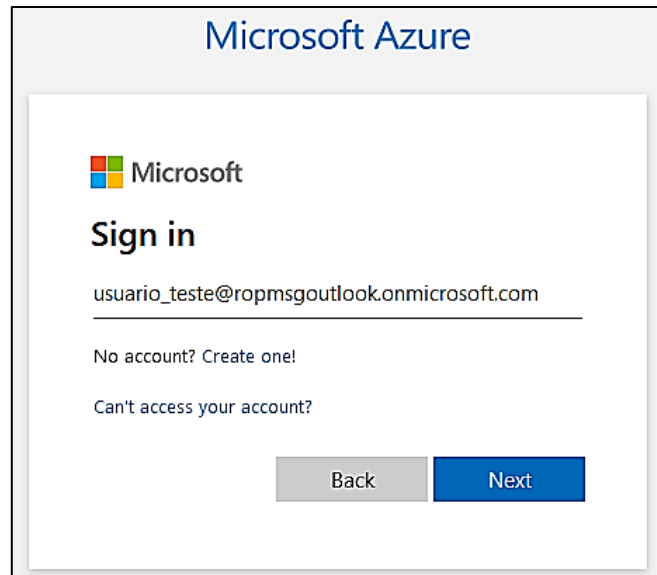
Fonte: Capturado pelo autor desse trabalho a partir de Azure Storage Explorer, 2024.

O sistema redireciona o usuário ao seu navegador padrão para continuar a autenticação, conforme as Figuras 46 e 47.

Figura 46: *Login* no Azure Storage Explorer



Fonte: Capturado pelo autor desse trabalho a partir de Azure Storage Explorer, 2024.

Figura 47: *Login* no Azure Storage Explorer

Microsoft Azure

Microsoft

Sign in

usuario_teste@ropmsgoutlook.onmicrosoft.com

No account? [Create one!](#)

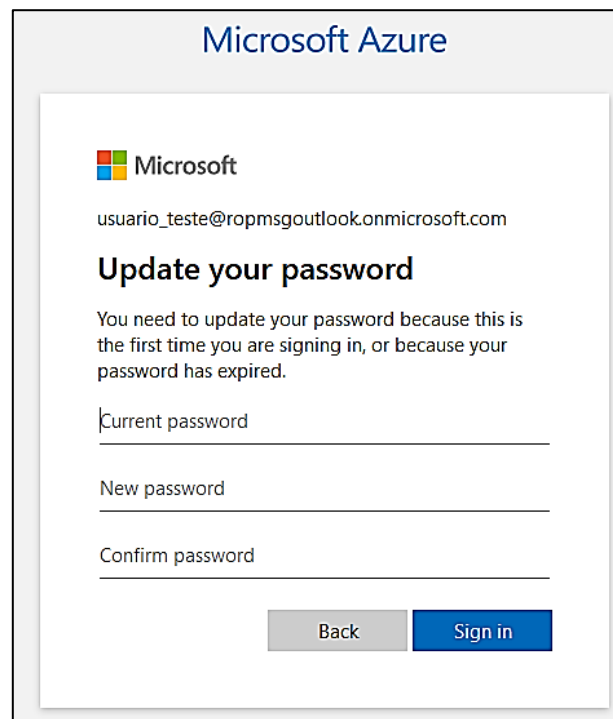
Can't access [your account?](#)

Back Next

Fonte: Capturado pelo autor desse trabalho a partir de Azure, 2024.

Após o *login* ser feito com as credenciais criadas pelo administrador, o usuário é obrigado a criar a sua própria senha, conforme a Figura 48:

Figura 48: Registro de Senha



Microsoft Azure

Microsoft

usuario_teste@ropmsgoutlook.onmicrosoft.com

Update your password

You need to update your password because this is the first time you are signing in, or because your password has expired.

Current password

New password

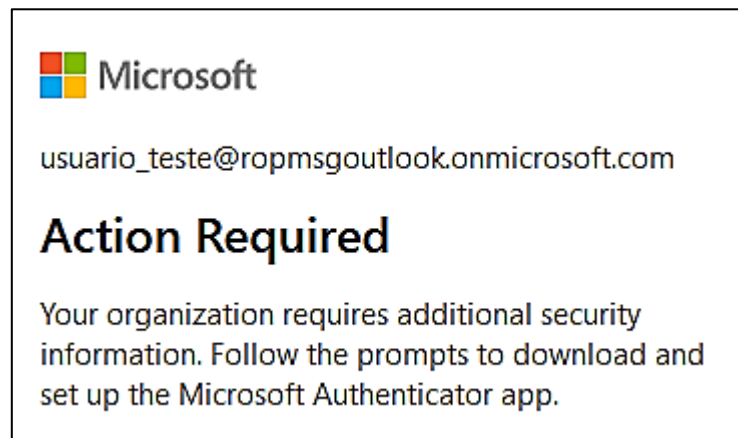
Confirm password

Back Sign in

Fonte: Capturado pelo autor desse trabalho a partir de Azure, 2024.

Com a sua nova senha escolhida, o usuário é redirecionado para realizar a autenticação multifator com um aplicativo autenticador no celular, conforme a figura 49. No caso, foi escolhido o Microsoft *Authenticator*.

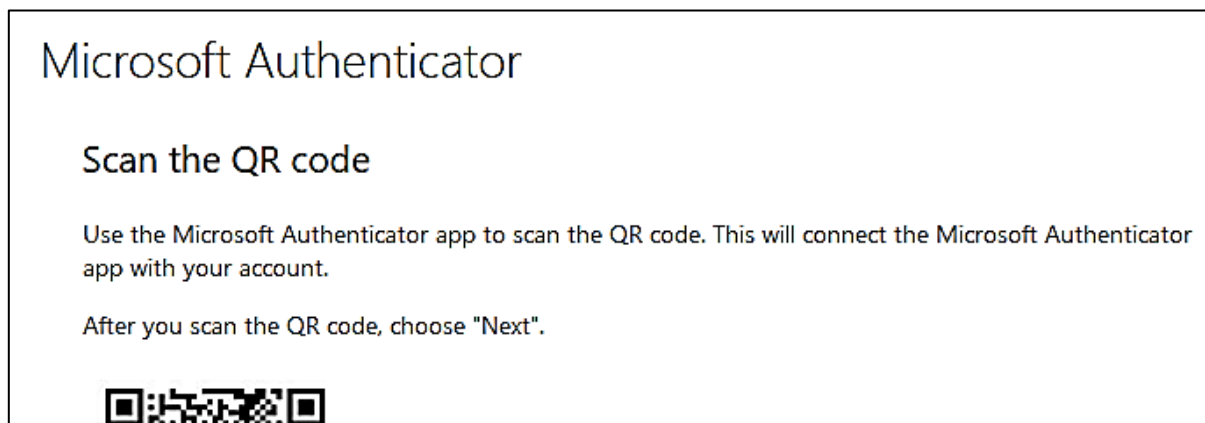
Figura 49: Solicitação de Autenticação Multifator



Fonte: Capturado pelo autor desse trabalho a partir de Azure, 2024.

Foi escaneado um *Quick-Response*, Resposta Rápida (QR) *code* com o aplicativo autenticador no celular, conforme a Figura 50:

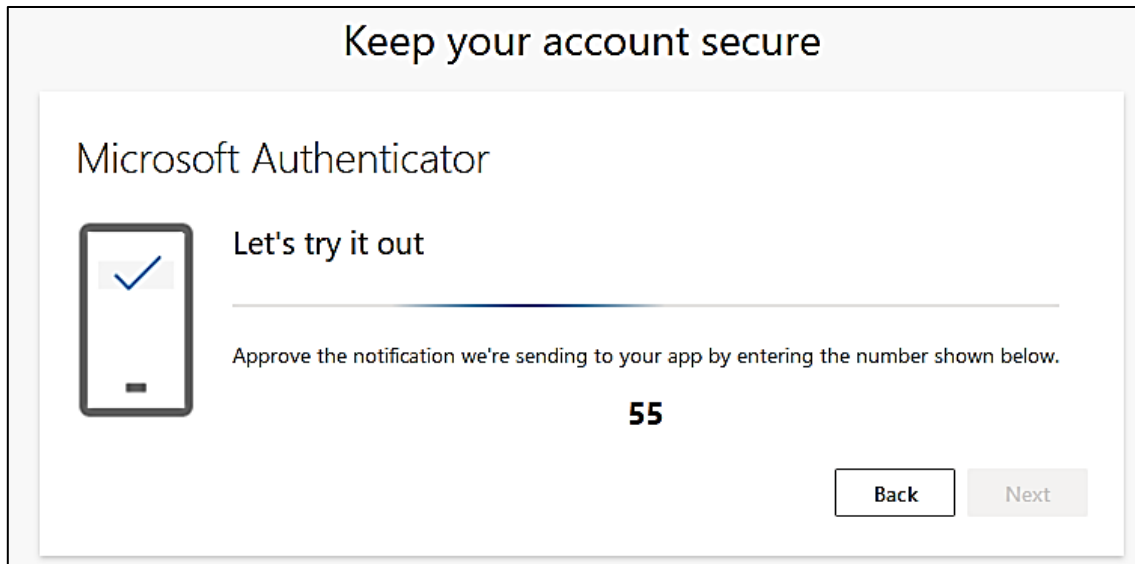
Figura 50: QR Code para autenticação multifator



Fonte: Capturado pelo autor desse trabalho a partir de Azure, 2024.

Um número foi exibido no navegador, que foi digitado no aplicativo autenticador no *smartphone*, conforme a Figura 51.

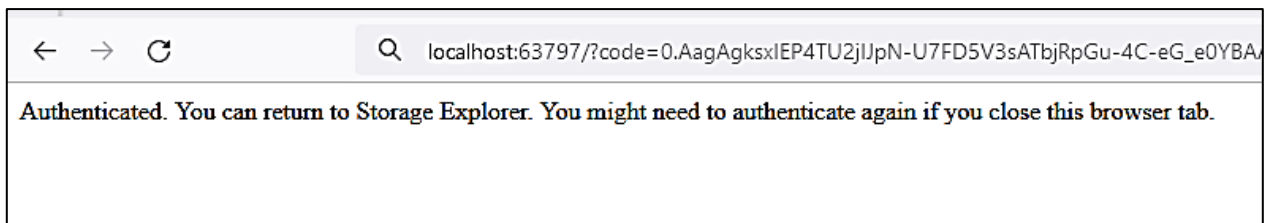
Figura 51: Pedido de Autenticação por Aplicativo



Fonte: Capturado pelo autor desse trabalho a partir de Azure, 2024.

A autenticação terminou com sucesso, conforme a Figura 52:

Figura 52: Autenticação Bem-Sucedida

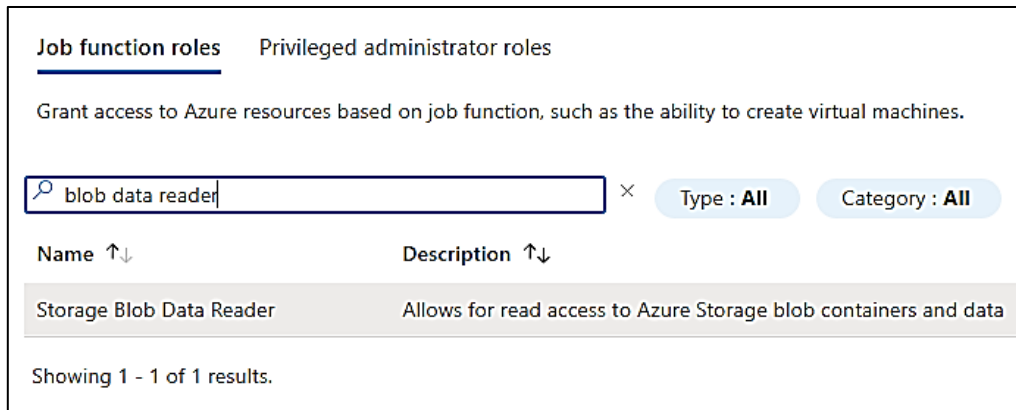


Fonte: Capturado pelo autor desse trabalho a partir de Azure, 2024.

5.3 Teste 2: autorização

O administrador entrou na seção *Access Control* da instância do *Azure Storage*, e adicionou um papel RBAC à conta criada anteriormente, conforme a Figura 53:

Figura 53: Atribuição de Papel RBAC

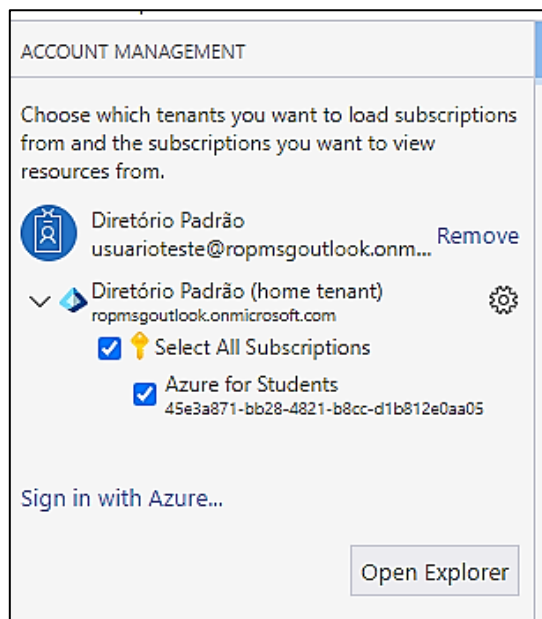


Fonte: Capturado pelo autor desse trabalho a partir de Azure *Storage Explorer*, 2024.

O papel *Blob Data Reader* garante permissões de leitura para o usuário, mas não permite que ele modifique os arquivos.

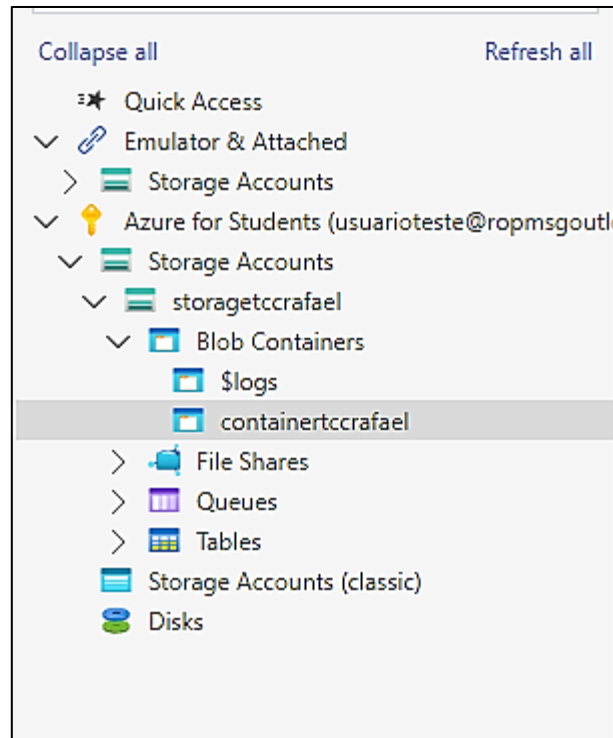
5.3.1 Acesso ao diretório compartilhado

Com o *login* finalizado e as permissões apropriadas, é possível acessar os arquivos pelo Microsoft Azure *Storage Explorer* através da opção *Open Explorer*, conforme as Figuras 54 e 55.

Figura 54: Interface do Azure *Storage Explorer*

Fonte: Capturado pelo autor desse trabalho a partir de Azure *Storage Explorer*, 2024.



Figura 55: Seleção de Container



Fonte: Capturado pelo autor desse trabalho a partir de Azure Storage Explorer, 2024.

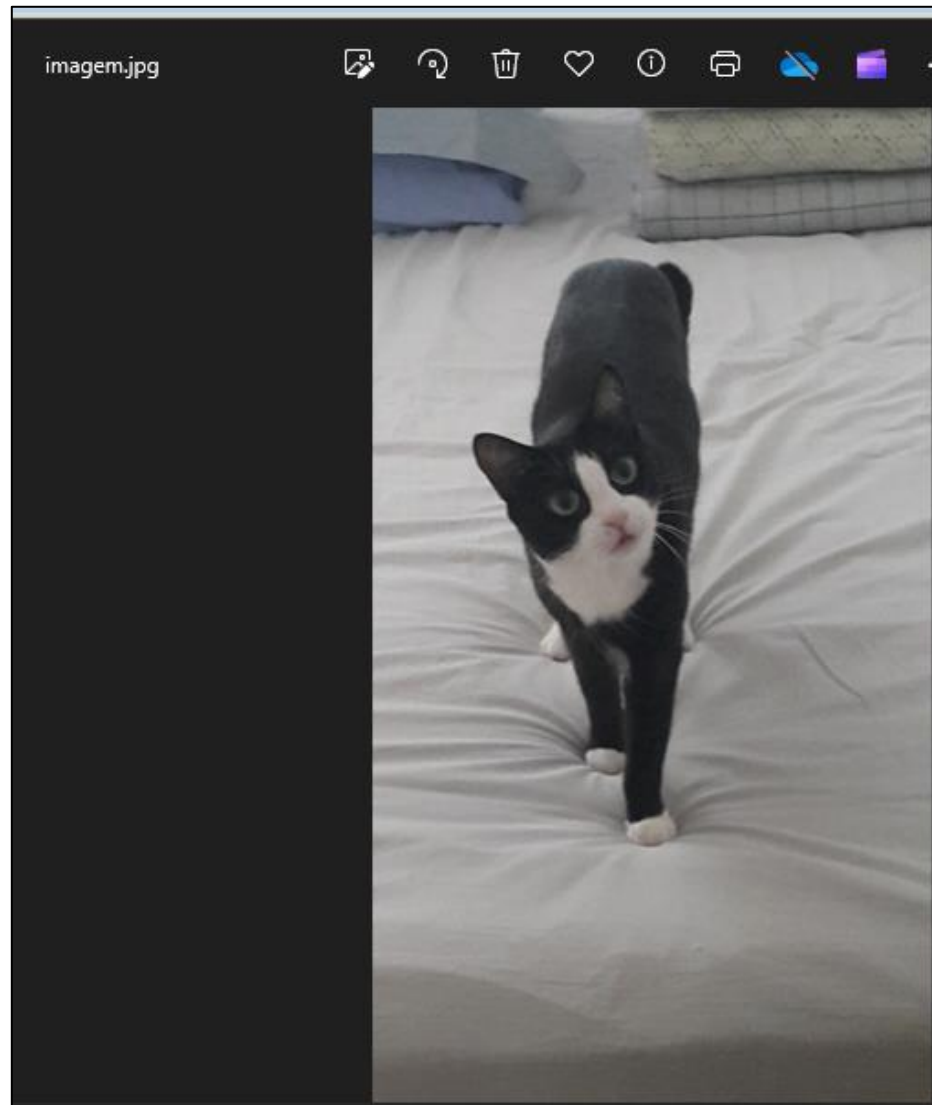
Os arquivos podem ser visualizados dentro do *container* conforme a Figura 56, e podem ser acessados conforme a Figura 57.

Figura 56: Arquivos do Azure Blob Storage

Name	Access Tier
 5a6b9863750630.920124335a6b98635be5f3.922	Hot (inferred)
 imagem.jpg	Hot (inferred)

Fonte: Capturado pelo autor desse trabalho a partir de Azure Storage Explorer, 2024.

Figura 57: Leitura de Arquivo

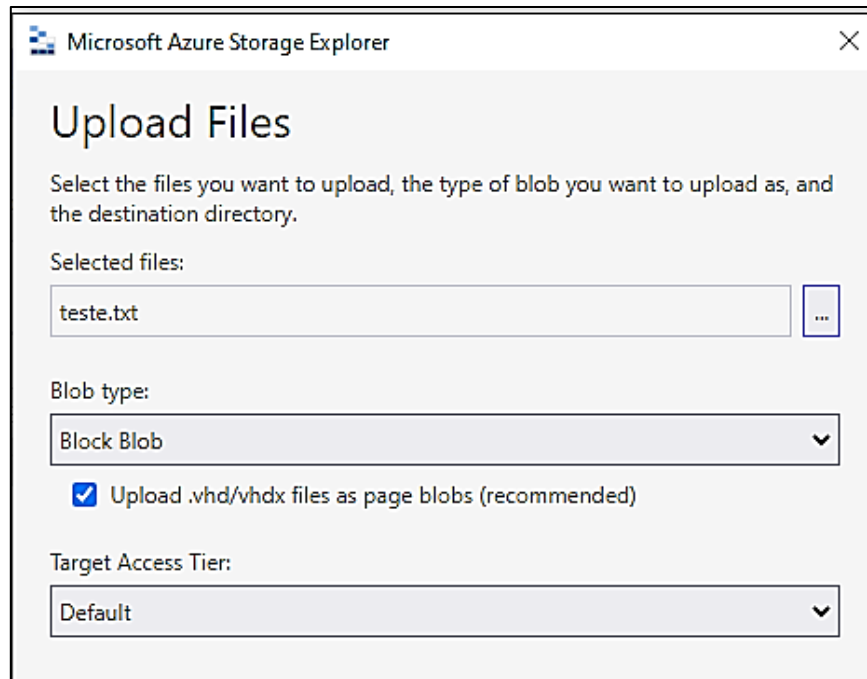


Fonte: Capturado pelo autor desse trabalho a partir de Azure Storage Explorer, 2024.

5.3.2 Testes em cada um dos perfis de usuário

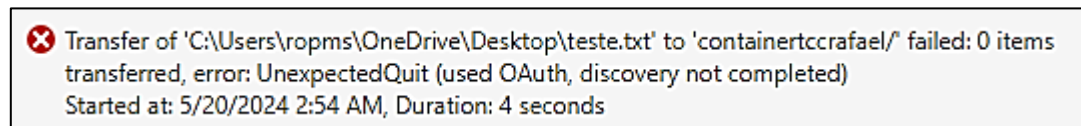
Foi testado o *upload* de arquivos, que não deveria funcionar, pois o usuário recebeu a autorização de somente leitura através do papel RBAC *Blob Data Reader*.

O *upload* não funcionou, como o esperado, conforme as figuras 58 e 59:

Figura 58: Teste de *Upload*

Fonte: Capturado pelo autor desse trabalho a partir de Azure *Storage Explorer*, 2024.

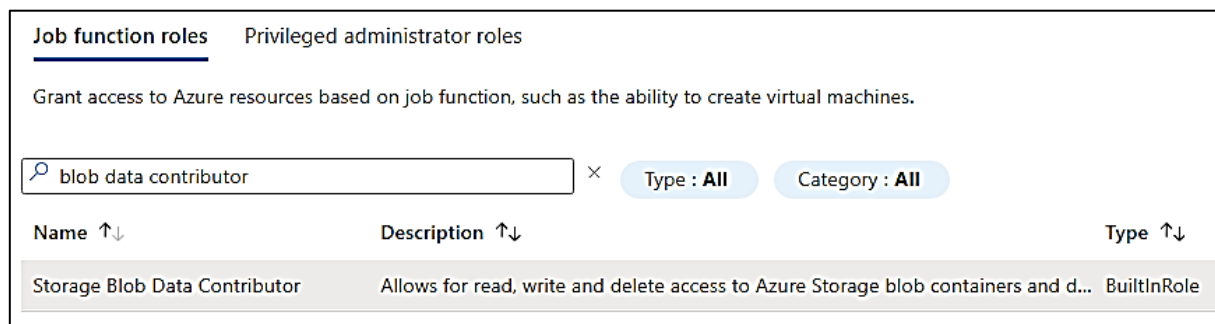
Figura 59: Erro de Upload



Fonte: Capturado pelo autor desse trabalho a partir de Azure *Storage Explorer*, 2024.

O administrador concedeu ao usuário o papel *Blob Data Contributor*, que garante direito de leitura, escrita, e de apagar arquivos, conforme a Figura 60:

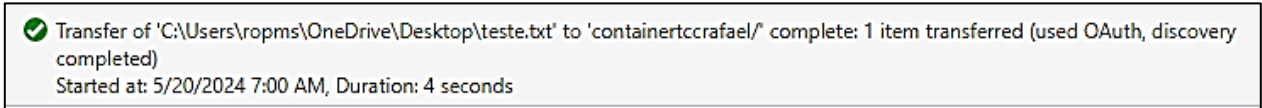
Figura 60: Atribuição de Papel RBAC



Fonte: Capturado pelo autor desse trabalho a partir de Azure *Storage Explorer*, 2024.




Foi feito o *upload* bem-sucedido de um arquivo, conforme as Figuras 61, 62 e 63:

Figura 61: *Upload Bem-Sucedido*



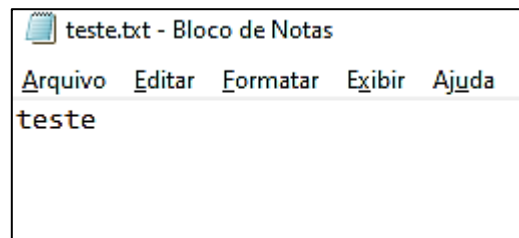
Fonte: Capturado pelo autor desse trabalho a partir de *Azure Storage Explorer*, 2024.

Figura 62: Lista de Arquivos

Name	Access Tier
 5a6b9863750630.920124335a6b98635be5f3.922	Hot (inferred)
 imagem.jpg	Hot (inferred)
 teste.txt	Hot (inferred)

Fonte: Capturado pelo autor desse trabalho a partir de *Azure Storage Explorer*, 2024.

Figura 63: Leitura de Arquivo Enviado Por Upload



Fonte: Capturado pelo autor desse trabalho a partir de *Azure Storage Explorer*, 2024.

5.4 Teste 3: criptografia

5.4.1 Criptografia em trânsito

Para verificação da criptografia em trânsito, os pacotes de autenticação e *download* da imagem foram rastreados pelo *software* Wireshark, conforme as Figuras 64 e 65.

Figura 64: Pacotes Rastreados no Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
54	10.834578	2620:1ec:46::33	2804:d59:7f48:c900:...	TLSv1.2	113	Application Data
55	10.834578	2620:1ec:46::33	2804:d59:7f48:c900:...	TLSv1.2	98	Application Data
71	12.409728	2620:1ec:46::33	2804:d59:7f48:c900:...	TLSv1.2	113	Application Data
72	12.409728	2620:1ec:46::33	2804:d59:7f48:c900:...	TLSv1.2	98	Application Data

Fonte: Capturado pelo autor desse trabalho a partir de Wireshark, 2024.

Figura 65: Pacotes Rastreados no Wireshark

```

v Transport Layer Security
  v TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
    Content Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 34
    Encrypted Application Data: 20e0d8f631c3496128d760c9573b41b3aa3059fbd63def9e22dbae6697f8ce3c18
    [Application Data Protocol: Hypertext Transfer Protocol]
  
```

Fonte: Capturado pelo autor desse trabalho a partir de Wireshark, 2024.

5.4.2 Criptografia em repouso

As configurações de criptografia em repouso podem ser vistas na seção *Encryption* do *Azure Blob Storage*.

Verificou-se que duas camadas de criptografia estão em funcionamento: a criptografia configurada no *Microsoft Key Vault*, e a criptografia de infraestrutura gerenciada pela Microsoft, conforme mostra a Figura 66.

Figura 66: Configurações da Criptografia em Repouso

The screenshot displays the 'Encryption' settings for the storage account 'storagetccrafael'. The left sidebar shows a navigation menu with 'Encryption' selected. The main content area is divided into two sections: 'Encryption selection' and 'Key selection'.

Encryption selection:

- 'Enable support for customer-managed keys' is set to 'All service types (blobs, files, tables, and queues)'. A help icon is present.
- 'Infrastructure encryption' is set to 'Enabled'. A help icon is present.
- 'Encryption type' is set to 'Customer-managed keys'. The 'Microsoft-managed keys' option is unselected, and 'Customer-managed keys' is selected. A help icon is present.

Key selection:

- 'Current key' is set to 'https://keyvaulttcc.vault.azure.net/keys/keyvault'.
- 'Automated key rotation' is set to 'Enabled - Using the latest key version'. A help icon is present.
- 'Key version in use' is set to 'fb5452a5fcb64d6ea2dd4e45dbf65c7e'. A help icon is present.

A warning message is displayed below the encryption type selection: 'When customer-managed keys are enabled, th access to the selected key vault. Both soft dele and cannot be disabled. Learn more'.

Fonte: Capturado pelo autor desse trabalho a partir de Azure Storage Explorer, 2024.

6 CONSIDERAÇÕES FINAIS

Considerando a porcentagem cada vez maior de dados empresariais armazenados em nuvem, e a necessidade de protegê-los contra ataques e acesso não autorizado, a segurança no armazenamento de arquivos em nuvem é um assunto pertinente. Neste estudo de caso, focado no Microsoft Azure, os métodos e as ferramentas utilizados para proporcionar a disponibilidade, a integridade e a confidencialidade dos dados armazenados na plataforma foram estudados e implementados, possibilitando uma visão abrangente do estado destas tecnologias.

O objetivo geral de implementar práticas de segurança em sistemas de armazenamento em nuvem foi atingido, assim como foram todos os objetivos específicos, como conhecer os recursos de segurança da plataforma Azure, e implementar um sistema de arquivos com técnicas de criptografia de dados em repouso e em trânsito.

A metodologia foi adequada para atingir os resultados, pois a abordagem de resumo de assunto permitiu uma maior absorção da documentação do Azure; o caráter experimental da pesquisa permitiu uma visão detalhada e prática sobre a segurança na armazenagem em nuvem; e ambos contribuíram para o caráter explicativo do objetivo da pesquisa.

Diversos desafios e dificuldades foram encontrados. Limitações financeiras impuseram restrições ao uso de determinadas funcionalidades avançadas, dificultando uma análise mais abrangente. Além disso, a documentação *online* oficial da Microsoft sobre o Azure descreve muitas das tecnologias apenas como partes individuais, o que exigiu um esforço adicional para tentar integrá-las como um todo. Foram encontrados livros sobre o tema, mas eles se mostraram desatualizados em relação à documentação *online*, e não foram utilizados.

Houve diversas correções de rota. Inicialmente pretendia-se programar o sistema de gerenciamento de arquivos em Python. Contudo, optou-se por utilizar os serviços já existentes no Azure, como o Azure Blob *Storage*. Esta decisão foi feita com o objetivo de conhecer as tecnologias em uso no mercado, ao invés de programar uma aplicação simples.

Os resultados alcançados são coerentes com a proposta da Microsoft (2024b) de que o cliente escolhe onde os seus dados são armazenados, e que o Azure protege os dados com criptografia em repouso e em trânsito.

Como uma oportunidade de aprendizado, esse trabalho proporcionou um entendimento prático e atualizado sobre as tecnologias de nuvem, gestão de identidades, criptografia de dados em repouso e em trânsito, e a integração de medidas avançadas de segurança. E como ferramenta

para a formação profissional, proporcionou a familiarização com as tecnologias utilizadas no mercado.

A contribuição deste TCC para a sociedade é fornecer para gestores de segurança da informação e empresas que buscam aprimorar suas estratégias de proteção de dados uma perspectiva sobre as tecnologias atuais de segurança no armazenamento em nuvem, proporcionando possíveis caminhos para implementar a confidencialidade, integridade e disponibilidade.

6.1 Sugestões de trabalhos futuros

- Comparar os serviços e funcionalidades de segurança no armazenamento em nuvem do Azure com os de outras plataformas, como o AWS;
- Investigar as políticas de segurança no armazenamento em nuvem em sistemas *multi-cloud*, em que empresas utilizam múltiplas plataformas de nuvem simultaneamente;
- Estudar soluções híbridas de armazenamento em nuvem, que combinam *datacenters* locais de uma empresa com os serviços de armazenamento em nuvem.

REFERÊNCIAS

- AWS. Overview of Amazon Web Services.** Disponível em: <<https://docs.aws.amazon.com/whitepapers/latest/aws-overview/introduction.html>>. Acesso em: 17 de nov. de 2023.
- GOOGLE. Google Cloud overview | Overview.** Disponível em: <<https://cloud.google.com/docs/overview>>. Acesso em: 17 de nov. de 2023.
- KAVIS, M. Architecting the cloud: design decisions for cloud computing service models (SaaS, PaaS, and IaaS).** Hoboken, New Jersey: John Wiley & Sons, Inc., 2014.
- MICROSOFT. Azure Documentation | Microsoft Azure.** Disponível em: <<https://learn.microsoft.com/en-us/azure/>>. Acesso em: 7 de maio de 2024a.
- MICROSOFT. Privacy in Azure | Microsoft Azure.** Disponível em: <<https://azure.microsoft.com/en-gb/explore/trusted-cloud/privacy/>>. Acesso em: 20 de maio de 2024b.
- MICROSOFT. What is Azure—Microsoft Cloud Services | Microsoft Azure.** Disponível em: <<https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-azure>>. Acesso em: 17 de nov. de 2023.
- OPUS SOFTWARE. O Que Você Realmente Precisa Saber Sobre Computação Em Nuvem.** Opus Software Com. e Repr. Ltda., 2015.
- STALLINGS, W.; BROWN, L. Segurança de Computadores.** Elsevier, 2014.
- STATISTA. Percent of corporate data stored in the cloud 2022.** Disponível em: <<https://www.statista.com/statistics/1062879/worldwide-cloud-Storage-of-corporate-data>>. Acesso em: 17 de nov. de 2023a.
- STATISTA. Infographic: Amazon, Microsoft & Google Dominate Cloud Market.** Disponível em: <<https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers>>. Acesso em: 17 de nov. de 2023b.

TENCENT CLOUD. **What are the differences between RSA and ECC?** Disponível em: <<https://www.tencentcloud.com/document/product/1007/39989>>. Acesso em 16 de maio de 2024.

RESOLUÇÃO n° 038/2020 – CEPE

ANEXO I

APÊNDICE ao TCC

Termo de autorização de publicação de produção acadêmica

O(A) estudante RAFAEL OLIVEIRA PORFÍRIO
do Curso de CIÊNCIA DA COMPUTAÇÃO, matrícula 20221002801943,
telefone: xxx e-mail 20221002801943@pucgo.edu.br, na qualidade de titular dos
direitos autorais, em consonância com a Lei n° 9.610/98 (Lei dos Direitos do autor),
autoriza a Pontificia Universidade Católica de Goiás (PUC Goiás) a disponibilizar o
Trabalho de Conclusão de Curso intitulado
SEGURANÇA NO ARMAZENAMENTO DE ARQUIVOS EM NUVEM: ESTUDO DE CASO COM
O MICROSOFT AZURE, gratuitamente, sem ressarcimento dos direitos autorais, por 5
(cinco) anos, conforme permissões do documento, em meio eletrônico, na rede mundial
de computadores, no formato especificado (Texto (PDF); Imagem (GIF ou JPEG); Som
(WAVE, MPEG, AIFF, SND); Vídeo (MPEG, MWV, AVI, QT); outros, específicos da
área; para fins de leitura e/ou impressão pela internet, a título de divulgação da
produção científica gerada nos cursos de graduação da PUC Goiás.

Goiânia, 26 de junho de 2024.

Assinatura do(s) autor(es): _____



Documento assinado digitalmente

RAFAEL OLIVEIRA PORFÍRIO

Data: 25/06/2024 16:12:20-0300

Verifique em <https://validar.iti.gov.br>

Nome completo do autor: RAFAEL OLIVEIRA PORFÍRIO

Assinatura do professor-orientador: _____



Documento assinado digitalmente

ANGÉLICA DA SILVA NUNES

Data: 24/06/2024 16:48:02-0300

Verifique em <https://validar.iti.gov.br>

Nome completo do professor-orientador: ANGÉLICA DA SILVA NUNES