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

CRIPTOGRAFIA E TÉCNICAS PARA GARANTIR A SEGURANÇA DA INFORMAÇÃO EM NUVEM, UTILIZANDO A AMAZON WEB SERVICES

LUIS GUILHERME RIBEIRO CAMPOS

GOIÂNIA
2023

LUIS GUILHERME RIBEIRO CAMPOS

CRIPTOGRAFIA E TÉCNICAS PARA GARANTIR A SEGURANÇA DA INFORMAÇÃO EM NUVEM, UTILIZANDO A AMAZON WEB SERVICES

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 Engenharia da Computação.

Orientadora:

Profa. Dra. Solange Da Silva

Banca examinadora:

Prof. Dr. José Luiz de Freitas Junior
Prof. Me. Rafael Leal Martins

GOIÂNIA

2023

LUIS GUILHERME RIBEIRO CAMPOS

CRIPTOGRAFIA E TÉCNICAS PARA GARANTIR A SEGURANÇA DA INFORMAÇÃO EM NUVEM, UTILIZANDO A AMAZON WEB SERVICES

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 Engenharia da Computação, em 12/12/2023.

Banca Examinadora:

_____
Orientadora: Profa. Dra. Solange da Silva

_____
Prof. Dr. José Luiz de Freitas Junior

_____
Prof. Me. Rafael Leal Martins

GOIÂNIA

2023

AGRADECIMENTOS

Agradeço a Deus por ter me dado saúde e resiliência para superar todos os obstáculos e dificuldades encontrados.

A minha família, minha mãe Maria Fernanda, meu pai Adelson, meus irmãos João e Gustavo, que me ajudaram a reerguer e me apoiaram nos meus momentos mais difíceis.

Em especial, meus pais que me forneceram o conhecimento, sabedoria, fé e me ensinaram a ter resiliência para enfrentar tudo e todos.

A minha orientadora professora Solange da Silva, pela paciência e ensino que foram de muito valor e pelo apoio no caminho para realizar essa monografia.

A todos, que de uma forma ou de outra, contribuíram no desenvolvimento deste trabalho.

RESUMO

O objetivo desse trabalho foi descrever algumas técnicas de criptografia, leis, normas de segurança e recursos da *Amazon Web Service* (AWS), visando garantir a segurança da informação em empresas. Quanto aos aspectos metodológicos, é uma pesquisa bibliográfica, documental e experimental. A presente monografia apresenta seis técnicas de criptografia e suas aplicabilidades, leis e normas de segurança da informação a fim de assegurar que empresas tratem de forma correta os dados de clientes, funcionários, parceiros e oito recursos da AWS relacionados a segurança de dados. O estudo permitiu concluir que conhecer as leis e normas de proteção de dados é essencial para garantir conformidade legal e ética no manuseio de informações pessoais. Com a crescente preocupação com a privacidade, estudar essas regulamentações, capacita profissionais a implementar práticas que respeitem os direitos individuais e evitem penalidades legais. Os serviços da AWS em conjunto com boas práticas de segurança, geram um ambiente altamente confiável, protegido e seguro, proporcionando aos usuários a confiança necessária para operar suas aplicações de forma eficiente e robusta. A segurança na nuvem é uma responsabilidade compartilhada entre a AWS e o cliente. A AWS é responsável por fornecer uma infraestrutura segura e ferramentas de segurança, as organizações são responsáveis por implementar práticas adequadas, monitoramento de acesso e permissões, gerenciamento de identidades, autenticações e configurações adequadas de firewalls e atualizações regulares de software.

Palavras Chaves: Criptografia, Normas de Segurança, Segurança da Informação, Segurança de Dados, *Amazon Web Service*.

ABSTRACT

The objective of this work was to describe some encryption techniques, laws, security standards, and features of Amazon Web Services (AWS), aiming to ensure information security in companies. Regarding methodological aspects, it is a bibliographic, documentary, and experimental research. This monograph presents six encryption techniques and their applicabilities, information security laws and standards to ensure that companies handle customer, employee, and partner data correctly, and eight AWS resources related to data security. The study concluded that knowing data protection laws and standards is essential to ensure legal and ethical compliance in handling personal information. With the growing concern for privacy, studying these regulations enables professionals to implement practices that respect individual rights and avoid legal penalties. AWS services, combined with good security practices, create a highly reliable, protected, and secure environment, providing users with the necessary confidence to operate their applications efficiently and robustly. Cloud security is a shared responsibility between AWS and the customer. AWS is responsible for providing a secure infrastructure and security tools, while organizations are responsible for implementing appropriate practices, access monitoring and permissions, identity management, authentication, and proper firewall configurations, as well as regular software updates.

Keywords: Encryption, Security Standards, Information Security, Data Security, Amazon Web Services.

LISTA DE ILUSTRAÇÕES

LISTA DE SIGLAS

AMI	*Amazon Machine Image*
AWS	*Amazon Web Services*
CIDR	*Classless Inter-Domain Routing*
DDoS	*Distributed Denial of Service*
EBS	*Elastic Block Store*
EC2	*Elastic Compute Cloud*
FIP	Publicação Federal de Processamento de Informações
GCP	*Google Cloud Platform*
IAM	*Identity and Access Management*
IGW	*Internet Gateway*
IP	*Internet Protocol*
KMS	*Key Management Service*
OECD	Organização para Cooperação e Desenvolvimento Econômico
RDS	*Relational Database Service*
SGSI	Sistemas de Gerenciamento de Segurança da Informação
SNS	*Simple Notification Service*
TI	Tecnologia da Informação
VPC	*Amazon Virtual Private Cloud*
VPN	*Virtual Private Network* ou Redes Virtuais Privadas
WAF	*Web Application Firewall*
RDP	*Remote Desktop Protocol*
SI	Segurança da Informação
SSH	*Secure Shell*

SUMÁRIO

1 INTRODUÇÃO

A proteção da informação tem se tornado um desafio crescente em instituições pelo mundo. A relevância do tema tem crescido nos últimos anos e às constantes mudanças de paradigmas torna a adoção de medidas para a mitigação de riscos premissas fundamentais para garantia da continuidade dos negócios e a boa prestação dos serviços públicos (Almeida, 2019).

Grandes empresas estão cada vez mais dependentes das tecnologias e estas precisam garantir que a informação utilizada esteja segura, respeitando os níveis de prioridade e necessidade de cada uma. A Segurança da Informação (SI) está associada à proteção existente sobre os dados de uma determinada empresa ou pessoa e por este motivo é um dos assuntos que possui mais relevância em praticamente todas as organizações (Cardoso e Moraes, 2018).

A computação em nuvem tem ganhado cada vez mais destaque como uma alternativa viável para empresas e usuários individuais, oferecendo uma abordagem flexível e escalável para o armazenamento e processamento de dados. De acordo com Doe et al. (2019), a tecnologia de nuvem proporciona uma infraestrutura de Tecnologia da Informação (TI) baseada em serviços que permite o acesso remoto a recursos computacionais por meio da Internet. Nesse contexto, a segurança dos dados em computação em nuvem tem sido amplamente debatida e considerada uma preocupação crítica (Smith, 2018).

Com a crescente integração da computação em nuvem, as organizações passaram a considerar como prioridade assegurar a segurança dos dados que são armazenados e processados nesse ambiente, ressaltando a relevância deste serviço (Jones e Johnson 2020).

Todos os dias as empresas produzem informações, independente do seu porte. Tais informações agregam valor e aumentam a produtividade e competitividade no mercado. Quando em uso conectado à Internet, estes dados precisam ser protegidos e, por este motivo, existem tantos sistemas e ferramentas de segurança (Zimmer, 2020).

Ao longo dos anos, diversas formas de criptografar uma mensagem foram desenvolvidas. As mais modernas surgiram, especialmente, para uso em operações militares. Entretanto, com a popularização dos sistemas digitais, os protocolos de criptografia tornaram-se padrão em várias ferramentas digitais (Sales, 2018).

A criptografia, cada vez mais, vem sendo adotada como medida de segurança e ainda gera muita curiosidade para quem não a conhece. O aumento da sua utilização ocorre principalmente em função dos casos de vazamento de dados que acenderam o alerta da necessidade de aumentar a segurança com as informações coletadas armazenadas na Internet (Adil, 2020).

As falhas mais comuns podem ir de uma senha de algum aplicativo sendo capturada por terceiros, dados pessoais de clientes vazados de sistemas corporativos ou mesmo um conjunto de senhas de vários clientes sendo acessado de dentro de um banco, sem sua autorização, comprometendo todo o sistema. Quanto mais o sistema estiver em contato com a Internet, mais ele estará sujeito a essas violações no sistema (Cardoso e Moraes, 2018).

A tecnologia está em constante transformação. O que torna o ambiente corporativo mais ágil e eficiente. No entanto, os hackers estão se beneficiando das novas tecnologias para praticar crimes cada vez mais sofisticados e difíceis de serem identificados. Neste caso, é preciso estar atento às novas formas de invasões e atuar de forma preventiva, combatendo ataques cibernéticos (Stefanello, 2021).

Justifica-se estudar esse tema, pois a criptografia e a computação em nuvem desempenham um papel crucial na SI. É por meio dessas técnicas, que se tornou viável minimizar perdas de dados, prevenir vazamentos e roubos de informações, ao mesmo tempo, em que assegura escalabilidade, flexibilidade e eficiência. Vale ressaltar que a segurança na nuvem também está intrinsecamente ligada às práticas e configurações adotadas pelos usuários. Além disso, a SI tornou-se uma demanda essencial para organizações de todos os tamanhos, dado o fluxo constante de documentos, arquivos e processos em empresas, visando evitar danos a dados confidenciais. Essa necessidade tornou-se ainda mais premente após a pandemia, devido à urgência das organizações em acelerarem a transformação digital (Stoque, 2021).

Diante deste contexto, esse projeto visa responder a seguinte questão de pesquisa: - **Como que a criptografia, as normas de segurança e técnicas da AWS podem garantir a SI das empresas?**

O objetivo geral deste trabalho é identificar e descrever algumas técnicas de criptografia, normas de segurança de dados e também algumas das técnicas da AWS para garantir a SI das empresas.

Os objetivos específicos são:

- Mapear e descrever as técnicas de criptografia e normas de segurança de dados para garantir da SI das empresas.
- Mapear e descrever alguns dos serviços da ferramenta *Amazon* AWS.

Espera-se que os resultados deste trabalho possam contribuir:

- Informando as técnicas e criptografia, normas de segurança de dados e alguns serviços da AWS para garantia da SI das empresas;
- Apresentando algumas das principais tecnologias de computação em nuvem utilizadas;

Quantos aos aspectos metodológicos, a natureza desta pesquisa é um resumo de assunto. Em relação aos procedimentos técnicos, é uma pesquisa bibliográfica.

Esta monografia está estruturada da seguinte maneira: neste capítulo é apresentado o contexto do trabalho, a questão de pesquisa, objetivo e resultados esperados. O capítulo 2 traz o referencial teórico com conceitos, definições, leis de proteção aos dados e trabalhos relacionados com o tema. No capítulo 3 é descrito o método, mostrando como o trabalho foi desenvolvido e o que foi feito para atingir o objetivo geral. No capítulo 4 são apresentadas as principais técnicas de computação em novem utilizando a AWS e suas ferramentas de proteção de dados já conhecidos. O capítulo 5 traz os experimentos para compreender a eficácia de alguns dos serviços descritos. Por fim, o capítulo 6 traz as considerações finais do TCC e sugestões para trabalhos futuros.

2 REFERENCIAL TEÓRICO

Este capítulo está dividido em duas partes: uma de conceitos e definições e a outra de trabalhos relacionados. A primeira parte explora os conceitos fundamentais e as definições da área, enquanto a segunda apresenta uma abordagem teórica, incluindo alguns trabalhos relacionados ao assunto.

2.1 Conceitos e Definições

Muitas mudanças ocorreram com a introdução da Internet, a informação, por exemplo, não era um ativo muito importante nas organizações há certo tempo. O importante eram os equipamentos, considerados o maior patrimônio de uma empresa. Com o passar dos tempos e a modernização das estruturas de trabalho, novos modelos de gestão foram surgindo e alguns ativos, anteriormente sem importância, assumiram a primeira posição. A informação é um ativo muito desejado e valioso tanto para uma pessoa como para uma organização, devendo obrigatoriamente estar protegido de acessos não autorizados (Fernandes, 2018).

A SI é um tema em ascensão e está diretamente relacionado com a proteção dos ativos tendo como objetivo preservar o seu valor. Na era da informação a constante evolução tecnológica abre novas perspectivas assim como novas ameaças e riscos (Almeida, 2019).

O Tribunal de Contas da União reconhece a importância da informação quando, em seu Manual de Boas Práticas em Segurança da Informação. (Mascarenhas, 2016).

> [...]Porque a informação é um ativo muito importante para qualquer instituição, podendo ser considerada, atualmente, o recurso patrimonial mais crítico. Informações adulteradas, não disponíveis, sob o conhecimento de pessoas de má-fé ou concorrentes podem comprometer significativamente não apenas a imagem da instituição perante terceiros, como também o andamento dos próprios processos institucionais. É possível inviabilizar a continuidade de uma instituição se não for dada a devida atenção à segurança de suas informações (Tribunal de Contas da União, 2012, p.10).

O fundamento da SI possui como finalidade garantir a segurança e privacidade de dados críticos, como detalhes de contas de clientes, informações financeiras ou propriedade intelectual. Ainda, permitir seu acesso, sempre que preciso, por quem tem autorização para isso. Garantir a proteção dos dados deve ser prioridade para empresas de todos os segmentos e portes, uma vez que informações confidenciais em mãos erradas podem resultar em prejuízo financeiro, perda da reputação,

problemas com clientes e penalidades com a Lei Geral de Proteção de Dados Pessoais (LGPD) (Stefanello, 2021).

A SI diz respeito ao conjunto de ações para proteção de um grupo de dados baseando-se nos seguintes pilares: confidencialidade, integridade, disponibilidade e autenticidade, sendo esses aspectos os pilares da proteção de dados (Durbano, 2018).

A SI se refere à proteção existente sobre as informações de uma determinada empresa ou pessoa, podendo ser aplicada métricas (com o uso ou não de ferramentas) para a definição do nível de segurança existente e, com isto, serem estabelecidas as bases para análise da melhoria ou piora da situação de segurança existente. A tríade CIA *(Confidentiality, Integrity and Availability)*, Confidencialidade, Integridade e Disponibilidade representa os principais atributos que, atualmente, orientam a análise, o planejamento e a implementação da segurança para um determinado grupo de informações que se deseja proteger (Ferreira, 2017).

A criptografia é um conjunto de técnicas pensadas para proteger uma informação de modo que apenas o emissor e receptor consigam compreendê-la. É utilizada em comunicações digitais, como na troca de mensagens ou em pagamentos online. São usados algoritmos para realizar a codificação e para decodificação sendo necessário ter acesso à chave utilizada no primeiro processo. O princípio básico da criptografia é garantir que duas entidades compartilhem mensagens entre si, sem que sejam acessadas por terceiros (Totvs, 2022).

A criptografia de segurança de dados é amplamente usada por usuários individuais e grandes corporações para proteger as informações entre um navegador e um servidor. Essas informações podem incluir de tudo, desde dados de pagamento até informações pessoais. Os softwares de criptografia de dados, também conhecidos como algoritmo de criptografia ou codificação, são usados para desenvolver um esquema de criptografia que teoricamente pode ser desvendado apenas com uma grande capacidade de processamento (Kaspersky, 2019).

A segurança de dados refere-se às medidas de proteção empregadas para proteger os dados contra acesso não aprovado e para preservar a confidencialidade, integridade e disponibilidade dos dados (Oracle, 2020).

As boas práticas de segurança de dados incluem técnicas de proteção de dados, como criptografia de dados, gerenciamento de chaves, edição de dados, subconjunto de dados e mascaramento de dados, bem como controles de acesso de

usuário privilegiado, auditoria e monitoramento. Usando técnicas de criptografia, esses processos protegem a empresa e o titular dos dados (Oracle, 2020).

Garantir boas práticas de SI, também é necessário para se ter um sistema seguro, é preciso seguir algumas recomendações. Entre elas: atualizar softwares, controlar acessos, fazer cópias de segurança, estabelecer uma política de segurança, usar senhas fortes e adotar um bom antivírus (Lyceum, 2022).

Um ataque à segurança digital pode resultar em qualquer coisa, desde roubo de identidade a tentativas de extorsão e perda de dados importantes, como fotos de família. Todos dependem de uma infraestrutura importante, como usinas, hospitais e empresas de serviços financeiros. A segurança dessas e de outras empresas é essencial para manter o funcionamento da sociedade (Cisco, 2019).

2.2 Leis e Normas

Esta seção apresenta algumas leis relacionadas a segurança dos dados e normas para a segurança da informação.

2.2.1 Lei Geral de Proteção de Dados Pessoais (LGPD)

Aprovada em agosto de 2018, a LGPD, também conhecida como Lei n° 13.709, foi promulgada com o objetivo de preservar os direitos essenciais de liberdade, privacidade e autodeterminação de cada pessoa. Essa legislação busca estabelecer um ambiente seguro e confiável, estabelecendo diretrizes e procedimentos uniformes para todos, promovendo a segurança jurídica e a igualdade de tratamento.

Esta lei tem como principal objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Tendo foco a criação de um cenário de segurança jurídica, com a padronização de regulamentos e práticas para promover a proteção aos dados pessoais de todo cidadão que esteja no Brasil, de acordo com os parâmetros internacionais existentes (Mpf, 2019).

A legislação se fundamenta em diversos valores e tem como principais objetivos:

- Assegurar o direito à privacidade e à proteção de dados pessoais dos usuários.
- Estabelecer regras claras sobre o tratamento de dados pessoais.
- Fortalecer a segurança das relações jurídicas e a confiança do titular no tratamento de dados pessoais
- Promover a concorrência e a livre atividade econômica, inclusive com portabilidade de dados.

A LGPD é aplicável a todas as empresas e entidades que realizam atividades de tratamento de dados pessoais no Brasil, independentemente de seu tamanho ou setor de atuação. Ela visa garantir que os dados pessoais sejam tratados de forma transparente, segura e em conformidade com a legislação.

A lei exige que o tratamento de dados pessoais seja realizado com base no consentimento do titular dos dados ou em outras bases legais específicas. A LGPD também estabelece diversos direitos para os titulares dos dados, como o direito de acesso aos seus dados, retificação, exclusão, portabilidade, entre outros.

A implementação da LGPD tem impacto significativo nas práticas de proteção de dados das empresas, exigindo a adoção de medidas de segurança, governança e transparência no tratamento das informações pessoais. A legislação busca promover uma cultura de respeito à privacidade e proteção dos dados, fortalecendo a confiança dos indivíduos no ambiente digital e estimulando a inovação responsável. A Figura 1 mostra os principais pontos da LGPD.

Figura 1 – Principais pontos da LGPD.

Fonte: Serpro, 2018.

O Brasil conta com a Autoridade Nacional de Proteção de Dados Pessoais, a ANPD, para fiscalizar e aplicar penalidades pelos descumprimentos da LGPD. As falhas de segurança podem gerar multas de até 2% do faturamento anual da organização no Brasil, limitado a R$ 50 milhões por infração. A autoridade nacional fixará níveis de penalidade segundo a gravidade da falha e enviará alertas e orientações antes de aplicar sanções às organizações (Mpf, 2019).

Portanto, esta nova lei mostra quem é o verdadeiro dono do dado, que não é aquele que o utiliza nem aquele que o salvaguarda em bancos de dados. O dado pessoal é estritamente da pessoa a quem ele diz respeito (Sepro, 2018).

2.2.2 Marco Civil da Internet

O Marco Civil da Internet, também conhecido como Lei 12.965/14, é o responsável por regularizar o uso da Internet no Brasil. Tem como objetivo estabelecer direitos, deveres e garantias no meio digital, sendo encarregado por regulamentar os direitos, garantias e deveres no uso da Internet (Aurum, 2022).

Pode-se entender que um dos objetivos da sua criação é retirar a sensação de "Terra sem Lei" que o ambiente tecnológico traz consigo. Afinal, antes do Marco Civil da Internet não havia legislação específica para tratar sobre o tema, até então dependendo apenas do art. 5 da CF.

- Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
- XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

O Marco Civil norteia todo processo de aplicação da Internet, elegendo os usuários como protagonistas, contexto da inovação da sociedade em rede, com foco na tutela dos direitos fundamentais consagrados em sede constitucional (Santos, 2021).

2.2.3 Norma ABNT NBR ISO 27001

A norma ISO 27001 é uma norma internacional de gestão de segurança da informação, que tem como principal objetivo o atendimento de uma série de requisitos,

processos e controles, que visam gerir a segurança da informação presentes em uma empresa.

A implementação da norma ISO 27001 busca garantir um alto compromisso com a proteção da informação, oferecendo às empresas uma referência e as normas práticas para identificar, analisar e implementar controles para gerenciar riscos de segurança da informação e proteger a confidencialidade, integridade e disponibilidade de dados essenciais aos negócios (Albuquerque, 2023).

O objetivo da ISO 27001 é de gerenciar e proteger a informação de uma empresa, utilizando a filosofia de gestão de riscos. Serão então descobertos os possíveis riscos sofridos para ser realizada a implementação de salvaguardas.

Essas salvaguardas (também chamadas de “controles”) são inseridas em determinadas políticas, implementações e também procedimentos técnicos. Caso a empresa em questão já utilize softwares e hardwares para a função, a ISO 27001 terá como foco definir ações para a prevenção de possíveis brechas na segurança da organização (Santos, 2022).

Para obter a certificação ISO 27001, é necessário alinhar o Sistemas de Gerenciamento de Segurança da Informação (SGSI) com os requisitos da norma. Esses requisitos visam ajudar as organizações a criar, manter e melhorar continuamente sua postura SGSI (Bueno, 2023).

Segundo o documento de diretrizes básicas da Organização para a Cooperação e Desenvolvimento Econômico (OECD), existem alguns princípios de Segurança da Informação (conscientização, responsabilidade, resposta, análise/avaliação de riscos, arquitetura e implementação de segurança, gestão de segurança e reavaliação, ética e democracia), a ISO 27001 com o seu SGSI implementa 7 deles (Bueno, 2023).

Além desses sete requisitos, a ISO 27001 também inclui anexos para auxiliar na implementação do SGSI. Os anexos incluem informações sobre a análise de riscos, os controles de segurança, a avaliação de conformidade, a auditoria do SGSI, a formação do pessoal e a documentação apresentado na Figura 2.

Figura 2 - ISO 27001.

Fonte: Clicksign, 2023.

2.2.4 Norma ABNT NBR ISO 27002

A Norma ABNT NBR ISO/IEC 27002/2022 foi concebida para ser usada por organizações de todos os tipos e tamanhos e pode ser usada como uma referência para determinar e implementar controles, visando o tratamento de riscos de SI de um Sistema de Gestão de Segurança da Informação (ABNT, 2022).

ISO 17799 se refere a um conjunto de práticas orientadas para a gestão da SI. Devido ao aumento das ameaças digitais e da crescente exposição de dados na Internet, sua importância é cada vez maior. De acordo como a ISO 17799, qualquer coisa que tenha um valor para a empresa é um ativo. Assim sendo, a gestão desses ativos é um dos seus pontos mais importantes, afinal, isso significa a proteção das informações do negócio (Gazola, 2018).

A ISO 17799 foi atualizada para numeração ISO 27002 em julho de 2007. Ela foi uma norma que estabelecia um referencial para que as empresas desenvolvessem e avaliassem o gerenciamento da TI. Assim, promovendo a confiabilidade das transações comerciais e a proteção das informações de negócio, como um todo.

O principal objetivo da ISO 27002 é estabelecer diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Isso também inclui a seleção, a implementação e o gerenciamento de controles, levando em conta os ambientes de risco encontrados na empresa (Ostec, 2016).

A ISO 27002 é mais um código de prática para controles de segurança. Ela descreve as melhores práticas para aqueles que implementam o SGSI, que é um sistema estratégico focado na proteção das empresas que trabalham com dados e informações confidenciais. Ele fornece diretrizes sobre a seleção, implementação e gerenciamento de controles, levando em consideração os ambientes de risco da organização (Rodrigues, 2021).

A Imagem ilustrativa sobre a Tríade Confidencialidade, Integridade e Disponibilidade ou CIA está apresentada na Figura 3.

Figura 3 – Tríade CIA.

Fonte: 4Future, 2017.

Observando a Figura 3, nota-se que a Tríade CIA são os 3 pilares que sustentam a SI e, juntos, tem como assegurar que informações confidenciais e críticas não sejam roubadas dos sistemas organizacionais por meio de ciberataques, espionagem, entre outras práticas (Telium, 2018).

2.3 Criptografia

Quando dados ou informações são partilhados através da rede mundial de computadores, eles percorrem um caminho através de vários dispositivos interconectados, distribuídos globalmente na internet pública. Durante essa trajetória, os dados ficam expostos a possíveis ameaças de comprometimento ou roubo por indivíduos mal-intencionados, também conhecidos como hackers. A criptografia consiste no processo de transformar o conteúdo legível por humanos em uma forma de texto incompreensível, denominada cifra.

A criptografia tem diversas aplicações e é amplamente utilizada em diferentes áreas para garantir a segurança e privacidade das informações. Algumas das principais aplicações da criptografia incluem:

Comunicações seguras: A criptografia é amplamente utilizada para proteger a confidencialidade e integridade das comunicações. As empresas empregam a criptografia para proteger as comunicações internas e externas. Isso pode incluir a criptografia de e-mails, mensagens instantâneas, videoconferências e chamadas telefônicas para evitar que terceiros interceptem e acessem informações confidenciais. Ela também pode autenticar remetentes e destinatários entre si. Os sistemas de software geralmente têm vários terminais, normalmente vários clientes e um ou mais servidores (Kovacs, 2021).

Armazenamento de dados: A criptografia de armazenamento de arquivos é uma medida importante de segurança para proteger informações confidenciais e pessoais contra acesso não autorizado. Ela também é empregada para proteger informações confidenciais armazenadas em dispositivos, como discos rígidos, unidades flash e servidores (Guedes, 2023).

Autenticação e identificação: O objetivo da autenticação consiste em identificar as diversas entidades de um sistema computacional. Utilizada para verificar a autenticidade e integridade dos dados, a criptografia garante que eles não tenham sido alterados ou corrompidos durante a transmissão ou armazenamento. Além disso, a criptografia também é empregada em sistemas de autenticação, como senhas e certificados digitais, para confirmar a identidade de usuários e dispositivos (Mazeiro, 2019).

Pagamentos eletrônicos: O comércio eletrônico anda de mãos dadas com o movimento de pagamentos digitais. A criptografia desempenha um papel fundamental

na segurança de transações financeiras online, como pagamentos com cartão de crédito e transferências bancárias eletrônicas. Ela protege as informações confidenciais do usuário, como números de cartão de crédito e dados pessoais, durante a transmissão e processamento dessas transações (Neistein, 2021).

Segurança de dispositivos e redes: A segurança de redes consiste na proteção da integridade, confidencialidade e acessibilidade dos dados que fazem uso de softwares e hardwares, a partir de um conjunto de regras e configurações. As empresas implementam a criptografia em dispositivos e redes para proteger a comunicação entre eles. Isso inclui a criptografia de redes sem fio, Redes Virtuais Privadas ou *Virtual Private* Network (VPN) e a criptografia de dados em dispositivos móveis, como smartphones e tablets, garantindo que os dados sejam transmitidos e armazenados com segurança (Keevo, 2020).

Proteção de dados sensíveis: A criptografia descarta qualquer acesso suspeito e, sempre que automatizada, também possibilita mais agilidade aos processos de codificação de dados e eventos. A segurança da informação é essencial para o crescimento saudável de qualquer negócio, sendo aplicada para proteger dados sensíveis em setores como saúde, governo e empresas. Ela é utilizada para garantir a confidencialidade de informações pessoais, registros médicos, dados de pesquisa e desenvolvimento, segredos comerciais e outros tipos de informações confidenciais que requerem proteção contra acesso não autorizado (Aim7, 2020).

Em essência, a criptografia desempenha um papel fundamental na garantia da segurança das informações em diversos contextos, protegendo a privacidade, a confidencialidade e a integridade dos dados.

2.3.1 Chaves de criptografia Simétrica

A chave simétrica, também chamada de chave privada, é o método mais frequente e simples de criptografia. Nesse modelo, a mesma chave é utilizada tanto pelo emissor quanto pelo receptor da mensagem, sendo especialmente adequado para usuários individuais e sistemas isolados.

A segurança de um sistema de criptografia vai variar conforme o tamanho da chave utilizada. Um algoritmo baseado no *Data Encryption Standart* (DES) padrão de criptografia de dados, em tradução livre) permite a criação de 72 quatrilhões de chaves

diferentes. Pode parecer muito, mas esse padrão já é considerado inseguro diante da capacidade de processamento dos dispositivos atuais (Cryptoid, 2018).

A segurança dos sistemas de criptografia simétrica é fundamentada na dificuldade de adivinhar, de forma aleatória, a chave correspondente do sistema. Por exemplo, uma chave de 128 bits exigiria bilhões de anos para ser descoberta, mesmo utilizando um computador comum. Quanto maior for o comprimento da chave de criptografia, mais difícil será desvendá-la. A Figura 4 ilustra um exemplo dessa situação.

Figura 4 – Criptografia Simétrica.

Fonte: CRYPTO ID, 2022.

Chaves com comprimento de 256 bits são consideradas altamente seguras e teoricamente resistentes até mesmo a ataques forçados por computador quântico (Binance, 2020).

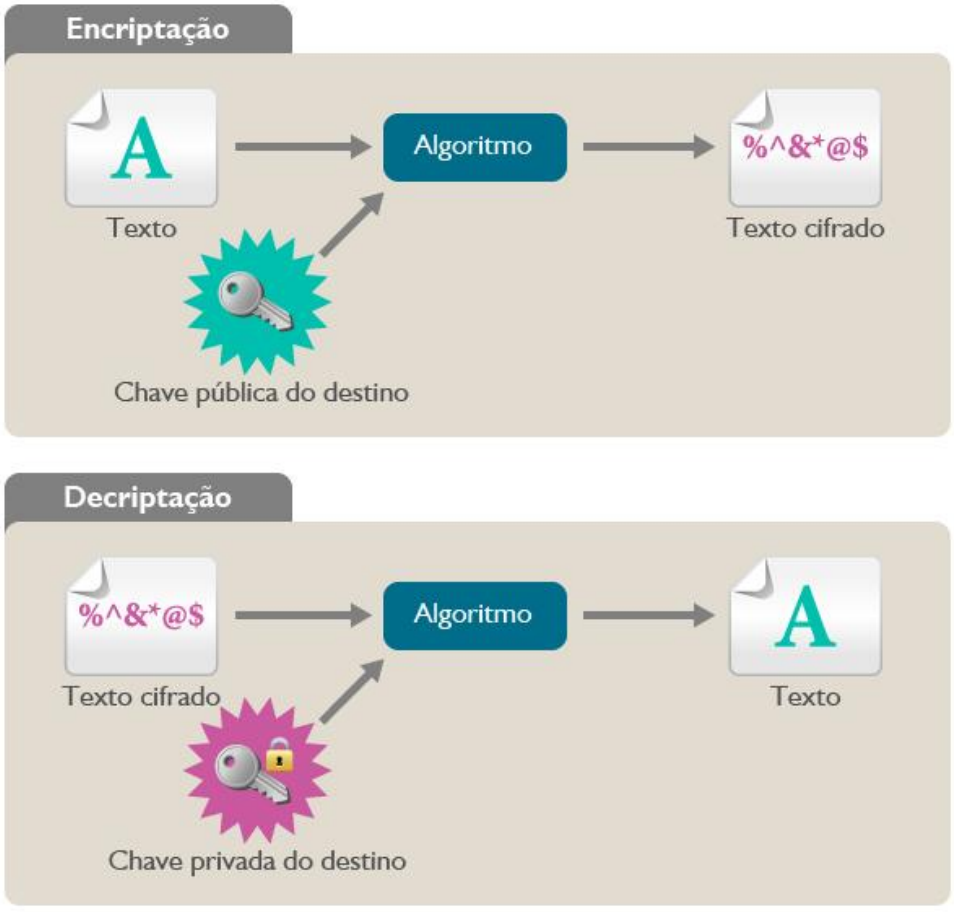
Apesar da sua eficiência, a criptografia simétrica apresenta algumas vulnerabilidades significativas em relação à segurança. Um dos desafios é a gestão das chaves, que se torna mais complexa à medida que aumenta o número de pessoas envolvidas na comunicação. Para cada N usuários, seria necessário o uso de N2 chaves distintas.

2.3.2 Chaves de criptografia Assimétrica

A criptografia assimétrica difere em cada extremidade de uma comunicação criptografada. Como o nome sugere, há dois lados envolvidos: o remetente, que realiza a criptografia dos dados e o destinatário, que os descriptografa. A criptografia assimétrica, também conhecida como criptografia de chave pública, utiliza um par de chaves: uma chave pública e uma chave privada. Os dados criptografados com a chave pública só podem ser descriptografados com a chave privada correspondente.

Uma chave é uma sequência de dados que, quando combinada com um algoritmo de criptografia, permite criptografar ou descriptografar mensagens. Os dados criptografados com a chave parecerão uma sequência aleatória de caracteres, mas qualquer pessoa que possua a chave correta pode convertê-los novamente para o formato de texto não criptografado. A Figura 5 ilustra um exemplo desse processo.

Figura 5 – Chave de Criptografia Assimétrica.



Fonte: IMD, 2017.

Nos algoritmos de criptografia assimétrica, são utilizadas chaves relacionadas, mas distintas, uma para criptografar e outra para descriptografar. Além disso, não é possível obter a chave de descriptografia a partir do conhecimento da chave de criptografia. Esses algoritmos sempre geram pares de chaves: uma chave para criptografar e sua correspondente para descriptografar.

Ao usar chaves diferentes, a criptografia assimétrica elimina o desafio de gerenciar e transmitir chaves que existe na criptografia simétrica. No entanto, os algoritmos de criptografia assimétrica também têm suas limitações. O principal desafio é o desempenho, pois esses algoritmos requerem um nível mais elevado de processamento em comparação com a criptografia simétrica.

A criptografia assimétrica não tem problema de distribuição de chaves, pois há uma chave pública que todo mundo pode conhecer. Contudo, isso tem um custo (Gran, 2020).

Segundo Nakamura (2007), os algoritmos assimétricos são muito mais lentos do que os algoritmos simétricos. Isso faz com que uma estratégia bem interessante seja usar os dois tipos de algoritmos em conjunto, visando aproveitar os pontos fortes e reduzir, então, os pontos fracos de ambos os tipos de criptografia.

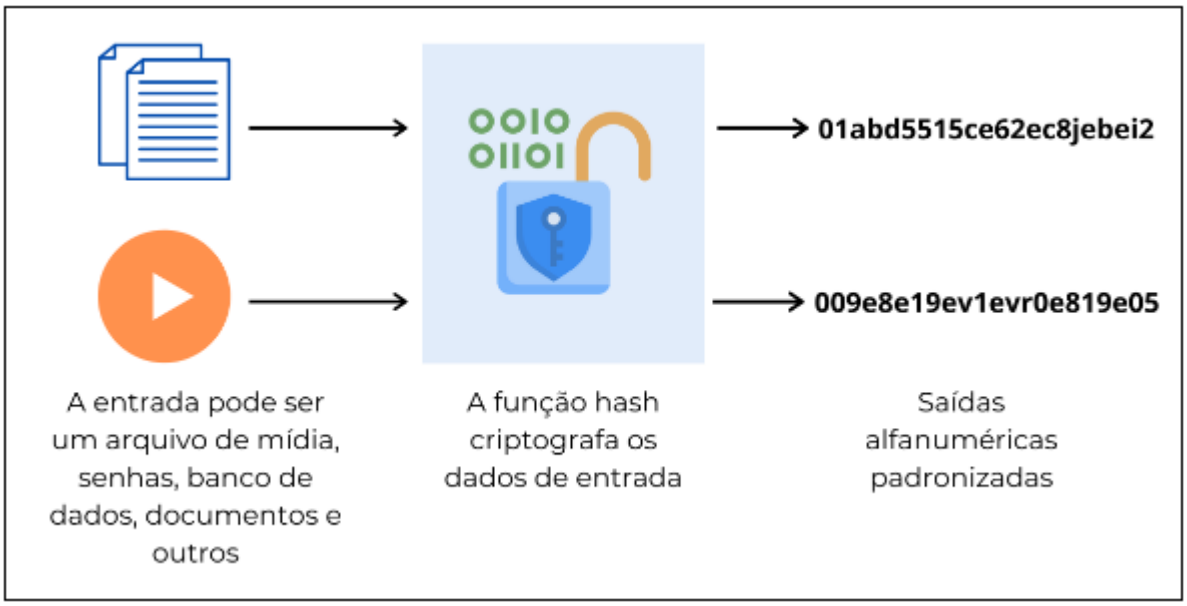
Existem vários algoritmos assimétricos amplamente utilizados e um dos mais conhecidos é o RSA, cujo nome veio das iniciais dos sobremos dos seus criadores, ou seja, Rivest, Shamir e Adleman. O RSA é amplamente empregado em navegadores para garantir a segurança de sites, bem como para criptografar e-mails.

2.3.3 Função *Hash*

A criptografia *hash* é usada em várias áreas, incluindo a SI, para garantir que os dados não sejam alterados e impedindo que dados sejam falsificados. A proteção de dados pessoais e das empresas é uma questão de extrema importância, pois os dados são susceptíveis de serem utilizados para fins ilícitos, caso não sejam protegidos adequadamente (Xpeduc, 2023).

Uma função de *hash* criptográfico é um algoritmo matemático que transforma um bloco de dados (como um arquivo, senha ou informações) em um conjunto alfanumérico com comprimento fixo de caracteres. A Figura 6 ilustra esse processo.

Figura 6 – Função Hash Criptográfico.



Fonte: Voitto, 2020.

Ao contrário de uma criptografia baseada em senha que tem como objetivo a confidencialidade da informação e pode ser revertida para seu estado original, a função *hash* é irreversível. Ela trata um arquivo de qualquer tamanho e o converte para algo bem pequeno, sem oferecer nenhuma senha para que os dados sejam lidos. Assim, se a pessoa não guardou de alguma forma o item, ela o perde assim que passa pelos algoritmos do *hash* (Carissimi, 2022).

Embora *hash* e criptografia sejam termos correlacionados, não são exatamente a mesma coisa. Um *hash* é um código criado a partir de um bloco de dados e utiliza um algoritmo criptográfico para garantir a segurança.

O *hash* identifica um bloco de dados singular e funciona para interligar blocos de uma cadeia. Isso significa que, para o *hash* funcionar, ele utiliza a lógica criptográfica. Por isso os hashes, por exemplo, estão associados aos blocos de dados do blockchain, o sistema por meio do qual circulam as criptomoedas (Brenol, 2023).

2.3.4 Criptografia RSA

O RSA é amplamente adotado como o principal método de criptografia globalmente. Em sua aplicação, são utilizadas duas chaves distintas, uma para cifrar e outra para decifrar. Esse sistema aborda o desafio da distribuição de chaves

encontrado na criptografia simétrica através do conceito de "envelopamento digital", enquanto sua segurança é fundamentada na complexidade da fatorização de números extensos. Aumentar o tamanho da chave contribui para reforçar a segurança, no entanto, isso também implica em um maior poder de processamento requerido.

O RSA é construído com base em um dos ramos mais tradicionais da matemática, a teoria dos números. Sua segurança é fundamentada na dificuldade de fatorar um número em seus fatores primos (números divisíveis apenas por 1 e por si mesmos). Todo número inteiro positivo maior que 1 pode ser decomposto de maneira exclusiva em um produto de números primos. Embora seja relativamente simples fatorar números pequenos, a tarefa se torna extremamente complexa e demorada quando lidamos com números grandes, tornando-se insolúvel em um tempo determinístico e polinomial.

No RSA, a chave pública e a chave privada são geradas por meio da multiplicação de dois números primos. O resultado dessa multiplicação, conhecido como módulo, é tornada pública. No entanto, se o número resultante dessa multiplicação for suficientemente grande, a fatoração para descobrir os primos que o compõem pode levar anos. Essa característica é o que confere segurança ao RSA, tornando virtualmente impossível quebrar a sua criptografia.

O menor número que foi usado na criptografia RSA tinha 100 dígitos (RSA-100 de 330 bits). O último número RSA quebrado foi o RSA-230 (762 bits). Foi fatorado em 15 de agosto de 2018. O maior número RSA usado hoje, 2023, tem 617 dígitos (RSA-2048).

2.3.5 *Data Encryption Standard* (DES)

A criptografia *Data Encryption Standart* (DES) é um dos modelos mais básicos, tendo sido um dos primeiros a ser criados (pela IBM, em 1977) e implementados. Consequentemente, é um dos mais difundidos mundialmente, pois fornece uma proteção básica de apenas cerca de 56 bits, oferecendo até 72 quatrilhões de combinações (Zanini, 2021).

O algoritmo DES opera fundamentalmente com duas operações em sua entrada: deslocamento de bits e substituição de bits. O processo é controlado pela chave utilizada. Por meio dessas operações, realizadas repetidamente e de maneira

não-linear, é obtido um resultado que não pode ser revertido à entrada original sem o uso da chave. Dessa forma, a chave desempenha um papel crucial no processo de criptografia do DES.

DES é um sistema de codificação simétrico por blocos de 64 bits, dos quais 8 bits (um byte) servem de teste de paridade (para verificar a integridade da chave). O algoritmo efetua combinações, substituições e permutações entre o texto a ser codificado e a chave, de modo com que as operações possam ser feitas nos dois sentidos (Spadari, 2020).

Embora o DES tenha sido amplamente utilizado e considerado seguro por muitos anos, a comunidade criptográfica começou a questionar sua resistência aos ataques no final do século XX. Como resultado, o algoritmo foi substituído pelo AES (*A*) em muitas aplicações, devido à sua maior segurança e eficiência.

Uma das principais limitações do DES é o tamanho da chave relativamente curto, o que o torna mais suscetível a ataques de força bruta e técnicas avançadas de criptoanálise. Além disso, o DES utiliza um algoritmo de criptografia de bloco simples, o que significa que blocos idênticos de texto plano sempre produzirão blocos de texto cifrado idênticos, tornando possível a análise de padrões (UFPE, 2017).

No entanto, em 17 de junho de 1997, um grupo de cientistas e voluntários de todo o mundo realizava a quebra do sistema de criptografia DES. A empresa de segurança norte-americana “RSA Security” resolveu colocar definitivamente à prova o sistema DES, promovendo a competição “DES Challenger” que oferecia um prêmio de 10mil dólares, para quem conseguisse quebrar o sistema.

A competição foi vencida pelo grupo DESCHALL, utilizando computadores de voluntários de todo o mundo conectados à internet. Esta operação provou que ataques por força-bruta já não eram tão “inviáveis” para os cidadãos comuns. Isso fez com que o governo americano abandonasse o sistema DES (usado desde a década de 70) algum tempo depois.

Para superar algumas das limitações do DES, surgiram variantes mais seguras, como o Triple DES (3DES) ou TDEA, que aplica o algoritmo DES três vezes consecutivas com duas ou três chaves diferentes. Essa abordagem aumenta o tamanho efetivo da chave para 112 ou 168 bits, proporcionando uma camada adicional de segurança. A grande desvantagem desse algoritmo é que ele é mais lento do que deveria ser comparado a algoritmos padrão (UFRJ, 2015).

Ainda assim, o DES tem seu valor histórico e é usado em algumas aplicações específicas que não requerem um nível de segurança tão alto quanto os padrões atuais (Mccomp, 2022).

2.3.6 *Advanced Encryption Standard* (AES)

A criptografia *Advanced Encryption Standard (*AES) é um algoritmo simétrico amplamente utilizado para criptografar e proteger dados sensíveis. Foi adotado pelo governo dos Estados Unidos como padrão de criptografia em 2001, substituindo o algoritmo DES.

O algoritmo de criptografia AES, é uma das técnicas de criptografia mais seguros da atualidade. Sua criptografia é feita em blocos de 128 bits, mas as chaves podem ser aplicadas também em 192 e 256 bits, tornando essa chave extremamente difícil de ser quebrada em ataques convencionais de cibercriminosos (Zanini, 2021).

O AES apresentou ser altamente eficaz e eficiente. Quando a chave correta é aplicada, ele adiciona uma sobrecarga mínima ou imperceptível a qualquer processo em que é utilizado. O AES é essencialmente uma forma de criptografia rápida e extremamente segura, sendo amplamente preferida por empresas e governos em todo o mundo.

A criptografia AES é amplamente utilizada em sistemas e aplicativos que exigem segurança de dados, como comunicações seguras, transações bancárias, proteção de dados pessoais e armazenamento criptografado. Sua adoção generalizada e confiança na segurança que oferece fazem do AES uma escolha popular tanto para uso comercial quanto governamental.

A *National Security Agency* (NSA), bem como outros órgãos governamentais, utilizam criptografia AES e chaves para proteger informações classificadas ou outras informações confidenciais. Além disso, o AES é frequentemente incluído em produtos de base comercial, incluindo, mas limitado a:

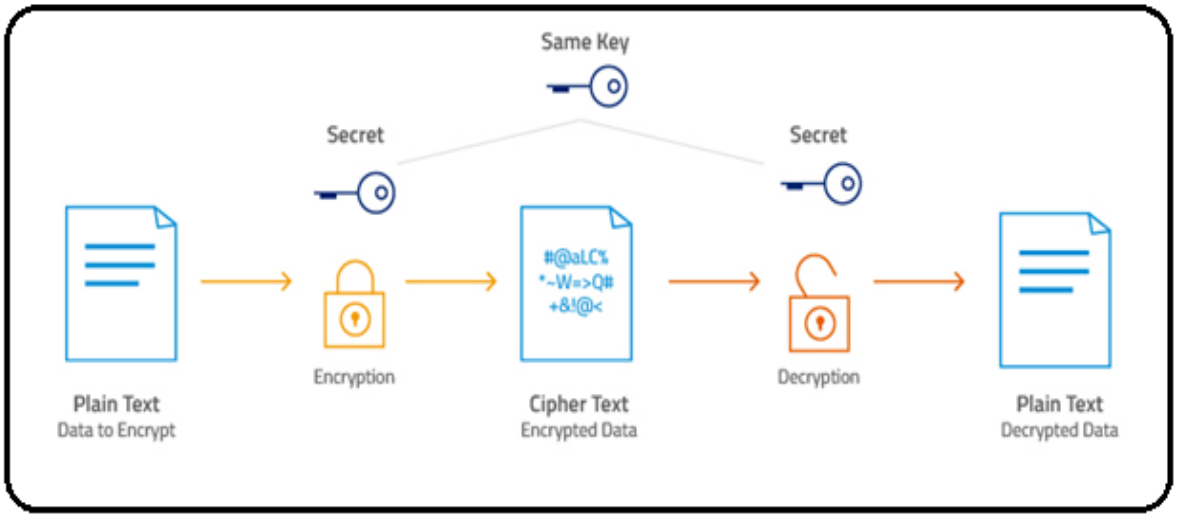
- Wi-Fi (pode ser usado como parte do WPA2).
- Aplicativos móveis (como WhatsApp e LastPass).
- Suporte à processador nativo.
- Bibliotecas em muitas linguagens de desenvolvimento de software.
- Implementações VPN.

- Componentes do sistema operacional, como sistemas de arquivos.

O AES é composto de AES-128, AES-192 e AES-256. Os numerais representam o número de bits-chave em cada bloco de criptografia e descriptografia. Para cada bit adicionado, o número de chaves possíveis dobra, o que significa que a criptografia de 256 bits é igual a 2 elevado à 256. Por sua vez, cada bit-chave tem um número diferente de etapas.

Para os 256 bits, há 14 etapas. Então, a chance de um hacker encontrar a sequência correta de 2 elevado à 256 bits, sendo misturada 14 vezes é incrivelmente baixa, para dizer o mínimo. Sem mencionar, o tempo e capacidade de processamento necessários para o trabalho (Kingston, 2021). A Figura 6 ilustra a Criptografia AES.

Figura 7 – Criptografia AES.



Fonte: *Cloud Storage,* 2023.

Segundo Nash (2019), o AES foi projetado para ser simples e fácil, tanto no software quanto no hardware, juntamente com outros ambientes mais restritos. Quinze projetos concorrentes de algoritmos de chave simétrica foram submetidos a análises preliminares pela comunidade criptográfica mundial, incluindo a NSA.

A AES obteve um enorme sucesso ao proteger informações sensíveis do governo dos Estados Unidos. Esse êxito impulsionou sua ampla adoção no setor de segurança privada, fazendo da AES o algoritmo mais utilizado na criptografia de chave

simétrica. A confiabilidade e a robustez da AES consolidaram sua posição como um padrão de referência para a proteção de dados em várias indústrias.

É importante destacar que a segurança da criptografia AES depende da proteção adequada das chaves de criptografia, pois qualquer pessoa que tenha acesso à chave correta pode descriptografar os dados. Portanto, a gestão adequada de chaves é essencial para garantir a eficácia da criptografia AES.

2.4 Computação em nuvem

A *Cloud Computing*, também conhecida como computação em nuvem, refere-se à disponibilização sob demanda de recursos de tecnologia da informação (TI) através da Internet, com a definição de preço baseada no uso. Em vez de investir na aquisição, posse e manutenção de data centers e servidores físicos, é possível obter acesso a serviços tecnológicos, como capacidade computacional, armazenamento e banco de dados, de acordo com as necessidades, utilizando um provedor de nuvem, como a AWS (Amazon, 2022).

A concepção inicial da computação em nuvem remonta aproximadamente à década de 1950, quando a ideia era "compartilhar o tempo" de um único computador central, permitindo a comunicação de vários usuários com esse mainframe, onde todo o processamento ocorria. Na década de 1970, predominava o uso de recursos locais para dados e programas. Foi nesse período que se introduziu a virtualização, marcando um avanço significativo nesse campo (Zaharia; Radu, 2017).

Segundo Microsoft Azure (2023), computação em nuvem representa uma significativa transformação na abordagem convencional das empresas em relação aos recursos de TI. Há seis motivos frequentemente observados para a adoção dos serviços de computação em nuvem por organizações, a seguir:

- **Custo**: Migrar para a nuvem permite otimizar os custos de TI ao eliminar despesas de capital associadas à compra de hardware e software, além de reduzir gastos com data centers locais e a necessidade de especialistas de TI para gerenciar a infraestrutura.
- **Escala global**: Os serviços de computação em nuvem proporcionam dimensionamento elástico, permitindo ajustar os recursos de TI

conforme necessário, garantindo potência de computação, armazenamento e largura de banda adequados na localização geográfica correta.

- **Desempenho**: Os principais serviços de nuvem operam em uma rede global de data centers seguros, oferecendo benefícios como redução da latência de rede para aplicativos e eficiência econômica resultante de atualizações regulares com hardware de última geração.
- **Segurança**: Provedores de nuvem oferecem políticas, tecnologias e controles abrangentes para fortalecer a segurança dos dados, aplicativos e infraestrutura, protegendo contra ameaças potenciais.
- **Velocidade**: Os serviços de nuvem, geralmente fornecidos sob demanda, permitem a rápida provisionamento de grandes quantidades de recursos de computação em minutos, proporcionando flexibilidade e aliviando a pressão do planejamento de capacidade.
- **Produtividade**: A computação em nuvem elimina tarefas demoradas associadas à gestão de *data centers* locais, como configuração de hardware e correção de software, permitindo que as equipes de TI concentrem seu tempo em metas comerciais essenciais.
- **Confiabilidade**: A nuvem facilita e reduz os custos de *backup* de dados, recuperação de desastres e continuidade dos negócios, ao permitir a replicação dos dados em vários sites redundantes na rede do provedor de serviços de nuvem.

A concepção fundamental por trás da computação em nuvem é proporcionar aos clientes uma abordagem mais simplificada, direta e eficiente para a utilização de recursos e serviços vinculados à área de Tecnologia da Informação. Nesse contexto, uma empresa disponibiliza serviços como banco de dados, armazenamento e rede, possibilitando que outras organizações os acessem sem a necessidade de realizar investimentos em equipamentos (Syozi, 2021).

2.4 Trabalhos Relacionados

Esta seção apresenta alguns trabalhos relacionados ao tema em estudo.

2.4.1 Um estudo sobre serviços de segurança oferecidos pela tecnologia de c*loud computing* na Google e suas aplicações

Dantas (2022) teve como objetivo identificar e descrever os serviços de segurança oferecidos pela *Google Cloud*, mapeando suas ferramentas e identificando as principais práticas de segurança de cada serviço. O trabalho foi realizado demonstrando os conceitos e definições do *Google Cloud Platform* (GCP), bem como *Assured Workloads* que é uma ferramenta da Google Cloud com objetivo de aplicar controles de segurança e suporte a requisitos de conformidade, bem como outras 24 ferramentas.

O estudo permitiu observar que conhecer os serviços e ferramentas de segurança oferecidas pela *Google Cloud* é essencial para se ter uma infraestrutura bem configurada e segura de ataques e vazamentos de dados.

Além disso, ter o conhecimento de quais são os principais tipos de vulnerabilidade e ataques é um grande fator para se ter uma boa configuração de segurança coma escolha de serviços apropriados.

2.4.2 As formas de ataques aos dados mais conhecidas e as correspondentes vulnerabilidades

Machado (2021) teve como objetivo identificar e descrever formas de ataques aos dados mais conhecidas, demonstrando suas vulnerabilidades, foi identificado as formas preventivas de ataque, bem como empresas alvo desses ataques utilizando um *SQL injection.*

O estudo permitiu identificar que *Port Scanning Attack, Phishing, Spoofing, Sniffing e SQL Injection,* são formas de ataques bastante frequente, os cibercriminosos utilizam falhas no sistema para roubar dados de funcionários e monitorar essas empresas, assim realizando o roubo.

Com base no estudo, foi concluído que, conhecer as formas de ataques e as correspondentes vulnerabilidades é uma das maneiras de prevenir as organizações desses ataques. Os ataques cibernéticos atingem desde pequenas empresas até multinacionais, por isso, a segurança dos dados é muito importante.

O conhecimento de alguns dos ataques e as vulnerabilidades que permitem o acesso indesejado pela empresa, ajudar a conscientizar seus funcionários e a prevenir o roubo de dados, pois o vazamento das informações pode gerar consequências, com altos custos e grandes prejuízos.

2.4.3 Tratamento de dados pessoas, por que precisamos saber como os nossos dados pessoais são tratados

Martins (2020) teve como objetivo identificar os tratamentos de dados e entender de que forma as empresas tratam os dados pessoais, foi demonstrado o surgimento da LGPD e sua importância para o tratamento de dados, além de demonstra o tratamento de dados pessoais pelo poder público brasileiro. Todo o estudo teve como objetivo a conscientização do titular dos dados pessoais.

As empresas que trabalham com tecnologia ou que oferecem serviços que necessitam de dados pessoais, passaram a realizar uma constante coleta de dados pessoais do usuário/titular. Portanto, houve a necessidade de regulamentação do uso desses dados, a fim de evitar a violação aos direitos fundamentais dos usuários, dentre eles, a privacidade e a intimidade.

Portanto, concluíram que é necessário que os agentes de tratamento busquem diversas maneiras de proteger os dados pessoais, mas também informar o titular, levar a informação do que está acontecendo de maneira clara e precisa, gerando uma cultura de proteção de dados.

3. PROCEDIMENTOS METODOLOGICOS

Esta pesquisa, segundo sua natureza é um resumo de assunto, buscando explicar a área do conhecimento do projeto, indicando sua evolução histórica, como resultado da investigação das informações obtidas, levando ao entendimento de suas causas e explicações (Wazlawick, 2014).

Segundo os objetivos é uma pesquisa exploratória e descritiva. A descritiva busca dada mais consistentes sobre determinado assunto, porém, não ocorre a interferência do pesquisador, apenas expõe os fatos como realmente são. A pesquisa exploratória muitas vezes é considerada como a primeira parte do processo de

pesquisa, porque não necessariamente o autor tem um objetivo ou hipótese definida (Wazlawick, 2014).

Quanto aos procedimentos técnicos, é uma pesquisa é bibliográfica, documental e experimental. Pesquisa bibliográfica implica no estudo de artigos, teses, livros e outras publicações que podem ser citados no projeto (Wazlawick, 2014).

A pesquisa bibliográfica, será elaborada a partir de materiais já publicados, podendo incluir livros, teses, materiais disponibilizados na Internet, revistas, entre outros. A principal vantagem é permitir uma sucessão de fenômenos maior do que seria capaz de pesquisar diretamente (Gil, 2017).

De acordo com Gil (2017) a pesquisa bibliográfica deve seguir os seguintes passos:

a) Escolha do tema de pesquisa, que deve estar relacionado com o interesse do aluno, o tema escolhido foi: **criptografia e técnicas para garantir a segurança da informação em nuvem, utilizando a *Amazon Web Services***;

b) Fazer o levantamento bibliográfico preliminar de periódicos e artigos relacionados ao assunto de pesquisa dos ultimos 5 anos. No caso foram: criptografia, leis e normas e serviços da AWS.

c) Fazer a formulação do problema com base no levantamento bibliográfico, que será: Como que a criptografia, as normas de segurança e técnicas da AWS podem garantir a SI das empresas?

d) Busca das fontes: As pesquisas foram feitas na base de dados da CAPES, repositório da PUCGO (RAG), *Web of Science,* Documentação da AWS;

e) Leitura do material selecionado para responder o problema, periódicos, artigos, jornais e etc, de preferência materiais publicados a pelo menos cinco anos atrás;

f) Foi realizado o fichamento de todo o material lido, para facilitar a escrita do TCC e relembrar principalmente da referência bibliográfica;

g) Realizada redação do TCC de acordo com as normas da ABNT.

A pesquisa documental consiste na análise de documentos ou dados, sendo eles relatórios de empresas, banco de dados, correspondências etc. (Wazlawick, 2014). Segundo Gil (2017), uma pesquisa é considerada documental quando o material consultado é interno à organização. Foram lidos documentos do site da AWS sobre o tema estudado.

A pesquisa experimental, consiste que o pesquisador provoque mudanças no ambiente de pesquisa, observando se as alterações realizadas são de acordo com os resultados esperados (Wazlawick, 2014).

A pesquisa experimental é composta das seguintes etapas, conforme Gil (2017):

a) Fazer a formulação do problema com base no levantamento bibliográfico, que será: **Como que a criptografia, as normas de segurança e técnicas da AWS podem garantir a SI das empresas?**

b) Definição do plano experimental: foi descrito alguns serviços de segurança no ambiente da AWS e apresentado a criação de três desses serviços que foram: IAM, EC2, VPC. Foi utilizado o ambiente da plataforma *Amazon*, sendo apresentadas as etapas de configurações e definições de suas criações;

c) Determinação do ambiente: o ambiente que foi utilizado para desenvolvimento dos experimentos foi constituído por uma máquina com o sistema operacional *Microsoft Windows* versão 11. Todos os experimentos foram feitos utilizando o console da *Amazon Web Service*. A máquina virtual EC2 foi configurada utilizando uma AMI Ubuntu Server 22.04 LTS (HMV), com SSD volume *Type* em uma instancia t3.micro, 2vCPU de 1 GB de memória RAM e um espaço em disco de 8 GB;

d) Coleta de dados: Foram realizados testes com os serviços IAM, EC2 e VPC, sendo criados e implementados conforme apresentados na documentação oficial da AWS, cada um destes 3 serviços.

e) Análise e interpretação dos dados: foram monitorados e analisados os resultados obtidos de acordo com as configurações de regras, políticas de segurança do IAM, foram feitos testes para as redes VPC e para o funcionamento da máquina virtual EC2;

f) Realizada redação do TCC de acordo com as normas da ABNT.

4. SERVIÇOS DA AWS QUE PODEM GARANTIR A SI NAS EMPRESAS

Este capítulo descreve oito categorias complementares de serviços de segurança da AWS, com o propósito de introduzir um sistema de segurança robusto destinado a usuários e empresas de diversas dimensões. O conteúdo presente nesta seção foi extraído da documentação oficial da *Amazon Web Services* (AWS, 2023).

Os recursos de segurança da AWS estão divididos entre os 8 serviços, a seguir:

- *Identity and Access Management* (IAM);
- *Amazon Virtual Private Cloud* (VPC);
- *Elastic Compute Cloud* (EC2);
- *Amazon CloudWatch;*
- *Key Management Service* (KMS);
- *AWS Shield;*
- *Amazon S3;*
- *Amazon RDS.*

4.1 *Identity and Access Management* (IAM)

O *Identity and Access Management Identity* (IAM) ou Gerenciamento de Identidade e Acesso, é uma parte essencial de um programa de segurança da informação, que garante que apenas usuários autorizados e autenticados possam acessar seus recursos e ferramentas.

Com o IAM, é possível criar e gerenciar usuários, grupos e permissões para controlar o acesso aos serviços e recursos da AWS. As normas ABNT NBR ISO 27001 e 27002 ajudam a entender e aplicar o princípio do menor privilégio que o IAM pratica em seu funcionamento, garantindo que os usuários tenham apenas as permissões necessárias para realizar suas tarefas.

Sabendo da importância de estabelecer práticas robustas de segurança e gestão de identidade em um ambiente digital, é recomendado definição claras sobre entidades principais, tais como, contas, usuários, funções e serviços que possam realizar ações dentro de uma aplicação.

Além disso, é muito importante implementar um sistema de gerenciamento de credenciais, visando assegurar a autenticidade e a autorização adequada das

entidades envolvidas. Tal prática contribui significativamente para a prevenção de acessos não autorizados e potenciais brechas de segurança.

Por meio do IAM, os administradores têm a capacidade de definir políticas granulares que especificam quais ações podem ser executadas em recursos específicos por diferentes entidades, como usuários, grupos e funções.

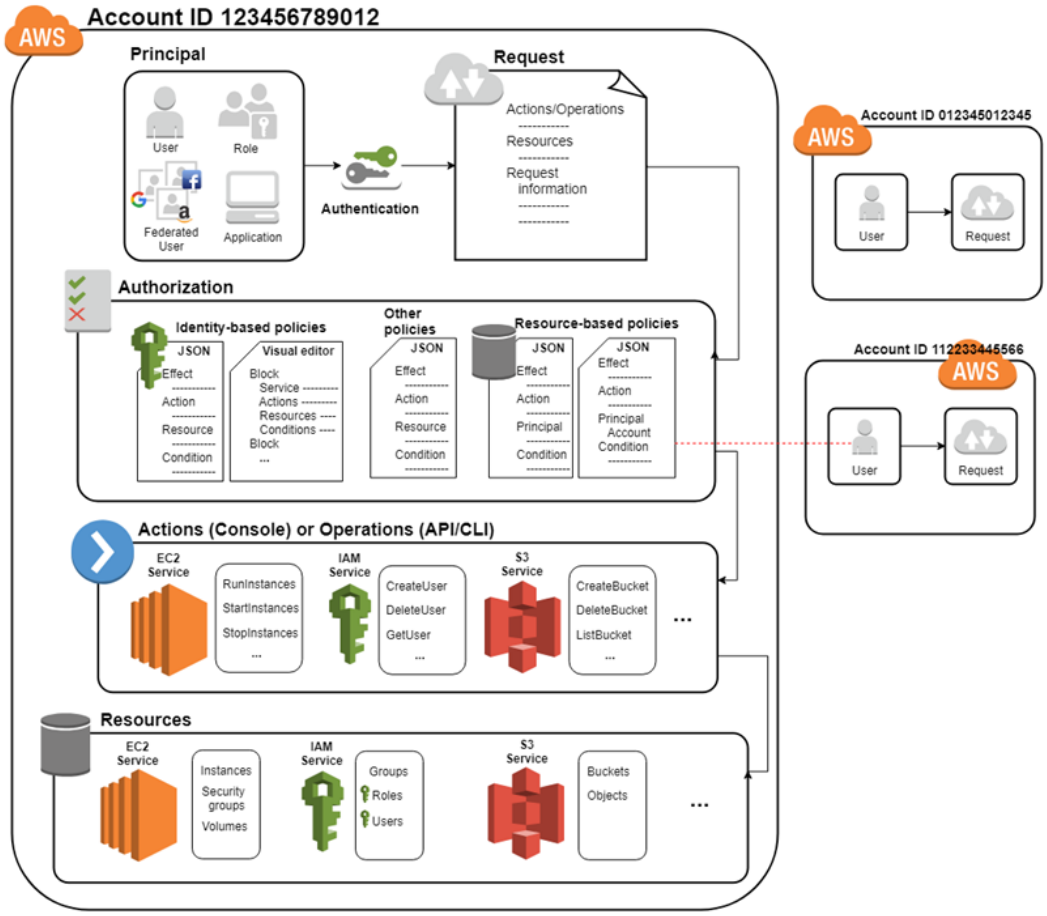
A implementação adequada do IAM, contribui significativamente para fortalecer a postura de segurança, garantindo que apenas as entidades autorizadas possam realizar ações específicas, alinhando-se assim às melhores práticas de controle de acesso e gestão de privilégios em ambientes de computação em nuvem.

Em relação ao usuário do IAM, ao empregar os serviços da AWS para a execução de tarefas, as credenciais e permissões essenciais serão fornecidas pelo administrador. À medida que se utiliza funcionalidades mais avançadas, pode ser necessário solicitar permissões adicionais. Adquirir compreensão sobre o gerenciamento de acesso é fundamental para requisitar, de maneira apropriada, as permissões necessárias ao administrador.

Um usuário do IAM representa uma identidade dentro da conta da AWS, possuindo permissões específicas designadas a uma única pessoa ou aplicação. É recomendado, sempre que viável, a utilização de credenciais temporárias em detrimento da criação de usuários do IAM com credenciais de longo prazo, tais como senhas e chaves de acesso.

Compete ao administrador determinar quais funcionalidades e recursos do IAM os usuários do serviço devem acessar. Nesse sentido, é recomendado encaminhar solicitações ao administrador do IAM para efetuar alterações nas permissões dos usuários. No papel de administrador do IAM, esta função envolve a gestão das identidades do IAM e a elaboração de políticas para controlar o acesso. A Figura 8 ilustra a criação do IAM, com a criação de usuários e as permissões aplicadas a ele. Posteriormente na Figura, é observado a integração das permissões do IAM com outros serviços da AWS, como o EC2 e o S3:

Figura 8 – Gerenciamento de Identidade e Acesso.



Fonte: *Amazon Web Service,* 2023.

Observando a Figura 8, inicialmente, um usuário ou uma aplicação emprega suas credenciais de *login* para autenticar-se na AWS. A autenticação é efetuada por meio da combinação das credenciais de *login* com uma entidade principal (usuário do IAM, usuário federado, perfil do IAM ou aplicação) na qual a Conta da AWS deposita confiança.

Posteriormente, uma solicitação é efetuada para conceder acesso aos recursos à entidade principal. A concessão de acesso ocorre em resposta a uma solicitação de autorização. Quando um serviço é selecionado, a solicitação de autorização é encaminhada para esse serviço, o qual verifica se a sua identidade está autorizada, quais políticas estão sendo aplicadas para controlar o nível de acesso concedido e outras políticas pertinentes. Tais solicitações de autorização podem ser originadas

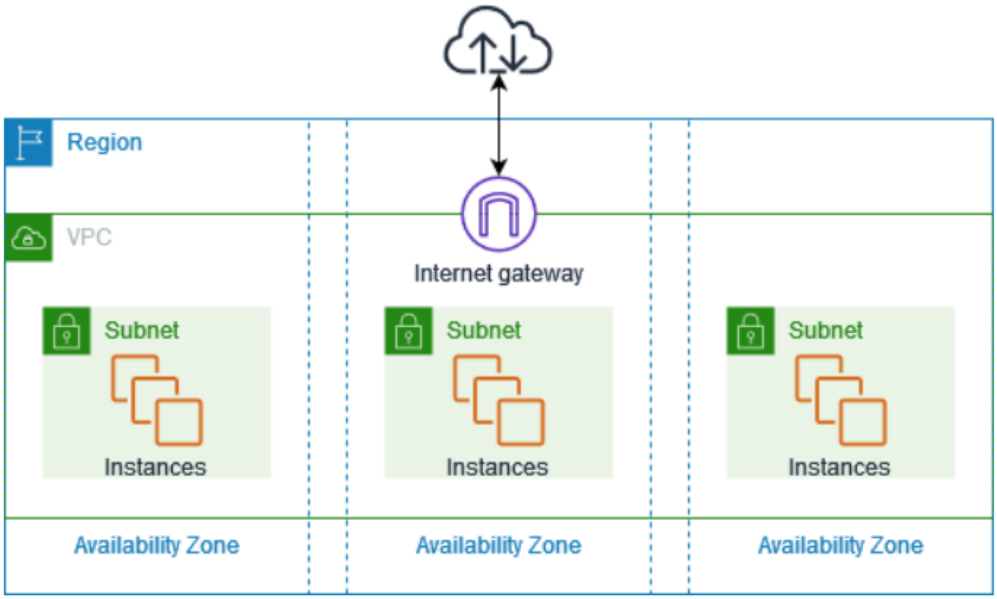
tanto por entidades principais em uma conta da AWS quanto por outras contas da AWS nas quais o administrador reconhece.

4.2 *Amazon Virtual Private Cloud* (VPC)

Amazon Virtual Private Cloud (Amazon VPC) é um serviço que permite provisionar uma seção logicamente isolada da infraestrutura de computação em nuvem da AWS. Ou seja, o Amazon VPC permite que o usuário crie uma rede virtual na nuvem AWS, semelhante à infraestrutura de rede que ele teria em um *data center* físico, mas com os benefícios da escalabilidade, flexibilidade e recursos da AWS.

A Figura 9 subsequente ilustra uma *Virtual Private Cloud* (VPC) exemplar. A VPC apresenta uma sub-rede situada em uma das zonas de disponibilidade na região, instâncias do EC2 distribuídas em cada sub-rede e um *gateway* de Internet com a finalidade de viabilizar a comunicação entre os recursos dentro de sua VPC e a Internet.

Figura 9 – *Amazon Virtual Private Cloud*.

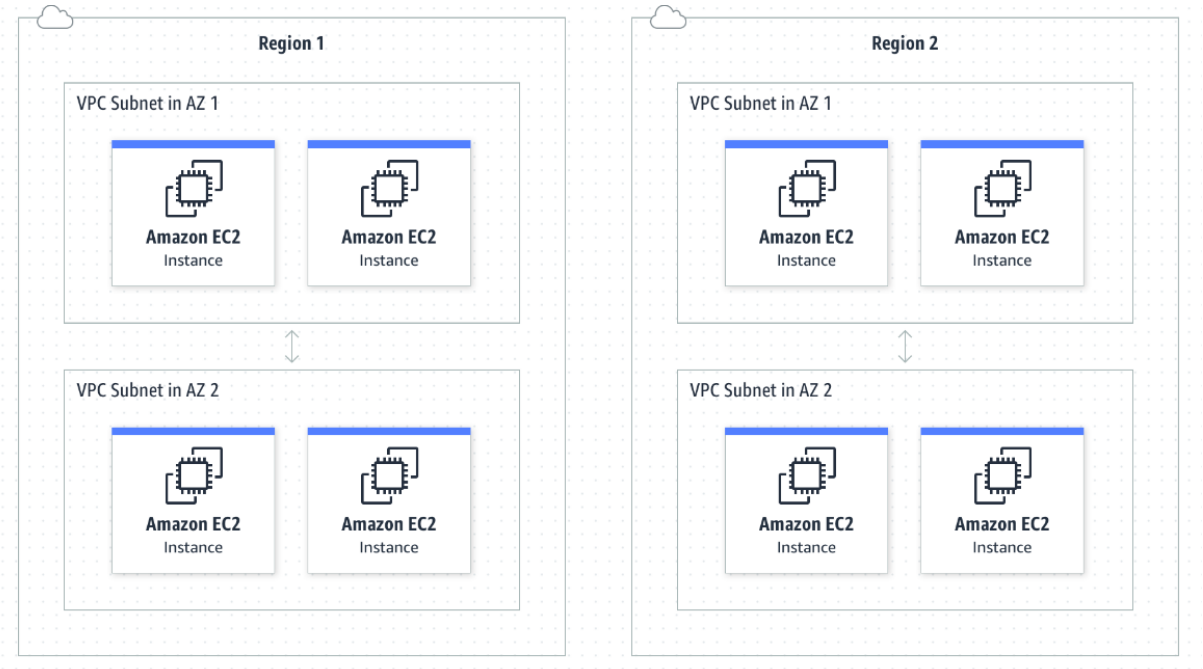


Fonte: *Amazon Web Service,* 2023.

O *Amazon Elastic Compute Cloud* (EC2) é um recurso da AWS que permite que os usuários executem máquinas virtuais (também conhecidas como instâncias) na nuvem. Essas instâncias podem ser configuradas com diferentes tipos de recursos, como poder computacional, memória e capacidade de armazenamento, para atender às necessidades específicas de um aplicativo ou carga de trabalho.

O Amazon VPC proporciona controle total sobre o ambiente de rede virtual, permitindo a gestão do posicionamento de recursos, conectividade e segurança. Para iniciar, é necessário configurar a VPC no console de serviços da AWS. Posteriormente, acrescente recursos, como instâncias do EC2 e *Amazon Relational Database Service* (RDS). Por fim, é necessário estabelecer as diretrizes de comunicação entre suas VPCs, seja entre elas, entre contas, zonas de disponibilidade (AZs) ou Regiões da AWS. Na Figura 10, é possível observar o compartilhamento de tráfego de rede entre duas VPCs em cada região.

Figura 10 – *Amazon Virtual Private Cloud* por região.



Fonte: *Amazon Web Service,* 2023.

As VPCs têm a capacidade de estabelecer comunicação entre si, podendo abranger diferentes contas, zonas de disponibilidade ou Regiões da AWS. O diagrama em questão ilustra uma configuração possível, na qual, dentro da Região 1, o tráfego de rede é compartilhado entre uma VPC na zona de disponibilidade 1 e outra na zona de disponibilidade 2. A mesma arquitetura é replicada na Região 2. Importante notar que, neste exemplo específico, as VPCs nas Regiões 1 e 2 não estabelecem conexão direta entre si.

A VPC constitui uma rede virtual exclusiva associada à conta do usuário na AWS, sendo logicamente isolada de outras redes virtuais na Nuvem da AWS. Neste contexto, é possível especificar um intervalo de endereços *Internet Protocol* (IP) para a VPC, incluir sub-redes, agregar *gateways* e associar grupos de segurança.

Com a VPC é possível conectar outros recursos da AWS, como instâncias do Amazon EC2, bancos de dados do Amazon RDS e *buckets* do Amazon S3, dentro de um ambiente virtualmente isolado. Além disso, o VPC fornece um controle granular sobre a infraestrutura na nuvem criada. Os principais conceitos e componentes de um VPC na AWS são:

- **CIDR Block (Intervalo de Endereços IP):** Ao criar um VPC, o usuário precisa especificar um bloco de *Classless Inter-Domain Routing* (CIDR), que é o intervalo de endereços IP. Este bloco determina a faixa de endereços IP disponíveis para os recursos dentro do VPC. O bloco CIDR representa um intervalo de endereços IP. Por exemplo, 10.0.0.0/16, que representa todos os endereços IP no intervalo de 10.0.0.0 a 10.0.255.255. Ao criar um VPC, é necessário especificar este bloco, determinando a faixa de endereços IP disponíveis para os recursos dentro do VPC.
- **Subnets (Sub-redes):** Dentro de um VPC, o usuário cria sub-redes para organizar e isolar recursos. Cada sub-rede é associada a uma ou mais zonas de disponibilidade e possui seu próprio intervalo de endereços IP dentro do bloco CIDR do VPC. As sub-redes são divisões lógicas da VPC. Cada sub-rede está associada a uma zona de disponibilidade (AZ). Isso permite distribuir recursos em várias zonas de disponibilidade para aumentar a resiliência e a disponibilidade.

- **Rotas e Tabelas de Rotas:** Cada VPC tem uma tabela de rotas que controla o tráfego de rede. O usuário pode personalizar as rotas para direcionar o tráfego entre sub-redes e para a Internet ou outros serviços AWS. As rotas podem ser configuradas para direcionar o tráfego para gateways, instâncias EC2 ou outros recursos. Isso fornece flexibilidade na configuração da conectividade dentro do seu ambiente VPC.
- ***Gateway* de Internet:** O *Internet Gatway* (IGW) é um componente muito importante para permitir a comunicação entre instâncias dentro do VPC e a Internet. Ele fornece uma rota para o tráfego de entrada e saída da Internet, permitindo que instâncias dentro do VPC acessem recursos externos e sejam acessíveis a partir da Internet.
- ***Security Groups* (Grupos de Segurança):** *Security Groups* são *firewalls* virtuais associados a instâncias. Eles permitem ou negam o tráfego com base em regras configuradas pelo usuário para cada porta, protocolos e endereços IP. Cada instância pode ter múltiplos *security groups* e as regras são aplicadas de maneira implícita e por padrão negando todo o tráfego.
- **Network Access Control Lists (ACLs):** *Access Cotrol List* (ACLs) atuam como *firewalls* na camada de subnet, controlando o tráfego de entrada e saída. Elas são compostas por regras de permissão e negação que podem ser aplicadas a uma subnet inteira. Ao contrário dos *Security Groups*, as ACLs são explícitas e avaliadas na ordem.
- ***Peering* de VPC:** O *peering* de VPC permite a comunicação direta entre VPCs sem a necessidade de um *gateway* ou conexão VPN. Esse recurso é útil quando o usuário possui recursos distribuídos em VPCs separados, mas precisa que eles se comuniquem entre si.
- **VPN e *Direct Connect*:** O VPN e o *Direct Connect* oferecem opções para conexões seguras entre o ambiente local e o VPC, estabelecendo uma rede privada e segura.
- ***Endpoints*:** Os Endpoints permitem que as instâncias no VPC acessem serviços AWS, como S3 ou DynamoDB, sem a necessidade de uma conexão direta com a Internet.

4.3 *Elastic Compute Cloud* (EC2)

O Amazon EC2 é um serviço de computação em nuvem que permite aos usuários executarem máquinas virtuais escaláveis. Essas máquinas virtuais são conhecidas como instâncias EC2 e podem ser configuradas conforme necessário para atender a diferentes requisitos de computação.

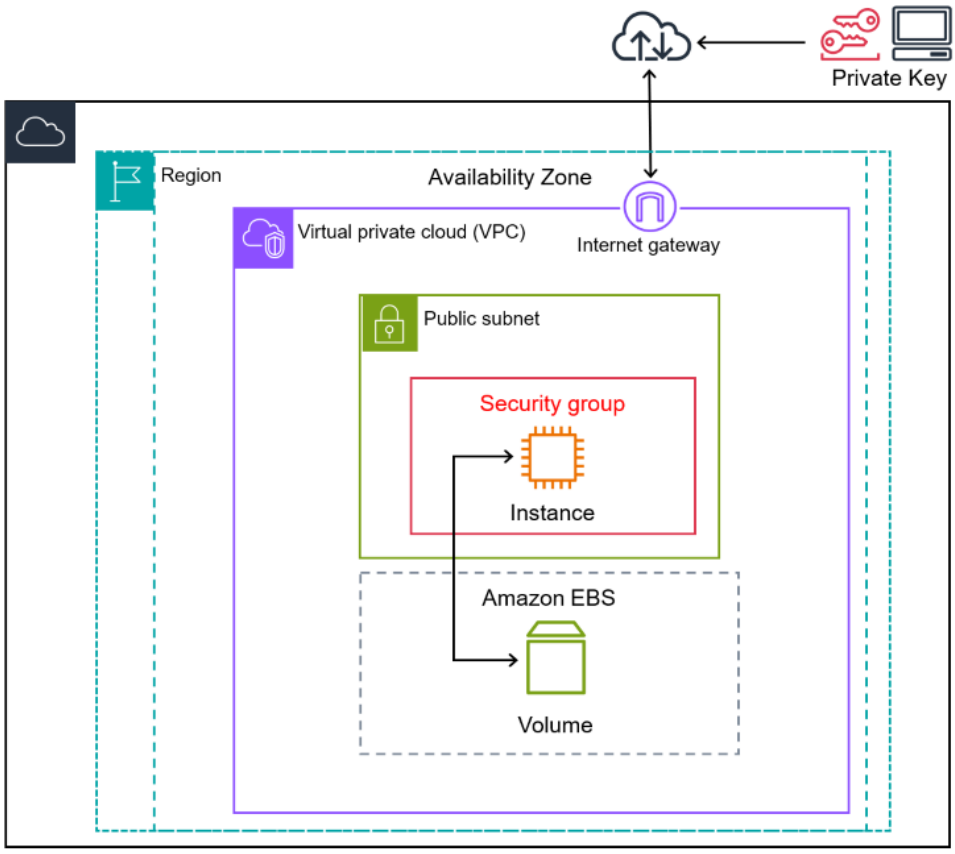
Elas representam a capacidade de computação virtual na nuvem e são essenciais para a execução de aplicativos na infraestrutura da AWS. Cada instância EC2 é uma máquina virtual independente que pode ser configurada com recursos de computação, armazenamento e rede conforme necessário.

O termo elasticidade refere-se à capacidade de um sistema se adaptar dinamicamente à carga de trabalho. No contexto do Amazon EC2, a elasticidade é uma característica fundamental que permite ajustar automaticamente a capacidade de computação em resposta às mudanças na demanda. Isso significa que o usuário pode aumentar ou diminuir o número de instâncias EC2 em execução conforme necessário, sem a necessidade de intervenção manual.

A utilização do Amazon EC2 propicia a diminuição dos custos associados à infraestrutura de *hardware*, permitindo assim, o desenvolvimento e a implementação ágeis de aplicações. O Amazon EC2 possibilita a execução de múltiplos servidores virtuais conforme necessário, a configuração de parâmetros de segurança e redes, bem como a administração eficiente do armazenamento.

O diagrama da Figura 11 mostra uma arquitetura básica de uma instância do Amazon EC2 implantada em uma nuvem privada virtual (VPC) da Amazon.

Figura 11 – *Elastic Compute Cloud*.



Fonte: *Amazon Web Service,* 2023.

Observa-se na Figura 11 que a instância do Amazon EC2 está alocada dentro de uma zona de disponibilidade específica dentro da região. Essa instância é protegida por meio de um grupo de segurança, que funciona como um *firewall* virtual, controlando o tráfego de entrada e saída. Uma chave privada é armazenada localmente no computador, enquanto a chave pública correspondente é armazenada na instância. Ambas as chaves são configuradas como um par para autenticar a identidade do usuário.

Nesse cenário, a instância é respaldada por um volume do *Elastic Block Store* (EBS). A comunicação da VPC com a Internet é possibilitada por meio de um gateway da Internet.

Um recurso para a criação e gestão de instâncias EC2 é o *Security Group*, que desempenha um papel crucial na implementação de uma estratégia de segurança

eficaz. Esse recurso atua como um *firewall* virtual, controlando o tráfego de entrada e saída com base em regras configuradas pelo usuário.

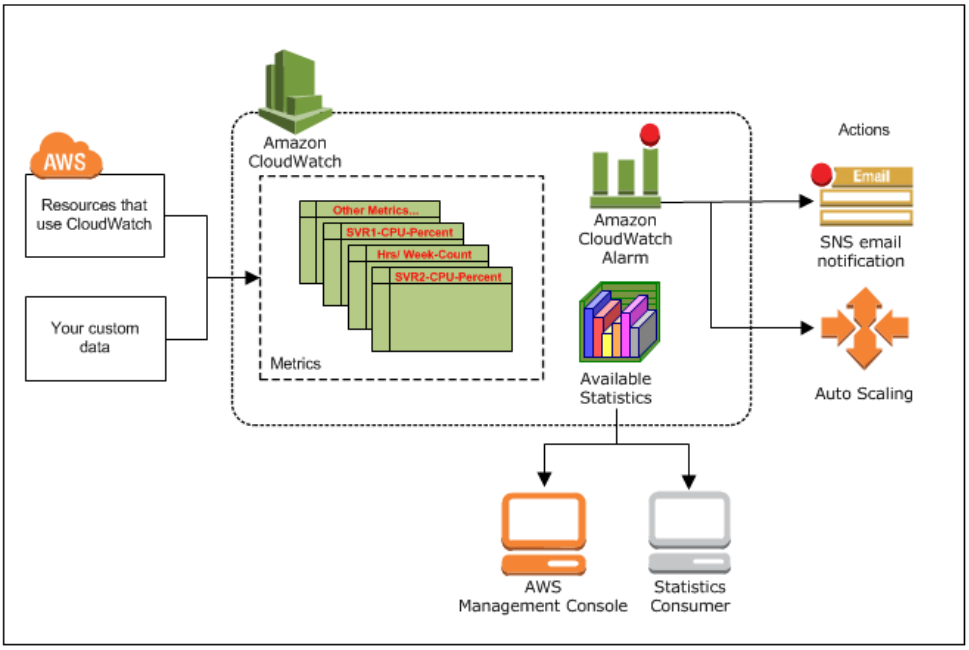
O *Security Group* permite que os usuários definam regras de controle de tráfego, especificando quais tipos são permitidos ou negados para instâncias associadas. As regras são baseadas em protocolos, portas e intervalos de endereços IP.

Ao utilizar o EC2 em conjunto com o VPC e o IAM, o usuário é capaz de criar uma infraestrutura na nuvem altamente segura e personalizada, adaptada às necessidades específicas do seu aplicativo ou serviço.

4.4 *Amazon CloudWatch*

O Amazon *CloudWatch* é um serviço de monitoramento e observação da AWS, que fornece informações e dados sobre os recursos de uma aplicação, sistemas e serviços em nuvem. Ele coleta dados em tempo real sobre métricas, criação de registros e eventos, permitindo que o usuário monitore, analise e reaja a alterações no desempenho das operações. A Figura 12 mostra o funcionamento do AWS *CloudWatch.*

Figura 12 – Amazon *CloudWatch*.



Fonte: *Amazon Web Service,* 2023.

Analisando a Figura 12 é notado a possibilidade de utilizar métricas para calcular estatísticas e apresentar os dados graficamente no console do *CloudWatch*. Configurando ações de alarmes para interromper, iniciar ou terminar uma instância do Amazon EC2 quando determinados critérios são atendidos. Além disso, é possível criar alarmes que iniciam ações do Amazon EC2 *Auto Scaling* e do Amazon *Simple Notification Service* (SNS).

Embora o *CloudWatch* não seja diretamente uma ferramenta de segurança, ele desempenha um papel crucial na segurança de um serviço ao fornecer recursos que ajudam a identificar e responder a eventos e comportamentos suspeitos. A seguir estão algumas maneiras pelas quais o *CloudWatch* é importante para a segurança de um serviço.

- Coleta de métricas: O *CloudWatch* permite que o usuário colete dados de métricas, como utilização de CPU, tráfego de rede e outros indicadores de desempenho. Essas métricas podem ser visualizadas em gráficos e utilizadas para análise de desempenho. O monitoramento contínuo permite a detecção precoce de anomalias. Essas anomalias podem indicar atividades suspeitas, como picos de tráfego incomuns ou alterações abruptas no consumo de recursos. Ao configurar alarmes no *CloudWatch* para notificar automaticamente quando ultrapassam limites definidos, as equipes de segurança podem ser alertadas rapidamente para investigar e responder a possíveis ameaças.
- Monitoramento de Logs: A coleta e monitoramento de logs são essenciais para a identificação e análise de eventos de segurança. O *CloudWatch* permite que o usuário monitore logs de sistemas distribuídos e aplicações, procurando por padrões ou comportamentos suspeitos. Isso facilita a detecção de atividades maliciosas, como tentativas de acesso não autorizado e alterações não autorizadas em configurações do sistema.
- Retenção de Dados: A retenção de dados no *CloudWatch* permite que as equipes de segurança analisem o histórico de métricas e logs para identificar padrões de comportamento ao longo do tempo. Essa análise retrospectiva é valiosa para investigações de segurança e para entender a evolução de possíveis ameaças ao longo do tempo.

o Amazon *CloudWatch* desempenha um papel crítico na operação de uma aplicação na nuvem, proporcionando visibilidade, alertas proativos, automação e ferramentas analíticas que são essenciais para garantir o desempenho e a

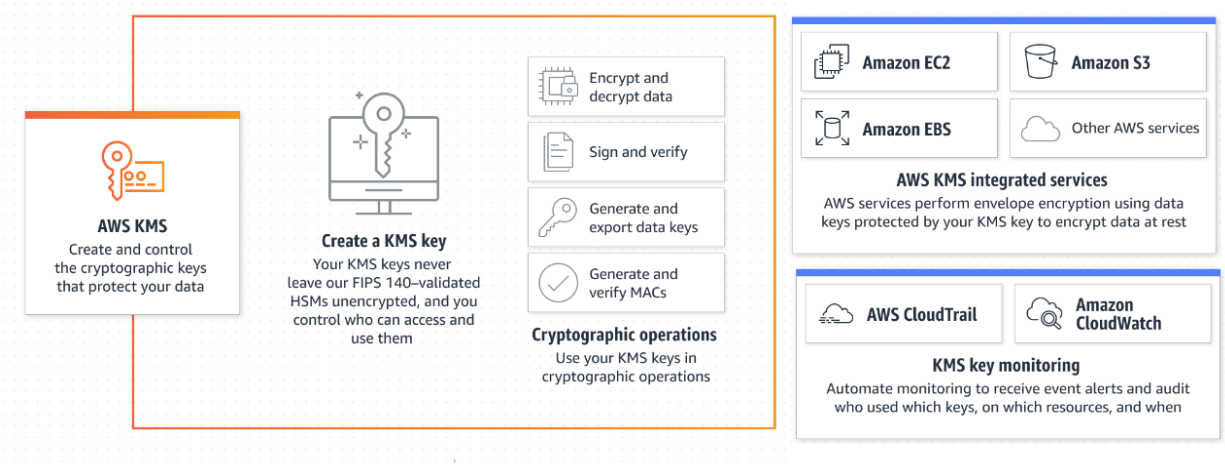
confiabilidade de sistemas hospedados na AWS. Integrar o *CloudWatch* em uma arquitetura de aplicação na nuvem é uma prática recomendada para aproveitar ao máximo os benefícios da computação em nuvem.

4.5 *Key Management Service* (KMS)

o *Amazon Key Management Service* (KMS) é um serviço projetado para facilitar a criação e o controle de chaves de criptografia para proteger dados do usuário. Ele fornece um serviço de gerenciamento de chaves seguro e durável que integra diretamente com outros serviços da AWS como Amazon S3, Amazon IAM, Amazon CloudWatch, Amazon EC2.

Na Figura 13, o diagrama mostra os principais recursos do KMS e as integrações disponíveis com outros serviços da AWS. Exibido em três sessões.

Figura 13 – *Key Management Service*.



Fonte: *Amazon Web Service,* 2023.

Na primeira seção, é possível analisar a criação e controle das chaves criptografadas, bem como informações sobre a política de segurança, intitulada como Publicação Federal de Processamento de Informações (FIP), que é um padrão de segurança de computador do governo dos EUA, usado para aprovar módulos

criptográficos. A lista destaca os principais recursos do KMS, incluindo operações como "Criptografia e descriptografia de dados" e "Geração e exportação de chaves de dados".

Na segunda e terceira seção é notado que o KMS possibilita automatizar o monitoramento para receber alertas de eventos, auditar quem usou quais chaves e quando há necessidade de realizar criptografia envelopada usando chaves de dados do usuário protegidas por chaves do KMS. Os serviços listados são: Amazon CloudWatch, Amazon EC2, Amazon S3 e outros serviços da AWS.

O KMS utiliza uma abordagem híbrida de criptografia, combinando criptografia assimétrica e simétrica para fornecer segurança em diferentes aspectos do gerenciamento de chaves e proteção de dados.

Criptografia Assimétrica para Chaves Mestras: Quando o usuário cria uma Chave Mestra de Criptografia (CMK) no AWS KMS, ela está associada a um par de chaves assimétricas, ou seja, uma chave pública e uma chave privada são geradas. A chave pública é usada para criptografar informações, mas não pode ser usada para descriptografá-las. Essa chave é disponibilizada publicamente. A chave privada é mantida de forma segura nos servidores do AWS KMS e é usada para operações de descriptografia.

Criptografia Simétrica para Dados: Quando o usuário precisa criptografar dados, o AWS KMS gera uma chave de dados aleatória (também chamada de chave de envelope) de forma simétrica. Essa chave de dados é então criptografada usando a chave pública associada à criptografia assimétrica. A chave de dados criptografada é então retornada para o administrador. Essa chave de dados criptografada é usada para criptografar e descriptografar os dados propriamente ditos de maneira eficiente e rápida. Essa parte da operação utiliza criptografia simétrica, que é mais eficiente para grandes volumes de dados.

Pata criptografia simétrica o KMS oferece suporte aos seguintes algoritmos de criptografia, AES-128, AES-192, AES-256 e para a criptografia assimétrica o KMS oferece suporte com os algoritmos de criptografia RSA.

Ao utilizar o AWS KMS, as organizações podem garantir a segurança de dados sensíveis, cumprir requisitos regulatórios e simplificar o gerenciamento de chaves, enquanto aproveitam a infraestrutura escalável da AWS.

4.6 *AWS Shield*

A AWS *Shield* é um serviço de segurança oferecido pela AWS para proteger aplicações web contra-ataques *Distributed Denial of Service* (DDoS) e outros tipos de ameaças online. Ele é projetado para detectar, mitigar e responder automaticamente a ataques, ajudando a garantir a disponibilidade contínua dos aplicativos.

O AWS *Shield* é um conjunto abrangente, focado em proteger os aplicativos e os recursos hospedados na nuvem contra ameaças cibernéticas. Ele é programado para garantir a disponibilidade, a integridade e o desempenho dos aplicativos, mesmo em face de ataques maliciosos. Existem duas camadas principais do AWS *Shield*:

- AWS *Shield Standard* sendo uma oferta de segurança que é automaticamente incluída em todos os recursos da AWS implantados na nuvem. A principal funcionalidade do AWS *Shield Standard* é oferecer proteção contra-ataques DDoS, que visam sobrecarregar um serviço online, aplicativo ou site, tornando-o inacessível para usuários legítimos. Esses ataques podem ser classificados em diferentes tipos, como ataques volumétricos, ataques de exaustão de recursos e ataques de aplicativos. Usando tecnologias automatizadas e algoritmos para detectar padrões de tráfego maliciosos e em seguida, aplicando medidas de mitigação para filtrar ou atenuar o impacto desses ataques. Ele se torna uma camada de segurança essencial para proteger os recursos da AWS contra ameaças comuns, proporcionando maior resiliência e disponibilidade.
- AWS Shield *Advanced* é a camada mais avançada do serviço de proteção contra DDoS. Ela é uma escolha mais adequada para organizações que enfrentam ameaças mais complexas e que exigem uma resposta mais avançada e personalizada para proteger seus ativos na nuvem. O AWS *Shield Advanced* inclui suporte 24/7 de uma equipe de resposta a incidentes da AWS e uma integração com o AWS *Web Application Firewall* (WAF), que é um *firewall* de aplicativos da web. A principal diferença entre os dois é que o AWS *Shield Standard* fornece uma proteção automática e básica contra ameaças DDoS comuns, enquanto o AWS *Shield Advanced* oferece recursos mais avançados, incluindo suporte especializado, integração, além de permitir a personalização das estratégias de mitigação. Utilizar o AWS *Shield* é

fundamental para garantir a resiliência e a segurança dos aplicativos na nuvem, protegendo contra ameaças DDoS e proporcionando tranquilidade durante situações de segurança críticas.

4.7 *Amazon Simple Storage Service (Amazon S3)*

Amazon *Simple Storage Service* (Amazon S3) é um serviço de armazenamento de objetos que oferece escalabilidade, disponibilidade de dados, segurança e performance. Ele é projetado para armazenar e recuperar qualquer quantidade de dados de qualquer lugar da web. O Amazon S3 é amplamente utilizado para armazenar e recuperar imagens, vídeos, arquivos de backup e logs.

No Amazon S3, os dados são organizados em "objetos". Um objeto consiste em dados com um identificador único chamado de chave e metadados associados a esse objeto, podendo variar em tamanho de *bytes* a *terabytes*. Os objetos são armazenados em "*buckets*", que são recipientes de nível superior de armazenamento. Cada objeto armazenado em um *bucket* terá um nome exclusivo.

O Amazon S3 é projetado para ter durabilidade e disponibilidade elevadas, sendo adequado para ter acesso frequente a esses dados. Para proporcionar uma durabilidade dos objetos é usado uma replicação automática dos dados em vários dispositivos em várias instalações de *data centers*.

Em relação a segurança, o Amazon S3 permite que o usuário controle o acesso aos seus *buckets* e objetos usando políticas de controle de acesso, listas de controle de acesso e autenticação baseada em identidade IAM oferecendo várias opções para criptografar dados em repouso, como o KMS.

O Amazon S3 é frequentemente utilizado para *backup* e recuperação de dados. A capacidade de criar cópias de objetos, versionamento e a opção de armazenamento em diferentes classes faz dele uma escolha eficiente para essas implementações. Ele oferece uma solução de armazenamento na nuvem robusta, flexível e altamente escalável, adequada para uma ampla variedade de casos de uso, desde o armazenamento simples de arquivos até implementações complexas de *big data* e soluções de *backup*.

4.8 *Amazon Relational Database Service (RDS)*

O Amazon *Relational Database Service* (Amazon RDS) é um serviço de banco de dados gerenciado oferecido pela AWS. Ele foi projetado para facilitar a tarefa de configurar, operar e escalar bancos de dados relacionais na nuvem, removendo a complexidade associada à administração de bancos de dados tradicionais. O Amazon RDS suporta vários tipos de banco de dados, incluindo MySQL, PostgreSQL, MariaDB, Oracle e Microsoft SQL Server. Além disso, a AWS oferece um serviço chamado Amazon Aurora, que é um banco de dados compatível com MySQL e PostgreSQL, com desempenho aprimorado e recursos adicionais. Na Figura 14 é possível observar os principais recursos e benefícios do Amazon RDS.

Figura 14 – Amazon *Relational Database Service*.

Fonte: *Amazon Web Service,* 2023.

Conforme é observado na Figura 14, com o RDS é possível configurar, operar e escalar um banco de dados relacional na nuvem com apenas alguns cliques. Os recursos gerenciados pelo RDS estão divididos em 6 categorias, que são: Segurança e conformidade, desempenho e escalabilidade, atualizações e aplicação de patches automatizados, durabilidade e redundância dos dados, monitoramento, *backup* e recuperação.

Os benefícios do RDS são, conforme a Figura 14, foco na inovação, migrar sem a necessidade de redefinir a arquitetura de uma aplicação, diminuir o tempo de

gerenciamento de bancos de dados, melhorar a eficiência do banco de dados e da infraestrutura e reduzir as despesas de capital e operacionais.

O Amazon RDS automatiza várias tarefas administrativas, incluindo *backups* regulares, aplicação de *patches* de software e atualizações de segurança. Isso libera os desenvolvedores e administradores de banco de dados para se concentrarem em atividades mais críticas para o negócio.

Em relação à segurança o RDS oferece recursos avançados, como criptografia de dados em repouso e em trânsito KMS, integração com o IAM para gerenciamento de acessos, grupos de segurança para controle de tráfego de rede e a capacidade de executar em uma VPC para isolamento adicional.

O RDS também fornece ferramentas integradas para monitorar o desempenho do banco de dados. Os usuários podem acessar métricas vitais, como uso de CPU, I/O de disco e memória e configurar alertas com o Amazon *CloudWatch* para responder proativamente a eventos de desempenho.

Ao utilizar o Amazon RDS, as organizações podem se beneficiar da eficiência operacional, escalabilidade elástica e alta disponibilidade para seus aplicativos que dependem de bancos de dados relacionais.

5. EXPERIMENTOS

Neste capítulo, são abordados os procedimentos para a configuração de serviços fundamentais na plataforma *Amazon Web Services* (AWS), tais como: o IAM, EC2 e o VPC. O enfoque concentra-se em demonstrar o passo a passo de como criar e configurar essas 3 ferramentas, garantindo segurança adequada em uma implementação.

5.1 *Identity and Access Management* (IAM)

O *Identity and Access Management* (IAM) é um serviço essencial que oferece controle de acesso e visibilidade para o gerenciamento centralizado de recursos em nuvem. Com o IAM, o administrador define, por meio de identidades e papéis, quais usuários têm acesso a quais recursos, garantindo uma gestão precisa e segura das permissões em ambientes computacionais distribuídos. Essa abordagem contribui

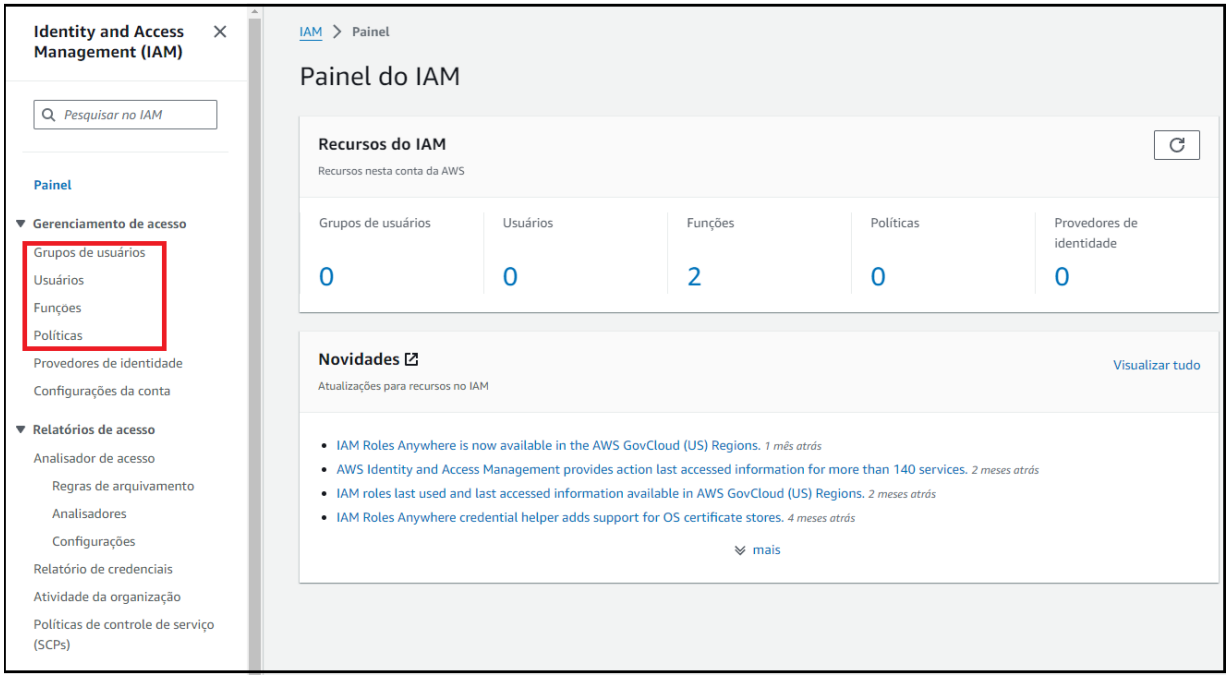
significativamente para a segurança e conformidade na administração de recursos na nuvem.

5.1.1 Usuários (IAM)

Os usuários são entidades básicas do IAM. Eles podem ser pessoas, aplicativos ou serviços. Quando se cria um usuário, é preciso fornecer um nome de usuário, um endereço de e-mail e uma senha. Também é possível escolher quais permissões conceder ao usuário.

Para criar um usuário do IAM, siga estas etapas: No painel de navegação do console da AWS, canto esquerdo, selecione Usuários, conforme mostrado na Figura 15.

Figura 15 – Console da AWS.



Fonte: *Amazon Web Service,* 2023.

Na página Criar Usuário, insira as seguintes informações:

- Nome de usuário: O nome de usuário deve ser exclusivo e deve conter de 1 a 64 caracteres alfanuméricos.

- Política de acesso inicial: Selecione uma política que defina as permissões que o usuário terá. No caso, um usuário do IAM.
- Autenticação multifatorial (MFA): Habilite a autenticação multifatorial para o usuário aumentar a segurança.

Após isso selecione criar usuário, conforme mostrado na Figura 16.

Figura 16 – Criação de usuário IAM.

Fonte: *Amazon Web Service,* 2023.

O usuário será criado e uma notificação será enviada para o endereço de e-mail especificado. A notificação incluirá as credenciais do usuário, que são uma senha e um token de acesso.

Para definir permissões para um usuário, é preciso atribuir uma política a ele. Uma política é um documento que define as ações que um usuário pode executar em recursos da AWS.

5.1.2 Política (IAM)

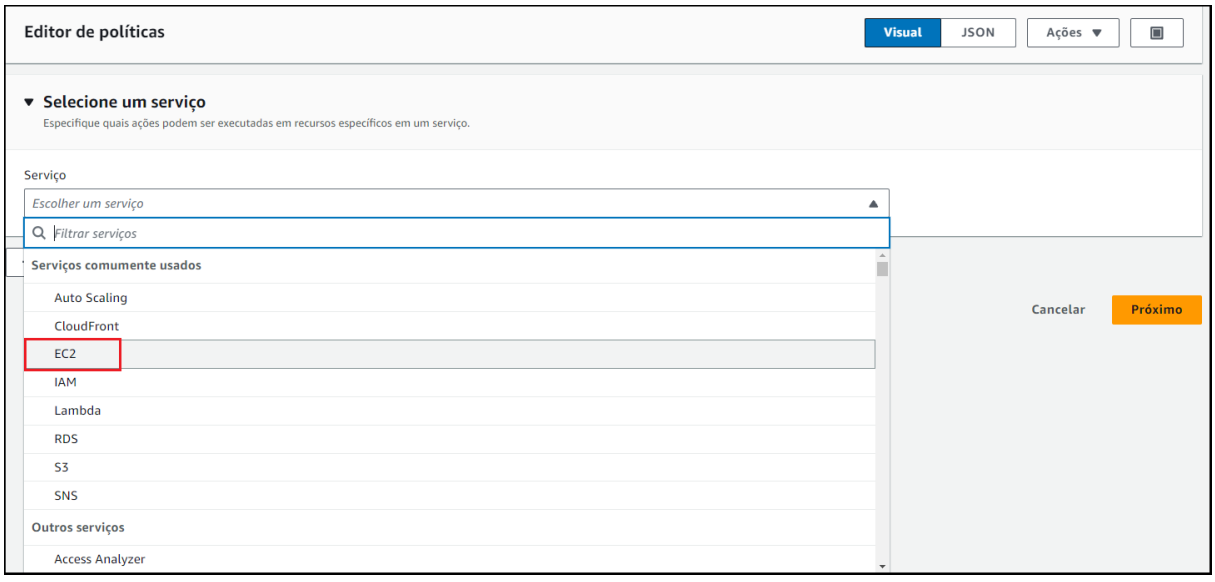
As políticas são documentos que definem as permissões de um usuário, função ou recurso sendo compostas por declarações. Cada declaração define uma ação que um usuário pode executar em um recurso da AWS.

No painel de navegação do console da AWS, canto esquerdo, selecione Políticas, conforme mostrado na Figura 15.

Na parte de criação de política, selecione o tipo de política desejado, nessa parte é possível adicionar permissões selecionando serviços, ações, recursos e condições, sendo possível criar instruções de permissão usando o editor JSON.

Exemplo de configuração de permissões: Um usuário necessita de permissão para criar e gerenciar instâncias do EC2. Escolha o serviço na barra de filtro. Conforme demonstrado na Figura 17.

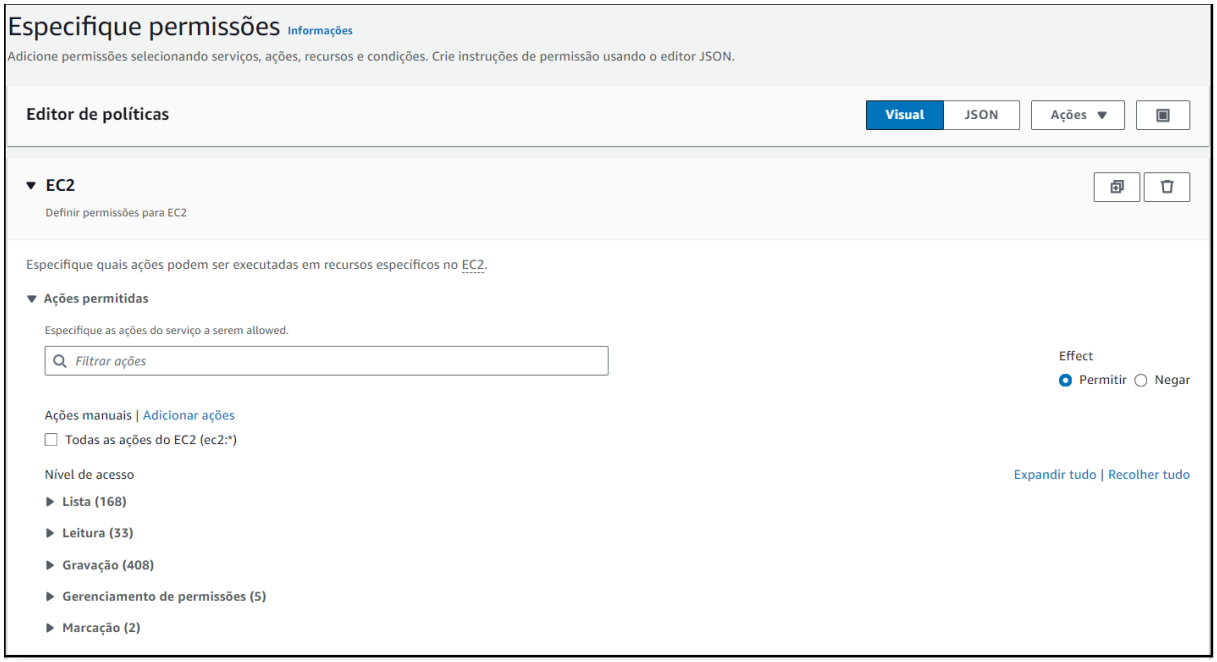
Figura 17 – Criação de políticas.



Fonte: *Amazon Web Service,* 2023.

Ao selecionar o EC2 será possível escolher todo tipo de nível de acesso, permissões, listas e gerenciamento de instâncias. As permissões representam um conjunto de funções de entidades podendo ser usadas para conceder acesso a aplicativos ou serviços, conforme a Figura 18.

Figura 18 – Especificação de permissões.



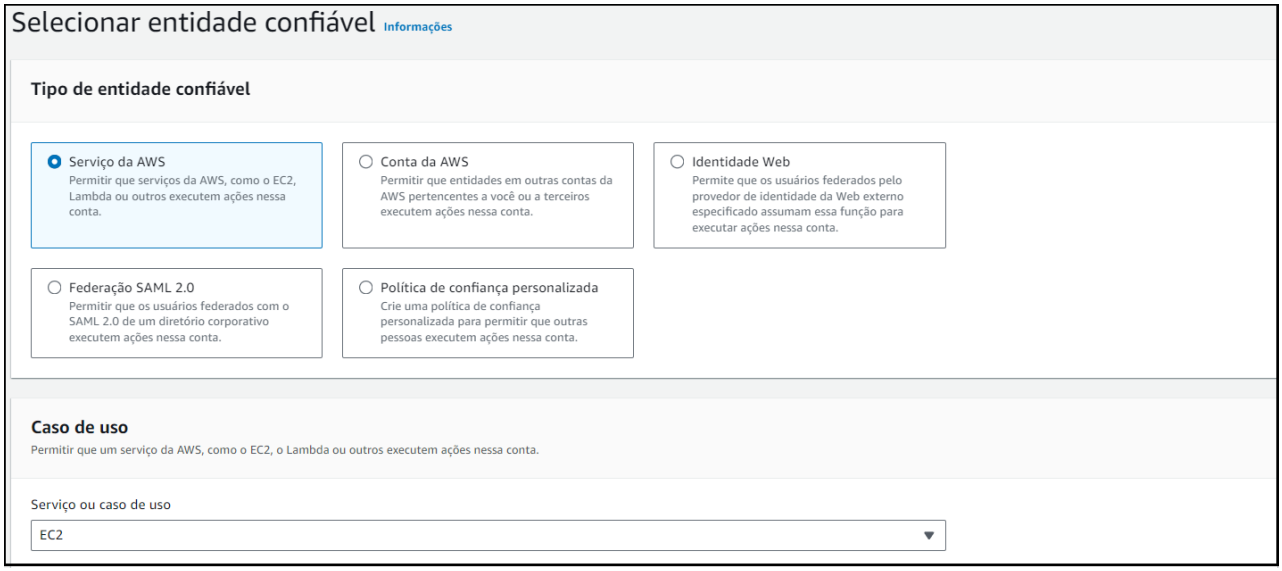
Fonte: *Amazon Web Service,* 2023.

5.1.3 Função (IAM)

Uma função é diferente de um usuário, ou seja, a função é atribuída diretamente a instância ou ao serviço ao quão o usuário quer dar permissões especiais. A página de criação para funções está no console da AWS, canto esquerdo, selecione Funções, conforme mostrado na Figura 16.

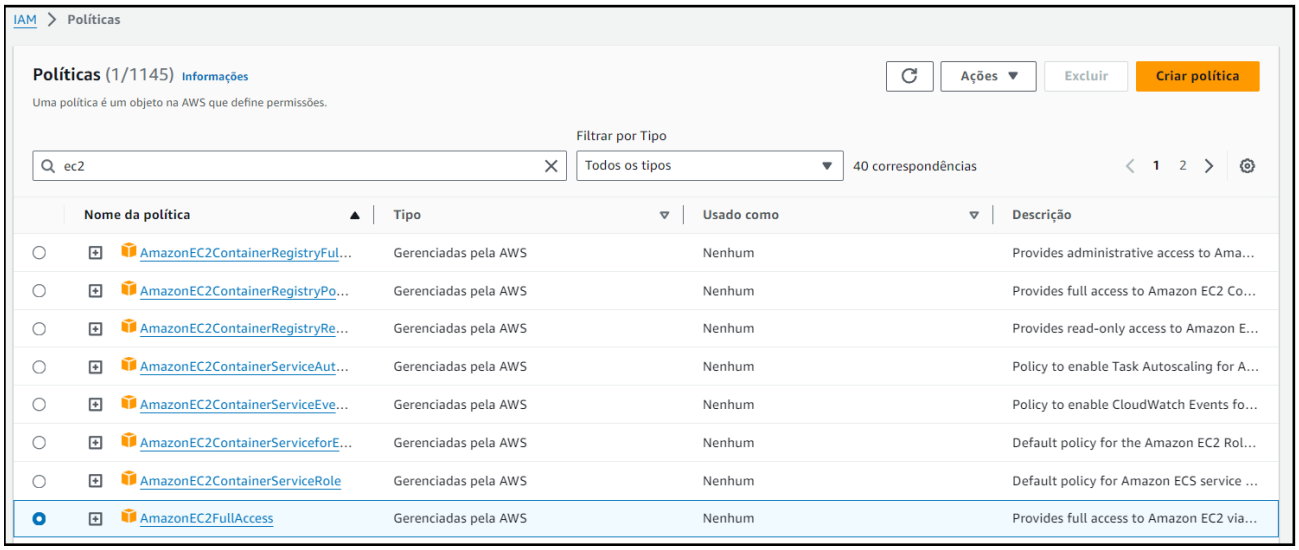
A primeira etapa da criação de uma função é determinar qual serviço irá consumir essa função. No caso a escolhida foi a EC2 conforme mostrado nas Figuras 19 e 20.

Figura 19 – Criação de Funções.



Fonte: *Amazon Web Service,* 2023.

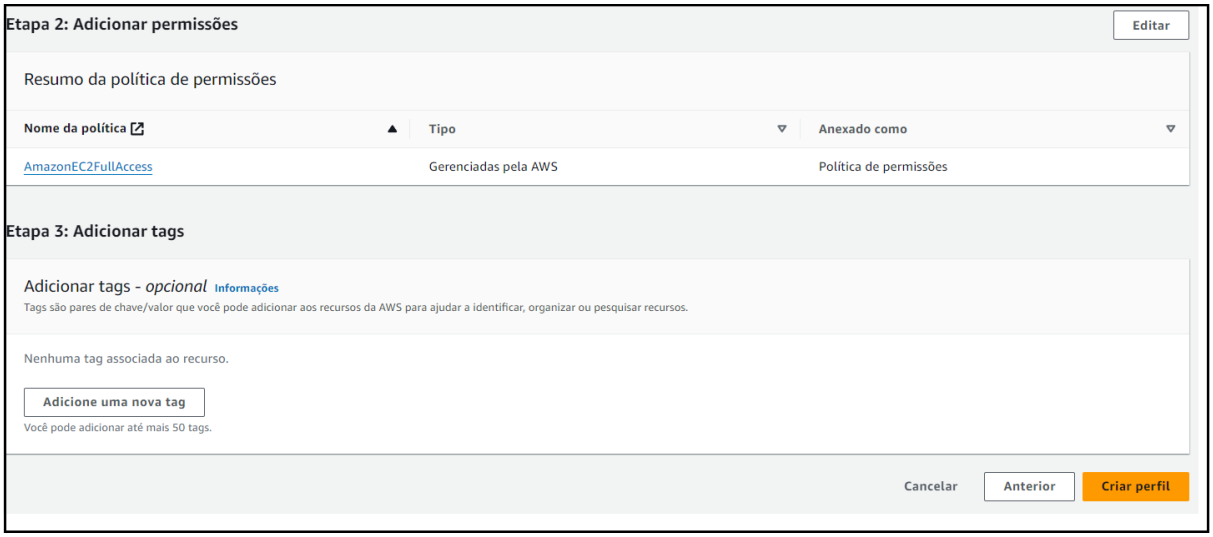
Figura 20 – Configuração de acesso da função.



Fonte: *Amazon Web Service,* 2023.

Após determinar as políticas de permissões, é necessário nomear e descrever as suas *tags*, conforme mostrado na Figura 21.

Figura 21 – Nome e *tag* da função.



Fonte: *Amazon Web Service,* 2023.

Com a função criada é possível gerenciar e excluir recursos na AWS, delegar acesso a usuários, serviços e aplicativos dentre outras funcionalidades.

A implementação do IAM possibilita a verificação de um nível robusto e detalhado de segurança sobre os recursos da AWS. Permitindo que os usuários e/ou grupos acessem apenas os recursos essenciais para suas tarefas, tornando-se assim fundamental para assegurar um elevado padrão de segurança na administração de usuários e políticas nas contas.

5.2 *Elastic Compute Cloud (EC2)*

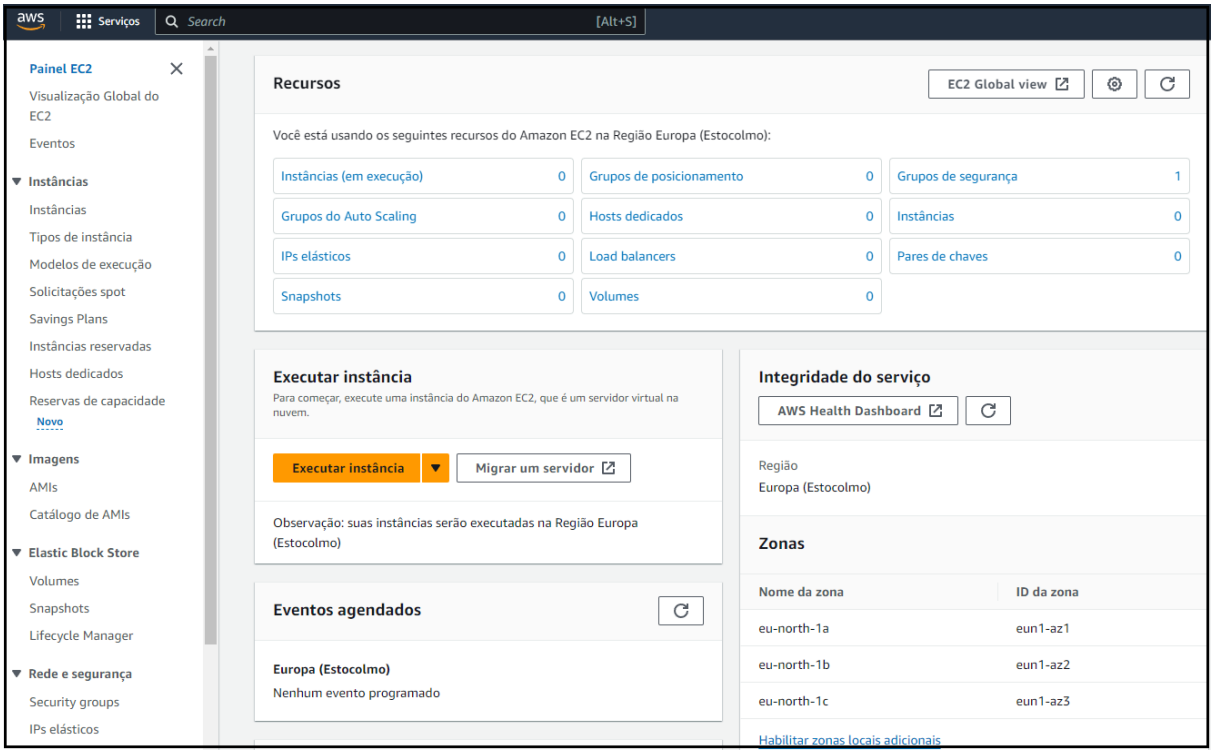
O EC2 é um serviço de infraestrutura que fornece capacidade de computação sob demanda na nuvem. Ele permite que os clientes provisionem e iniciem instâncias de máquinas virtuais em minutos, com base nas suas necessidades específicas.

O papel do EC2 é fornecer uma plataforma de computação segura e confiável para os clientes. A AWS investe continuamente em segurança e fornece uma ampla gama de recursos e serviços para ajudar os clientes a protegerem seus dados e aplicações. Os clientes são responsáveis por implementar as melhores práticas de segurança para suas instâncias do EC2. Isso inclui: configurações de segurança

padrão, aplicação de atualizações de segurança e monitoramento de instâncias para atividade suspeita.

Para criar e gerenciar uma instancia EC2 é necessário acessar o console da AWS, conforme mostrado na Figura 22.

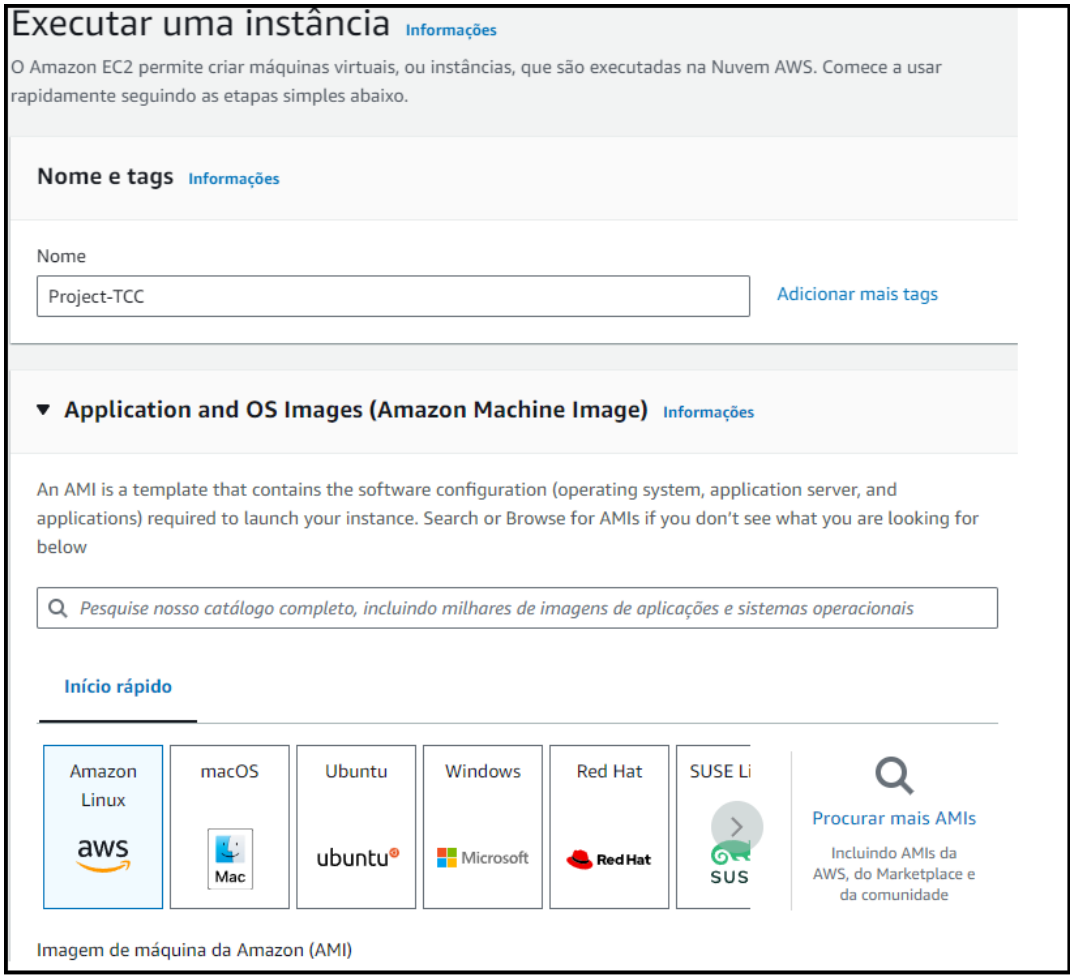
Figura 22 – Criação de uma instância EC2.



Fonte: *Amazon Web Service,* 2023.

No console da AWS, click em “Executar instância” que a página será automaticamente reconfigurada para a parte de criação das máquinas virtuais. Nessa parte que será necessário escolher qual *Amazon Machine Image* (AMI), será configurada na máquina virtual escolhida. Uma AMI é um modelo que contém a configuração de software (sistema operacional, servidor de aplicativos e aplicativos) necessária para iniciar a instância desejada, conforme mostrada na Figura 23.

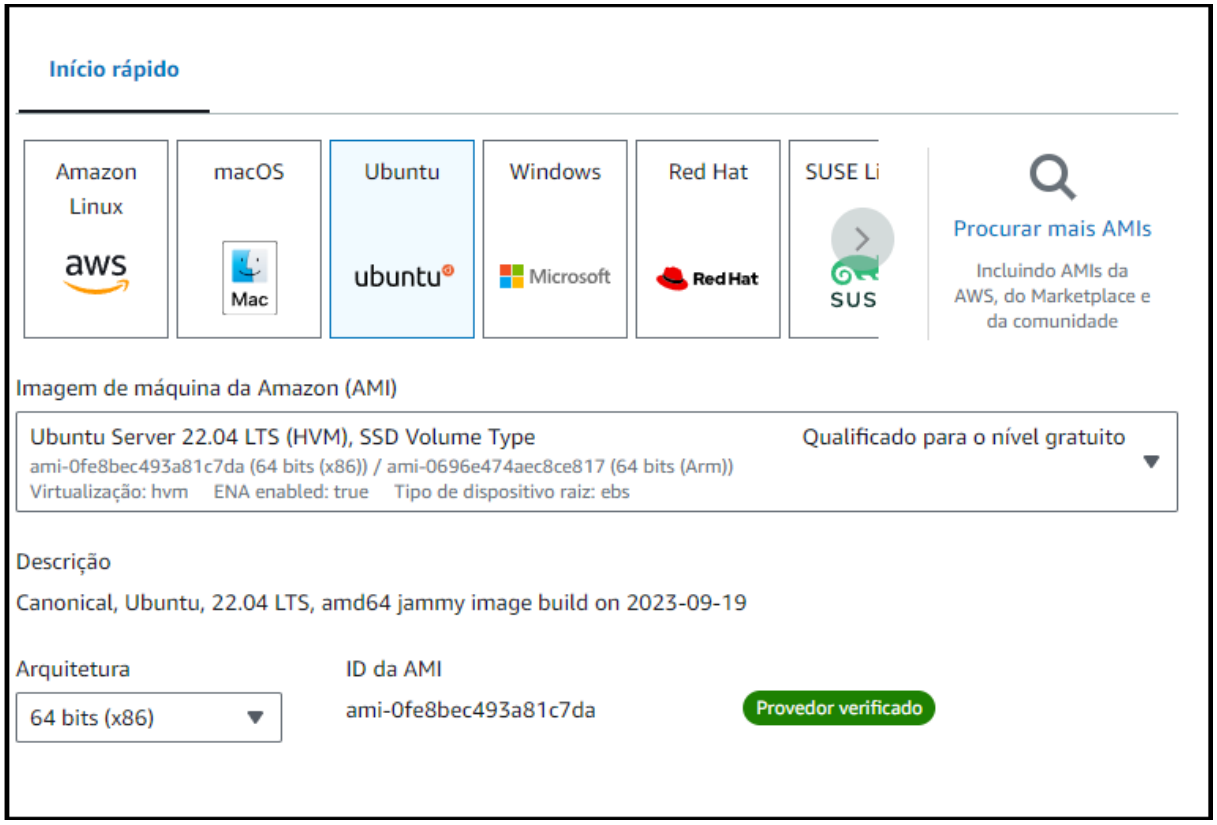
Figura 23 – Execução de uma instância EC2.



Fonte: *Amazon Web Service,* 2023.

No caso da aplicação desse trabalho, foi escolhido a AMI Ubuntu Server 22.04 LTS (HMV), SSD volume *Type*, que está qualificado para ser criada no nível gratuito, conforme demonstrado na Figura 24.

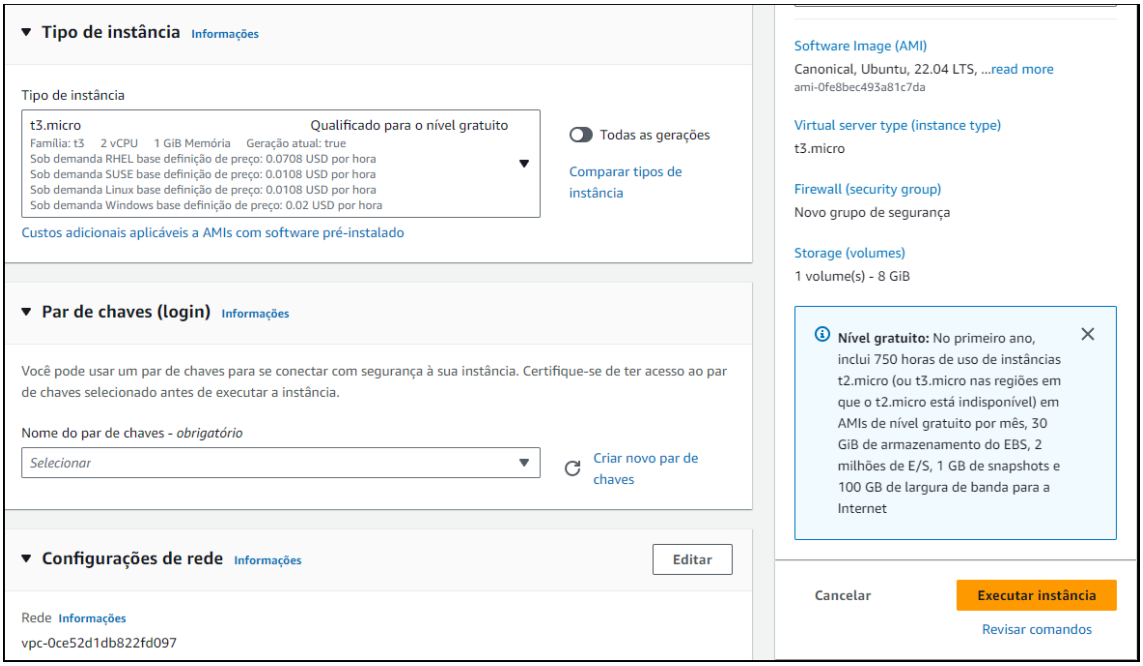
Figura 24 – Definição da AMI.



Fonte: *Amazon Web Service,* 2023.

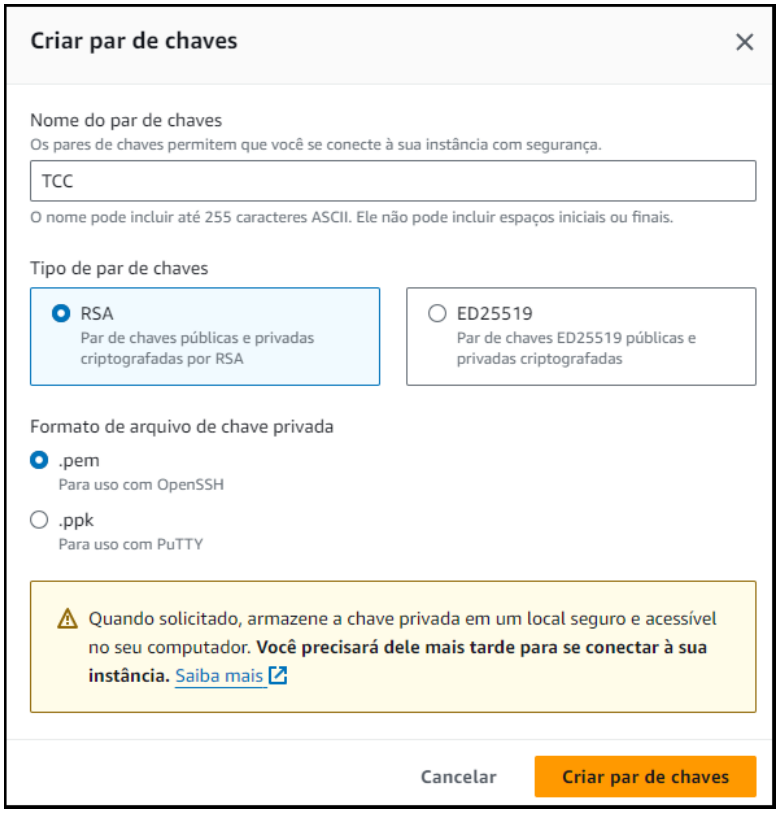
O segundo passo é definir o tipo de instância que correspondem às necessidades de computação, memória, rede ou armazenamento. Por padrão, a AMI escolhida vem com instância t3.micro que disponibiliza de forma gratuita 2 CPU e 1GiB de memória. Após isso, é possível criar um par de chaves para se conectar com segurança à sua instância, esse par de chave é criptografada por RSA que dará ainda mais segurança para a aplicação, conforme mostrado, respectivamente, nas Figuras 25 e 26.

Figura 25 – Definição da instância.



Fonte: *Amazon Web Service,* 2023.

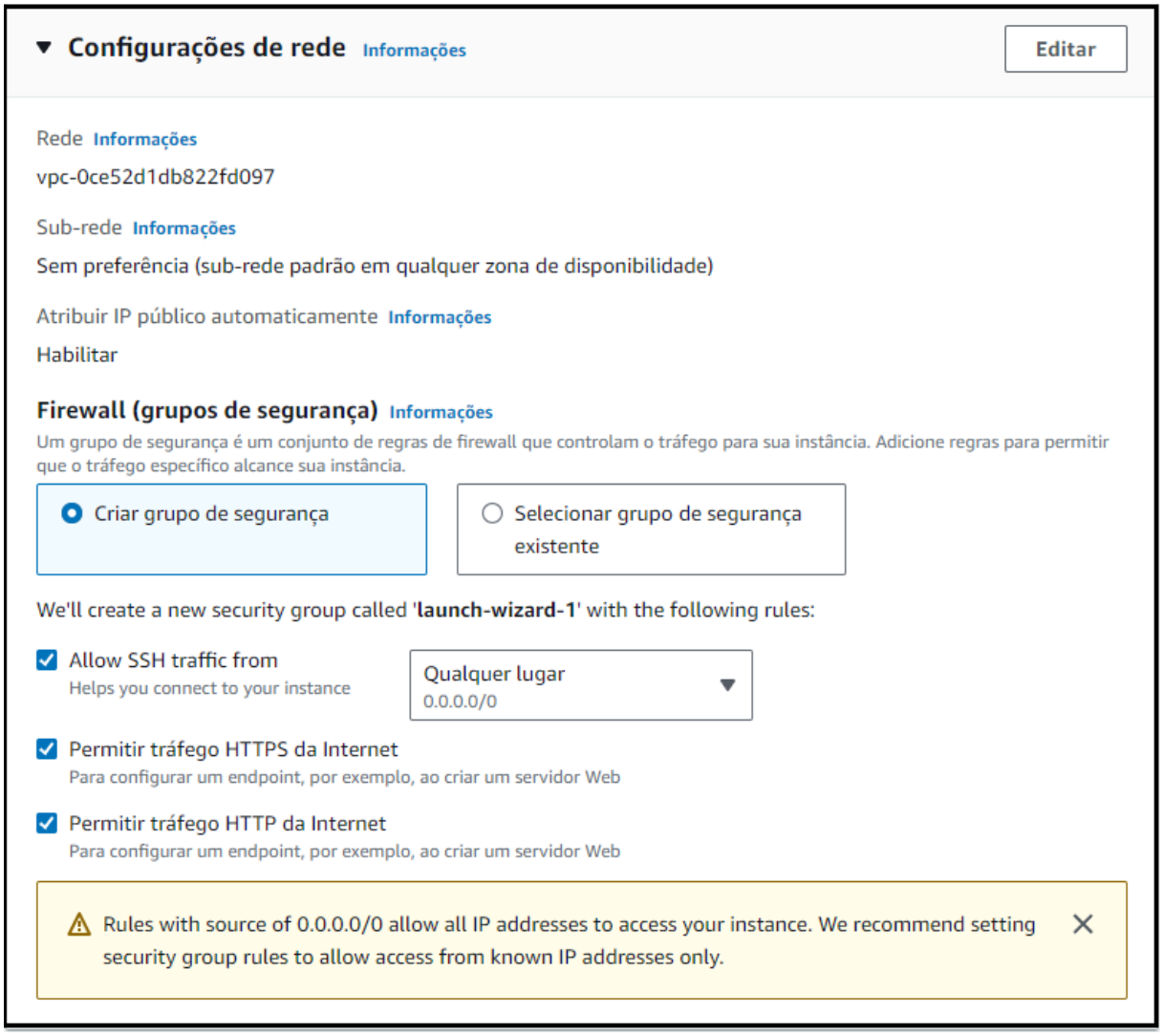
Figura 26 – Criação do par de Chaves.



Fonte: *Amazon Web Service,* 2023.

O próximo passo é a configuração de rede que essa instância EC2 terá. Nessa parte é possível criar instâncias à qual o usuário pode conectar pela Internet utilizando *Secure Shell* (SSH) ou *Remote Desktop Protocol* (RDP) que são protocolos específicos de segurança de troca de arquivos entre cliente e servidor de internet, usando criptografia. O serviço da AWS também da disponibilidade de criar um servidor web ou serviço de aplicativo, ou até conexões com bando de dados RDS, sendo possível observar na Figura 27.

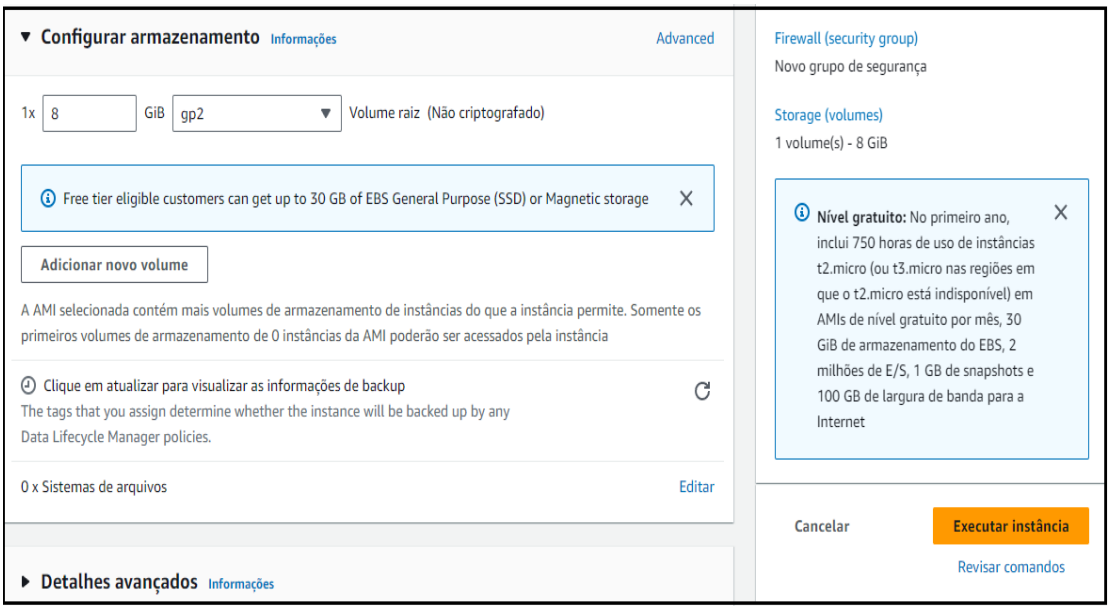
Figura 27 – Configuração de rede das instâncias EC2.



Fonte: *Amazon Web Service,* 2023.

A última parte da criação da instância é configurar o armazenamento da máquina virtual. No caso, será a padrão que é 1 de 8 GiB SSD *General Purpose*, conforme mostrado na Figura 28.

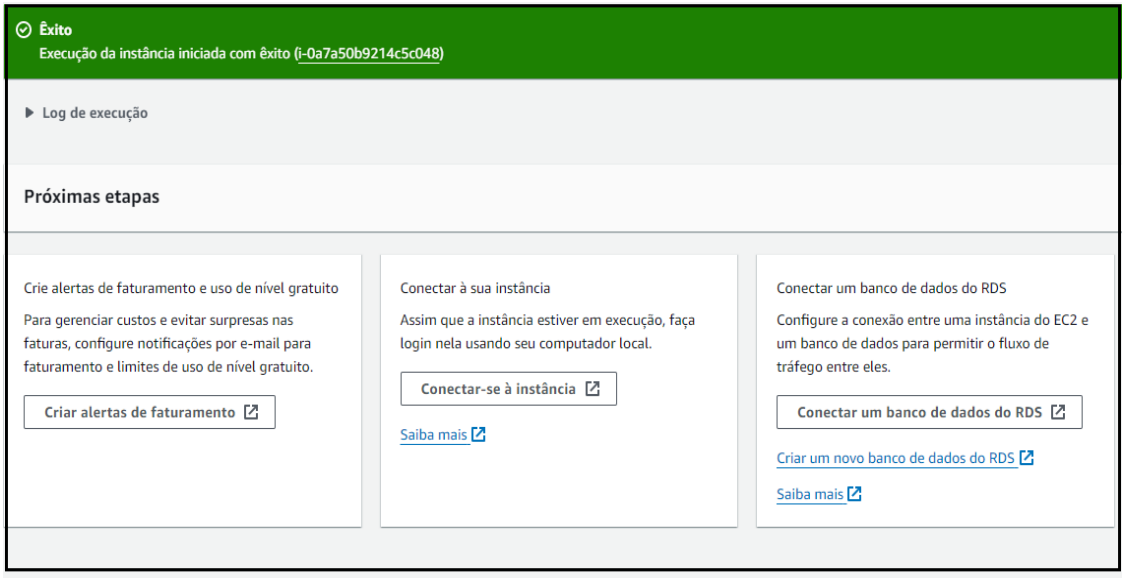
Figura 28 – Configuração de armazenamento.



Fonte: *Amazon Web Service,* 2023.

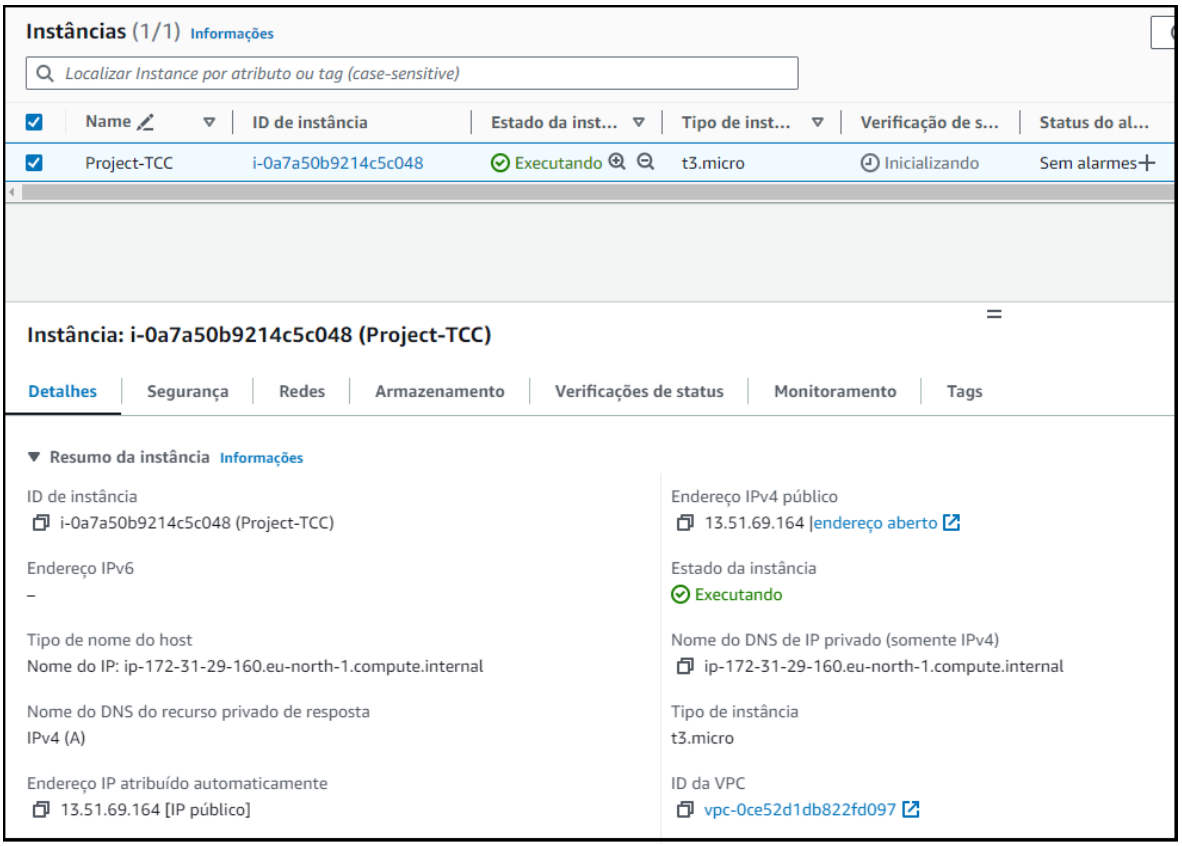
Com todas as partes configuradas, basta clicar na opção “Executar Instância” que a máquina virtual estará pronta para ser utilizada, conforme mostrada nas Figuras 29 e 30, respectivamente.

Figura 29 – Êxito criação instância.



Fonte: *Amazon Web Service,* 2023.

Figura 30 – MV funcionando.



Fonte: *Amazon Web Service,* 2023.

Uma máquina virtual EC2 da AWS configurada de maneira correta pode ajudar a proteger sua aplicação de várias maneiras, incluindo:

- Restrição do acesso: Os grupos de segurança do EC2 permitem que o usuário restrinja o acesso à sua máquina virtual a partir de endereços IP específicos ou intervalos de endereços IP. Isso ajuda a impedir que invasores acessem a máquina virtual de forma não autorizada.
- Atualizações de segurança: O Amazon EC2 fornece atualizações de segurança automáticas para o software do sistema operacional e outros componentes da máquina virtual. Essas atualizações ajudam a proteger a máquina virtual contra vulnerabilidades conhecidas.
- Segurança de rede: O Amazon EC2 oferece uma variedade de recursos de segurança de rede, incluindo firewalls, VPNs e criptografia. Esses recursos ajudam a proteger o tráfego de rede.

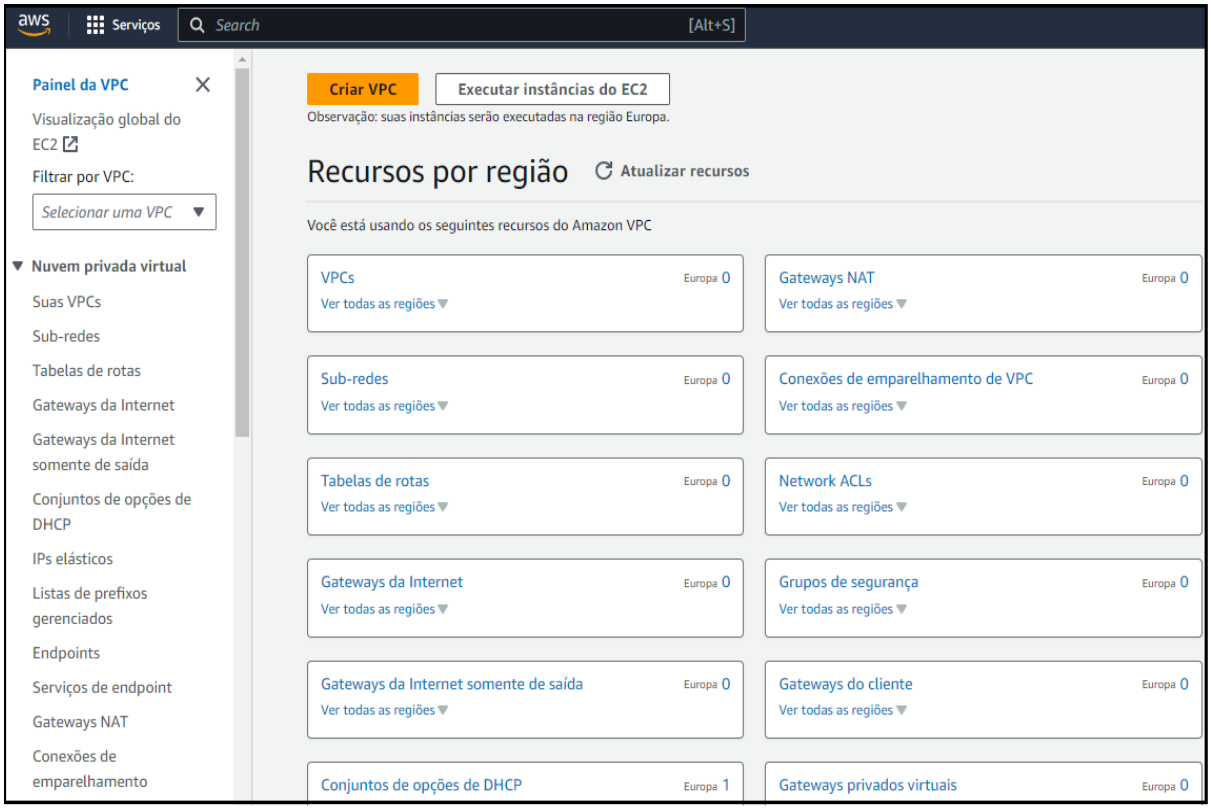
5.3 *Amazon Virtual Private Cloud (VPC)*

A VPC é uma rede virtual privada dedicada a uma conta da AWS. Ela é isolada de maneira lógica de outras redes virtuais na nuvem da AWS, com isso, é possível especificar um intervalo de endereços IP para cada VPC, adicionar *sub-redes*, *gateways* e grupos de segurança.

A VPC é importante porque permite que o usuário controle o acesso ao seu ambiente de rede, podendo utilizar grupos de segurança para definir quais portas e protocolos estão abertos para tráfego e também usar *gateways* para conectar uma VPC à Internet ou a outras VPCs.

Para criar e gerenciar uma VPC é necessário acessar o console da AWS, conforme mostrado na Figura 31.

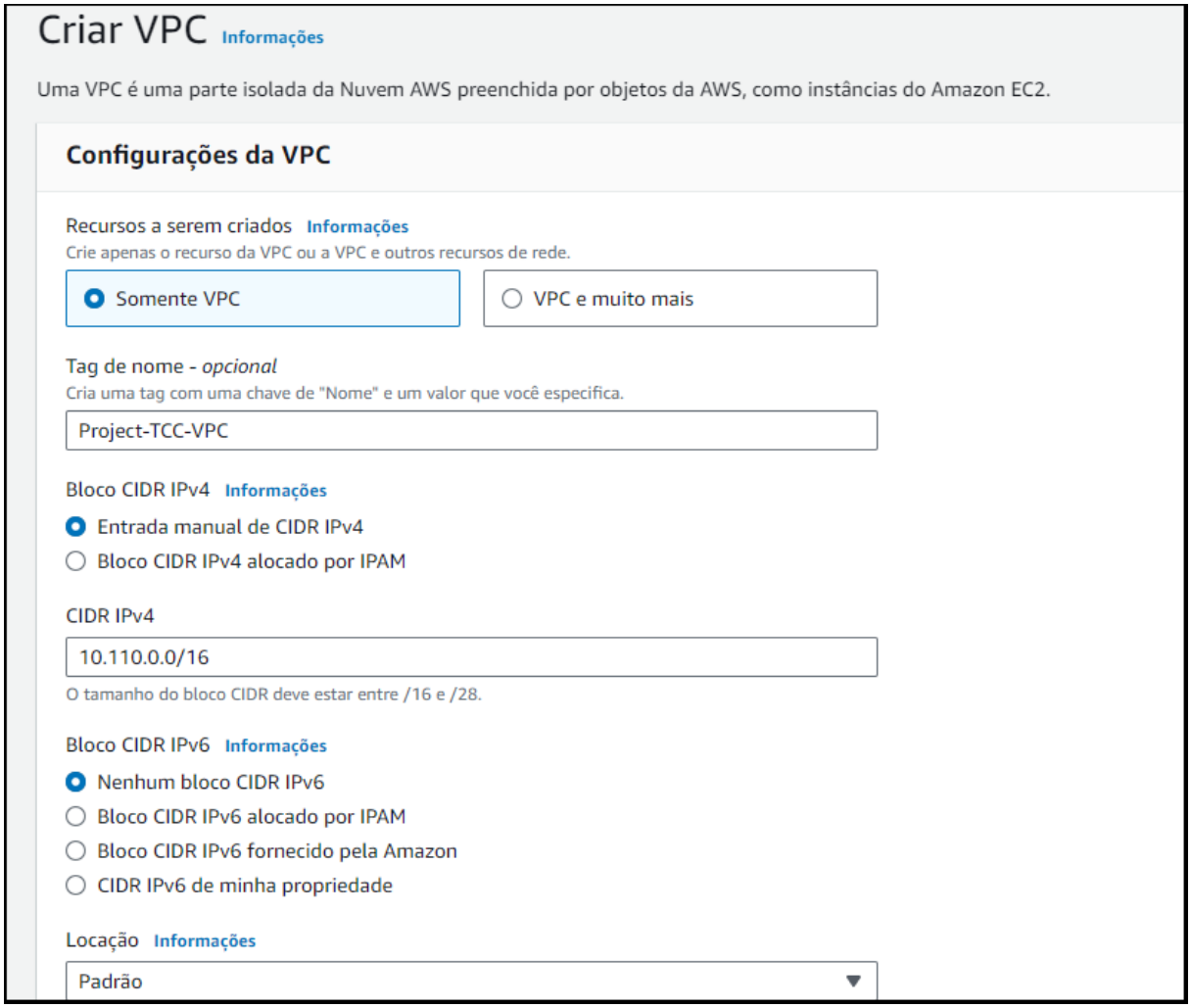
Figura 31 – Console AWS VPC.



Fonte: *Amazon Web Service,* 2023.

Ao criar a VPC, será necessário escolher um nome opcional, o bloco CIDR IPv4, que é um método de alocação de endereços IP para a eficiência do encaminhamento de dados na Internet. No caso, neste trabalho será uma entrada manual de CIDR IPv4, com range de IP de “10.110.0.0/16”, sendo possível observar na Figura 32.

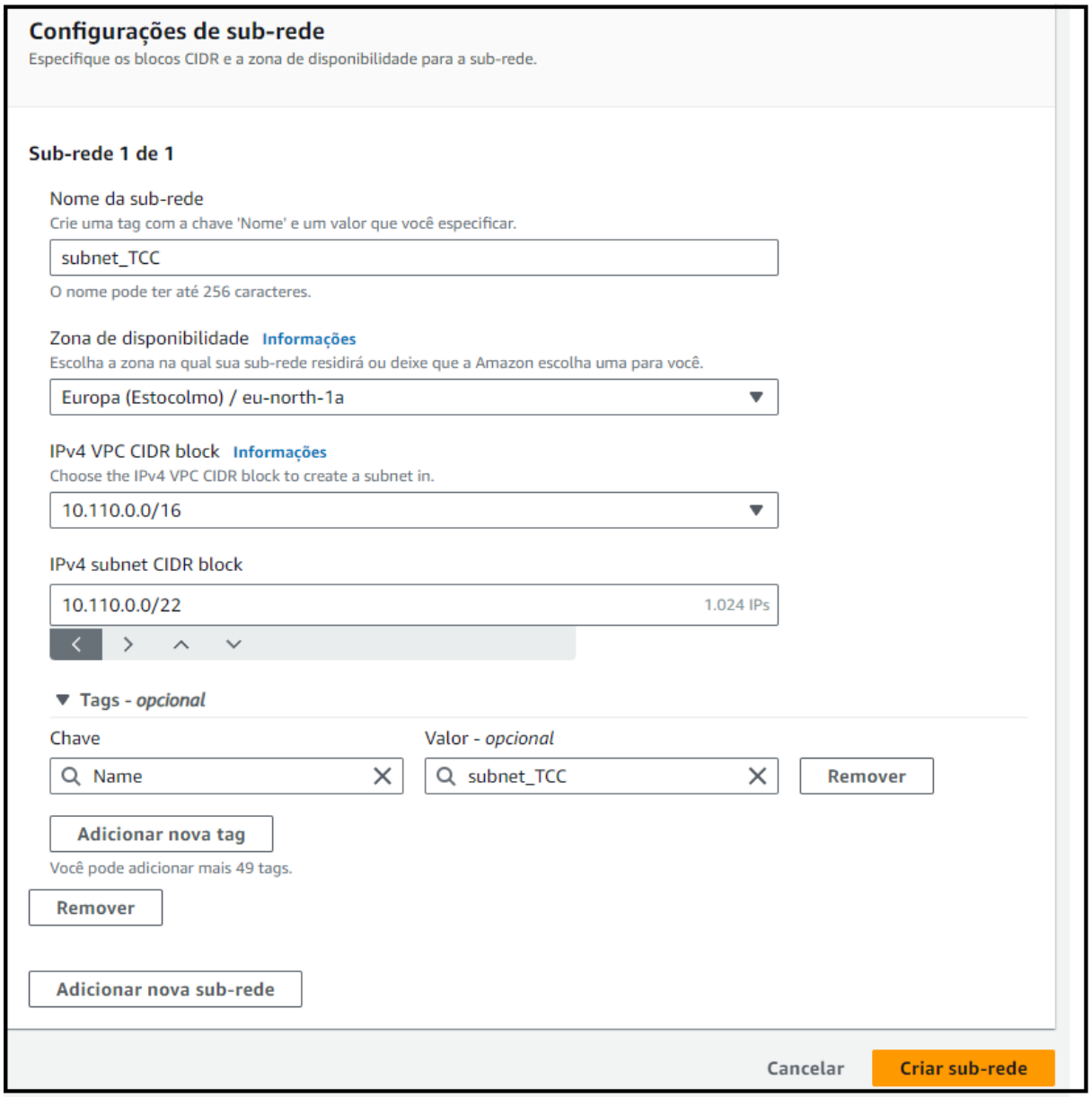
Figura 32 – Criação da VPC.



Fonte: *Amazon Web Service,* 2023.

Com a VPC criada, agora é necessário a criação de *sub-redes* utilizadas para dividir uma VPC em redes menores, o que pode facilitar a administração e a segurança. Para criar uma *sub-rede,* é necessário acessar novamente o console da AWS VPC mostrado na Figura 31 e acessar o painel de *sub-redes*. É possível visualizar o painel de criação da sub-rede na Figura 33.

Figura 33 – Criação da *sub-rede* VPC.

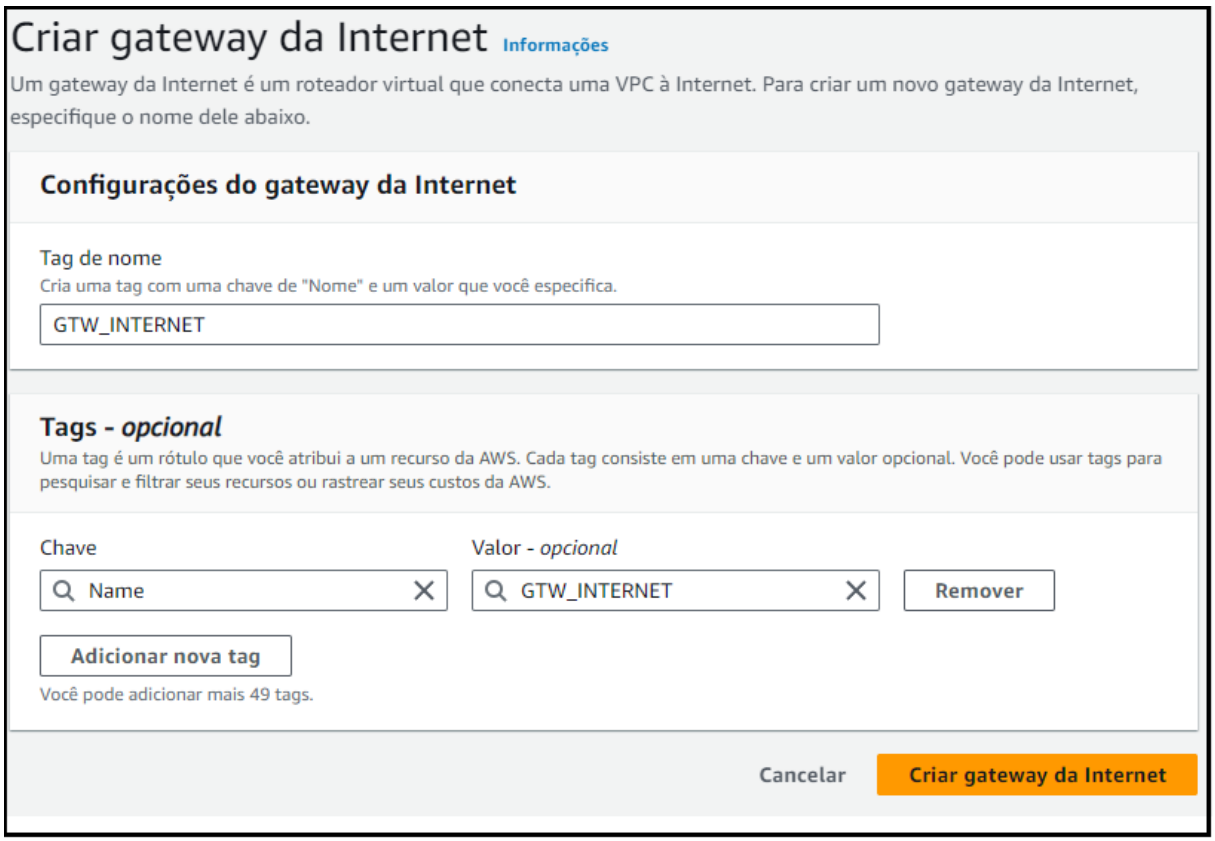


Fonte: *Amazon Web Service,* 2023.

Para ter um *gateway* de saída para a internet é necessária sua criação no console da AWS VPC, conforme mostrado na Figura 31. Um *gateway* da Internet é um roteador virtual que conecta uma VPC à Internet. Os *gateways* de Internet da VPC são recursos altamente disponíveis e escalonáveis. Eles são gerenciados pela AWS

e não requerem nenhuma manutenção ou configuração. A Figura 34 mostra a criação de um *gateway* de Internet.

Figura 34 – Criação de gateway da Internet.



Fonte: *Amazon Web Service,* 2023.

Após a criação do *gateway* da Internet, a sub-rede já está funcionando com acesso à Internet.

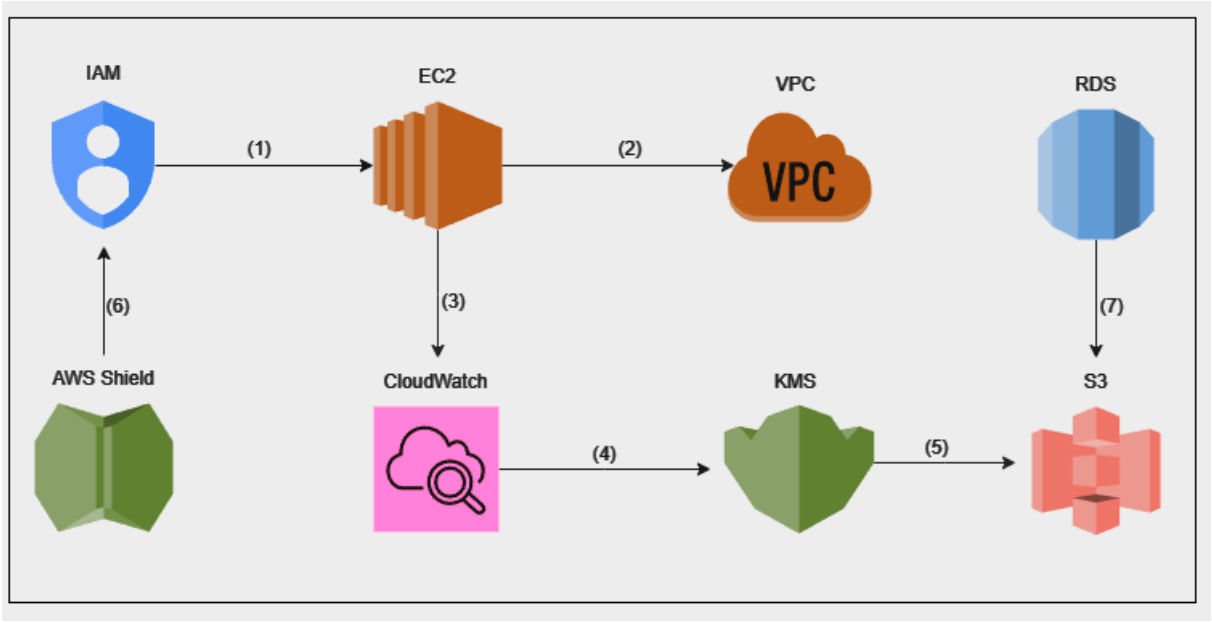
Uma configuração correta de VPC e sub-rede dá segurança a uma aplicação de diferentes maneiras, duas delas são: isolamento e controle de acesso. Na parte do isolamento os recursos em uma VPC não podem se comunicar diretamente com recursos em outras VPCs, a menos que o usuário configure explicitamente o acesso, ajudando a proteger os recursos de ataques externos. Já na parte de controle os grupos de segurança e as listas de controle de acesso (ACLs) de rede, permitem que

o usuário controle o tráfego de entrada e saída para seus recursos, possibilitando a proteção dos recursos de acesso não autorizado.

5.4 Arquitetura e abordagens

O fluxo de dados apresentado na Figura 35 retrata um exemplo de como seria o processo de uma aplicação utilizando 8 serviços da AWS em conjunto, com a finalidade de obter uma aplicação segura em diferentes níveis.

Figura 35 – Fluxo de dados utilizado.



Fonte: Autoria própria, 2023.

Legenda das etapas Figura 35:

1. IAM define as permissões que as instâncias EC2 irão possuir.
2. As instâncias EC2 residem dentro de *subnets* da VPC.
3. O EC2 utilizará o *CloudWatch* para monitorar métricas de desempenho.

4. *CloudWatch* utilizará o KMS para criptografar chaves de métricas geradas pelas instâncias EC2.
5. Chaves gerenciadas pelo KMS podem ser usadas para criptografar dados em serviços como o Amazon S3.
6. AWS Shield oferece proteção DDoS para todos os recursos no ambiente.
7. RDS pode ser configurado para fazer backup no S3.

O conjunto de serviços essenciais da AWS abrange uma gama de funcionalidades para otimizar a infraestrutura na nuvem. O IAM destaca-se na gestão de identidades e permissões, definindo de maneira precisa quem tem acesso aos recursos AWS e quais ações podem ser executadas. O VPC contribui para a segurança ao isolar logicamente a infraestrutura na nuvem, estabelecendo redes privadas virtuais, *subnets* e configurações de roteamento.

Para atender às demandas de capacidade computacional escalável na nuvem, o EC2 oferece flexibilidade ao hospedar aplicativos e serviços. O *Amazon CloudWatch* desempenha um papel crucial no monitoramento da infraestrutura e aplicativos na nuvem, coletando e rastreando métricas, logs e eventos. A criptografia é assegurada pelo KMS, proporcionando gerenciamento centralizado de chaves criptográficas para criptografar dados em repouso e em trânsito.

A segurança é reforçada pelo AWS Shield, que oferece proteção contra-ataques de negação de serviço distribuídos DDoS. No âmbito do *backup* e recuperação de desastres, o Amazon S3 fornece armazenamento de objetos escalável. Além disso, a segurança de bancos de dados é endereçada pelo Amazon RDS, que oferece serviços gerenciados de banco de dados relacional. Esses serviços combinados formam uma base sólida para operações na nuvem, priorizando robustez, segurança e eficiência.

6 CONCLUSÃO

Este projeto tem o intuito de responder a seguinte questão de pesquisa: **Como que a criptografia, as normas de segurança e técnicas da AWS podem garantir a SI das empresas?**

Este estudo permitiu concluir que a SI é uma área complexa e em constante evolução, as organizações devem estar sempre atualizadas sobre as últimas ameaças e tendências de segurança para garantir a proteção de seus dados.

As técnicas de criptografia são ferramentas essenciais para a proteção da informação, integridade e privacidade. A criptografia é utilizada para proteger dados confidenciais, autenticar a identidade das partes envolvidas, proporcionar não repúdio e manter a conformidade com as regulamentações. Seu uso é fundamental para estabelecer a confiança e a segurança no mundo digital.

Entender sobre as leis e normas relacionadas à proteção de dados pessoais é essencial para qualquer pessoa ou organização que esteja envolvida na manipulação dessas informações. Essas leis e normas estabelecem diretrizes e princípios para a coleta, armazenamento, utilização e compartilhamento de dados, visando salvaguardar a privacidade e os direitos dos titulares. O propósito fundamental desse entendimento é assegurar que as organizações estejam em conformidade com a legislação, garantindo assim, a devida proteção dos dados pessoais de clientes, funcionários e parceiros.

A segurança é uma das principais preocupações de empresas ao migrar para a nuvem. Afinal, os dados armazenados e processados são valiosos e sensíveis. Garantir a integridade, confidencialidade e disponibilidade dessas informações é crucial para preservar a reputação e operações de empresas. A computação em nuvem introduz novos desafios e recursos para a proteção e armazenamento de dados. Estratégias de criptografia, autenticação robusta e monitoramento contínuo são indispensáveis para mitigar ameaças cibernéticas, garantindo um ambiente confiável e seguro para as operações empresariais na nuvem.

Além disso, esta pesquisa possibilitou concluir que:

- A criptografia se destaca como uma ferramenta essencial para a proteção da informação e estratégias bem definidas de seu uso a tornam indispensáveis para mitigar ameaças.

- Conhecer as leis e normas de proteção de dados é essencial para garantir conformidade legal e ética no manuseio de informações pessoais. Com a crescente preocupação com a privacidade, estudar essas regulamentações, capacita profissionais a implementar práticas que respeitem os direitos individuais e evitem penalidades legais.
- Os serviços da AWS em conjunto com boas práticas de segurança, geram um ambiente altamente confiável, protegido e seguro, proporcionando aos usuários a confiança necessária para operar suas aplicações de forma eficiente e robusta.
- A segurança na nuvem é uma responsabilidade compartilhada entre a AWS e o cliente. A AWS é responsável por fornece uma infraestrutura segura e ferramentas de segurança, as organizações são responsáveis por implementar práticas adequadas, monitoramento de acesso e permissões, gerenciamento de identidades, autenticações e configurações adequadas de firewalls e atualizações regulares de software.

Para continuidade desta pesquisa sugere-se os seguintes trabalhos futuros:

- Implementar um ambiente utilizando os oito recursos da AWS apresentados;
- Criar um ambiente de teste para monitorar e analisar as técnicas apresentadas.

7 REFERÊNCIAS

AHLGREN, Matt. **What Is AES 256 Encryption**? 2023. Disponível em: <https://www.websiterating.com/pt/cloud-storage/what-is-aes-256-encryption/.> Acesso em: 16 maio 2023.

AMAZON. **AMAZON RDS**. Disponível em: <https://aws.amazon.com/pt/rds/> Acesso em: 10 nov. 2023.

AMAZON. **AMAZON RDS**. Disponível em: <https://aws.amazon.com/pt/rds/resources/> Acesso em: 10 nov. 2023.

AMAZON. **AMAZON S3**. Disponível em: <https://aws.amazon.com/pt/s3/> Acesso em: 10 nov. 2023.

AMAZON. **AMAZON S3**. Disponível em: <https://aws.amazon.com/pt/s3/security/?nc=sn&loc=5> Acesso em: 10 nov. 2023.

AMAZON. **Amazon Virtual Private Cloud (VPC)**. Disponível em: <https://docs.aws.amazon.com/pt_br/vpc/latest/userguide/how-it-works.html> Acesso em: 01 nov. 2023.

AMAZON. **Amazon Virtual Private Cloud (VPC)**. Disponível em: <https://docs.aws.amazon.com/pt_br/vpc/latest/userguide/what-is-amazon-vpc.html> Acesso em: 01 nov. 2023.

AMAZON. **AmazonCloudWatch**. Disponível em: <https://docs.aws.amazon.com/pt_br/AmazonCloudWatch/latest/monitoring/cloudwatch_architecture.html> Acesso em: 05 nov. 2023.

AMAZON. **AmazonCloudWatch**. Disponível em: <https://docs.aws.amazon.com/pt_br/AmazonCloudWatch/latest/monitoring/WhatIsCloudWatch.html> Acesso em: 05 nov. 2023.

AMAZON. **AWS SHIELD**. Disponível em: <https://aws.amazon.com/pt/shield/> Acesso em: 10 nov. 2023.

AMAZON. **AWS SHIELD**. Disponível em: <https://aws.amazon.com/pt/shield/features/> Acesso em: 10 nov. 2023.

AMAZON. **Elastic Compute Cloud (EC2)**. Disponível em: <https://docs.aws.amazon.com/pt_br/AWSEC2/latest/WindowsGuide/concepts.html> Acesso em: 29 out. 2023.

AMAZON. **Elastic Compute Cloud (EC2)**. Disponível em: <https://docs.aws.amazon.com/pt_br/AWSEC2/latest/WindowsGuide/get-set-up-for-amazon-ec2.html> Acesso em: 29 out. 2023.

AMAZON. **Identity and Access Management (IAM)**. Disponível em: <https://docs.aws.amazon.com/pt_br/IAM/latest/UserGuide/introduction.html> Acesso em: 15 out. 2023.

AMAZON. **Identity and Access Management (IAM)**. Disponível em: <https://docs.aws.amazon.com/pt_br/IAM/latest/UserGuide/when-to-use-iam.html> Acesso em: 15 out. 2023.

AMAZON. **Key Management Service (KMS)**. Disponível em: <https://docs.aws.amazon.com/pt_br/kms/latest/developerguide/overview.html> Acesso em: 06 nov. 2023.

AMAZON. **Key Management Service (KMS)**. Disponível em: <https://docs.aws.amazon.com/pt_br/kms/latest/developerguide/concepts.html> Acesso em: 06 nov. 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Dispõe sobre a proteção de dados pessoais**. Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.> Acesso em: 16 maio 2023.

CARDOSO, Giuliano B.; MORAES, Ricardo. **Segurança em banco de dados - Aplicando normas e procedimentos**. Disponível em: <https://www.devmedia.com.br/seguranca-em-bancos-de-dados-aplicando-normas-e-procedimentos-revista-sql-magazine-103/25669.> Acessado em: 24 mar. 2023.

CISCO. **O que é segurança cibernética**. Cisco, [S.l.], 2019. Disponível em: <-<https://www.cisco.com/c/pt_br/products/security/what-is-cybersecurity.html.> Acesso em: 16 maio 2023.

COSTA, Celso; FIGUEIREDO, Luiz Manoel. **Introdução à Criptografia**. Rio de Janeiro: Campus, 2010.

DURBANO, Vinicius. **Segurança da informação: o que é e 12 dicas práticas para garantir**. Disponível em: <https://dicasdehospedagem.com/seguranca-da-informacao/.> Acesso em: 18 de abril de 2023.

FERNANDES, Nélia O. Campo. **Segurança da Informação**. Rio de Janeiro: Brasport, 2018.

FERREIRA, Milton. **Conceitos de Segurança da Informação**. Disponível em: <https://www.apinfo2.com/apinfo/informacao/artigo81.cfm.> Acesso em: 18 de abril de 2023.

GAEA. **Criptografia: o que é e qual a sua importância?** Disponível em: <https://gaea.com.br/criptografia/#:~:text=Qual%20a%20import%C3%A2ncia%20da%20ades%C3%A3o,dados%20que%20transitam%20pela%20solu%C3%A7%C3%A3o.> Acesso em: 18 de abril de 2023.

GUEDES, Kayobrussy. **O que é a criptografia de armazenamento de arquivos**. Disponível em: <https://www.topgadget.com.br/howto/seguranca-howto/o-que-e-a-criptografia-de-armazenamento-de-arquivos.htm.> Acesso em: 31 maio 2023.

HINTZBERGEN, Jule et al. **Fundamentos de Segurança da informação com base na ISO 27001 e na ISO 27002.** São Paulo: Novatec Editora, 2016.

JONES, M.; JOHNSON, R. **Ensuring Data Security in Cloud Computing: A Comprehensive Study. International Journal of Advanced Computer Science and Applications**, v. 11, n. 6, p. 278-288, 2020.

KASPERSKY. **Encryption**. 2019. Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/encryption.> Acesso em: 16 maio 2023.

KINGSTON. **How SSD Encryption Works**. Disponível em: <https://www.kingston.com/br/blog/data-security/how-ssd-encryption-works#:~:text=O%20AES%20(Padr%C3%A3o%20de%20Criptografia,a%20chave%20de%20256%20bits/.> Acesso em: 16 maio 2023.

KOVACS, Leandro. **O que é criptografia e quais os tipos**. Disponível em: <https://tecnoblog.net/responde/o-que-e-criptografia-e-quais-os-tipos/#:~:text=A%20criptografia%20pode%20garantir%20a,ou%20mais%20servidores%20back%2Dend.> Acesso em: 31 maio 2023.

LYCEUM. **Boas práticas de segurança da informação**. Disponível em: <https://blog.lyceum.com.br/boas-praticas-de-seguranca-da-informacao/#:~:text=Como%20voc%C3%AA%20pode%20perceber%2C%20para,e%20adotar%20um%20bom%20antiv%C3%ADrus.> Acesso em: 16 maio 2023.

MASCARENHAS NETO, Pedro Tenório; ARAÚJO, Wagner Junqueira. **Segurança da Informação**. São Paulo: Novatec, 2016. Acesso em: 16 maio 2023.

MAZIERO, Carlos. **Segurança Computacional**. Universidade Federal do Paraná, 2019. Disponível em: <https://wiki.inf.ufpr.br/maziero/lib/exe/fetch.php?media=sc:seg-texto-05.pdf.> Acesso em: 31 maio 2023.

NEISTEIN, Rubens. **Como a criptografia vem transformando o comércio eletrônico**. Disponível em: <https://cryptoid.com.br/criptografia-identificacao-digital-id-biometria/como-a-criptografia-vem-transformando-o-comercio-eletronico/.> Acesso em: 31 maio 2023.

ORACLE. **What Is Data Security? Oracle**. Disponível em: <https://www.oracle.com/br/security/database-security/what-is-data-security/.> Acesso em: 16 maio 2023.

RODRIGUES, Rafael. **ISO 27002: o que é e qual sua importância para a LGPD**. Disponível em: <https://promovesolucoes.com/iso-27002-o-que-e-e-qual-sua-importancia-para-a-lgpd/.> Acesso em: 16 maio 2023.

SANTOS, Rahellen. **Marco Civil da Internet**. Disponível em: <https://www.politize.com.br/marco-civil-da-internet/.> Acesso em: 16 maio 2023.

SEBRAE. **Conheça a LGPD (Lei Geral de Proteção de Dados).** Sebrae, 2018. Disponível em:

<https://www.sebrae.com.br/sites/PortalSebrae/canais_adicionais/conheca_lgpd.> Acesso em: 16 maio 2023.

SERPRO. **O que muda com a LGPD (Lei Geral de Proteção de Dados)**. Serpro, 2018. Disponível em: <https://www.serpro.gov.br/lgpd/menu/a-lgpd/o-que-muda-com-a-lgpd.> Acesso em: 16 maio 2023.

SMITH, L. **Cloud Computing: Benefits, Risks, and Recommendations for Information Security. Journal of Information Privacy and Security**, v. 14, n. 2, p. 43-58, 2018.

SOUZA**, Fernando. Criptografia Simétrica**. Disponível em: <https://medium.com/prognosys/criptografia-sim%C3%A9trica-6b4271ff697c.> Acesso em: 16 maio 2023.

STEFANELLO, Lucas Adiers. **Fundamentos de Segurança da Informação**. Disponível em: <https://incuca.net/fundamentos-de-seguranca-da-informacao/.> Acesso em: 18 de abril de 2023.

TELIUM. **Confidencialidade, integridade e disponibilidade: os três pilares da segurança da informação**. Disponível em: <https://www.telium.com.br/blog/confidencialidade-integridade-e-disponibilidade-os-tres-pilares-da-seguranca-da-informacao.> Acesso em: 16 maio 2023.

TOTVS. **Criptografia: o que é e qual a sua importância para as empresas**. Disponível em: <https://www.totvs.com/blog/negócios/criptografia/.> Acesso em: 18 abr. 2023.

ZANETTI, David. **Profissional de segurança da informação**. Disponível em: <https://promovesolucoes.com/profissional-de-seguranca-da-informacao-como-esta-o-mercado-de-ti/#:~:text=Um%20especialista%20em%20seguran%C3%A7a%20da,seguran%C3%A7a%20e%20arquiteto%20de%20seguran%C3%A7a.> Acesso em: 18 abr. 2023.

ZANINI, Marco. T**ipos de criptografia: descubra as mais importantes para a sua empresa**. Disponível em: <https://inova.globalweb.com.br/post/tipos-de-criptografia-descubra-as-mais-importantes-para-a-sua-empresa.> Acesso em: 16 maio 2023.

ZIMMER, Kelvin. **O que é segurança na internet e por que é importante**? Disponível em: <https://www.lumiun.com/blog/o-que-e-seguranca-na-internet-e-por-que-e-importante/.> Acesso em: 16 maio 2023.

ZAHARIA-Rădulescu A.M., RADU I. **Cloud computing and public administration: approaches in several European countries. Proceedings of the International Conference on Business Excellence**. Vol. 11, Issue 1, p. 739-749, 2017.

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
GABINETE DO REITOR

Av. Universitária, 1069 • Setor Universitário
Caixa Postal 86 • CEP 74605-010
Goiânia • Goiás • Brasil
Fone: (62) 3946.1000
www.pucgoias.edu.br • reitoria@pucgoias.edu.br

RESOLUÇÃO nº 038/2020 – CEPE

ANEXO I

APÊNDICE ao TCC

Termo de autorização de publicação de produção acadêmica

O estudante Luis Guilherme Ribeiro Campos do Curso de Engenharia da Computação, matrícula 20171003302169, telefone: 62 986361697 e-mail luispucgo1107@gmail.com, na qualidade de titular dos direitos autorais, em consonância com a Lei nº 9.610/98 (Lei dos Direitos do Autor), autoriza a Pontifícia Universidade Católica de Goiás (PUC Goiás) a disponibilizar o Trabalho de Conclusão de Curso intitulado CRIPTOGRAFIA E TÉCNICAS PARA GARANTIR A SEGURANÇA DA INFORMAÇÃO EM NUVEM, UTILIZANDO A AMAZON WEB SERVICES, 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, 06 de Setembro de 2023.

gov.br Documento assinado digitalmente
LUIS GUILHERME RIBEIRO CAMPOS
Data: 13/12/2023 11:08:29-0300
Verifique em https://validar.iti.gov.br

Assinatura do autor: _____

Nome completo do autor: Luis Guilherme Ribeiro Campos

Assinatura do professor–orientador: SOLANGE DA SILVA

Nome completo do professor-orientador: gov.br Documento assinado digitalmente
SOLANGE DA SILVA
Data: 14/12/2023 21:49:21-0300
Verifique em https://validar.iti.gov.br