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

SERVIÇOS DE SEGURANÇA EM COMPUTAÇÃO EM NUVEM USANDO A PLATAFORMA *AMAZON WEB SERVICE* (AWS)

BRUNO EMILIO LUIZ SILVA

GOIÂNIA
2023

BRUNO EMILIO LUIZ SILVA

SERVIÇOS DE SEGURANÇA EM COMPUTAÇÃO EM NUVEM USANDO A PLATAFORMA *AMAZON WEB SERVICE* (AWS)

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.

GOIÂNIA

2023

BRUNO EMILIO LUIZ SILVA

SERVIÇOS DE SEGURANÇA EM COMPUTAÇÃO EM NUVEM USANDO A PLATAFORMA *AMAZON WEB SERVICE* (AWS)

Este Trabalho de Conclusão de Curso julgado adequado para obtenção o título de Bacharel em Engenharia da Computação, e aprovado em sua forma final pela Escola Politécnica da Pontifícia Universidade Católica de Goiás, em 16/06/2023_.

_____

Profa. Ma. Ludmilla Reis Pinheiro dos Santos

Coordenadora de Trabalho de Conclusão de Curso

Banca Examinadora:

_____

Orientadora: Profª. Drª. Solange da Silva

_____

Prof. Me. Fernando Gonçalves Abadia

_____

Prof. Me. Wilmar Oliveira de Queiroz

GOIÂNIA

2023

Dedico este trabalho aos meus pais pelo carinho e apoio que tiveram em todos os momentos da minha vida.

AGRADECIMENTOS

A Deus por ter me dado força e saúde para superar as dificuldades e me permitido ultrapassar os obstáculos encontrados.

Gostaria de agradecer a minha família, minha mãe Bernadete, meu pai Aparecido, por sempre me apoiarem e me incentivarem ao longo da vida.

Em especial, gostaria de agradecer aos meus pais, por terem me proporcionado oportunidades de estudo, me apoiado e auxiliado ao longo da minha vida estudantil. Além de terem caminhado e comemorado todas as minhas conquistas junto comigo.

A minha orientadora professora Solange da Silva, pelo apoio, paciência e por sempre ter me ajudado a realizar cada passo dessa monografia.

RESUMO

O objetivo deste trabalho é identificar e descrever os serviços de segurança oferecidos pela Amazon AWS, apresentando sua aplicação na computação em nuvem. Para este estudo, foi selecionada a plataforma AWS, da empresa Amazon, a fim de explorar os principais serviços disponibilizados aos usuários. Foram identificados todos os 27 serviços relacionados à segurança e descritos como se aplicam a plataforma. Os resultados permitiram concluir que os serviços de segurança da AWS oferecem recursos avançados, conformidade com regulamentações e proteção contra ameaças cibernéticas em constante evolução. Ao utilizar esses serviços em conjunto com boas práticas de segurança, as organizações podem aproveitar todos os benefícios da computação em nuvem, mantendo seus dados seguros e reduzindo os riscos de segurança.

Palavras Chaves: Plataforma AWS, Computação em Nuvem, Segurança de Dados, Segurança da Informação.

ABSTRACT

The objective of this work is to identify and describe the security services offered by Amazon AWS, presenting their application in cloud computing. For this study, the AWS platform from Amazon was selected in order to explore the main services available to users. All 27 security-related services were identified and described in terms of their application to the platform. The results led to the conclusion that AWS security services offer advanced features, compliance with regulations, and protection against constantly evolving cyber threats. By using these services in conjunction with good security practices, organizations can take advantage of all the benefits of cloud computing while keeping their data secure and reducing security risks.

Key Words: AWS Platform, Cloud Computing, Data Security, Information Security.

LISTA DE ILUSTRAÇÕES

LISTA DE SIGLAS

ACM	*AWS Certificate Manager*
AD	*Active Directory*
AES	*Advanced Encryption Standard* ou Padrão de Criptografia Avançada
API	*Application Programming Interface* ou Interface de Programação de Aplicação
AWS	*Amazon Web Service*
CAPEX	Custo de Capital
CLI	*Command-Line Interface* ou Interface de Linha de Comando
CVE	*Common Vulnerabilities and Exposures* ou Vulnerabilidades e Exposições Comuns
DDoS	*Distributed Denial of Service* ou Ataque Distribuído de Negação de Serviço
DNS	Sistema de Nomes de Domínio
DPI	*Deep Packet Inspection* ou Inspeção Profunda de Pacotes
EC2	*Elastic Compute Cloud*
ECC	*Elliptic Curve Cryptography* ou Criptografía de Curvas Elípticas
EBS	*Elastic Block Store*
ECR	*Elastic Container Registry*
EKS	*Elastic Kubernetes Service*
FIPS	*Federal Information Processing Standard*

GCM	*Galois Counter Mode*
GDPR	*General Data Protection Regulation* ou Regulamento Geral de Proteção de Dados
HSM	*Hardware Security Module* ou Módulo de Segurança de Hardware
HTTP	*Hypertext Transfer Protocol* ou Protocolo de Transferência de Hipertexto
IAM	*Identity and Access Management*
IaaS	*Infrastructure as a Servic*e ou Infraestrutura como Serviço
IoT	*Internet of Things* ou Internet das Coisas
IP	*Internet Protocol* ou Protocolo de Rede
KMS	*Key Management Service* ou Serviço de Gerenciamento de Chaves
LGPD	Lei Geral de Proteção de Dados
MDC	*Multi-Domains Certificate* ou Certificado de Domínio Múltiplo
MTTR	*Mean Time to Resolution* ou Tempo Médio de Resolução
OPEX	Custo de Operação
PII	*Personally Identifiable Information* ou Informações de Identificação Pessoal
RAM	*Resource Access Manager*
RDS	*Relational Database Service*
RSA	*Rivest-Shamir-Adleman*
S3	*Simple Storage Service*
SDC	*Single Domain Certificate* ou Certificado de Domínio Único

SDK	*Software Development Kit* ou Kit de Desenvolvimento de Software
SO	Sistema Operacional
SSL	*Secure Sockets Layer* ou Camada de Soquete Seguro
TI	Tecnologia da Informação
TLS	*Transport Layer Security*
VPC	*Virtual Private Cloud*
WAF	*Web Application Firewall* ou *Firewall* de Aplicativos Web
XSS	*Cross-Site Scripting*

SUMÁRIO

1 INTRODUÇÃO

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 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).

A importância dos serviços de segurança em nuvem é destacada por Jones e Johnson (2020), que afirmam que, com a crescente adoção da computação em nuvem, garantir a segurança dos dados armazenados e processados na nuvem se tornou uma prioridade para muitas organizações.

No contexto da computação em nuvem, o termo "nuvem" refere-se a um modelo de entrega de serviços de TI baseado na Internet, no qual os recursos são disponibilizados sob demanda (DOE et al., 2019). A computação em nuvem oferece uma variedade de benefícios, como a escalabilidade e a flexibilidade dos recursos computacionais, permitindo que empresas de todos os tamanhos utilizem a infraestrutura de TI de forma eficiente e econômica (SMITH, 2018).

No entanto, a segurança de dados em nuvem apresenta desafios únicos. Segundo Brown (2017), a segurança dos dados na nuvem envolve medidas para garantir a confidencialidade, integridade e disponibilidade dos dados armazenados. A adoção de serviços de segurança em nuvem, como criptografia de dados e controle de acesso, é fundamental para mitigar essas preocupações (BROWN, 2017).

Os *data centers* são edifícios projetados para abrigar múltiplos servidores e equipamentos de comunicação. Normalmente hospedam um grande número de aplicativos de tamanho relativamente pequeno ou médio, cada um rodando em uma infraestrutura de hardware dedicada que é desacoplada e protegida de outros sistemas na mesma instalação. Esses *data centers* hospedam hardware e software para várias unidades organizacionais ou até mesmo empresas diferentes (BARROSO et al., 2019).

Este estudo faz parte de uma serie de pesquisas de servicos relacionados com seguranca de dados oferecidos pelas plataformas em nuvens, sendo que este trabalho vai focar essencialmente na *Amazon Web Services* (AWS).

A AWS é uma plataforma de nuvem amplamente utilizada por empresas de diferentes tamanhos e segmentos. Com o aumento da adoção da nuvem, as empresas precisam garantir a segurança de seus dados e aplicativos hospedados na nuvem. A AWS fornece um conjunto abrangente de serviços de segurança para ajudar as empresas a proteger seus recursos na nuvem (AWS, 2023).

Inicialmente, a concepção do *Cloud Computing* era realizar o processamento de aplicações e o armazenamento de dados fora do ambiente corporativo, utilizando a vasta rede de infraestrutura conhecida como *data centers*. Essa abordagem visava otimizar a utilização dos recursos, permitindo que as aplicações fossem executadas e os dados fossem armazenados de forma centralizada para organizações que operam em rede (VERAS, 2015).

Justifica estudar este assunto devido à ampla utilização dos serviços em nuvem por serviços populares da Internet, tais como e-mail, pesquisas na web, redes sociais, mapas online, *streaming* de vídeo e música. Além disso, a crescente disponibilidade global de conexões de alta velocidade impulsionou a tendência para a computação baseada em servidores ou na nuvem. Portanto, é importante estudar essa área considerando a relevância desses serviços e o aumento da conectividade de alta velocidade em todo o mundo (BARROSO et al., 2019).

Diante deste contexto, esse projeto visa responder a seguinte questão de pesquisa: **- Quais são os serviços de segurança oferecidos pela tecnologia de *cloud computing* na Amazon Web Service e suas aplicações?**

O objetivo geral deste trabalho é identificar e descrever os serviços de segurança oferecidos pela Amazon AWS, apresentando como esses serviços são aplicados na computação em nuvem.

Os objetivos específicos são:

- Mapear os serviços de segurança da ferramenta Amazon AWS;
- Identificar as principais práticas de segurança aplicada em cada um destes serviço de segurança;

Espera-se que os resultados deste trabalho possam contribuir:

- Informando a comunidade a identificar os principais riscos de segurança ao se utilizar estas tecnologias de computação em nuvem;
- Apresentando as principais tecnologias de computação em nuvem utilizadas;
- Mostrando a importância de se ter uma política de segurança;
- Apresentando as soluções e as normas de segurança oferecidas nas empresas que fornecem computação em nuvem.

Quanto aos aspectos metodológicos, a natureza desta pesquisa é um resumo de assunto. Quanto aos seus objetivos é uma pesquisa exploratória. Em relação aos procedimentos técnicos, é uma pesquisa bibliográfica e documental.

Esta monografia está estruturada da seguinte maneira: neste Capítulo é apresentado o contexto do trabalho, a questão de pesquisa, objetivos e resultados esperados. O Capítulo 2 traz duas partes: uma de conceitos e definições da AWS e outra dos serviços de segurança e Leis. 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 estão descritos os serviços da AWS relacionados com a segurança de dados. O Capítulo 5 traz a implementação realizada neste trabalho. No Capítulo 6 apresenta as considerações finais e sugestões de trabalhos futuros.

2. REFERENCIAL TEÓRICO

Neste capítulo são apresentadas duas partes: uma de conceitos e definições, a segunda de trabalhos relacionados.

2.1 Conceitos e Definições

Com o surgimento dos computadores pessoais e sistemas operacionais, as empresas passaram a adotar a arquitetura cliente/servidor. Em seguida, a Internet padronizou os protocolos de comunicação e aumentou rapidamente a disponibilidade de banda, tornando-se um meio de conexão acessível para essa arquitetura. Com isso, os processadores se tornaram mais poderosos e acessíveis em termos de custo. Adquirir recursos tornou-se mais fácil, porém a utilização total desses recursos passou a ser negligenciada.

Nesse contexto, uma nova arquitetura foi empregada, centralizando as informações e introduzindo o conceito de computação em nuvem. Agora, os processos de aplicação e armazenamento não são mais centralizados em ambientes corporativos, mas sim em data centers. Esses data centers atuam em rede com outros data centers, o que deu origem ao conceito de nuvem e seus recursos ilimitados. Com o modelo "pague-pelo-uso", a computação em nuvem ganhou elasticidade e flexibilidade de utilização de recursos, características que a arquitetura cliente/servidor não possuía.

A computação em nuvem, também conhecida como "*cloud computing*", é um modelo de prestação de serviços de TI que tem sido amplamente adotado nos últimos anos. De acordo com Mohsin, Ab Hamid, e Ibrahim (2020), a nuvem é um ambiente virtualizado que oferece acesso flexível e sob demanda a recursos computacionais compartilhados pela Internet.

Há algumas formas de disponibilidade de nuvem sendo elas: privada, híbrida e pública. Segundo AMAZON, uma nuvem privada é uma infraestrutura de nuvem dedicada exclusivamente a uma única organização. Ela pode ser hospedada no local ou em um ambiente de data center de terceiros. Na nuvem privada, todos os recursos, como servidores, armazenamento e rede, são mantidos e gerenciados pela organização. Isso proporciona maior controle, segurança e privacidade em relação

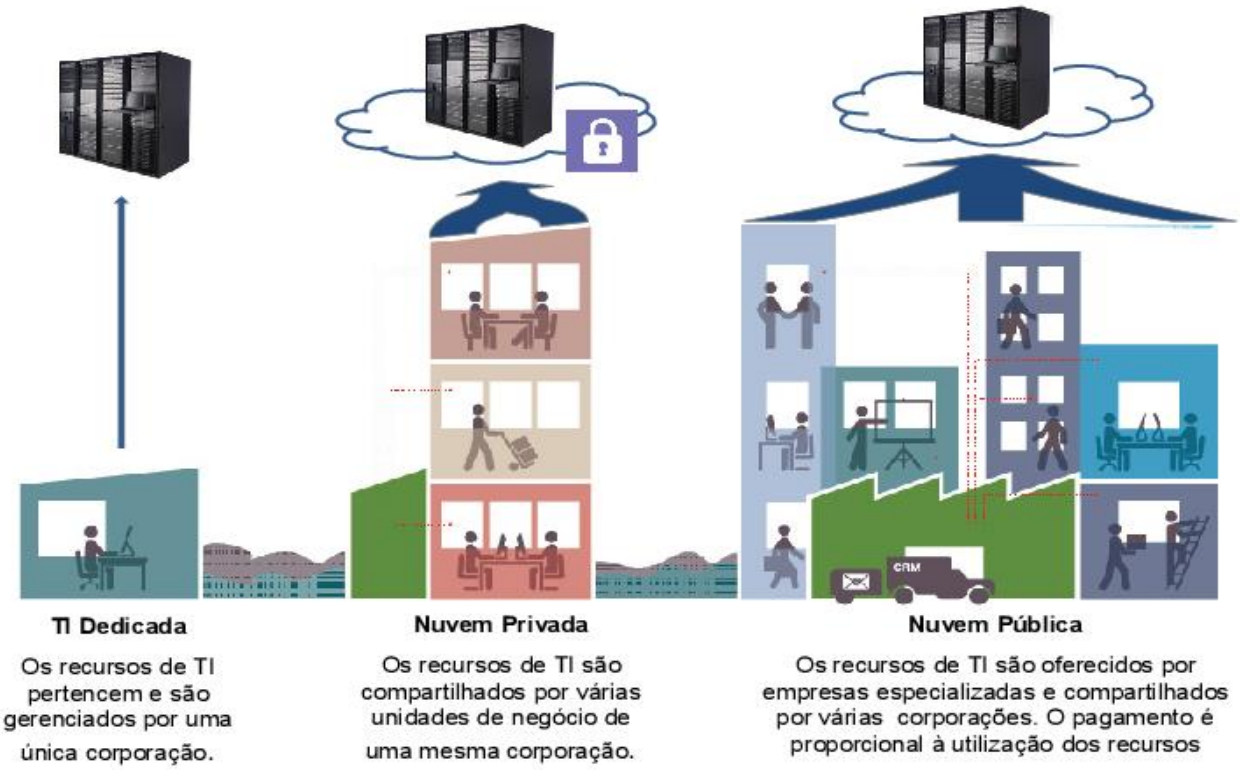
aos dados e aplicativos da empresa. No entanto, a nuvem privada também exige um investimento maior em termos de infraestrutura e gerenciamento.

A nuvem pública é uma infraestrutura de computação em nuvem oferecida por provedores de serviços, como a Amazon Web Services, Google Cloud Platform e Microsoft Azure. Nesse modelo, os recursos de computação são compartilhados entre várias organizações e acessados pela internet. A nuvem pública é altamente escalável, flexível e geralmente mais econômica em comparação com a construção e manutenção de infraestruturas de TI no local. Os provedores de nuvem pública gerenciam e mantêm os recursos, como servidores, armazenamento e rede, permitindo que as empresas se concentrem em desenvolver aplicativos e atender às suas necessidades de negócios.

Uma nuvem híbrida é uma combinação de nuvem privada e nuvem pública, permitindo que as organizações aproveitem os benefícios de ambos os ambientes. Com uma abordagem híbrida, as empresas podem manter dados e aplicativos sensíveis na nuvem privada, enquanto utilizam a nuvem pública para cargas de trabalho menos críticas ou para lidar com picos de demanda. A nuvem híbrida oferece flexibilidade, escalabilidade e custos otimizados, permitindo que as empresas ajustem suas necessidades de computação conforme necessário.

A Figura 1 ilustra as principais diferenças entre ter uma infraestrutura de TI convencional, uma nuvem privada e uma nuvem pública.

Figura 1 – Diferenças TI Dedicada, Nuvem Privada e Nuvem Pública



Fonte: IVAN (2023).

Esses recursos incluem servidores, armazenamento, redes e aplicativos, que são fornecidos por provedores de serviços em nuvem, como a AWS.

Conforme Khan et al. (2021), a nuvem oferece vantagens como escalabilidade, redução de custos, agilidade nos processos de negócios e colaboração eficiente entre equipes geograficamente dispersas.

A natureza virtualizada da nuvem permite que os usuários acessem e utilizem os recursos computacionais de forma eficiente e econômica. Conforme destacado por Aljawarneh, Al-Sharafi e Aldwairi (2019), a nuvem oferece escalabilidade, ou seja, a capacidade de aumentar ou diminuir a quantidade de recursos conforme a demanda. Isso permite que empresas e usuários individuais se adaptem facilmente às mudanças nas necessidades de processamento e armazenamento de dados.

Segundo Sampaio et al. (2019), a nuvem oferece vantagens significativas, como redução de custos, maior agilidade nos processos de negócios e acesso global aos dados e aplicativos. Além disso, a nuvem possibilita a colaboração e o

compartilhamento de informações de forma mais eficiente entre equipes geograficamente dispersas (RABKIN et al., 2018).

Na computação em nuvem pública a ideia é permitir que as organizações executem uma boa parte dos serviços, que hoje são executados localmente nas empresas ou em data center na rede podendo sair do modo Capex (custo de capital) para um modo Opex (custo de operação), em que o custo e o desempenho estão ligados aos níveis de serviços. Isso significa mudar a forma de operar a TI, saindo de um modelo em que as empresas compram recursos de hardware para um modelo baseado em aquisição de serviços (VERAS, 2015).

A segurança da informação na computação em nuvem abrange uma série de práticas, políticas e tecnologias que visam proteger os dados e sistemas hospedados na nuvem contra ameaças cibernéticas. De acordo com Sharma, Rani e Singh (2021), a segurança da informação na nuvem envolve medidas como criptografia, controle de acesso, detecção de ameaças e conformidade regulatória. Essas medidas garantem a confidencialidade, integridade e disponibilidade das informações na nuvem, protegendo os dados sensíveis e pessoais dos usuários, bem como garantindo a confiança e a reputação das empresas.

Em 2020, os serviços de *cloud computing* são fornecidos em sua maioria por grandes empresas como Google, Microsoft e Amazon. As propostas são de melhorar e otimizar o uso de recursos e tornar a operação de TI mais econômica e com resultados positivos (VERAS, 2015).

A Amazon vem desenvolvendo os serviços de nuvem desde 2006 e hoje possui uma oferta única de serviços com foco em IaaS. A Amazon aproveitou sua experiência no suporte a sua plataforma de e-commerce e criou o Amazon AWS (AMAZON).

A AWS é uma das principais provedoras de serviços em nuvem, oferecendo uma ampla gama de recursos e soluções para empresas e desenvolvedores. Conforme Alqarni et al. (2020), a AWS é conhecida por sua elasticidade, alta disponibilidade, segurança avançada e conformidade com regulamentações. Ela permite que os usuários ajustem a capacidade dos recursos de acordo com a demanda, garantindo a eficiência operacional e a escalabilidade dos sistemas na nuvem. A AWS oferece uma infraestrutura global resiliente, proporcionando disponibilidade e baixa latência dos serviços.

Os serviços AWS permitem o acesso a recursos de computação, armazenamento e banco de dados e outros serviços de infraestrutura *on demand*. A ideia é que esta forma de computação reduza custos, melhore o fluxo de caixa da organização contratante, minimize os riscos do negócio e maximize as oportunidades (AMAZON).

Segundo a AMAZON, o serviço tradicional de *data center*, o *hosting*, quando comparado ao serviço de nuvem, é pouco eficaz, considerando que o uso e a capacidade dos recursos estão otimizados no modelo AWS.

A plataforma da Amazon, propõe ser uma plataforma com pouca interação humana, no que diz respeito ao suporte das aplicações. A ideia é que a plataforma funcione sem intervenção humana, melhorando a eficiência. (VERAS, 2015).

A AWS é uma plataforma de serviços em nuvem amplamente utilizada, oferecendo uma variedade de recursos e soluções para empresas e desenvolvedores. Conforme destacado por Sharma, Rani e Singh (2021), a AWS é uma provedora líder de serviços em nuvem, que abrange desde computação, armazenamento e banco de dados até serviços avançados de inteligência artificial e análise de dados.

Um dos conceitos fundamentais da AWS é a elasticidade. Conforme mencionado por Alqarni et al. (2020), a elasticidade na AWS permite que os usuários ajustem a capacidade dos recursos de acordo com a demanda, aumentando ou reduzindo a escala de forma dinâmica. Isso proporciona flexibilidade e eficiência aos usuários, permitindo que se adaptem facilmente às flutuações de tráfego e demanda de recursos.

A segurança também é um aspecto fundamental na AWS. De acordo com Choudhary, Sahu e Pradhan (2020), a AWS oferece uma ampla gama de recursos e serviços para garantir a segurança dos dados e sistemas hospedados em sua plataforma. Isso inclui controles de acesso granulares, criptografia de dados em repouso e em trânsito, detecção e prevenção de ameaças, além de conformidade com diversas regulamentações de segurança.

Outro conceito importante na AWS é a disponibilidade. Conforme ressaltado por Lopes, Siqueira e Gonçalves (2021), a AWS possui uma infraestrutura global que garante alta disponibilidade dos serviços, com uma arquitetura resiliente que permite a replicação e o balanceamento de carga entre regiões e zonas de disponibilidade.

Isso garante que os serviços na AWS estejam sempre disponíveis e com baixa latência para os usuários

2.1.1 Segurança da Informação

A segurança da informação é um aspecto fundamental na computação em nuvem, visando garantir a proteção dos dados e sistemas hospedados nesse ambiente. De acordo com Khan et al. (2021), a segurança da informação na nuvem abrange uma série de princípios, políticas e tecnologias que visam mitigar riscos e proteger as informações contra ameaças cibernéticas.

Um dos principais desafios em segurança da informação na nuvem é a proteção dos dados em trânsito e em repouso. Conforme destacado por Sharma, Kumar e Tyagi (2020), a criptografia é uma medida essencial para garantir a confidencialidade dos dados, tanto durante a transferência entre os sistemas como no armazenamento nos servidores em nuvem. Além disso, o gerenciamento adequado das chaves de criptografia é crucial para evitar acessos não autorizados.

Outro aspecto importante da segurança da informação na nuvem é o controle de acesso. De acordo com Alshamrani et al. (2019), mecanismos de autenticação multifator, como senhas, tokens e biometria, são essenciais para garantir que apenas usuários autorizados tenham acesso aos recursos e dados na nuvem. Além disso, a implementação de políticas de autorização granulares e a monitoração contínua de atividades ajudam a detectar e responder a possíveis violações de segurança.

A conformidade regulatória e a privacidade dos dados são aspectos críticos na segurança da informação na nuvem. Segundo Zeng et al. (2020), as organizações devem garantir que suas práticas de segurança estejam em conformidade com regulamentações, como o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, e adotar medidas adequadas para proteger informações sensíveis e pessoais dos usuários.

2.1.2 Leis de Proteção de Dados

A Lei Geral de Proteção de Dados (LGPD) é uma legislação brasileira que tem como objetivo proteger os direitos dos indivíduos em relação ao tratamento de seus

dados pessoais de todo cidadão que esteja no Brasil. Aprovada em agosto de 2018, a LGPD, de n° 13.709.

Conforme destacado por Alves et al. (2022), a LGPD estabelece princípios e regras para a coleta, armazenamento, processamento e compartilhamento de informações pessoais, garantindo a privacidade e a segurança dos dados.

Um dos conceitos fundamentais da LGPD é o dado pessoal, que é definido como qualquer informação relacionada a uma pessoa física identificada ou identificável. De acordo com Vianna et al. (2021), a LGPD ampliou o escopo da definição de dado pessoal, incluindo informações como endereço IP, *cookies* e identificadores de dispositivos, o que reflete a necessidade de proteção desses dados no ambiente digital.

Outro conceito importante é o consentimento do titular dos dados. Conforme ressaltado por Barros e Santin (2020), a LGPD exige que o tratamento de dados pessoais seja baseado no consentimento livre, informado e inequívoco do titular. Isso significa que as organizações devem obter o consentimento explícito dos indivíduos antes de coletar, processar ou compartilhar seus dados pessoais, garantindo assim a transparência e o controle sobre o uso dessas informações.

A LGPD também estabelece a figura do controlador e do operador de dados. Segundo Costa et al. (2020), o controlador é a pessoa física ou jurídica que decide sobre o tratamento dos dados pessoais, enquanto o operador é responsável por realizar o processamento desses dados em nome do controlador. Essa distinção é importante para atribuir responsabilidades e garantir a conformidade com os requisitos legais estabelecidos pela LGPD.

Na Figura 2 estão ilustrados os principais pontos dessa lei.

Figura 2 – Os principais pontos da lei LGPD

Fonte: CIEE (2023).

Além disso, a LGPD prevê a implementação de medidas de segurança da informação. De acordo com Gomes et al. (2021), as organizações devem adotar medidas técnicas e organizacionais adequadas para proteger os dados pessoais contra acessos não autorizados, perdas, alterações ou destruições acidentais ou ilícitas. Isso envolve a implementação de controles de acesso, criptografia, monitoramento de atividades e a realização de avaliações de impacto à privacidade.

2.2 Trabalhos Relacionados

Este capítulo apresenta alguns trabalhos relacionados ao tema em estudo.

2.2.1 Revisão sistemática dos últimos avanços em questões de segurança e privacidade em *Cloud Computing*

O Ristenpart et al. (2009) faz é uma revisão sistemática dos últimos avanços em questões de segurança e privacidade em *Cloud Computing*. Revisa várias

questões de segurança e privacidade em nuvem e discute as soluções propostas para enfrentar esses problemas.

Este trabalho de pesquisa analisa as questões de vazamento de informações em nuvens de computação de terceiros e investigam as vulnerabilidades de segurança presentes nos ambientes de computação em nuvem. Além disso, examinam os riscos associados ao armazenamento e processamento de dados sensíveis em tais plataformas. Eles identificam várias áreas de preocupação, incluindo a possibilidade de acesso não autorizado, compartilhamento inadequado de dados e violação da privacidade dos usuários. O estudo explora estratégias para mitigar esses riscos e propõe diretrizes para melhorar a segurança das nuvens de computação.

Os resultados mostraram insights valiosos para a compreensão dos desafios e soluções relacionados à segurança em ambientes de computação em nuvem. Utilizando o Amazon EC2 como exemplo, foi demonstrado que é viável mapear a infraestrutura interna de nuvem, identificar a provável localização de uma máquina virtual de destino e, em seguida, criar novas máquinas virtuais até que uma esteja co-localizada com o destino. Explorou-se o potencial desse posicionamento para realizar ataques de canal lateral entre as máquinas virtuais, a fim de extrair informações de uma máquina virtual de destino localizada no mesmo ambiente.

2.2.2 Descrição da arquitetura de segurança da Amazon Web Services

Hashizume et al. (2013) "*Security in the Amazon Web Services Cloud*" descreve a arquitetura de segurança da Amazon Web Services e como ela protege os dados dos usuários. Apresenta também as práticas recomendadas de segurança para usuários da AWS.

Este trabalho de revisão analisa o panorama atual de segurança, privacidade e confiança na computação em nuvem. Os autores examinam os desenvolvimentos recentes nesses aspectos, abordando as preocupações relacionadas à segurança dos dados, privacidade dos usuários e estabelecimento de confiança em ambientes de nuvem. Eles revisam as principais ameaças e desafios de segurança na computação em nuvem, além de discutir as soluções e práticas recomendadas para mitigar esses riscos. O estudo destaca a importância de medidas de segurança

robustas, políticas de privacidade claras e mecanismos confiáveis de autenticação e controle de acesso.

Os resultados fornecem uma visão abrangente das últimas tendências e avanços na segurança da computação em nuvem, servindo como um guia valioso para profissionais e pesquisadores interessados nesse campo. Uma estrutura de segurança em nuvem foi disponibilizada, abrangendo várias linhas de defesa e identificando a interdependência entre elas. Foram detectadas 28 ameaças de segurança na nuvem, classificadas em cinco categorias distintas. Além disso, foram apresentados nove tipos de ataques comuns em ambientes de nuvem, juntamente com diversos incidentes de ataque, e foi realizada uma análise da eficácia das contramedidas propostas.

2.2.3 Documento que relata as melhores práticas de segurança para ambientes na AWS

A própria AWS fornece o "*AWS Security Best Practices*" -que contém as melhores práticas de segurança para ambientes na AWS. Ele inclui orientações sobre como configurar as opções de segurança e como gerenciar a segurança dos recursos na AWS.

Este documento fornecido pela AWS apresenta as melhores práticas de segurança para ambientes na AWS. O material aborda uma ampla gama de tópicos relacionados à segurança, incluindo autenticação, controle de acesso, criptografia, monitoramento, conformidade regulatória e muito mais. O guia destaca as medidas de segurança recomendadas para proteger os dados e sistemas hospedados na plataforma da AWS, juntamente com diretrizes para configurar corretamente os serviços de segurança da AWS. Ao seguir essas melhores práticas, os usuários da AWS podem fortalecer a segurança de suas aplicações e mitigar potenciais ameaças à integridade, confidencialidade e disponibilidade dos dados.

O documento é uma referência importante para profissionais de segurança, administradores de sistemas e desenvolvedores que desejam implantar e gerenciar infraestruturas seguras na AWS.

3. METODO

Esta pesquisa, segundo sua natureza, é um resumo de assunto, pois busca sistematizar uma área de conhecimento. O autor deve possuir um sólido conhecimento na área, buscando explicar a área do conhecimento do projeto, incluindo seu desenvolvimento e os problemas em aberto (WAZLAWICK, 2014).

Segundo seus objetivos trata-se de uma pesquisa exploratória, que pode ser considerada como o estágio inicial de um processo de pesquisa mais abrangente. Nesse tipo de pesquisa, o autor busca examinar anomalias desconhecidas que possam ser a base para pesquisas mais elaborada (WAZLAWICK, 2014).

Quanto aos procedimentos técnicos, esta 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 foi 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 - Serviços de segurança oferecidos pela tecnologia de *cloud computing* na Amazon Web Service.

b) Fazer o levantamento bibliográfico preliminar de periódicos e artigos relacionados ao assunto de pesquisa, no caso a computação em nuvem e seus serviços de segurança foram feitas na base de dados da CAPES, repositório da PUCGO, *Web of Science;*

c) Elaboração do plano provisório de assunto: definir a estrutura do trabalho, incluindo uma apresentação organizada das partes.

d) Busca das fontes: identificar as fontes bibliográficas que forneçam informações relevantes para responder ao problema proposto, consultando dissertações, periódicos científicos, obras de referência, entre outros.

e) Leitura do material: identificar as informações e dados relevantes, estabelecer relações com o problema proposto e analisar a coerência das informações apresentadas pelos autores.

f) Fichamento: com o objetivo de identificar as fontes, registrar ideias, informações relevantes e comentários, e organizar as informações adquiridas.

g) Organização lógica do assunto: com o propósito de atender aos objetivos da pesquisa. Essa etapa é um dos elementos essenciais para a elaboração dessa parte.

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 consiste em estabelecer um objeto de estudo, escolher as variáveis que a influenciam e determinar as formas de controle e observar os efeitos que a variável gera no objeto. Realiza pelo menos um dos elementos que julga ser responsável pela circunstância que está sendo pesquisado (GIL, 2017).

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

a) Fazer a formulação do problema com base no levantamento bibliográfico, que será: **Quais são os serviços de segurança oferecidos pela tecnologia de *cloud computing* na Amazon Web Service e suas aplicações?**

b) Definição do plano experimental: foi descrito os serviços de segurança no ambiente AWS e implementado um desses serviços o qual foi IAM. Foi utilizado um ambiente de cloud da plataforma Amazon, sendo desenvolvido todas as etapas de configurações e definições de políticas do serviço.

c) Coleta de dados: Realizados testes internos na aplicação desenvolvida nesta monografia, simulando uma aplicação real.

d) Analisado um dos serviços de definição das políticas de segurança.

e) Escrita do TCC.

4. SERVIÇOS RELACIONADOS A SEGURANÇA NO AMBIENTE AWS

Neste capítulo são apresentadas as principais ferramentas de segurança da AWS, cujas informações foram retiradas do site da AMAZON, como referência.

4.1 Gerenciamento de identidade e acesso

O gerenciamento seguro de identidades, recursos e permissões em ambientes de grande escala é facilitado pelos serviços de identidade da AWS. Esses serviços garantem a segurança dos dados e sistemas, oferecendo controle preciso sobre as identidades e permissões associadas, em conformidade com as melhores práticas de segurança da AWS.

A) AWS *Identity and Access Management* (IAM)

O *AWS Identity and Access Management* (IAM) fornece controle de acesso em todos os recursos da AWS. Com o IAM, é possível controlar o acesso a serviços e recursos sob condições específicas. As políticas do IAM podem ser usadas para gerenciar permissões para um quadro de funcionários e sistemas para garantir permissões com privilégio mínimo. Seu funcionamento está apresentado na Figura 3.

Figura 3 – Funcionamento AWS *Identity and Access Management*

Fonte: Amazon, 2020.

Segundo AMAZON, o IAM fornece autenticação e autorização para produtos da AWS. Um serviço avalia se a solicitação da AWS será permitida ou negada. O acesso é negado por padrão e é permitido somente quando uma política concede acesso explícito.

É possível anexar políticas a funções e a recursos para controlar o acesso na AWS. Com o IAM, é possível especificar quem ou o que pode acessar serviços e recursos na AWS, gerenciar permissões refinadas de maneira centralizada e analisar o acesso para refinar as permissões na AWS.

B) Centro de Identidade do AWS IAM

É uma extensão do IAM, já descrito. O AWS IAM *Identity Center* (sucessor do AWS *Single Sign-On*) ajuda a criar ou conectar com segurança as identidades da força de trabalho e gerenciar o acesso delas de maneira centralizada em contas e aplicações da AWS. O IAM *Identity Center* constitui a abordagem recomendada para autenticação e autorização da força de trabalho na AWS para organizações de qualquer tamanho e tipo.

Conforme AMAZON, o IAM *Identity Center* configura e mantém todas as permissões necessárias para as contas automaticamente, sem exigir nenhuma configuração adicional nas contas individuais. É atribuido permissões de usuário com base em funções de trabalho comuns e as personaliza para atender a requisitos de segurança específicos.

C) Amazon Cognito

O Amazon Cognito oferece um armazenamento de identidade que pode ser dimensionado para milhões de usuários, oferece suporte à federação de identidades sociais e corporativas e oferece recursos avançados de segurança para proteger consumidores e negócios.

Construído com padrões de identidade aberta, o Amazon Cognito oferece suporte a vários regulamentos de conformidade e se integra a recursos de desenvolvimento de *frontend e backend*. (AMAZON). Seu funcionamento está apresentado na Figura 4.

Figura 4 – Funcionamento Amazon Cognito

Fonte: Amazon, 2020.

Segundo a Amazon, o Cognito fornece autenticação, autorização e gerenciamento de usuários para aplicações Web e móveis. Os usuários podem fazer login diretamente com um nome de usuário e uma senha ou por meio de terceiros, como o Facebook, a Amazon, o Google ou a Apple.

D) AWS *Directory Service*

O AWS *Directory Service for Microsoft Active Directory*, também conhecido como AWS *Managed Microsoft AD* é o próprio *Microsoft Active Directory* em execução na infraestrutura gerenciada da AWS. Assim, pode se administrar usuários e dispositivos no AWS *Managed Microsoft AD* usando as ferramentas que já conhecidas, como a Central Administrativa do AD e Usuários e Computadores do AD.

O AWS *Managed Microsoft AD* é executado na infraestrutura gerenciada da AWS com monitoramento que detecta e substitui automaticamente controladores de domínio com falha. Além disso, a replicação de dados e os snapshots automáticos diários são configurados. Não é necessário instalar software e a AWS executa todas as aplicações de *patches* e as atualizações de software.

E) AWS *Resource Access Manager*

O AWS *Resource Access Manager* (RAM) ajuda a compartilhar os recursos com segurança entre contas da AWS, dentro da organização ou unidades organizacionais no AWS *Organizations* e com funções do IAM e usuários do IAM para tipos de recursos compatíveis.

O AWS RAM pode ser usado para compartilhar recursos com outras contas da AWS. Isso elimina a necessidade de supervisionar e gerenciar recursos em todas as contas. Quando é compartilhado um recurso com outra conta, essa conta recebe acesso ao recurso e todas as políticas e permissões dessa conta e se aplicam ao recurso compartilhado.

F) AWS *Organizations*

O AWS *Organizations* oferece a capacidade de gerenciar e controlar o ambiente de nuvem de maneira centralizada. Pode gerenciar e organizar contas em uma única fatura, definir políticas centrais e requisitos de configuração para toda a organização, criar permissões ou recursos personalizados dentro da organização e delegar responsabilidades a outras contas para que possam gerenciar em nome da organização.

Além disso, o AWS *Organizations* é integrado a outros serviços da AWS para que possa definir configurações centrais, mecanismos de segurança, requisitos de auditoria e compartilhamento de recursos entre contas.

4.2 Detecção

Os serviços de detecção e resposta fornecidos pela AWS desempenham um papel fundamental na identificação de configurações de segurança inadequadas, ameaças em potencial e comportamentos inesperados. Esses serviços têm como objetivo possibilitar uma resposta rápida diante de atividades que possam indicar a presença de ações não autorizadas ou maliciosas em seu ambiente.

A) AWS *Security Hub*

O AWS *Security Hub* é um serviço de gerenciamento de postura de segurança na nuvem que realiza verificações de práticas recomendadas de segurança contínuas e automatizadas em relação aos seus recursos da AWS. O *Security Hub*

agrega alertas de segurança de vários serviços da AWS e produtos de parceiros em um formato padronizado para que o gerente da conta possa agir com mais facilidade.

O *Security Hub* simplifica como entender e melhorar a postura de segurança com verificações automatizadas de práticas recomendadas de segurança baseadas em regras do AWS Config e integrações automatizadas com dezenas de serviços da AWS e produtos de parceiros.

B) Amazon *GuardDuty*

O Amazon *GuardDuty* é um serviço de detecção de ameaças que monitora continuamente atividades mal-intencionadas e comportamentos não autorizados para proteger contas da AWS, *workloads* do EC2, aplicativos de contêiner e dados armazenados no Amazon *Simple Storage Service* (S3).

O *GuardDuty* combina machine learning, detecção de anomalias, monitoramento de rede e detecção de arquivos mal-intencionados utilizando fontes desenvolvidas pela AWS e de terceiros líderes do setor para ajudar a proteger as *workloads* e os dados na AWS. O *GuardDuty* é capaz de analisar dezenas de bilhões de eventos em várias fontes de dados da AWS, como logs de eventos do AWS *CloudTrail*, logs de fluxo da Amazon *Virtual Private Cloud* (VPC), logs de auditoria do Amazon *Elastic Kubernetes Service* (Amazon EKS) e logs de consulta ao DNS (AMAZON).

C) Amazon *Inspector*

Amazon *Inspector* é um serviço de gerenciamento de vulnerabilidade que verifica continuamente as *workloads* da AWS em busca de vulnerabilidades de software e exposição não intencional à rede. O Amazon *Inspector* pode ser usado em todas as contas da organização.

Depois de iniciado, o Amazon *Inspector* descobre automaticamente instâncias e imagens de contêineres em execução do Amazon *Elastic Compute Cloud* (EC2) residentes no Amazon *Elastic Container Registry* (ECR), em qualquer escala e começa a avaliá-las imediatamente quanto a vulnerabilidades conhecidas.

Segundo Amazon, o Inspector calcula uma pontuação de risco altamente contextualizada para cada descoberta, correlacionando informações de *Common Vulnerabilities and Exposures* (CVE) ou Vulnerabilidades e exposições comuns, com

fatores como acesso à rede e potencial de exploração. Essa pontuação é usada para priorizar as vulnerabilidades mais críticas com o objetivo de melhorar a eficiência da resposta de remediação.

Todas as descobertas são agregadas em um console do Amazon *Inspector* recém-projetado e enviadas ao AWS *Security Hub* e ao Amazon *EventBridge* para automatizar fluxos de trabalho. As vulnerabilidades encontradas em imagens de contêineres também são enviadas ao Amazon ECR para que os proprietários de recursos as visualizem e corrijam. Com o Amazon *Inspector*, até mesmo as pequenas equipes de segurança e desenvolvedores podem garantir a segurança e a conformidade das *workloads* de infraestrutura em suas *workloads* da AWS.

D) AWS Config

O AWS Config registra detalhes de alterações em recursos da AWS para fornecer um histórico de configuração. Pode utilizar o Console de gerenciamento da AWS, a API ou a CLI para obter detalhes de como era a configuração de um recurso em qualquer momento do passado.

O AWS Config também entregará automaticamente um arquivo de histórico de configuração ao bucket do Amazon S3 que for especificado. O AWS Config avalia, audita e avalia continuamente as configurações e os relacionamentos de recursos (AMAZON).

E) Amazon *CloudWatch*

O Amazon *CloudWatch* é um serviço de monitoramento e gerenciamento que oferece dados e insights práticos para recursos de aplicações e infraestrutura on-premises, híbridos e da AWS. Pode coletar e acessar todos os dados de performance e operacionais, na forma de logs e métricas, em uma única plataforma, em vez de monitorá-los em silos (servidor, rede ou banco de dados).

O *CloudWatch* permite monitorar a pilha inteira (aplicações, infraestrutura e serviços) e usar alarmes, logs e dados de eventos para executar ações automatizadas e reduzir o *Mean Time to Resolution* (MTTR) ou Tempo médio de resolução). O *CloudWatch* oferece insights práticos que ajudam a otimizar a performance de aplicações, gerenciar a utilização de recursos e compreender a integridade operacional de todo o sistema.

O *CloudWatch* oferece uma visibilidade de dados de métricas e logs com até um segundo de resolução, 15 meses de retenção de dados (métrica) e a capacidade de executar cálculos com base nas métricas. Assim, pode executar análises históricas para otimizar custos e obter real time insights para otimizar recursos de aplicações e infraestrutura. (AMAZON).

F) AWS *CloudTrail*

O AWS *CloudTrail* monitora e registra a atividade da conta por toda a infraestrutura da AWS, oferecendo controle sobre o armazenamento, análise e ações de remediação. O AWS *CloudTrail* permite auditoria, monitoramento de segurança e solução de problemas operacionais.

O *CloudTrail* registra a atividade do usuário e as chamadas de API nos serviços da AWS como eventos. Os eventos do *CloudTrail* ajudam a responder às perguntas "quem fez o quê, onde e quando?". (AMAZON).

G) AWS IoT *Device Defender*

O AWS IoT *Device Defender* é um serviço totalmente gerenciado para auditoria e monitoramento de dispositivos conectados ao AWS IoT. Avalia a configuração da cloud da frota de dispositivos IoT, fornece monitoramento contínuo das atividades do dispositivo por meio de recursos de detecção baseados em regras e ML, dispara um alarme quando uma violação de auditoria ou anomalia de comportamento é identificada e permite que resolva problemas rapidamente com ações de mitigação integradas. (AMAZON).

4.3 Proteção de Rede e Aplicações

Os serviços de proteção de rede e aplicações oferecidos pela AWS desempenham um papel essencial ao permitir a aplicação de políticas de segurança avançadas nos pontos de controle de rede dentro da organização. Esses serviços da AWS possibilitam a inspeção e filtragem do tráfego de forma a evitar o acesso não autorizado aos recursos em diferentes níveis, abrangendo desde o nível de host até os limites de rede e aplicação.

A) AWS *Network Firewall*

O AWS *Network Firewall* é um serviço de *firewall* gerenciado pela AWS que permite a criação e gerenciamento de políticas de segurança de rede personalizadas. De acordo com a AWS, o serviço "fornece visibilidade do tráfego de rede em tempo real, incluindo a capacidade de inspecionar pacotes em profundidade para identificar ameaças, como malwares e tentativas de invasão, e bloqueá-las".

O *Network Firewall* é baseado em uma arquitetura de regras flexível, que permite que os usuários definam suas próprias regras de *firewall*, usando várias condições, tais como endereços IP de origem e destino, portas e protocolos. Além disso, o serviço é altamente escalável e pode ser facilmente integrado com outros serviços da AWS, como o Amazon *Virtual Private Cloud* (VPC) e o AWS *CloudFormation*.

Segundo a AWS, o *Network Firewall* "usa uma combinação de regras baseadas em estado e inspeção profunda de pacotes (DPI) para filtrar e monitorar o tráfego de rede". Isso significa que o serviço pode identificar ameaças de segurança, como tentativas de invasão e malware, e bloqueá-las antes que possam causar danos aos sistemas da empresa.

Uma das principais vantagens do AWS *Network Firewall* é que ele é altamente automatizado e gerenciado pela AWS. Isso significa que os usuários não precisam se preocupar com a configuração e manutenção do *firewall*, pois a AWS cuida de todas as atualizações e patches necessários. Além disso, o serviço oferece uma interface gráfica intuitiva que permite aos usuários gerenciar facilmente políticas de segurança de rede.

B) AWS *Shield*

O AWS *Shield* é um serviço gerenciado pela AWS que fornece proteção contra ataques distribuídos de negação de serviço (DDoS). De acordo com a AWS, o serviço "ajuda a proteger os aplicativos da web executados na AWS, como sites, aplicativos móveis e APIs, contra interrupções causadas por ataques DDoS".

O AWS *Shield* é composto por dois tipos de proteções: AWS *Shield Standard* e AWS *Shield Advanced*. A proteção AWS *Shield Standard* é fornecida gratuitamente para todos os clientes da AWS e ajuda a proteger contra a maioria dos ataques DDoS comuns. Já o AWS *Shield Advanced* é uma opção paga que

oferece proteção adicional contra ataques mais sofisticados, além de recursos avançados de monitoramento e suporte técnico especializado.

O AWS *Shield* funciona detectando e filtrando o tráfego malicioso antes que atinja a infraestrutura da AWS. O serviço utiliza várias técnicas, incluindo análise comportamental, análise de reputação de IP e aprendizado de máquina, para identificar padrões de tráfego malicioso e bloqueá-los. Além disso, o AWS *Shield* pode ser facilmente integrado com outros serviços da AWS, como o Amazon *CloudFront* e o Amazon *Elastic Load Balancing*, para fornecer proteção adicional aos aplicativos da web executados na plataforma da AWS.

Uma das principais vantagens do AWS *Shield* é que ele é altamente escalável e gerenciado pela AWS. Isso significa que os usuários não precisam se preocupar com a configuração e manutenção do serviço, pois a AWS cuida de todas as atualizações e patches necessários. Além disso, o serviço oferece uma interface gráfica intuitiva que permite aos usuários monitorar facilmente aplicativos da web e analisar possíveis ameaças de segurança.

C) Firewall de DNS do Amazon *Route 53 Resolver*

O AWS *Firewall* de DNS do Amazon *Route 53 Resolver* é um serviço gerenciado pela AWS que permite a criação de políticas de segurança para o tráfego de DNS na infraestrutura da AWS. De acordo com a AWS, o serviço "fornece uma camada adicional de segurança ao monitorar e bloquear tráfego malicioso para evitar ataques de *phishing*, *malware* e *ransomware*".

D) AWS *Web Application Firewall* (WAF)

O AWS *Web Application Firewall* (WAF) é um serviço de segurança gerenciado que ajuda a proteger aplicativos web de ataques maliciosos, como *SQL Injection*, *cross-site scripting* (XSS), entre outros. Permite que seja definido regras personalizadas que controlam o tráfego de entrada para o aplicativo, bloqueando o acesso de solicitações que não atendem aos critérios definidos.

O AWS WAF permite que crie regras baseadas em IP, cabeçalhos HTTP e conteúdo do corpo da solicitação, bem como em outras informações relevantes. Ele também inclui um conjunto de regras de segurança gerenciadas pela AWS, que são continuamente atualizadas para proteger o aplicativo contra ameaças conhecidas.

Além disso, o serviço oferece recursos de monitoramento e registro para ajudar a detectar e solucionar problemas de segurança.

O AWS WAF é totalmente integrado com outros serviços da AWS, como o Amazon *CloudFront* e o Amazon API *Gateway*, permitindo que seja aplicado as mesmas regras de segurança em toda a arquitetura de aplicativos web. Ele também é altamente escalável, permitindo que lide com picos de tráfego e mantenha a proteção do aplicativo em todos os momentos.

E) AWS *Firewall Manager*

O AWS *Firewall Manager* é um serviço gerenciado que ajuda a automatizar a implantação e gerenciamento de firewalls em toda a organização. Permite que seja definido políticas de segurança centralizadas que podem ser aplicadas a todos os recursos da AWS da conta, incluindo VPCs, sub-redes e instâncias EC2.

Com o AWS Firewall Manager, pode criar regras de *firewall* personalizadas e aplicá-las automaticamente a todos os recursos da conta que atendem a certos critérios, como nome de tag ou tipo de recurso. O serviço também inclui regras gerenciadas pela AWS, que são atualizadas continuamente para ajudar a proteger recursos contra ameaças conhecidas.

O AWS *Firewall Manager* oferece um painel centralizado para monitorar e gerenciar a segurança em toda a organização. Ele permite que visualize o status de segurança de todos os recursos de conta, visualize os logs de *firewall* em tempo real e receba alertas sobre atividades de segurança suspeitas.

O serviço é altamente escalável e pode lidar com grandes volumes de tráfego. Ele também é compatível com outros serviços de segurança da AWS, como o AWS WAF e o Amazon *GuardDuty*, para fornecer uma solução abrangente de segurança para a organização.

4.4 Proteção de Dados

A AWS disponibiliza uma variedade de serviços projetados para garantir a proteção de dados, contas e workloads contra acesso não autorizado. Ao utilizar esses serviços, é possível fortalecer a segurança dos ativos digitais, garantindo a confidencialidade e a integridade das informações, ao mesmo tempo em que adere às melhores práticas de segurança estabelecidas pela AWS.

A) Amazon *Macie*

O Amazon *Macie* é um serviço gerenciado de segurança que usa inteligência artificial e aprendizado de máquina para descobrir, classificar e proteger dados confidenciais em contas da AWS. Ele ajuda a identificar dados confidenciais, como informações pessoais identificáveis (PII), informações de cartão de crédito e outros dados sensíveis que podem estar armazenados em recursos na nuvem.

Com o Amazon *Macie*, pode se visualizar o acesso aos dados confidenciais, criar políticas de segurança personalizadas e detectar atividades maliciosas em tempo real. O serviço também fornece relatórios de conformidade para ajudar a auditar o acesso aos dados e garantir que eles estejam protegidos contra ameaças internas e externas.

O Amazon *Macie* usa algoritmos de aprendizado de máquina para analisar continuamente dados em busca de comportamentos incomuns ou potencialmente maliciosos. Ele pode detectar atividades como tentativas de login suspeitas, tentativas de exfiltrar dados e movimentação de grandes quantidades de dados. O serviço também oferece integração com outros serviços da AWS, como o Amazon S3, para proteger automaticamente dados confidenciais.

B) AWS *Key Management Service* (AWS KMS)

O AWS *Key Management Service* (AWS KMS) é um serviço gerenciado de criptografia de chaves que permite criar e controlar chaves criptográficas para proteger dados e recursos na AWS. Com o AWS KMS, é possivel gerenciar e proteger chaves de criptografia, bem como usar chaves gerenciadas pela AWS para criptografar dados.

O serviço permite que crie chaves de criptografia e defina políticas de acesso para controlar quem pode usar essas chaves. Pode criar chaves mestras para criptografar e descriptografar dados ou chaves de dados para criptografar dados específicos em aplicações. Além disso, o AWS KMS é compatível com diversos algoritmos de criptografia, incluindo AES-GCM, RSA e ECC.

O AWS KMS ajuda a proteger dados em várias camadas de segurança. É usado técnicas de criptografia avançadas para proteger chaves e fornece recursos como a rotação automática de chaves, para ajudar a garantir que chaves estejam sempre atualizadas e protegidas contra ameaças.

O AWS KMS também é altamente integrado com outros serviços da AWS, como o Amazon S3 e o Amazon RDS, para ajudar a proteger dados em todos os pontos de integração. Ele fornece um alto nível de controle sobre chaves de criptografia e permite que se audite as atividades de criptografia na conta da AWS.

C) AWS *CloudHSM*

O AWS *CloudHSM* é um serviço de segurança gerenciado que oferece módulos de segurança de hardware (HSMs) dedicados e protegidos para armazenar e gerenciar chaves criptográficas e outros segredos sensíveis. O serviço permite que se crie e controle as próprias chaves criptográficas em um ambiente seguro e com certificação FIPS 140-2 nível 3.

O *CloudHSM* é um dispositivo físico que usa uma camada de segurança extra para proteger as chaves criptográficas em um ambiente seguro. O serviço é gerenciado pela AWS, mas os clientes têm acesso exclusivo às instâncias do HSM, permitindo total controle sobre as chaves criptográficas. Os HSMs *CloudHSM* também podem ser usados para implementar políticas de assinatura de transações, autenticação de documentos e garantir a conformidade com padrões regulatórios.

O *CloudHSM* é compatível com várias estruturas de criptografia, como RSA e *Elliptic Curve Cryptography* (ECC), além de suportar vários padrões de segurança, como a criptografia de chave dupla. O serviço permite que se gerencie chaves de criptografia em um ambiente seguro, com rotação automática de chaves e outras técnicas de proteção, como *backup* e restauração.

D) AWS *Certificate Manager*

O AWS *Certificate Manager* (ACM) é um serviço gerenciado que permite provisionar, gerenciar e implantar certificados SSL/TLS de forma fácil e rápida. O serviço torna o processo de gerenciamento de certificados SSL/TLS automatizado e simplificado, eliminando a necessidade de adquirir, instalar, configurar e renovar certificados manualmente.

Com o ACM, é possível obter certificados SSL/TLS de forma gratuita e configurá-los automaticamente em serviços da AWS, como *Elastic Load Balancing*, Amazon *CloudFront* e Amazon API *Gateway*. O serviço também oferece suporte para certificados particulares importados, permitindo que se gerencie todos os

certificados em um único lugar.

O ACM é compatível com vários tipos de certificados, incluindo certificados de domínio único (SDC), certificados de domínio múltiplo (MDC) e certificados curinga. Além disso, o ACM oferece uma interface de gerenciamento baseada em console, permitindo que se gerencie e monitore seus certificados SSL/TLS de forma simples e intuitiva.

E) AWS *Secrets Manager*

O AWS *Secrets Manager* é um serviço gerenciado que permite armazenar, gerenciar e recuperar segredos, como senhas, *tokens* e chaves de API, de forma segura e automatizada. Ele permite que seja armazenada e gerenciado segredos de forma centralizada, fornecendo um único local para gerenciar credenciais de acesso e outras informações sensíveis.

O *Secrets Manager* ajuda a proteger os segredos usando criptografia avançada e rotação automática de chaves. O serviço criptografa todos os segredos em repouso e em trânsito usando chaves gerenciadas pela AWS *Key Management Service* (KMS). Ele também oferece recursos de rotação automática de segredos, permitindo que se automatize o processo de troca regular de senhas e chaves de API, reduzindo o risco de exposição de informações sensíveis.

Além disso, o *Secrets Manager* oferece integração com outros serviços da AWS, permitindo que use facilmente os segredos em aplicativos e serviços em execução na nuvem da AWS. O serviço também fornece APIs e SDKs para que possa integrá-lo com as próprias aplicações e serviços.

4.5 Resposta a Incidentes

Apresenta uma visão geral dos fundamentos de resposta a incidentes de segurança no ambiente AWS de um cliente. Fornece uma visão geral dos conceitos de segurança em nuvem e resposta a incidentes, e identifica as capacidades, serviços e mecanismos em nuvem disponíveis para os clientes que lidam com questões de segurança.

A) Amazon *Detective*

O Amazon *Detective* é um serviço de análise de segurança gerenciado pela AWS que ajuda a investigar, identificar e solucionar problemas de segurança na infraestrutura na nuvem. O serviço coleta dados de *log* de vários serviços da AWS, como Amazon *GuardDuty*, AWS *CloudTrail* e Amazon VPC *Flow Logs*, e os organiza em um painel de controle interativo e intuitivo.

O Amazon *Detective* utiliza algoritmos de aprendizado de máquina para identificar automaticamente comportamentos anômalos e relacionamentos entre diferentes eventos de segurança, ajudando a priorizar a investigação de possíveis ameaças. O serviço também permite que os usuários pesquisem eventos de segurança específicos usando vários filtros e consultas para investigar ameaças específicas ou comportamentos suspeitos.

O Amazon *Detective* também ajuda a simplificar o processo de investigação de incidentes de segurança, fornecendo visualizações de gráficos e painéis que mostram relacionamentos entre diferentes eventos de segurança e recursos da AWS. Além disso, o serviço fornece informações detalhadas sobre atividades de usuários e contas, incluindo atividades de login e mudanças de permissão, ajudando a identificar possíveis brechas de segurança.

B) AWS *Elastic Disaster Recovery*

O AWS *Disaster Recovery* é uma solução gerenciada que ajuda a proteger e recuperar aplicativos e dados em caso de interrupções em ambientes de TI. Ele permite que o usuario crie e gerencie facilmente um plano de recuperação de desastres que pode ser acionado em caso de interrupção em ambientes de produção.

Com o AWS *Disaster Recovery*, o usuario pode replicar dados de aplicativos em tempo real para um ambiente de recuperação em outra região da AWS, permitindo que o usuario ative rapidamente aplicativos de recuperação em caso de falha na região primária. O serviço oferece suporte para vários aplicativos e bancos de dados, incluindo Amazon EC2, Amazon RDS e Amazon EBS, além de outras soluções de parceiros da AWS.

O AWS *Disaster Recovery* é altamente automatizado e oferece recursos de monitoramento e alerta, permitindo que o usuario monitore a saúde de aplicativos e

acione o plano de recuperação de desastres quando necessário. O serviço também é altamente escalável e pode ser personalizado para atender às necessidades específicas de recuperação de desastres da empresa.

4.6 Serviços Conforme a Conformidade

A AWS disponibiliza uma visão completa do status de conformidade, fornecendo monitoramento contínuo do ambiente por meio de verificações automatizadas de conformidade. Essas verificações são baseadas nas práticas recomendadas da AWS e nos padrões do setor adotados pela organização.

Dessa forma, a AWS assegura que o ambiente esteja em conformidade, seguindo rigorosamente os requisitos estabelecidos pelas melhores práticas da indústria e pelos padrões adotados pela organização. Esse monitoramento constante e abrangente garante a integridade das operações e reforça a segurança dos sistemas e dados na infraestrutura da AWS.

A) AWS *Artifact*

O AWS *Artifact* é um serviço que fornece aos usuários acesso fácil e seguro aos documentos de conformidade e segurança da AWS. Ele oferece uma interface centralizada para acesso a documentos de auditoria, como relatórios de conformidade com normas de segurança, acordos de privacidade e termos de serviço.

O AWS *Artifact* é um serviço gratuito que permite aos usuários baixar documentos sob demanda. Alguns documentos exigem uma assinatura prévia ou uma solicitação de aprovação da AWS, o que pode levar alguns dias para ser processado.

O serviço é altamente seguro e está em conformidade com as políticas de segurança da AWS. Está disponível para todos os clientes da AWS e pode ser acessado por meio do console da AWS ou por meio de APIs. O AWS *Artifact* é um recurso importante para os clientes que precisam comprovar a conformidade de sistemas e aplicativos com os requisitos de segurança e privacidade.

B) AWS *Audit Manager*

O AWS *Audit Manager* é um serviço gerenciado da AWS que ajuda as organizações a automatizar e simplificar a avaliação contínua e a conformidade com os padrões de segurança e privacidade.

O serviço permite que os usuários auditem os recursos da AWS em relação a um conjunto de controles pré-definidos, incluindo normas de segurança, regulamentos e práticas recomendadas do setor. O AWS *Audit Manager* inclui uma biblioteca de controles padrão que os usuários podem usar como ponto de partida para as auditorias.

O AWS *Audit Manager* permite que os usuários criem, gerenciem e conduzam auditorias de recursos da AWS, como Amazon EC2, Amazon S3 e AWS IAM, bem como serviços de terceiros integrados com a AWS. O serviço fornece uma interface visual para configurar e executar auditorias, bem como monitorar e gerenciar resultados de auditoria.

O AWS *Audit Manager* inclui recursos de automação para ajudar a acelerar o processo de auditoria, incluindo a geração automática de relatórios de auditoria e a criação de planos de ação para corrigir quaisquer problemas identificados durante a auditoria.

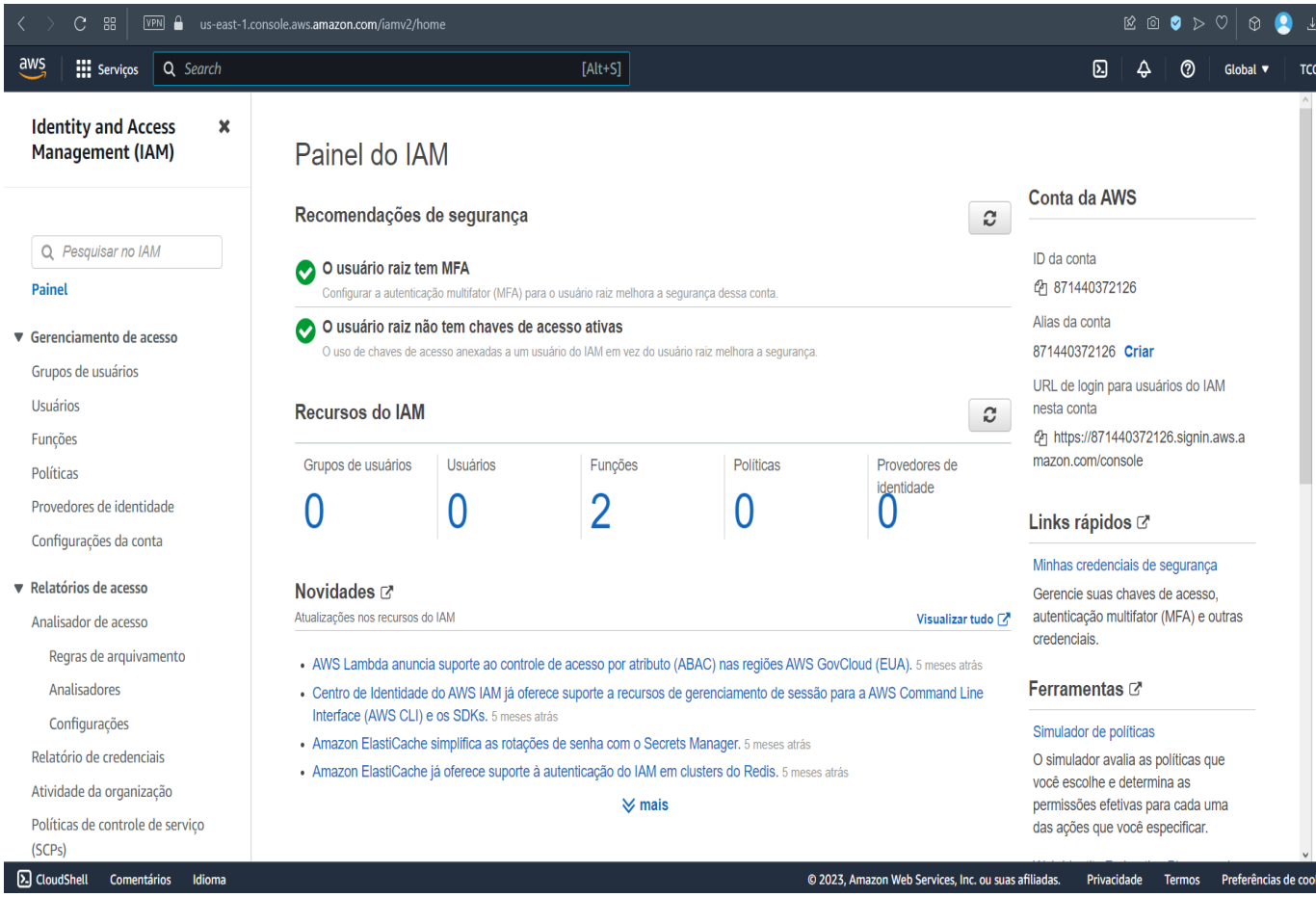
5. IMPLEMENTAÇÃO DO SERVIÇO AWS *IDENTIFY AND ACCESS MANAGEMENT* (IAM)

O objetivo desta implementação é ilustrar o serviço AWS *Identity and Access Management* (IAM), que é o principal serviço de segurança do ambiente AWS.

Ele permite gerenciar o acesso aos recursos da AWS de forma segura. O IAM é um serviço da AWS que permite gerenciar usuários, grupos e funções que podem acessar os recursos da AWS. Ele fornece controle granular sobre quem pode acessar quais recursos, bem como como eles podem acessá-los.

Nesta implementação, serão abordadas as etapas para configurar o IAM. A Figura 5 apresenta o Painel do IAM.

Figura 5 – Painel do IAM

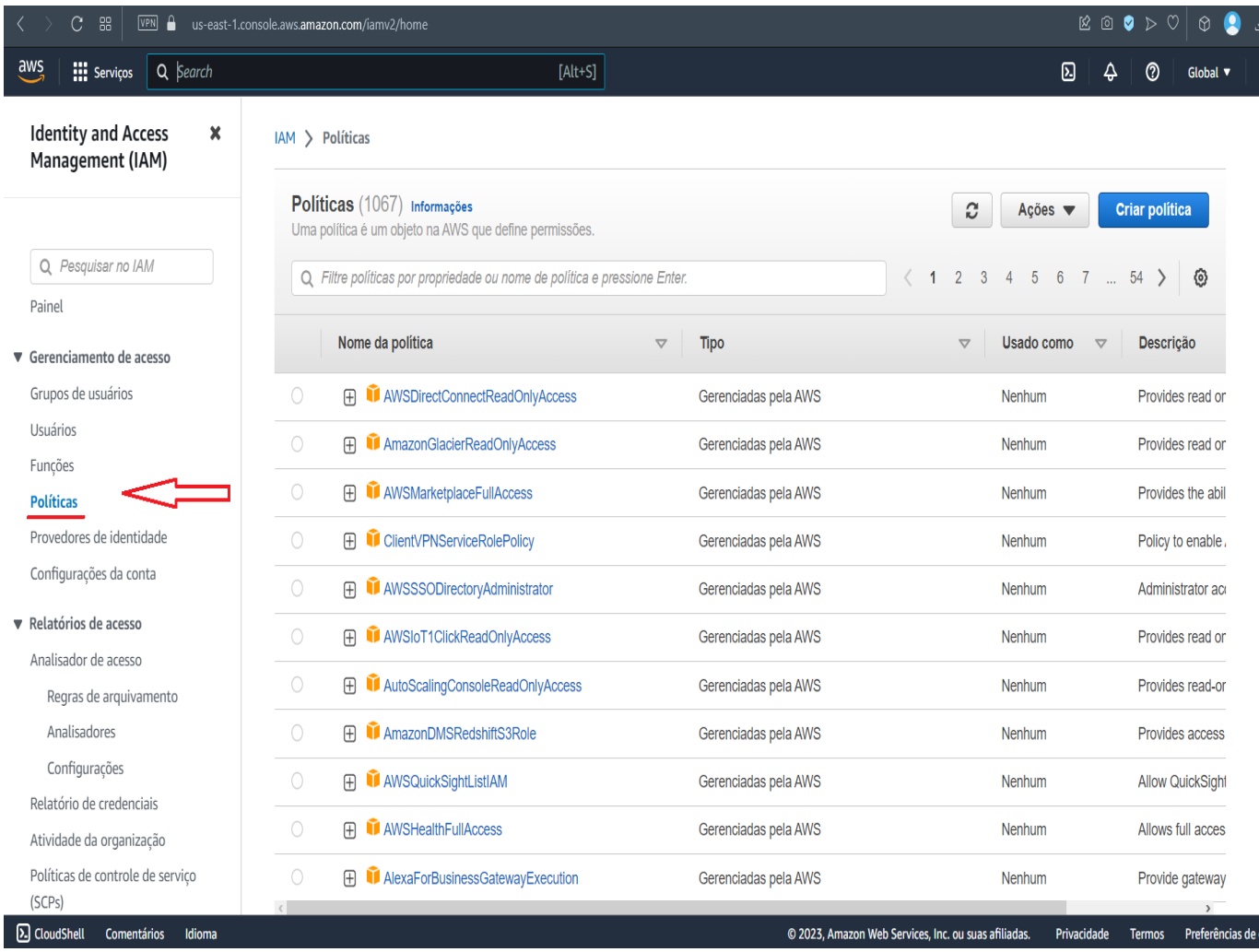


Fonte: AWS, 2023.

O primeiro passo é criar uma política de segurança. As políticas do IAM definem as permissões para acessar os recursos da AWS.

Para criar uma política, é necessário acessar o console do IAM e selecionar "Políticas" no painel esquerdo, mostrada na Figura 6.

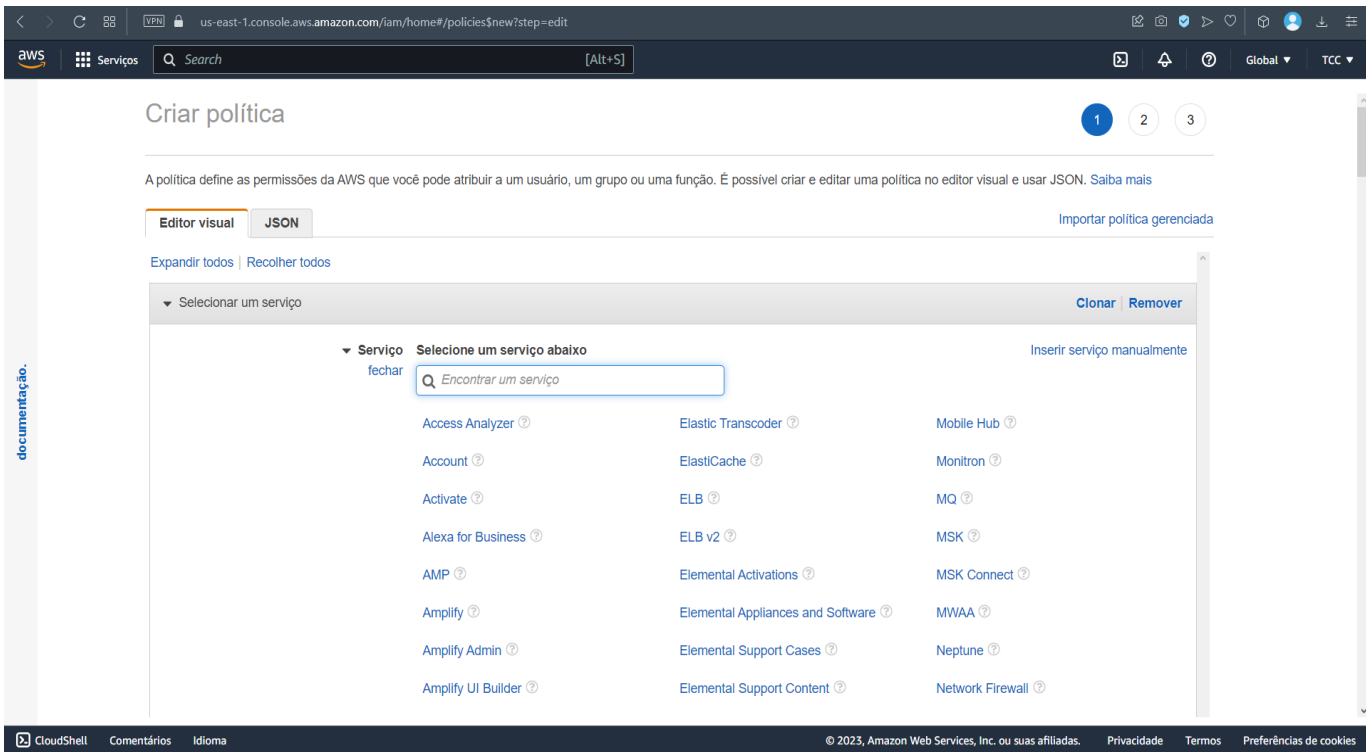
Figura 6: Políticas do serviço IAM



Fonte: AWS, 2023.

Em seguida, clique em "Criar política", mostrada na Figura 7 e selecione o tipo de política que deseja criar, como política do IAM ou política de *bucket* do S3.

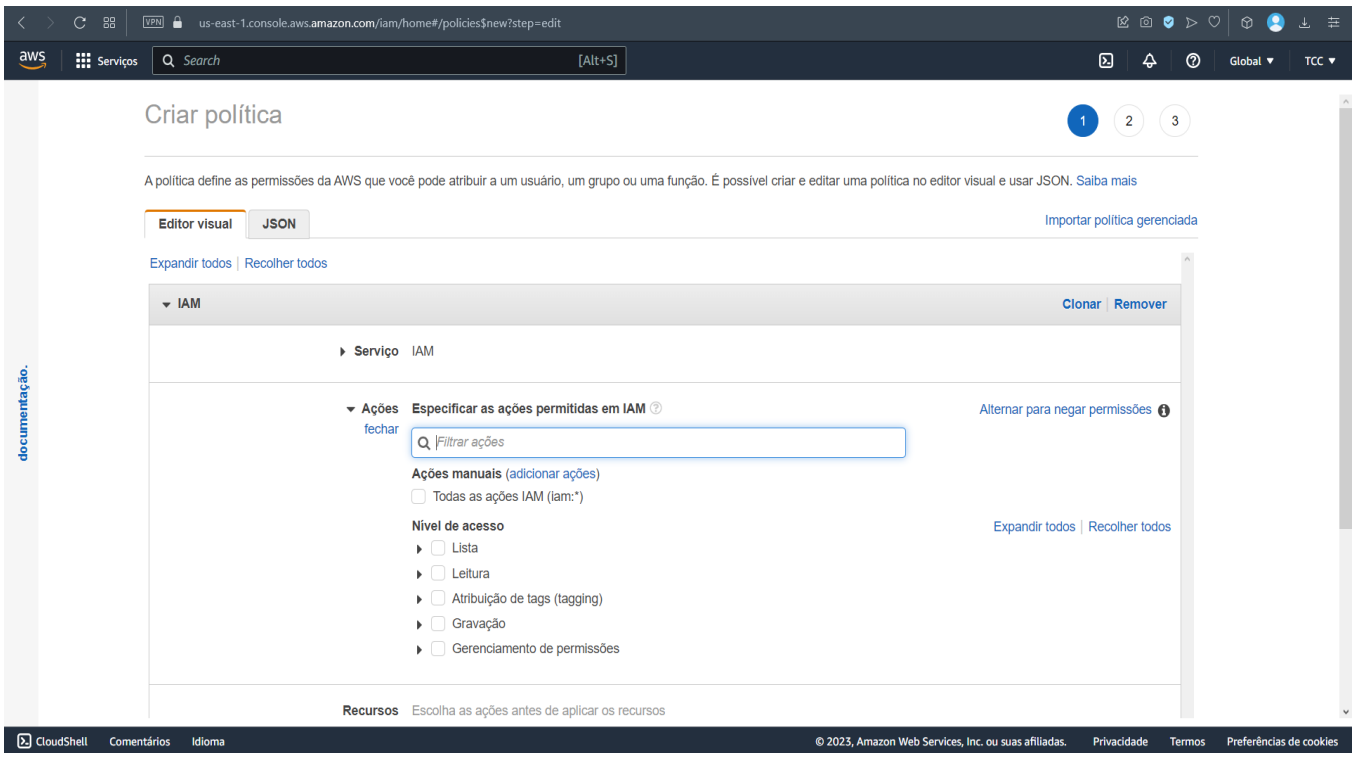
Figura 7: Criar Política



Fonte: AWS, 2023.

Em seguida, é possível selecionar as permissões necessárias para o grupo de usuários, ilustrado na Figura 8.

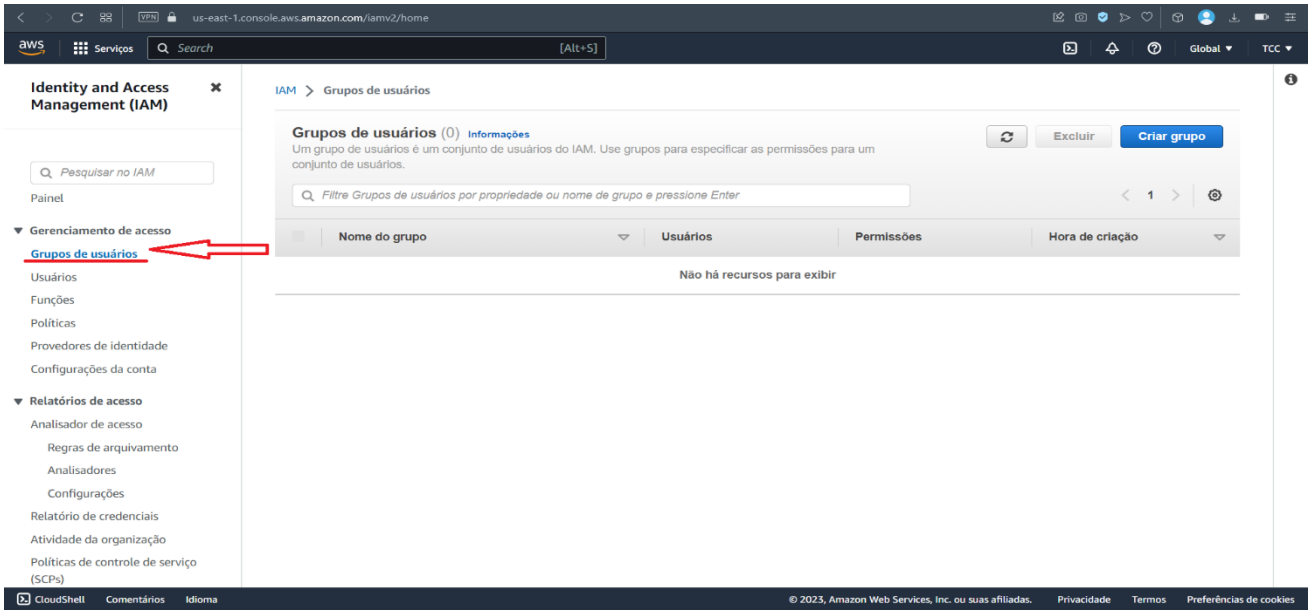
Figura 8: Permissões da Política



Fonte: AWS, 2023.

O próximo passo é criar um grupo de usuários, mostrado na Figura 9. Os grupos do IAM permitem agrupar usuários com permissões semelhantes. Para criar um grupo, é necessário acessar o console do IAM e selecionar "Grupos" no painel esquerdo.

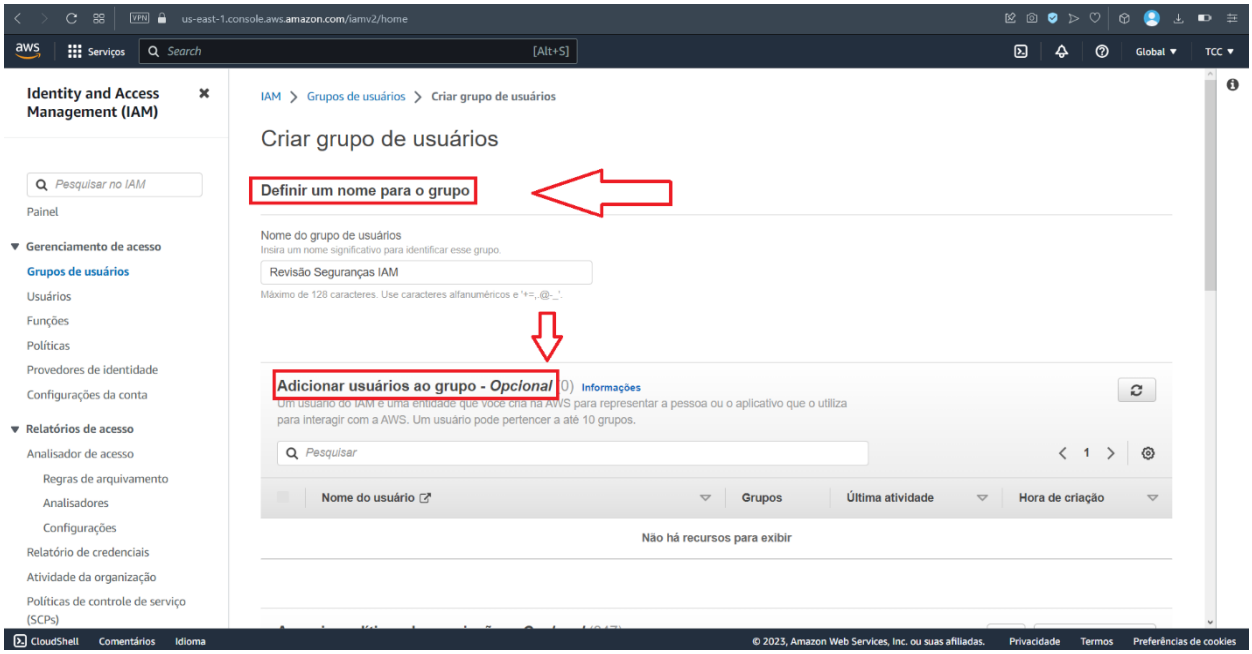
Figura 9: Grupos de Usuários da Política a ser criada



Fonte: AWS, 2023.

Em seguida, clique em "Criar grupo" e atribua um nome ao grupo, conforme mostra a Figura 10. Em seguida, é possível adicionar usuários ao grupo.

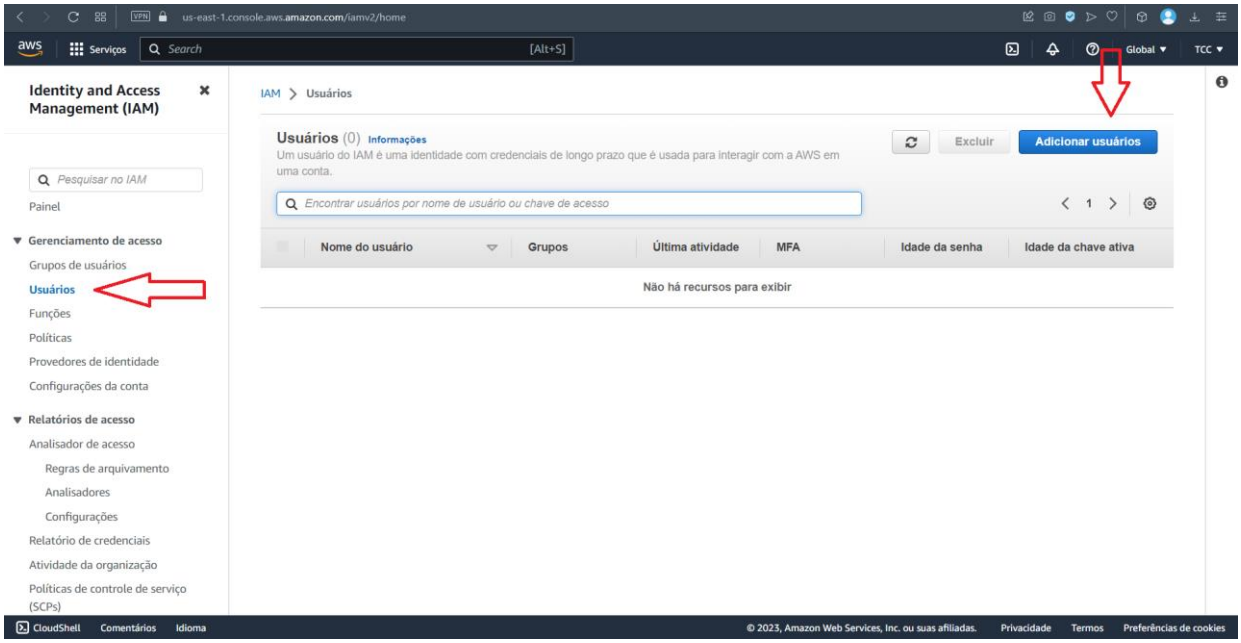
Figura 10: Criação Grupo de Usuários



Fonte: AWS, 2023.

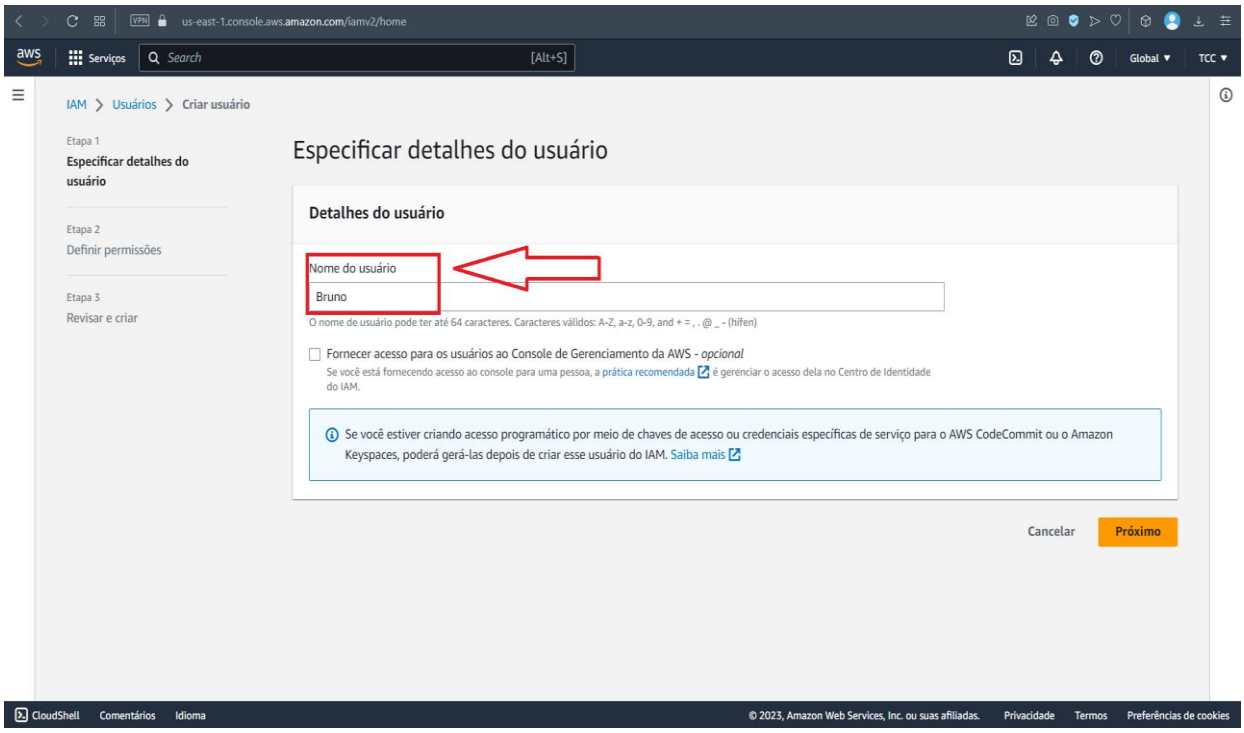
É necessário criar usuários, conforme ilustra as Figuras 11 e 12. Os usuários do IAM são as identidades que podem acessar os recursos da AWS. Para criar um usuário, é necessário acessar o console do IAM e selecionar "Usuários" no painel esquerdo. Em seguida, clique em "Adicionar usuário" e defina um nome de usuário.

Figura 11: Criação Usuários



Fonte: AWS, 2023.

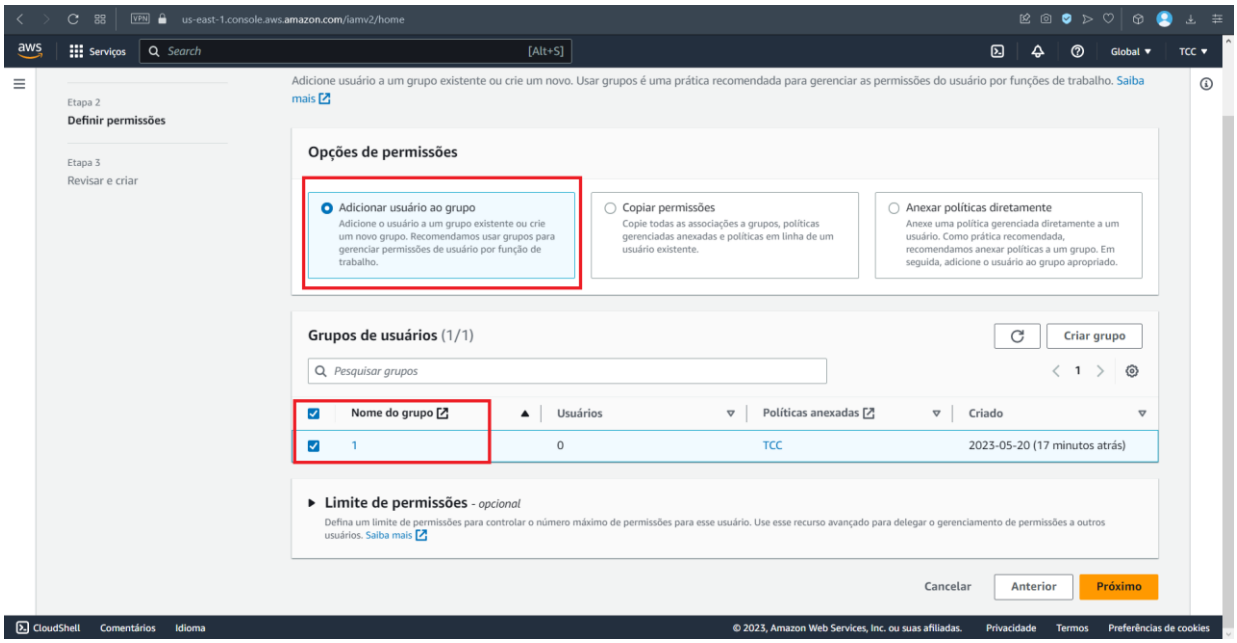
Figura 12: Nome Usuário Criado



Fonte: AWS, 2023.

Em seguida, selecione o tipo de acesso que o usuário terá e, em seguida, atribua o usuário ao grupo criado anteriormente, conforme mostra a Figura 13.

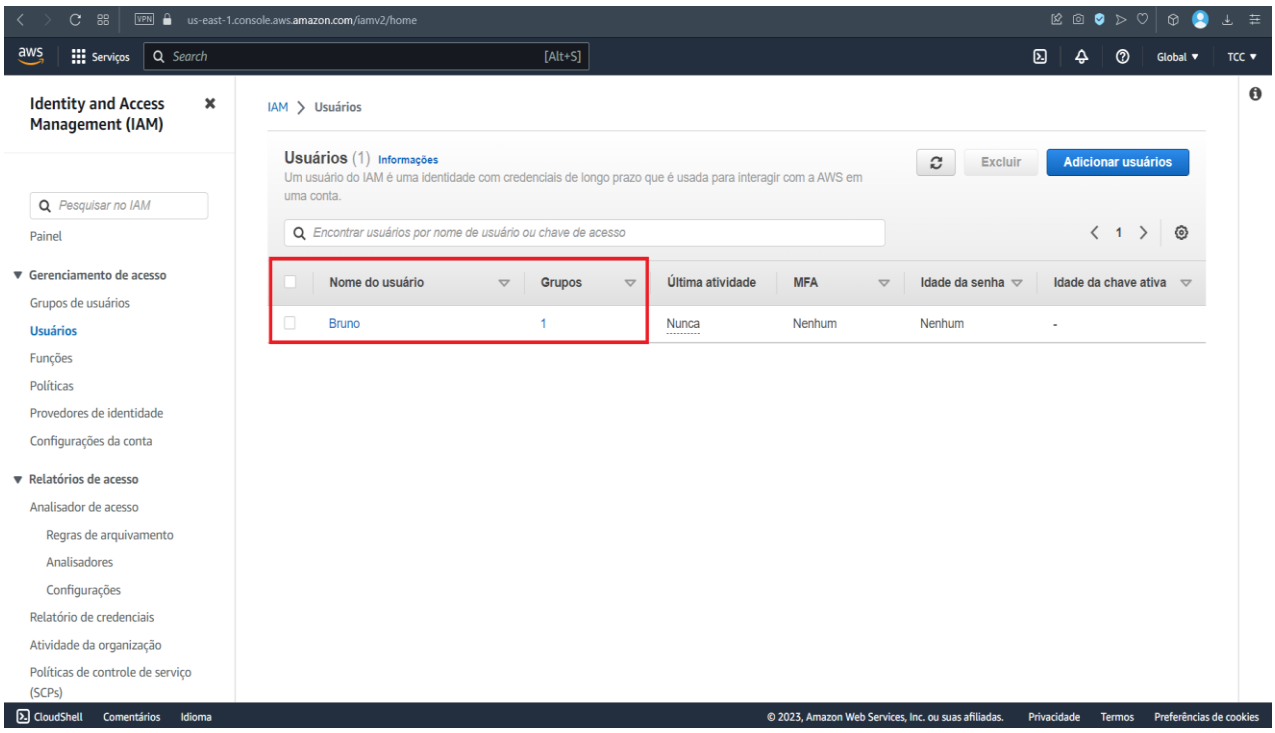
Figura 13: Acesso dos Usuários



Fonte: AWS, 2023.

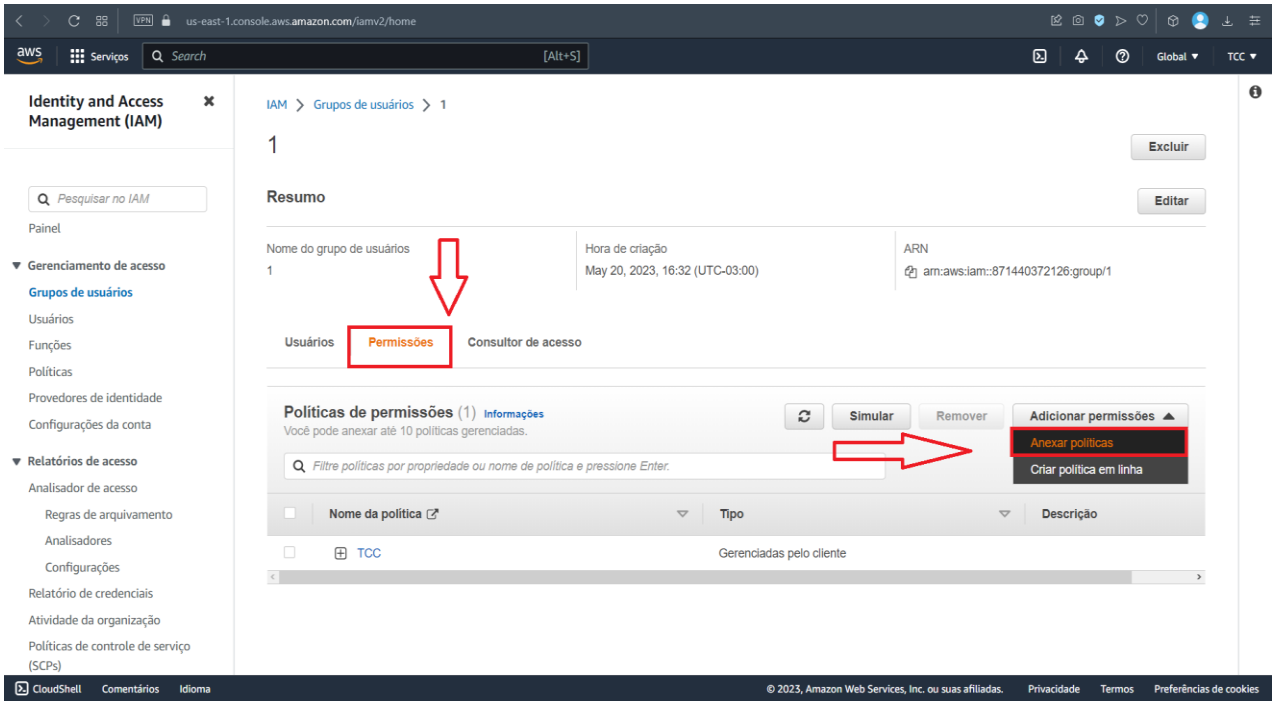
Agora, é possível conceder permissões aos usuários e grupos usando a política criada anteriormente. Para fazer isso, é necessário selecionar o usuário ou grupo desejado e, em seguida, selecionar "Anexar política" na guia "Permissões". Em seguida, selecione a política desejada e salve as alterações, conforme as Figuras 14 até 16.

Figura 14: Usuários do Grupo



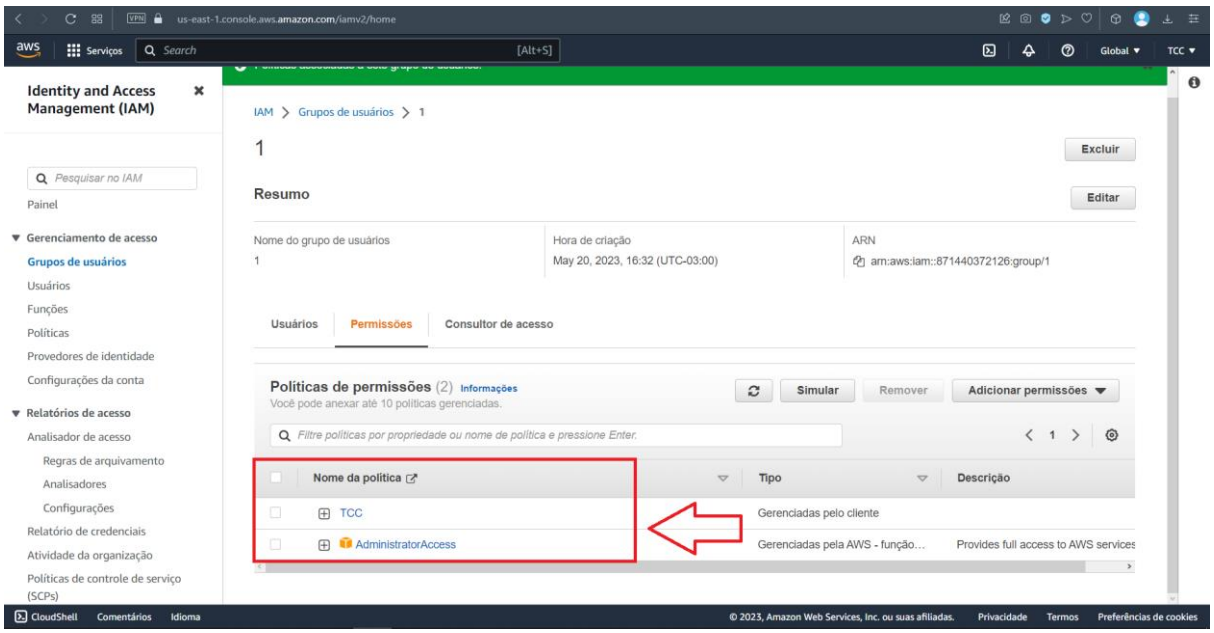
Fonte: AWS, 2023.

Figura 15: Anexando novas Políticas aos Usuários



Fonte: AWS, 2023.

Figura 16: Políticas dos Usuários



Fonte: AWS, 2023.

Com essa implementação do IAM é possível verificar um nível de segurança forte e granular sobre os recursos da AWS, permitindo que os usuários e grupos tenham acesso apenas aos recursos necessários para realizar suas tarefas. Com isso, essa implementação se torna importante para atestar o alto grau de segurança no gerenciamento de usuários e politicas nas contas.

6. CONSIDERAÇÕES FINAIS

Este projeto teve o intuito de responder a seguinte questão de pesquisa: **- Quais são os serviços de segurança oferecidos pela tecnologia de *cloud computing* na Amazon Web Service e suas aplicações?**

A AWS disponibiliza uma ampla variedade de serviços de segurança que abrangem diferentes aspectos da proteção, desde a criptografia de dados até o monitoramento de rede e a detecção de ameaças. Foram identificados 27 serviços oferecidos relacionados à segurança. Esses serviços fornecem as ferramentas necessárias para proteger os ambientes de nuvem, mitigar riscos de segurança e garantir a privacidade e a integridade dos dados.

Os serviços de segurança oferecidos pela plataforma AWS representam uma solução completa e confiável para proteger os ambientes de nuvem e os ativos digitais das organizações. Com o rápido crescimento da computação em nuvem e as ameaças cibernéticas cada vez mais sofisticadas, é crucial contar com recursos e ferramentas robustas para garantir a segurança dos dados e a conformidade com os regulamentos.

A AWS continua investindo significativamente em melhorias de segurança, com verificações automatizadas de conformidade, monitoramento constante e atualizações regulares para lidar com as ameaças em constante evolução. Ao adotar os serviços de segurança da AWS, as organizações podem se beneficiar de uma abordagem em camadas que fortalece sua postura de segurança.

É importante ressaltar que a segurança na nuvem é uma responsabilidade compartilhada entre a AWS e o cliente. Embora a AWS forneça uma infraestrutura segura e ferramentas de segurança, as organizações também devem implementar práticas adequadas, como gerenciamento de acesso, monitoramento proativo e resposta a incidentes, para garantir a proteção efetiva de seus dados e recursos.

O estudo permitiu concluir que:

- os serviços de segurança da AWS oferecem recursos avançados, conformidade com regulamentações e proteção contra ameaças cibernéticas em constante evolução.

- durante a condução dos testes em diversas redes, a plataforma em nuvem permaneceu online durante todo o tempo. Além disso, os recursos de segurança empregados funcionaram como foram configurados.
- Ao utilizar esses serviços em conjunto com boas práticas de segurança, as organizações podem aproveitar todos os benefícios da computação em nuvem, mantendo seus dados seguros e reduzindo os riscos de segurança.

Para continuidade desta pesquisa sugere-se para trabalhos futuros:

- Utilizar serviços de segurança disponíveis dentro do ambiente AWS em situações especificas, tais como: Firewall, acessos, dados, entre outros.
- Implementar outros serviços para verificar a segurança dos mesmos.

REFERÊNCIAS

ALJAWARNEH, S.; AL-SHARAFI, A.; ALDWAIRI, M. ***A Comprehensive Review on Cloud Computing: Overview, Security Issues, and Challenges. Journal of Supercomputing***, v. 75, n. 8, p. 4009-4047, 2019.

Amazon Web Services. (2021). **AWS Security Best Practices**. Disponível em: < https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf >. Acesso em Maio de 2023.

AMAZON. **Navegando na conformidade com a LGPD na AWS**. Amazon Web Services, Brasil: Março de 2020.

AMAZON. Site. **AWS Identity and Access Management (IAM)**. Disponivel em: < https://aws.amazon.com/iam/ >. Acesso em Março de 2023.

AMAZON. Site. **O que é uma nuvem privada?** Disponivel em: < https://aws.amazon.com/pt/what-is/private-cloud/ >. Acesso em Junho de 2023.

AMAZON. Site. **AWS CloudTrail**. Disponivel em: < https://aws.amazon.com/cloudtrail/ >. Acesso em Março de 2023.

AMAZON. Site. **Amazon GuardDuty**. Disponível em: < https://aws.amazon.com/guardduty/ >. Acesso em Março de 2023.

AMAZON. Site. Disponível em: < https://aws.amazon.com/pt/ >. Acesso em Maio de 2023.

ALQARNI, H. et al. ***Elasticity of Cloud Computing: A Survey. Computers, Materials & Continua***, v. 65, n. 2, p. 919-936, 2020.

ALSHAMRANI, A. et al. ***Security in Cloud Computing: Opportunities and Challenges. In: Proceedings of the 11th International Conference on Security of Information and Networks***. p. 83-89, 2019.

ALVES, T. A. et al. ***LGPD and Its Implications for Brazilian Public Organizations: Insights from an Exploratory Study. In: IEEE International Conference on Software Quality, Reliability and Security Companion*** (QRS-C). p. 135-142, 2022.

BARROS, L. C.; SANTIN, A. L. ***A GDPR/LGPD Analysis on the Use of the Personal Data in Mobile Apps: A Comparative Study. In: International Conference on Information Systems and Software Technologies*** (ICI2ST). p. 1-11, 2020.

BARROSO, Luiz André, HOLZLE, Urs, RANGANATHAN, Parthasarathy. **Datacenter As A Computer Designing Warehouse-Scale Machines.** Third Edition, Morgan & Claypool, 2019.

BROWN, A. ***Security Challenges in Cloud Computing. International Journal of Computer Science and Information Security***, v. 15, n. 12, p. 123-130, 2017.

CHOUDHARY, S. K.; SAHU, G. P.; PRADHAN, A. ***Security Challenges and Techniques in Cloud Computing. In: International Conference on Advanced Computing, Networking and Informatics***. p. 455-466, 2020.

CIEE. **Portal Centro de Integração Empresa-Escola** – CIEE. Disponível em: < https://portal.ciee.org.br/lgpd/ >. Acesso em Maio de 2023

COSTA, A. et al. ***An Analysis of Privacy Policies under GDPR and LGPD. In: European Symposium on Research in Computer Security***. p. 217-234, 2020.

DOE, J. et al. ***Cloud Computing: An Overview. Journal of Information Technology***, v. 21, n. 3, p. 45-58, 2019.

GIL, Antônio Carlos. **Como Elaborar Projetos de Pesquisa**. 6. ed. São Paulo: Editora Atlas Ltda., 2017.

GOMES, M. M. et al. ***A Study on Privacy by Design in the Context of the Brazilian General Data Protection Law (LGPD). In: International Conference on Human-Computer Interaction*** (INTERACT). p. 548-557, 2021.

IVAN. ***Dedicated IT vs. Private Cloud vs. Public Cloud, The Cloud Infographic*****.** Disponível em: <http://www.thecloudinfographic.com/2012/01/04/dedicated-it-vsprivate-cloud-vs-public-cloud.html > Acesso em Junho de 2023.

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.

KHAN, Z. et al. ***Cloud Computing Security: Concepts, Challenges, and Key Management Issues. Journal of Cloud Computing***, v. 10, n. 1, p. 20, 2021.

LOPES, L. M.; SIQUEIRA, F. S.; GONÇALVES, R. M. S. ***An Overview of Availability in Cloud Computing. In: IEEE Latin American Symposium on Dependable Computing***. p. 1-6, 2021.

MOHSIN, A.; AB HAMID, S. H.; IBRAHIM, R. ***Cloud Computing Security Issues and Challenges: A Survey. Journal of Network and Computer Applications***, v. 149, p. 102450, 2020.

RABKIN, A. et al. ***Exploring the Practicality of Collaborative Cloud Computing. IEEE Transactions on Cloud Computing***, v. 6, n. 2, p. 486-498, 2018.

RISTENPART, T., TROMER, E., SHACHAM, H., and SAVAGE, S. ***Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In Proceedings of the 16th ACM conference on Computer and communications security***, CCS (2009).

SAMPAIO, P. H. C. et al. ***Cloud Computing Adoption in SMEs: A Systematic Review of Empirical Literature. Journal of Information Systems Engineering & Management***, v. 4, n. 3, p. 183-194, 2019.

SHARMA, A.; KUMAR, S.; TYAGI, S. ***Cloud Computing Security: A Systematic Review. In: 5th International Conference on Computing, Communication and Security*** (ICCCS). p. 1-7, 2020.

SHARMA, P.; RANI, N.; SINGH, D. S. ***AWS Services: An Overview, Features, and Challenges. In: 5th International Conference on Computing, Communication and Security*** (ICCCS). p. 1-7, 2021.

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.

VERAS, Manoel. **Computação em Nuvem**: Nova Arquitetura de TI. Rio de Janeiro: Brasport, 2015.

VIANNA, R. P. et al. ***Privacy Impact Assessments and Data Protection Impact Assessments: An Analysis of GDPR and LGPD Requirements. In: International Conference on Information Security and Privacy*** (ISP). p. 67-83, 2021.

WAZLAWICK, R. S. **Metodologia da Pesquisa para Ciência da Computação**. 2ª. ed. [S.l.]: Campus, 2014.

ZENG, H. et al. ***Ensuring Data Security and Privacy in Cloud Computing: Strategies and Challenges. Information Systems Frontiers***, v. 22, n. 4, p. 821-835, 2020.