Universidade Federal de Juiz de Fora
Instituto de Ciências Exatas
Bacharelado em Ciência da Computação

Zero-Trust e Controle de Acesso Dinâmico Aplicados na Segurança de Arquivos

Lucca Oliveira Schröder

JUIZ DE FORA
MARÇO, 2025

Zero-Trust e Controle de Acesso Dinâmico Aplicados na Segurança de Arquivos

Lucca Oliveira Schröder

Universidade Federal de Juiz de Fora

Instituto de Ciências Exatas

Departamento de Ciência da Computação

Bacharelado em Ciência da Computação

Orientador: Edelberto Franco Silva

JUIZ DE FORA

MARÇO, 2025

Zero-Trust e Controle de Acesso Dinâmico Aplicados na Segurança de Arquivos

Lucca Oliveira Schröder

MONOGRAFIA SUBMETIDA AO CORPO DOCENTE DO INSTITUTO DE CIÊNCIAS EXATAS DA UNIVERSIDADE FEDERAL DE JUIZ DE FORA, COMO PARTE INTEGRANTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE BACHAREL EM CIÊNCIA DA COMPUTAÇÃO.

Aprovada por:

Edelberto Franco Silva
Doutor em Computação

Alex Borges Vieira
Doutor em Ciência da Computação

André Luiz de Oliveira
Doutor em Ciência da Computação

JUIZ DE FORA
12 DE MARÇO, 2025

Resumo

Com o avanço da tecnologia e o aumento das ameaças cibernéticas, a segurança da informação tornou-se um dos maiores desafios para empresas e indivíduos. A proteção de dados sensíveis exige estratégias robustas de controle de acesso, capazes de garantir que apenas usuários devidamente autorizados possam visualizar ou modificar informações. Nesse contexto, o modelo de segurança *Zero Trust* surge como uma abordagem inovadora, eliminando a confiança implícita e exigindo verificações contínuas para garantir acessos legítimos. Este trabalho explora a aplicação do *Zero Trust* no controle de acesso a arquivos, combinando dois modelos fundamentais: RBAC (*Role-Based Access Control*) e ABAC (*Attribute-Based Access Control*). O RBAC estrutura permissões com base nas funções dos usuários dentro da organização, enquanto o ABAC utiliza atributos como localização e comportamento para definir dinâmicas de acesso mais flexíveis e seguras. Por meio de simulações, este estudo avalia a eficácia dessa abordagem combinada, demonstrando como a verificação contínua da confiança do usuário pode fortalecer a segurança do sistema.

Palavras-chave: *Zero Trust*, controle de acesso, segurança de rede.

Abstract

With the advancement of technology and the increase in cyber threats, information security has become one of the greatest challenges for companies and individuals. Protecting sensitive data requires robust access control strategies capable of ensuring that only duly authorized users can view or modify information. In this context, the Zero Trust security model emerges as an innovative approach, eliminating implicit trust and requiring continuous verifications to ensure legitimate access. This paper explores the application of Zero Trust in file access control, combining two fundamental models: RBAC (Role-Based Access Control) and ABAC (Attribute-Based Access Control). RBAC structures permissions based on user roles within the organization, while ABAC uses attributes such as user behavior and history to define more flexible and secure access dynamics. Through simulations, this study evaluates the effectiveness of this combined approach, demonstrating how continuous verification of user trust can strengthen system security.

Keywords: Zero Trust, access control, network security.

Agradecimentos

À minha família, que sempre foi meu maior exemplo, estando ao meu lado em cada etapa desta jornada, com amor, apoio e incentivo incondicionais.

Aos meus amigos, que compartilharam comigo desafios e conquistas, e estiveram ao meu lado ao longo de todo esse processo.

À minha namorada, cujo carinho, amor e apoio incondicional tornaram esta caminhada muito mais leve, sempre me inspirando a ser uma pessoa melhor.

Ao professor Edelberto, por sua orientação, paciência e disposição em compartilhar conhecimento, elementos fundamentais para a realização deste trabalho.

Aos funcionários da UFJF, que, de diversas formas, contribuíram para minha trajetória acadêmica, tornando possível a concretização deste momento.

"Deus nos concede, a cada dia, uma página de vida nova no livro do tempo. Aquilo que colocarmos nela, corre por nossa conta."

Chico Xavier

Conteúdo

Lista de Figuras **7**

Lista de Tabelas **8**

Lista de Abreviações **9**

1 Introdução **10**
1.1 Apresentação do Tema . . . 10
1.2 Contextualização . . . 11
1.3 Descrição do Problema . . . 12
1.4 Justificativa . . . 12
1.5 Objetivos . . . 13
1.5.1 Objetivo Geral . . . 13
1.5.2 Objetivos Específicos . . . 13
1.6 Metodologia . . . 14

2 Fundamentação Teórica **15**
2.1 Introdução . . . 15
2.2 *Zero Trust* . . . 15
2.3 Arquitetura *Zero Trust* . . . 16
2.4 Controle de Acesso . . . 17
2.4.1 Controle de Acesso Baseado em Risco (RbAC) . . . 18
2.4.2 Controle de Acesso Baseado em Papéis (RBAC) . . . 20
2.4.3 Controle de Acesso Baseado em Atributos (ABAC) . . . 21
2.4.4 A combinação do ABAC e do RBAC . . . 23

3 Trabalhos Relacionados **25**
3.1 Introdução . . . 25
3.2 Modelos gerais de controle de acesso . . . 25
3.3 A utilização da Arquitetura *Zero Trust* em ambientes gerais . . . 26
3.4 A integração do modelo *Zero Trust* aos mecanismos de controle de acesso . 29
3.5 Considerações finais . . . 30

4 Material e métodos **31**
4.1 Ambiente simulado . . . 31
4.2 Acesso e confiança baseada em atributos . . . 32
4.3 Acesso e confiança baseada em papéis . . . 33
4.4 Tabela de permissões e recursos . . . 35

5 Cenários e Resultados **39**
5.1 Caso 1: Acesso normal . . . 39
5.2 Caso 2: Acesso - Administrador . . . 41
5.2.1 Caso 2.1: Acesso normal - Administrador . . . 41
5.2.2 Caso 2.2: Roubo de acesso - Administrador . . . 42
5.3 Caso 3: Tentativa de acessar recursos sensíveis . . . 42

5.4 Caso 4: Inatividade no sistema 44
5.5 Caso 5: Mudança repentina de localização 44

6 Conclusão e Trabalhos Futuros **46**

Bibliografia **47**

Lista de Figuras

2.1 Componentes da Arquitetura *Zero Trust* (TEERAKANOK; UEHARA; INOMATA, 2021) 18
2.2 Fluxo de uma operação de controle de acesso (ATLAM et al., 2020) 19
2.3 Controle de acesso baseado em atributos e funções (COYNE; WEIL, 2013) 24

4.1 Tabela de Permissões 36

5.1 Sensibilidade dos recursos acessados 40
5.2 Acesso normal - Estagiário 40
5.3 Acesso normal - Analista 41
5.4 Acesso normal - Administrador 42
5.5 Roubo de acesso - Administrador 43
5.6 Acesso indevido - Estagiário 43
5.7 Inatividade - Analista 44
5.8 Mudança repentina de localização 45

Lista de Tabelas

4.1 Tabela de confiança de acordo com funções/papéis. 34
4.2 Recurso: Material de treinamento e desenvolvimento 36
4.3 Recurso: Diretório de Projetos 37
4.4 Recurso: Documentos Operacionais 37
4.5 Recurso: Gerenciamento de Estagiários 38
4.6 Recurso: Dados Sensíveis da Empresa 38

Lista de Abreviações

ABAC	*Attribute-Based Access Control*
ADF	*Access Decision Function*
CH	*Context Handler*
IoT	*Internet of Things*
NIST	*National Institute of Standards and Technology*
OSN	*Online Social Networks*
PDP	*Policy Decision*
PE	*Policy Engine*
PEP	*Policy Enforcement Point*
RBAC	*Role-Based Access Control*
RbAC	*Risk-Based Access Control*
REF	*Risk Evaluation Function*
TBAC	*Trust-Based Access Control*
TBPF	*Trust Based Packet Filtering*
TRIS	*Transparency for better Internet Security*
ZT	*Zero Trust*
ZTA	*Zero Trust Architecture*
ZTN	*Zero Trust Networking*

1 Introdução

1.1 Apresentação do Tema

Com o avanço da tecnologia nos últimos anos, a segurança da informação tornou-se uma questão essencial para empresas e indivíduos. Proteger arquivos sensíveis e dados confidenciais exige a adoção de mecanismos eficazes de controle de acesso, garantindo que apenas pessoas autorizadas possam visualizar ou modificar essas informações, de acordo com seus níveis de permissão.

Dentro desse cenário, o modelo de segurança *Zero Trust* vem ganhando destaque como uma estratégia eficiente para controlar o acesso a arquivos. Diferentemente das abordagens tradicionais, que pressupõem confiança nos usuários e dispositivos internos, o *Zero Trust* parte do princípio de que nenhum acesso deve ser concedido automaticamente. Para isso, é necessário verificar constantemente a identidade e o comportamento dos usuários antes de permitir o acesso a informações sensíveis (BANSAL, 2024).

Duas abordagens fundamentais para controle de acesso que podem ser utilizadas dentro do modelo *Zero Trust* são o RBAC (*Role-Based Access Control*) e o ABAC (*Attribute-Based Access Control*). O RBAC é projetado para administrar a segurança em um nível organizacional, em vez de individual. As permissões de acesso a recursos são concedidas com base na função desempenhada pelo usuário dentro da organização (SAMARATI; VIMERCATI, 2021). Como essas funções são específicas de cada organização e agregam diferentes níveis de permissão, o RBAC oferece uma maneira escalável e eficiente de definir o controle de acesso. Por outro lado, o ABAC adota uma abordagem mais dinâmica, concedendo acesso a recursos com base em uma combinação de atributos do usuário, do recurso e do contexto da solicitação. O ABAC permite um controle mais refinado do que o RBAC, sendo aplicável a um conjunto mais amplo de cenários e requisitos de segurança. (XIAO et al., 2022)

Diante da complexidade dos sistemas de informação e do aumento das ameaças cibernéticas, a implementação do modelo *Zero Trust* para controle de acesso a arquivos

tornou-se uma estratégia essencial para a proteção de dados críticos. Nesse contexto, este trabalho tem como objetivo apresentar uma abordagem combinada e simular a implementação da arquitetura Zero Trust, integrada aos modelos de controle de acesso RBAC e ABAC, em um sistema de gerenciamento de arquivos. Essa combinação visa fortalecer a segurança, minimizar os riscos de acessos indevidos e garantir uma gestão mais segura e eficiente das informações.

1.2 Contextualização

O avanço da tecnologia tem se tornado cada vez mais essencial em diversos setores, proporcionando soluções mais eficazes e ágeis. No entanto, com o aumento do uso de sistemas digitais e da interconectividade entre dispositivos, cresce também a preocupação com a segurança da informação, especialmente no que diz respeito ao controle de acesso a dados e arquivos sensíveis.

Os ataques cibernéticos estão se tornando cada vez mais frequentes e sofisticados, explorando falhas em sistemas para obter acesso a informações sigilosas. Essa constante disputa entre profissionais de segurança e invasores cria um cenário desafiador, onde novas ameaças surgem a todo momento. Além das brechas tecnológicas, muitas dessas investidas exploram a engenharia social, manipulando pessoas para obter acesso indevido a sistemas e dados sensíveis, tornando o cenário ainda mais desafiador. Apesar dos avanços constantes em tecnologias de detecção de ameaças e medidas de segurança, as ameaças cibernéticas continuam a evoluir em complexidade, escala e sofisticação (TSAI; LEE; SHIEH, 2024).

Diante desse cenário, o modelo de segurança *Zero Trust* tem se destacado como uma solução eficaz para proteger arquivos e dados sensíveis. Diferente dos modelos tradicionais, que muitas vezes assumem a confiabilidade de usuários e dispositivos dentro da rede, o *Zero Trust* parte do princípio de que nenhuma entidade deve ser considerada confiável por padrão. Isso significa que cada tentativa de acesso é rigorosamente verificada, garantindo maior segurança e minimizando riscos (DUMITRU, 2022). Quando combinado com mecanismos de controle de acesso como RBAC e ABAC, esse modelo se torna ainda mais eficiente, ajudando a reduzir vulnerabilidades e fortalecer a proteção das informações.

1.3 Descrição do Problema

Embora o modelo de segurança baseado em Zero Trust seja altamente eficaz para proteger sistemas contra ameaças cibernéticas, sua implementação no controle de acesso a arquivos apresenta grandes desafios. Isso ocorre porque muitos sistemas tradicionais ainda confiam excessivamente em autenticação inicial e não realizam verificações contínuas, o que pode resultar em acessos indevidos e exposição de dados sensíveis.

Com o crescimento do número de usuários em sistemas de informação, o desafio de controlar quem pode acessar determinados recursos também aumentou. Para lidar com isso, pesquisadores e desenvolvedores buscaram formas de tornar a administração mais simples e eficiente. Uma das soluções encontradas foi a criação de grupos de usuários com as mesmas permissões de acesso, o que acabou servindo como base para o desenvolvimento do modelo de controle de acesso baseado em papéis (COYNE; WEIL, 2013).

Um dos principais problemas enfrentados é que, caso um invasor obtenha credenciais válidas de um usuário interno, ele pode explorar esse acesso para comprometer informações críticas, uma vez que os sistemas convencionais costumam conceder permissões amplas após a autenticação inicial. Esse risco é agravado pela falta de mecanismos dinâmicos que avaliem continuamente o comportamento do usuário e a confiabilidade de seu acesso ao longo do tempo.

Portanto, confiar apenas na autenticação inicial do usuário não é suficiente para garantir a segurança das informações. É essencial adotar um modelo de verificação contínua, para reforçar a segurança do sistema e reduzir os riscos de acessos indevidos.

1.4 Justificativa

Com a crescente dependência da tecnologia para o armazenamento e gerenciamento de informações, garantir a segurança dos dados se tornou uma prioridade essencial para organizações de todos os setores. Este trabalho se justifica pela necessidade de implementar mecanismos robustos de controle de acesso a arquivos, minimizando riscos de acessos indevidos e violações de segurança.

A abordagem baseada no modelo *Zero Trust*, aliada aos controles de acesso RBAC

e ABAC, oferece um meio eficaz para fortalecer a segurança da informação, eliminando a confiança implícita em usuários, dispositivos e sistemas. Ao adotar essa estratégia, as empresas passam a ter um controle mais granular e dinâmico sobre quem pode acessar determinados arquivos, reduzindo os riscos de ataques internos e externos.

Com a aplicação e testes deste modelo, espera-se demonstrar a eficácia da combinação entre *Zero Trust*, RBAC e ABAC na proteção de informações sensíveis, garantindo um ambiente seguro e confiável para a gestão de arquivos dentro das organizações.

1.5 Objetivos

1.5.1 Objetivo Geral

O objetivo geral deste trabalho é avaliar a efetividade da abordagem de segurança baseada em *Zero Trust* no controle de acesso a arquivos e dados sensíveis, com ênfase na prevenção de ataques cibernéticos e no fortalecimento das políticas de controle de acesso. Este estudo busca demonstrar como o modelo de segurança *Zero Trust* pode ser implementado em ambientes que exigem uma maior proteção de seus dados, destacando sua capacidade de reduzir riscos e garantir a segurança das informações.

Além disso, foi realizado um estudo de caso sobre a aplicação do modelo *Zero Trust* aliado a sistemas de controle de acesso, utilizando um ambiente simulado, com o intuito de comprovar a eficácia dessa abordagem.

1.5.2 Objetivos Específicos

Os objetivos específicos são listados a seguir:

- Estudar e avaliar sobre a arquitetura e a implementação do modelo *Zero Trust*;
- Investigar os diferentes modelos de controle de acesso, analisando suas características e adequação em ambientes de segurança;
- Comparar a eficácia dos diferentes modelos de controle de acesso, como RBAC e ABAC, focando em sua performance na prevenção de acessos não autorizados;

- Propor e implementar uma simulação da abordagem de segurança *Zero Trust* utilizando os modelos RBAC e ABAC como mecanismos de controle de acessos;

- Comparar os resultados obtidos e avaliar a eficácia da abordagem proposta, considerando sua capacidade de atender aos requisitos de segurança.

1.6 Metodologia

Para a elaboração deste trabalho, foi adotada uma metodologia focada na aplicação do modelo de segurança *Zero Trust*, no controle de acesso a arquivos, com foco nas abordagens de RBAC (*Role-Based Access Control*) e ABAC (*Attribute-Based Access Control*). A metodologia envolverá uma série de etapas que incluem o estudo do modelo utilizado, a simulação de cenários de segurança e a análise dos resultados obtidos, avaliando a eficácia dessa combinação de métodos para garantir a segurança e integridade dos dados em ambientes corporativos e sistemas de informação.

Primeiramente, será realizado um estudo aprofundado sobre o modelo *Zero Trust*, incluindo seus princípios e como ele pode ser aplicado no controle de acesso a arquivos. Além disso, serão analisados os modelos de controle de acesso, para entender suas vantagens e limitações em relação à proteção de dados.

Em seguida, foi montado um ambiente simulado para testar a implementação do *Zero Trust* em conjunto com os modelos RBAC e ABAC. Esse ambiente de testes permitirá verificar como o *Zero Trust* pode ser utilizado para gerenciar e controlar o acesso a arquivos de forma contínua e adaptativa, avaliando a eficácia dessa abordagem.

Por fim, foram realizados os testes e analisados os resultados, com o objetivo de discutir a viabilidade, as vantagens e as limitações do modelo *Zero Trust* no controle de acesso a arquivos.

2 Fundamentação Teórica

2.1 Introdução

Neste capítulo, serão apresentados todos os fundamentos necessários para o entendimento deste trabalho. São abordadas todas as definições de *Zero Trust* na Seção 2.2, aprofundando mais nos seus conceitos e na Seção 2.3 é detalhado sobre a sua arquitetura, sendo citado os seus componentes e funcionamento.

A Seção 2.4 abordará o tema do controle de acesso, destacando sua importância na segurança de dados sensíveis e a maneira como ele pode ser implementado em sistemas modernos. A partir disso, a Seção 2.4.1 explorará o Risk-based Access Control (RBAC), explicando seu funcionamento e como ele avalia os riscos antes de conceder ou negar o acesso. Na Seção 2.4.2, será abordado o Role-based Access Control (RBAC), com foco na atribuição de permissões com base nas funções de usuários dentro de uma organização. Já a Seção 2.4.3 discutirá o Attribute-based Access Control (ABAC), detalhando como ele utiliza atributos específicos de usuários, recursos e ambiente para definir permissões de acesso. E, por fim, na Seção 2.4.4, será abordada a combinação do ABAC e do RBAC.

2.2 *Zero Trust*

Segundo o NIST (ROSE et al., 2020), o modelo de confiança zero tem os seguintes pilares:

1. Todas as fontes de dados e serviços são recursos;
2. Toda comunicação é segura, independentemente da sua localização na rede;
3. O acesso aos recursos é dado por sessão (p. ex., por tarefa e não permanente para um componente);
4. O acesso aos recursos é determinado por uma política dinâmica;
5. A organização monitora a integridade e postura de segurança de seus ativos;

6. A autenticação e a autorização são constantes;

7. A organização coleta o máximo possível de informações sobre os ativos, rede e comunicações para melhorar a postura de segurança.

Zero Trust é uma abordagem de segurança cibernética que tem ganhado muita popularidade nos últimos anos. À medida que as ameaças cibernéticas continuam evoluindo, as organizações estão adotando cada vez mais marcos de segurança avançados, para proteger seus ativos digitais. *Zero Trust* opera sob o princípio de "nunca confiar, sempre verificar", reconhecendo que tanto as redes internas quanto as externas podem estar comprometidas (FILHO, 2025).

A ideia é de que todos os recursos e dados devem ser protegidos independentemente do local onde estão armazenados ou acessados. Isso significa que o controle de acesso deve ser aplicado de forma granular, avaliando constantemente o contexto de cada solicitação de acesso e autorizando apenas as que são legítimas.

O modelo *Zero Trust* é uma abordagem proativa e preventiva para a segurança da rede que fornece um nível mais alto de controle e visibilidade em um mundo cada vez mais conectado e digital (JIMMY, 2022). Uma ZTA (Arquitetura de Confiança Zero - *Zero Trust Architecture*) é uma arquitetura de segurança cibernética corporativa baseada em princípios de confiança zero e projetada para evitar violações de dados e restringir a propagação não autorizada dentro da rede (ROSE et al., 2020). Uma das principais vantagens da sua implementação é a capacidade de detectar e responder rapidamente a ameaças de segurança em tempo real. Na seção 2.3 é abordado mais a fundo sobre a ZTA.

2.3 Arquitetura *Zero Trust*

A Arquitetura Zero Trust é uma abordagem que considera implicitamente todos os usuários e dispositivos como não confiáveis, independentemente de sua localização (interna ou externa). Isso é diferente da abordagem de segurança de perímetro, que assume que os usuários e dispositivos internos são confiáveis. A confiança no ZTA é estabelecida através do processo de autenticação e autorização, em que os usuários e dispositivos devem se provar para ganhar acesso a recursos específicos (TEERAKANOK; UEHARA; INOMATA,

2021). Nos modelos comuns do *Zero Trust* os componentes presentes em sua arquitetura são os seguintes: assunto, recurso, ponto de decisão política (PDP), ponto de imposição de política (PEP) e suplemento, conforme apresentado na figura 2.1.

O assunto refere-se a um usuário ou qualquer dispositivo que solicita acesso aos recursos da empresa. Já o termo recurso, faz referência ao recurso corporativo/empresarial solicitado pelo usuário.

O ponto de decisão de política (PDP) é responsável por avaliar a solicitação de acesso a um recurso da empresa e determinar se deve ser permitido ou negado. Além disso, o PDP tem a função de gerenciar a comunicação entre o assunto que solicita o recurso e o recurso em si. Para cumprir essas funções, o PDP é composto por dois componentes: o mecanismo de política (PE) e o administrador de política (PA), que são os responsáveis pela tomada de decisão e gerenciamento de comunicação, respectivamente.

O funcionamento é feito da seguinte forma, um assunto envia uma solicitação para acessar um recurso da empresa, essa solicitação é direcionada ao ponto de aplicação de política (PEP). O PEP, por sua vez, encaminha a solicitação para o PDP e após avaliar, o PDP emite um comando de volta para o PEP, indicando se deve permitir ou negar o acesso ao recurso solicitado. O PEP funciona como uma espécie de porta de entrada entre o sujeito e os recursos e monitora o tráfego de rede entre o assunto e o recurso que foi solicitado.

Por fim, o suplemento ajuda a fornecer informações para o PE. Permitindo que o PE tome decisões mais precisas, o que também acaba aumentando a segurança geral do sistema.

2.4 Controle de Acesso

O controle de acesso é um mecanismo fundamental para a segurança da informação, assegurando que apenas usuários autorizados consigam acessar determinados recursos e informações dentro de um sistema. O seu objetivo principal é proteger dados sensíveis e evitar que indivíduos não autorizados ou sistemas maliciosos consigam acessar, modificar ou excluir informações importantes. O controle de acesso vai além do simples uso de senhas, envolvendo uma série de verificações e regras que definem quem pode acessar

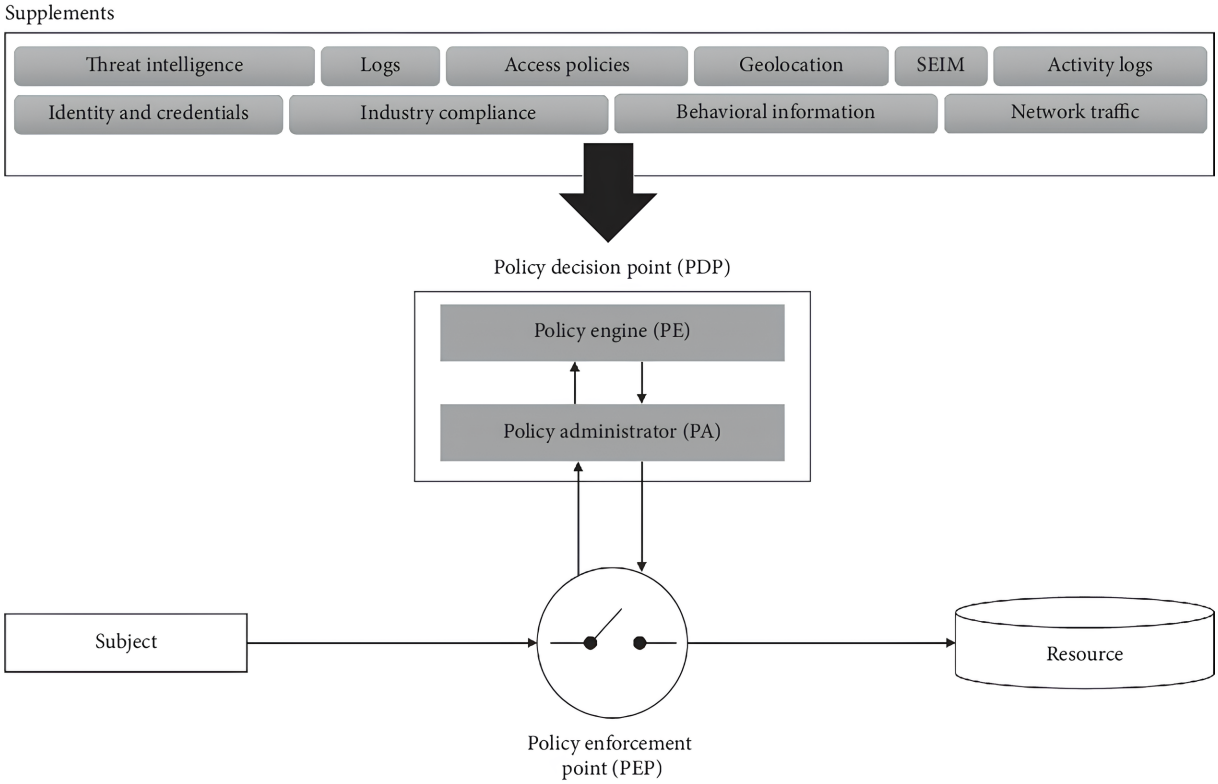

Figura 2.1: Componentes da Arquitetura *Zero Trust* (TEERAKANOK; UEHARA; INOMATA, 2021)

cada recurso do sistema.

O fluxo de um processo de controle de acesso pode ser ilustrado na figura 2.2. O processo começa quando um sujeito/usuário envia uma solicitação de acesso ao gerenciador de controle de acesso para acessar um objeto específico. Em seguida, o gerenciador de controle de acesso compara as credenciais do sujeito com as políticas de acesso para decidir se concede ou nega o acesso. Se o acesso for concedido, o gerenciador de controle de acesso permitirá que o usuário acesse o objeto. Caso o acesso seja negado, o gerenciador de controle de acesso enviará uma mensagem de aviso devido às credenciais insuficientes e solicitará que o sujeito utilize credenciais adequadas para acessar o objeto solicitado (ATLAM et al., 2020).

2.4.1 Controle de Acesso Baseado em Risco (RbAC)

O modelo de Controle de Acesso Baseado em Risco (RbAC) é uma abordagem dinâmica que utiliza o valor de risco relacionado a cada solicitação de acesso para determinar a decisão de permissão ou negação de acesso. Esse modelo visa melhorar a flexibilidade e re-

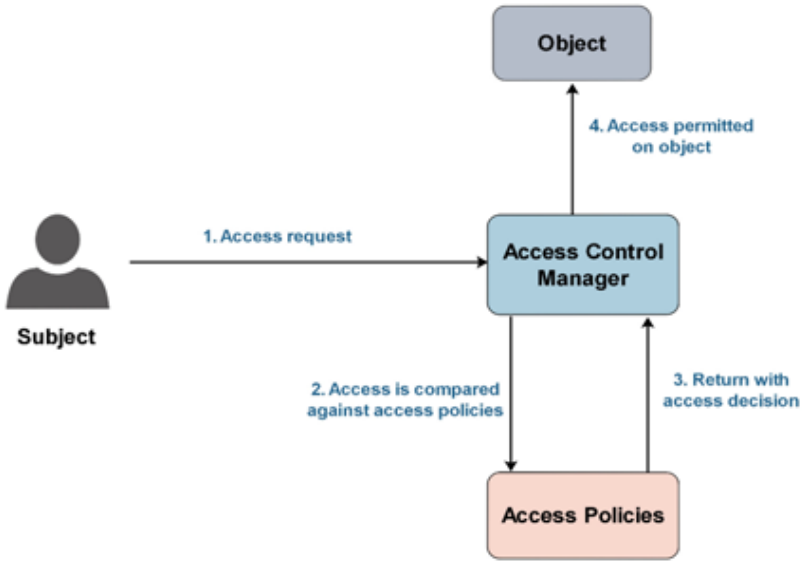

Figura 2.2: Fluxo de uma operação de controle de acesso (ATLAM et al., 2020)

siliência ao acesso a recursos do sistema, considerando elementos contextuais e dinâmicos. Além disso, ele é capaz de lidar com situações excepcionais e imprevisíveis, como no caso de aplicações em áreas críticas, como saúde e segurança, onde a decisão de acesso pode ser crucial para salvar vidas (ATLAM et al., 2020).

O principal objetivo do RbAC é garantir que apenas usuários autenticados e autorizados possam acessar os recursos, limitando atividades de usuários legítimos a ações previamente determinadas pelas políticas de segurança. O modelo é composto por três componentes principais: os sujeitos, que são os usuários que solicitam o acesso; os alvos, que são os recursos do sistema que estão sendo acessados; e as regras, que definem as permissões para o acesso (NGOC; LEE, 2007).

Uma das grandes vantagens do controle de acesso baseado em risco é a sua capacidade de adaptar a decisão de acesso conforme o risco associado à solicitação. A estimativa de risco é realizada com base em diversos fatores de contexto, como a localização do usuário, o tipo de dispositivo e o comportamento do solicitante, oferecendo uma resposta mais precisa e dinâmica para garantir a segurança do sistema (ATLAM et al., 2020).

Em essência, o objetivo final desse modelo é permitir um esquema de controle de acesso que promova o compartilhamento de informações de forma eficiente e segura, garantindo que os usuários sejam responsáveis por suas ações e prevenindo danos causados

pela divulgação de informações confidenciais. Esse tipo de controle de acesso pode ser mais adequado em ambientes que exigem decisões rápidas e ajustadas ao risco, como sistemas de saúde e operações militares (ATLAM et al., 2020).

Essa abordagem se diferencia de modelos tradicionais, como o RBAC baseado em papéis, que, embora simples e eficiente em muitos cenários, não leva em consideração fatores dinâmicos e contextuais, tornando-se limitado para novos ambientes que exigem maior flexibilidade de segurança (NGOC; LEE, 2007).

2.4.2 Controle de Acesso Baseado em Papéis (RBAC)

O Controle de Acesso Baseado em Papéis (RBAC) tem sido o modelo predominante nas empresas por mais de duas décadas, sendo amplamente utilizado para gerenciar o acesso aos recursos de sistemas complexos. Nesse modelo, as permissões são atribuídas com base em papéis específicos, e os usuários recebem as permissões associadas a esses papéis, simplificando o gerenciamento de acesso. O principal benefício do RBAC é sua simplicidade e escalabilidade, especialmente em ambientes organizacionais onde a estrutura hierárquica é clara e as funções são bem definidas. No entanto, quando aplicado em organizações grandes e diversificadas, o modelo pode se tornar difícil de gerenciar devido à rigidez na atribuição de permissões (TSAI; LEE; SHIEH, 2024).

Embora o RBAC seja eficaz em cenários estáticos, ele apresenta limitações em ambientes dinâmicos, onde sujeitos, recursos e permissões podem mudar frequentemente. O modelo não oferece flexibilidade suficiente para gerenciar mudanças rápidas ou imprevistas, o que o torna inadequado para cenários que exigem decisões rápidas ou ajustadas ao contexto. Além disso, o RBAC não leva em consideração fatores dinâmicos e contextuais, como o ambiente em que o acesso é realizado ou o comportamento do usuário, o que pode resultar em um controle de acesso menos seguro e adaptável (FATIMA et al., 2016).

Em grandes instituições, a rotatividade de cargos e as mudanças de papéis dos usuários representam outro desafio para o RBAC. Com a atribuição fixa de papéis, o modelo enfrenta dificuldades para acompanhar essas mudanças, o que pode gerar um alto custo administrativo e tornar o controle de acesso mais vulnerável. Mesmo com

a introdução de modelos estendidos de RBAC, a flexibilidade necessária para gerenciar permissões de forma mais granular e dinâmica ainda é limitada (LONG; YAN, 2019).

O RBAC também enfrenta desafios quando se trata de fornecer controle de acesso refinado. Como o modelo opera em uma granularidade mais ampla, ele não é adequado para cenários onde é necessário um controle mais específico, como limitar o acesso a dados sensíveis ou a ações específicas em determinados momentos. Isso se deve ao fato de que o RBAC não permite a atribuição dinâmica de permissões com base em atributos ou contexto, limitando a capacidade de adaptar as políticas de segurança às necessidades específicas do sistema ou da organização (YAO et al., 2021).

Embora o RBAC tenha sido uma solução eficaz por muito tempo, a evolução das necessidades de segurança, especialmente com o aumento de ambientes de computação dinâmica, exige novos modelos de controle de acesso que sejam mais flexíveis, contextualmente sensíveis e capazes de responder a riscos de forma mais eficaz (FATIMA et al., 2016).

2.4.3 Controle de Acesso Baseado em Atributos (ABAC)

O modelo de Controle de Acesso Baseado em Atributos (ABAC) surgiu como uma alternativa poderosa para superar as limitações enfrentadas pelo modelo RBAC. Comparado ao RBAC, o ABAC é relativamente novo, mas a ideia de utilizar atributos e comportamento para identificação e reconhecimento já é uma técnica amplamente estabelecida (FATIMA et al., 2016).

Em princípio, tanto o ABAC quanto o RBAC podem ser utilizados para fornecer controle de acesso dentro do conceito de *Zero Trust*. No entanto, o ABAC se destaca por oferecer um controle mais refinado e, por essa razão, tornou-se a abordagem dominante tanto na literatura quanto em sistemas comerciais (XIAO et al., 2022).

Uma das principais vantagens do ABAC é a flexibilidade no controle de acesso. Foi argumentado que ele pode fornecer essa flexibilidade de forma mais eficiente do que o RBAC e que ambos os modelos podem coexistir, considerando uma função como mais um atributo dentro do ABAC. Como o ABAC não depende de funções com permissões específicas, ele elimina a necessidade de projetar e gerenciar essas funções e permissões,

tornando sua implementação mais dinâmica.

O RBAC, apesar de amplamente adotado, apresenta desafios, pois é caro de implementar e não consegue acomodar estados ambientais em tempo real como parâmetros de controle de acesso. O ABAC, por outro lado, é mais moderno, mais simples de implementar e permite a incorporação de estados ambientais dinâmicos para decisões de acesso. Isso ocorre porque, no ABAC, atributos podem estar associados a usuários, recursos, ambientes ou até mesmo estados de aplicativos.

Além disso, diferentemente do RBAC, o ABAC possibilita decisões de acesso dinâmicas ao considerar atributos contextuais como horário, local e comportamento do usuário. No entanto, essa flexibilidade vem acompanhada de desafios, uma vez que um grande número de atributos precisa ser compreendido, gerenciado e selecionado por profissionais especializados. Outro ponto de atenção é que os atributos, por si só, não têm significado até que sejam associados a usuários, objetos ou relações específicas, o que pode dificultar auditorias sobre quais usuários possuem determinadas permissões e quais permissões foram concedidas a um usuário específico (COYNE; WEIL, 2013).

Apesar dessas dificuldades, o ABAC foi proposto como uma solução eficaz para controle de acesso em ambientes distribuídos, pois não depende de uma relação pré-definida entre sujeitos e objetos. Esse modelo é capaz de atualizar dinamicamente decisões de acesso conforme os atributos das entidades mudam, o que permite um gerenciamento de privilégios mais granular e adaptável. No entanto, definir regras no ABAC pode ser desafiador, demandando tempo para ajustes e testes a fim de evitar conflitos de regras (LONG; YAN, 2019).

Por fim, embora o ABAC tenha se mostrado uma abordagem promissora e amplamente adotada, ele apresenta dificuldades no processo de auditoria de permissões concedidas aos usuários. Por essa razão, o uso do RBAC com atributos pode ser preferível ao ABAC que utiliza nomes de funções como atributos. Assim, a coexistência entre os modelos pode ser uma solução viável, aproveitando os pontos fortes de cada um para um controle de acesso mais eficiente e seguro (COYNE; WEIL, 2013).

2.4.4 A combinação do ABAC e do RBAC

A combinação dos modelos ABAC e RBAC tem sido amplamente explorada como uma solução para aprimorar o controle de acesso em sistemas modernos. Inicialmente, ambos os esquemas podem ser utilizados dentro do conceito de *Zero Trust*, mas, na prática, o ABAC se destaca por oferecer um controle mais refinado. Por essa razão, tornou-se a abordagem dominante tanto na literatura quanto em sistemas comerciais. No entanto, o RBAC ainda desempenha um papel relevante, sendo utilizado como fonte de informações de contexto primárias ou secundárias em sistemas centrados no usuário (XIAO et al., 2022).

Com o avanço dos sistemas distribuídos e dinâmicos, as empresas perceberam que o modelo RBAC, baseado exclusivamente em grupos de usuários e permissões estáticas, já não era suficiente. Para superar essa limitação, passaram a incorporar atributos adicionais, como horário e localização do usuário, permitindo uma tomada de decisão mais contextualizada. Nesse contexto, o controle de acesso baseado em atributos foi identificado tanto como um substituto quanto como um complemento ao RBAC (COYNE; WEIL, 2013).

A coexistência entre os modelos também foi considerada uma abordagem viável. Foi argumentado que o ABAC pode oferecer a flexibilidade necessária para o controle de acesso e que, caso desejado, o RBAC poderia ser integrado ao ABAC, bastando tratar papéis como mais um atributo dentro do modelo baseado em atributos. Dessa forma, a união dos dois modelos permite a utilização das vantagens de ambos (RAJPOOT; JENSEN; KRISHNAN, 2015).

Embora o RBAC continue sendo amplamente adotado por suas vantagens administrativas e de segurança, ele apresenta desafios significativos. Seu modelo rígido torna a implementação onerosa, além de não permitir a adaptação a estados ambientais em tempo real. Em contraste, o ABAC é uma solução mais recente, de implementação mais simples e que possibilita a incorporação de atributos dinâmicos nas decisões de controle de acesso. Assim, uma abordagem híbrida, na qual funções do RBAC são tratadas como atributos dentro do ABAC, pode permitir um controle mais eficiente e adaptável (COYNE; WEIL, 2013).

Do ponto de vista arquitetônico, a combinação entre os dois modelos não apresenta grandes desafios. Como ilustrado na figura 2.3, cada modelo pode manter sua própria base de regras no ponto de informação de política (PIP), enquanto o ponto de decisão de política (PDP) deve ser capaz de avaliá-las para produzir uma decisão de acesso. Essa integração possibilita aproveitar a flexibilidade e a riqueza contextual do ABAC, ao mesmo tempo em que mantém os benefícios do RBAC, como a análise estruturada e o controle de risco. Assim, a união entre os modelos pode resultar em um controle de acesso mais seguro e eficiente.

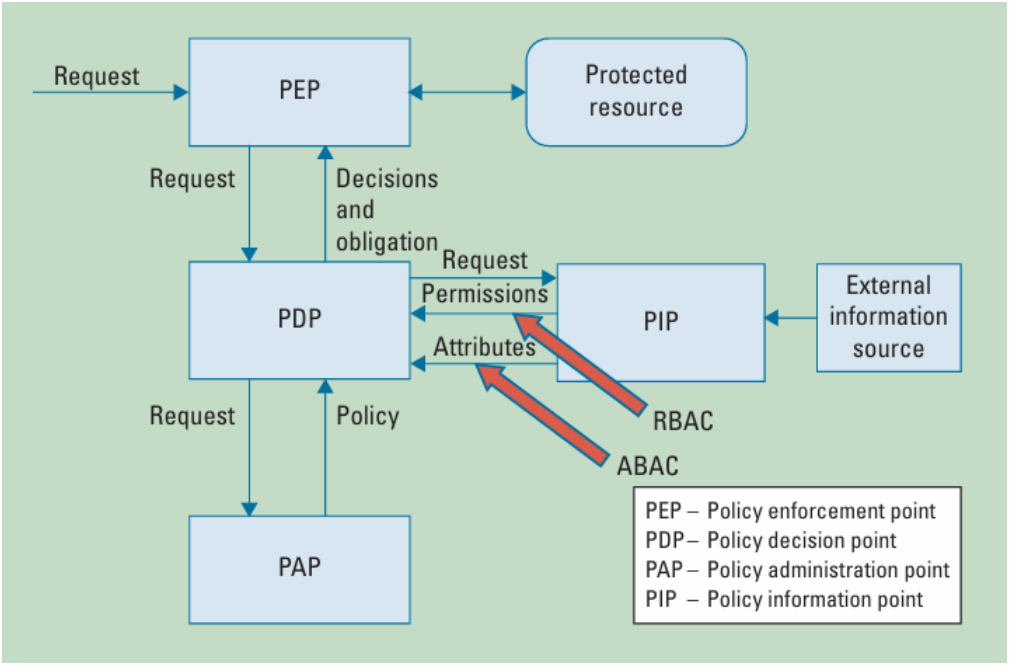

Figura 2.3: Controle de acesso baseado em atributos e funções (COYNE; WEIL, 2013)

3 Trabalhos Relacionados

3.1 Introdução

Neste capítulo, são abordados alguns trabalhos relacionados que, de alguma forma, fazem referência ao estudo que estamos implementando. Para os modelos de controle de acesso já foi falado da sua eficácia para garantir a sua segurança e a Seção 3.2 aborda trabalhos que citam modelos de controle de acesso específicos e comentam sobre sua usabilidade. A Seção 3.3 apresenta alguns ambientes onde é utilizada a arquitetura *Zero Trust*, mostrando toda sua forma de ser implementada e também a sua eficácia em comparação com a utilização de outros modelos. A Seção 3.4 discute a utilização do modelo *Zero Trust* integrado aos mecanismos de controle de acesso, visando garantir maior segurança. E, por fim, na Seção 3.5, são apresentadas as considerações finais deste capítulo.

3.2 Modelos gerais de controle de acesso

O trabalho de (FERRAIOLO et al., 2001) propõe um padrão para o Controle de Acesso Baseado em Papéis (RBAC), com o objetivo de unificar os conceitos. Embora a ideia central do RBAC seja parecida em diferentes modelos, há variações em detalhes e terminologias que dificultam sua adoção. Para resolver isso, os autores definem um modelo de referência e uma especificação funcional.

O modelo de referência proposto estabelece os principais elementos do RBAC, como usuários, papéis e permissões. Já a especificação funcional detalha requisitos administrativos e operacionais.

Por fim, de acordo com os autores, a padronização é essencial, especialmente pelo fato de grandes organizações adotarem cada vez mais esse modelo. Além de facilitar o desenvolvimento e a aquisição de sistemas, um padrão unificado permitirá maior interoperabilidade e portabilidade entre diferentes soluções.

Já no trabalho de (HU; KUHN; FERRAIOLO, 2015), os autores apresentam

o Controle de Acesso Baseado em Atributos (ABAC), citando as características desse modelo e destacando a flexibilidade como sua maior vantagem, permitindo a criação de regras dinâmicas sem a necessidade de estabelecer vínculos diretos entre cada usuário e recurso.

Os autores mencionam que a implementação do ABAC pode ser complexa, exigindo uma infraestrutura robusta para gerenciar atributos e políticas. Também discutem a garantia de atributos, que avalia a precisão, integridade e disponibilidade dos dados para definir acessos.

Por fim, reforçam o potencial do ABAC para aprimorar a segurança em aplicações modernas, tornando o controle de acesso mais adaptável e seguro.

No trabalho de (COYNE; WEIL, 2013), os autores abordaram a necessidade de um modelo híbrido de controle de acesso, de forma a unir o Controle de Acesso Baseado em Função (RBAC) e o Controle de Acesso Baseado em Atributos (ABAC). É notável que o RBAC é eficiente em ambientes bem estruturados, mas pode ser rígido em cenários dinâmicos. Já no caso do ABAC, ele oferece maior flexibilidade, mas pode se tornar complexo de gerenciar em sistemas grandes.

Para equilibrar essas características, os autores apresentam o RACAC, que tem como propósito combinar a infraestrutura do RBAC com a dinâmica dos atributos do ABAC, tornando a atribuição de permissões mais flexível e adaptável.

Os autores ainda incluem um estudo de caso, demonstrando como a utilização do RACAC simplifica a gestão de acesso e melhora a flexibilidade em comparação aos modelos tradicionais. Por fim, o trabalho conclui que o modelo híbrido RACAC representa um grande avanço, reduzindo a complexidade da administração de privilégios sem comprometer a segurança.

3.3 A utilização da Arquitetura *Zero Trust* em ambientes gerais

O trabalho de (TSAI; LEE; SHIEH, 2024) aborda os desafios de segurança cibernética decorrentes por conta do aumento do trabalho remoto na pandemia e apresenta a Arqui-

tetura *Zero Trust* (ZTA) como solução. A arquitetura se baseia em dois componentes principais: o Ponto de Decisão Política (PDP) e o Ponto de Aplicação Política (PEP).

Os autores afirmam que a ZTA segue um modelo cíclico, no qual os usuários são sempre tratados como não confiáveis, e os acessos são definidos pelo princípio do menor privilégio.

Por fim, os autores destacam que apesar das vantagens, a ZTA enfrenta desafios, como a dificuldade em distinguir atividades suspeitas de normais, gerando falsos positivos. O estudo conclui que a ZTA é uma abordagem promissora para fortalecer a segurança digital, mas sua adoção deve considerar as necessidades e a cultura de cada organização.

No trabalho de (CHEN et al., 2022), os autores propuseram a utilização da arquitetura *Zero Trust* para redes 6G, que é promissora para estabelecer um regime de segurança elástico e escalável, visto que é esperado que a próxima rede de sexta geração (6G) seja mais aberta e heterogênea do que as gerações anteriores, desafiando assim as arquiteturas de segurança convencionais, que são baseadas na construção de um perímetro de segurança da rede. Dessa forma, os autores utilizam da arquitetura *Zero Trust* por ela conseguir garantir um controle de acesso seguro através de colaborações adaptativas e poder prevenir de forma eficaz comportamento de acesso maliciosos, tais como ataques distribuídos de negação de serviço (DDoS), propagação de malware, dentre outros. Os autores apresentam os desafios que estão presentes na segurança 6G, abordando temas como modelo de ataque, desafios de segurança e o principal citado é o uso da ZTA e as suas limitações em 6G. Temos que as ZTAS atuais implementam estratégias de controle de acesso de granularidade fina para proteger todos os recursos de dados e serviços de computação, e essa característica não consegue fazer face aos desafios introduzidos pela grande escala das redes 6G. E além disso, os ZTAs existentes são principalmente concebidos para um único domínio de rede com um controlador logicamente centralizado, sendo assim, não podem ser aplicados a redes 6G heterogêneas com arquiteturas de gestão descentralizadas. Apesar dos desafios encontrados, os autores conseguiram verificar a eficácia do ZTA para redes 6G, fazendo comparações com duas arquiteturas de segurança, a *Trust Based Packet Filtering* (TBPF) e a *Transparency for better Internet Security* (TRIS). Foram definidas quatro comunidades, nomeadas de A, B, C e D, com 1000 UEs cada,

estabelecendo ligações entre A-B, A-C, B-D e C-D. Foi adotado o modelo suscetível-infeccioso-recuperado (SIR) para simular a propagação de worms em comunidades. E após todos testes feitos, os autores puderam concluir que o uso da arquitetura *Zero Trust* apresenta um desempenho muito melhor do que o TRIS e o TBPF, o que demonstra a robustez e eficácia do ZTA.

Já no trabalho de (ANDREWS, 2022) é tratado sobre a popularidade que a arquitetura *Zero Trust* vem ganhando no setor de energias elétricas virtuais, para poder defender e impedir as ciberameaças ou o cibercrime. A popularidade dos geradores distribuídos faz com que sejam auto-suficientes em termos de energia e permite que o consumidor forneça energia à rede. Dessa forma, a sua rede também está exposta a desafios de segurança e a proteção destes sistemas físicos, a proteção dos dados e a privacidade da informação tornam-se fundamentais. Dessa forma, este trabalho tem como objetivo apresentar uma arquitetura de segurança abrangente de *Zero Trust* para ajudar a reduzir os riscos e a proteger os sistemas físicos e garantir a privacidade e a proteção de dados. Os autores observaram que com o avanço dos geradores distribuídos e o estabelecimento de sistemas de centrais elétricas virtuais, gerou um interesse significativo de proteger os recursos. Além disso, o setor de energia é abrangido pelos serviços de infra-estruturas críticas. Devido à própria natureza das operações nas centrais elétricas virtuais (VPP), a probabilidade de paragens, disponibilidade e dados pessoais e privados é multiplicada. Com isso, estes desafios podem ter efeitos em cascata em termos de perdas econômicas, danos no equipamento pessoal e desafios sociais e políticos. O trabalho conclui que os métodos existentes de segurança de rede e avaliação de risco são essencialmente qualitativos e heurísticos. Dessa forma, foi realizada uma investigação sobre sistemas de segurança baseados no modelo *Zero Trust* para aplicação no setor de energias elétricas virtuais. Estas soluções tem o intuito de abordar a proteção fundamental dos dispositivos VPP, incluindo uma arquitetura de cibersegurança abrangente e a aplicação da ZTA.

3.4 A integração do modelo *Zero Trust* aos mecanismos de controle de acesso

O trabalho (VANICKIS; JACOB; DEHGHANZADEH, 2018) aborda a transição do modelo de segurança tradicional para o modelo *Zero Trust*, destacando a importância do controle de acesso nesse novo contexto. O ZTN divide as redes em zonas de diferentes níveis de confiança, tratando a rede interna com a mesma desconfiança da Internet, o que exige um controle de acesso rigoroso, tendo como base o perfil e contexto do usuário e dispositivo.

Os autores apresentam o FURZE (*Fuzzy Risk Framework for ZTN*), uma estrutura que facilita a gestão de políticas de Controle de Acesso Adaptável ao Risco (RAdAC), com avaliação de risco fuzzy e atualização dinâmica de firewalls. São definidas duas linguagens de política dentro dessa estrutura: PAROLE, para expressar políticas gerais de controle de acesso, e FACL, para definir regras de firewall.

O PAROLE oferece controle contínuo para acessos longos, determinando o risco de acesso e permitindo o controle baseado em risco. A arquitetura do FURZE inclui componentes como o *Policy Enforcement Point* (PEP), *Context Handler* (CH), *Risk Evaluation Function* (REF) e *Access Decision Function* (ADF), fundamentais para o controle de acesso no ZTN.

A ideia principal dos autores, é propor um framework de controle de acesso baseado em risco, para atender às necessidades de segurança no *Zero Trust*.

No trabalho (YAO et al., 2021), discutem-se os desafios de segurança das redes modernas diante do avanço de tecnologias como computação em nuvem e inteligência artificial. É argumentado que os modelos tradicionais, baseados na proteção de borda, não são mais eficazes e propõem um sistema dinâmico de controle de acesso e autorização fundamentado no conceito de *Zero Trust*.

O modelo proposto pelos autores, exige autenticação contínua e concessão mínima de privilégios, ajustando permissões em tempo real conforme o comportamento do usuário. Em vez de depender apenas da localização física, o sistema avalia fatores como ambiente e padrões de acesso. Além disso, adota um Controle de Acesso Baseado em Confiança

(TBAC), que adapta dinamicamente as permissões conforme a atividade do usuário.

Os autores concluem que a abordagem *Zero Trust* melhora a segurança das redes ao minimizar riscos e responder de forma adaptativa a ameaças emergentes.

3.5 Considerações finais

Os trabalhos apresentados mostram como os modelos de controle de acesso têm evoluído para enfrentar desafios cada vez mais complexos de segurança. O RBAC se destaca pela organização e padronização, enquanto o ABAC traz mais flexibilidade, apesar da maior complexidade. Já a proposta de um modelo híbrido busca equilibrar essas características, oferecendo um controle mais eficiente e adaptável.

A arquitetura *Zero Trust* também tem ganhado espaço por sua capacidade de reforçar a segurança em diferentes cenários, como redes 6G e sistemas críticos de energia. No entanto, sua implementação ainda enfrenta desafios, como o risco de falsos positivos e a necessidade de uma infraestrutura robusta.

A integração do *Zero Trust* com mecanismos de controle de acesso mostra que essa abordagem tem potencial para transformar a segurança digital. Os estudos analisados servem como base para este trabalho, que propõe um modelo focado na proteção de arquivos, combinando *Zero Trust* com RBAC e ABAC para um controle mais dinâmico e seguro.

4 Material e métodos

Neste capítulo, apresento de forma detalhada os materiais e métodos utilizados no desenvolvimento dos cenários e na obtenção dos resultados. Na Seção 4.1, descreveremos o ambiente utilizado para as simulações. A Seção 4.2 abordará a confiança baseada em atributos, enquanto a Seção 4.3 se concentrará na confiança baseada em funções. Por fim, na Seção 4.4, explicaremos a tabela de permissões e os recursos envolvidos.

4.1 Ambiente simulado

Para o desenvolvimento deste trabalho, foi utilizado como referência o modelo *Zero Trust* conforme definido pelo (YAO et al., 2021), que o descreve como o conjunto de conceitos e estratégias voltadas para reduzir a incerteza na tomada de decisões de acesso. Para garantir um controle de acesso eficiente e seguro, foram utilizados dois modelos de controle de acesso: o Role-Based Access Control (RBAC), que define permissões com base nas funções dos usuários, e o Attribute-Based Access Control (ABAC), que ajusta as permissões de acordo com atributos específicos e comportamentos observados.

O ambiente simulado utilizado teve como base o trabalho (FREITAS, 2023; FREITAS et al., 2024), que já havia uma estrutura voltada para a aplicação do modelo *Zero Trust*. A partir desse ambiente, foram adicionadas novas validações e mecanismos, incorporando o modelo RBAC e definindo diferentes papéis para os usuários, como estagiário, analista e administrador, cada um com permissões específicas de acesso a arquivos. Essa mudança exigiu adaptações no código para garantir que o controle de acesso considerasse tanto os papéis predefinidos quanto as avaliações contextuais do ABAC.

Todas as configurações e os dados gerados durante a execução do sistema foram armazenados em um banco de dados relacional. Este banco contém diversas tabelas essenciais, como aquelas que registram as informações e funções de cada usuário, os recursos, sub-recursos e seus respectivos níveis de sensibilidade. Além disso, há outras tabelas importantes, como a de acessos, que armazena todos os registros de acessos realizados, e

as tabelas de Senha, RegLogin e Token, que são necessárias para autenticar o usuário no sistema.

Nesse ambiente, é representada uma empresa com três diferentes papéis de usuários: estagiário, analista e administrador. Cada um desses usuários tenta acessar recursos dentro do sistema, e a permissão de acesso é determinada com base em dois fatores principais: o nível de sensibilidade do recurso e a confiança do usuário. A confiança é gerenciada de forma dinâmica, sendo influenciada tanto por atributos específicos do usuário e seu comportamento (ABAC) que estão descritos na Seção 4.2, quanto pelo papel que ele desempenha na empresa (RBAC) que se encontra na Seção 4.3. Com essa abordagem, o controle de acesso torna-se mais preciso, garantindo que os usuários tenham acesso apenas às informações e arquivos compatíveis com seu contexto e nível de confiança. Na Seção 4.4, serão detalhados os recursos e sub-recursos disponíveis no sistema, assim como a tabela de permissões que define as decisões de acesso para cada situação.

4.2 Acesso e confiança baseada em atributos

O modelo de confiança baseada em atributos implementado no ambiente simulado foi inspirado no trabalho (FREITAS, 2023; FREITAS et al., 2024), onde já estava desenvolvido um sistema que avalia a confiança do usuário a partir de três perspectivas principais: confiança ao usuário com base no contexto, confiança ao dispositivo e confiança com base no histórico. Cada uma dessas perspectivas gera um valor de confiança entre 0 e 100, que juntamente com a sensibilidade do sub-recurso será usado para determinar se o acesso será permitido, se será necessária reautenticação ou se o acesso será negado.

A primeira perspectiva, confiança ao usuário com base no contexto, leva em consideração as seguintes variáveis:

- Múltiplos logins falhos consecutivos recentes;
- Alteração de senha recente;
- Mudança considerável na localização com base nos acessos recentes;
- Mudança da rede que utiliza para conectar no sistema.

A segunda abordagem, que trata da confiança baseada no dispositivo, deve considerar o fato de que, em nosso caso, assumimos que a empresa fornece o dispositivo para o usuário, e ele não utiliza o próprio. Diante disso, é necessário avaliar apenas as seguintes duas variáveis:

- Dispositivo compartilhado por outros usuários;
- Alterações nas características do dispositivo (*Device Fingerprint*);

A terceira perspectiva, confiança baseada no histórico, analisa as variáveis:

- Frequência de acesso a recursos altamente sensíveis;
- Múltiplas requisições negadas

Embora o código base tenha sido construído com essas três perspectivas, a abordagem deste trabalho, que se concentra no controle de acesso a arquivos dentro de uma empresa, exige um foco mais específico. Dessa forma, não foram utilizadas todas as formas de calcular confiança conforme descritas no trabalho de referência. Em vez disso, foram implementadas novas regras, voltadas para o contexto corporativo e de acesso a dados sensíveis. Essas regras levam em consideração o papel do usuário e a sensibilidade dos recursos, o que proporcionou uma adaptação do modelo original.

Na Seção 4.3, foi descrito em detalhes essas novas regras e como elas impactaram o cálculo da confiança no ambiente simulado, permitindo um controle de acesso mais refinado e alinhado aos objetivos deste estudo.

4.3 Acesso e confiança baseada em papéis

Para adicionar um nível extra de segurança e garantir a diferenciação dos usuários dentro da organização, optamos por implementar o Controle de Acesso Baseado em Papéis (RBAC). Esse modelo permite definir regras e permissões específicas para cada usuário com base em seu cargo, garantindo que o acesso aos recursos seja concedido de maneira mais refinada e controlada.

No sistema implementado, existem três papéis principais: estagiário, analista e administrador. A implementação do RBAC assegura que, independentemente da confiança que o usuário possua, existem restrições de acesso a certos recursos que não poderão ser ultrapassadas. Por exemplo, o estagiário possui permissões mais restritas em comparação aos outros papéis, enquanto o analista tem permissões maiores, mas ainda assim não pode acessar recursos considerados extremamente sensíveis.

O ponto principal é que, apesar de o estagiário e o analista possuírem confiança crescente com base em suas ações e comportamentos, nem todos os recursos estarão ao seu alcance. Mesmo que um analista atinja um nível de confiança considerável, ele ainda não terá a confiança máxima no sistema, pois isso depende do cargo e das responsabilidades atribuídas a ele. Apenas o administrador terá a capacidade de atingir a confiança máxima no sistema.

Além disso, não seria viável que o administrador começasse com um nível de confiança igual a zero e fosse gradualmente adquirindo confiança ao longo do tempo, visto que ele precisa lidar com dados e arquivos mais sensíveis de forma imediata e eficiente. Portanto, o administrador já inicia com um nível de confiança mais alto, condizente com as suas responsabilidades e a necessidade de acesso rápido a recursos mais críticos.

A Tabela 4.1 ilustra a distribuição de confiança entre as diferentes funções, mostrando a confiança mínima de cada uma e o limite máximo que pode ser atingido. Esse modelo assegura que as permissões de acesso sejam concedidas de forma adequada, levando em consideração tanto a função do usuário quanto seu nível de confiança.

Função/Papel	**Confiança mínima**	**Confiança máxima**
Estagiário	0	60
Analista	0	80
Administrador	40	100

Tabela 4.1: Tabela de confiança de acordo com funções/papéis.

Além das regras de confiança baseadas nos papéis, foram implementadas novas regras de segurança para garantir uma proteção ainda maior ao sistema, conforme descrito

a seguir:

- Inatividade no sistema: Se o usuário tiver a função de estagiário ou analista e ficar 1 hora sem acessar nenhum recurso, será exigido um novo login para garantir a segurança e evitar acessos não autorizados durante períodos de inatividade.

- Reautenticação a cada 1 hora e 30 minutos: O administrador, por possuir acesso a recursos mais sensíveis e iniciar com um nível de confiança mais alto, requer uma validação mais rigorosa. Dessa forma, a cada 1 hora e 30 minutos de atividade contínua no sistema, o administrador será solicitado a realizar um novo login, confirmando sua identidade e reforçando a segurança do acesso aos recursos críticos.

Essas duas novas regras foram validadas e estão detalhadas nas Seções 5.2 e 5.4.

4.4 Tabela de permissões e recursos

Conforme mencionado anteriormente, para que um usuário consiga acessar os recursos e sub-recursos do sistema, é necessário atender a dois critérios principais: o nível de sensibilidade do sub-recurso e um nível de confiança suficiente. A Figura 4.1 apresenta a matriz de permissões, na qual a confiança do usuário é comparada com a sensibilidade do sub-recurso que ele deseja acessar. Com base nessa relação, o sistema determina se o acesso será permitido, exigirá reautenticação ou será negado. Tanto a confiança do usuário quanto a sensibilidade do recurso variam de 0 a 100, porém, esses limites podem variar conforme o papel do usuário, conforme explicado anteriormente.

Nota-se que, quanto mais sensível for o recurso, maior será o nível de confiança exigido do usuário para que o acesso seja concedido. Essa abordagem reforça a segurança do sistema, garantindo que informações críticas sejam acessadas apenas por usuários devidamente autorizados e com um histórico de comportamento confiável.

Além disso, como o cenário abordado trata do controle de acesso a arquivos dentro de uma empresa, foram definidos cinco recursos principais, cada um contendo sub-recursos específicos. Esses sub-recursos representam diferentes tipos de ações que um usuário pode realizar, como leitura, escrita, modificação ou exclusão.

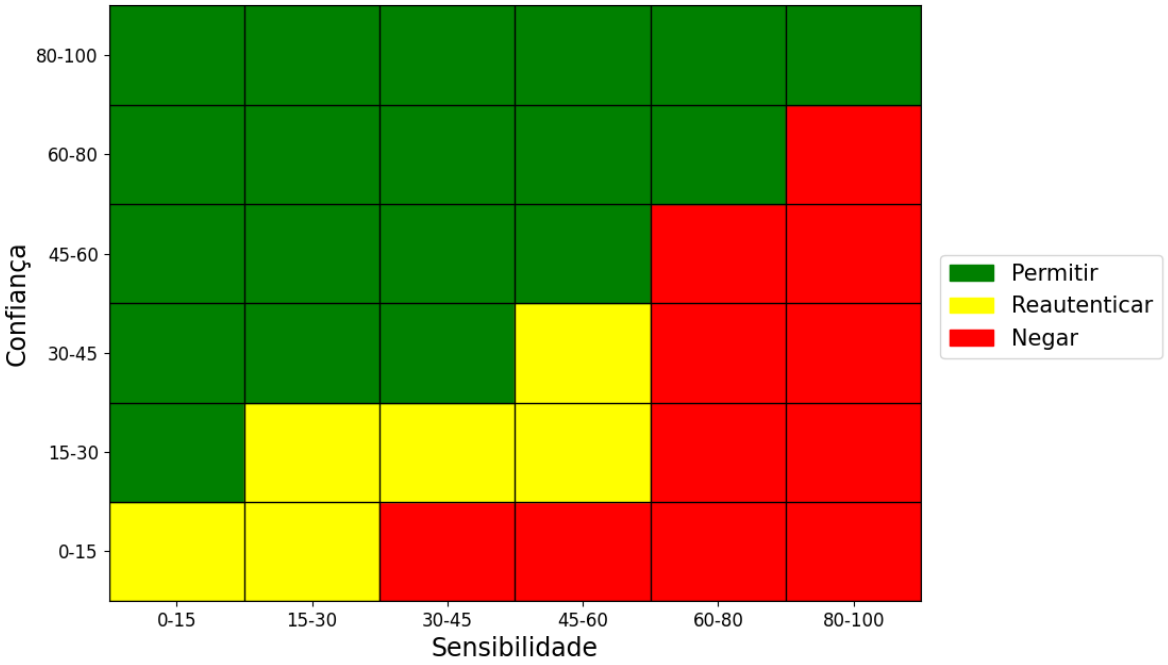

Figura 4.1: Tabela de Permissões

Cada sub-recurso possui um nível de sensibilidade atribuído, determinado com base em sua importância e no impacto que um acesso indevido poderia causar. Recursos mais críticos exigem níveis de confiança mais elevados para serem acessados, reforçando a abordagem de segurança baseada no modelo *Zero Trust*.

Nas Tabelas 4.2, 4.3, 4.4, 4.5, 4.6 detalhamos cada um dos recursos e seus respectivos sub-recursos, especificando suas ações permitidas e níveis de sensibilidade atribuídos.

Material de treinamento e desenvolvimento				
Sub-recurso	**Leitura**	**Escrita**	**Modificação**	**Exclusão**
Vídeos e apostilas de capacitação	13	-	-	-
Manuais de boas práticas	5	-	-	-
Simulados de certificações internas	10	20	45	70
Tutoriais de uso de ferramentas internas	15	-	-	-

Tabela 4.2: Recurso: Material de treinamento e desenvolvimento

Como foi descrito anteriormente, a função do usuário desempenha um papel crucial na definição do acesso aos recursos do sistema. O estagiário, por exemplo, tem acesso a uma quantidade restrita de recursos, como o Material de Treinamento e Desenvolvi-

Diretório de Projetos				
Sub-recurso	**Leitura**	**Escrita**	**Modificação**	**Exclusão**
Listagem de projetos ativos	22	-	30	-
Documentação geral do projeto	14	23	40	-
Ideias e propostas de inovação	13	22	45	-
Fórum de discussões	12	25	-	65
Repositório de projetos finalizados	30	-	-	-

Tabela 4.3: Recurso: Diretório de Projetos

Documentos Operacionais				
Sub-recurso	**Leitura**	**Escrita**	**Modificação**	**Exclusão**
Relatório de progresso	50	60	65	70
Planejamento e estruturação de projetos	35	-	61	-
Listas de tarefas	25	30	50	61
Controle de recursos do projeto	50	55	65	68
Gerenciamento de riscos e problemas	30	40	-	-

Tabela 4.4: Recurso: Documentos Operacionais

mento e o Diretório de Projetos. No entanto, sua permissão é mais restrita quando tenta acessar recursos como Documentos Operacionais e Gerenciamento de Estagiários, e ele não tem acesso algum aos Dados Sensíveis da Empresa. Já o analista possui os mesmos recursos que o estagiário, mas com permissões adicionais, como a capacidade de ler e escrever em alguns Dados Sensíveis da Empresa, embora não tenha permissão para modificar ou excluir essas informações. Por fim, o administrador tem acesso irrestrito a todos os recursos disponíveis no sistema, desde que tenha atingido a confiança necessária para isso.

Gerenciamento de Estagiários				
Sub-recurso	**Leitura**	**Escrita**	**Modificação**	**Exclusão**
Solicitações e históricos de acesso	45	-	-	-
Monitoramento de atividades	50	-	-	-
Relatórios de desempenho	61	-	63	-
Lançamento de horas	40	45	50	55
Histórico de estagiários	50	-	75	-

Tabela 4.5: Recurso: Gerenciamento de Estagiários

Dados Sensíveis da Empresa				
Sub-recurso	**Leitura**	**Escrita**	**Modificação**	**Exclusão**
Relatórios de faturamento	82	-	-	-
Dados de clientes	61	65	82	88
Contratos com fornecedores	65	75	81	85
Permissões de usuários	75	79	85	90
Planejamento estratégico	65	70	81	85
Folhas de pagamento	82	85	90	-
Informações médicas dos funcionários	62	-	-	-

Tabela 4.6: Recurso: Dados Sensíveis da Empresa

5 Cenários e Resultados

Neste capítulo, são apresentados diversos cenários de teste que abrangem desde o acesso normal de um usuário até tentativas de roubo de acesso, além de outros possíveis problemas no sistema. Para a realização dos testes, utilizamos instâncias de validação nas quais informações relevantes são fornecidas para garantir a execução bem-sucedida de cada cenário. A cada acesso a um recurso, um objeto contendo os seguintes dados é fornecido para validação:

- TYPE: Define se o acesso é um login no sistema ou uma tentativa de acesso a algum recurso específico;
- REGISTRY e PASSWORD: Informações do CPF e da senha do usuário, as quais permitem acessar sua função e outros dados relevantes para o controle de acesso;
- IP-ADDRESS: Utilizado para verificar se o usuário está efetuando o acesso a partir do computador autorizado pela empresa;
- LATITUDE e LONGITUDE: Dados necessários para validar a localização do usuário durante o acesso;
- TIME: Registra a data e a hora do acesso, possibilitando a análise do comportamento do usuário no sistema.

Esses dados são fundamentais para garantir que os testes sejam realizados de forma eficaz e que todas as validações de acesso sejam corretamente verificadas.

5.1 Caso 1: Acesso normal

Neste primeiro cenário, o objetivo é validar o acesso normal dentro da empresa. Para comparar o uso de acordo com as funções dos usuários, definimos um acesso comum aos mesmos recursos, como mostrado na Figura 5.1, onde é possível observar a sensibilidade dos recursos acessados.

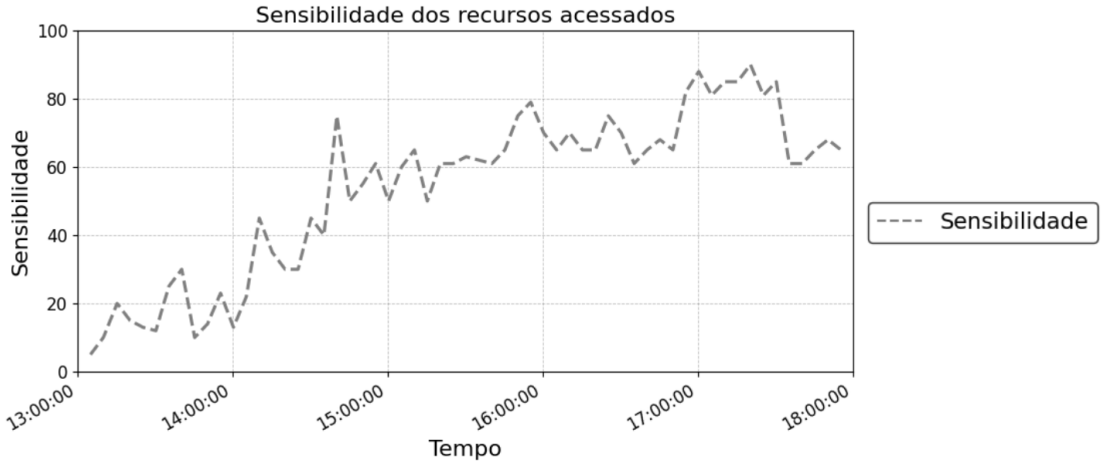

Figura 5.1: Sensibilidade dos recursos acessados

O acesso começa por recursos menos sensíveis, permitindo que o usuário ganhe confiança gradualmente dentro do sistema. No entanto, mesmo com essa progressão, o Estagiário e o Analista eventualmente precisam se reautenticar, conforme estabelecido na Tabela de Permissões 4.1. Com o tempo, a confiança do usuário aumenta, e ele passa a acessar recursos mais sensíveis. Nesse ponto, a implementação do RBAC entra em ação: o Estagiário, ao atingir sua confiança máxima de 60, já é bloqueado ao tentar acessar recursos com sensibilidade superior a esse valor. Com a insistência nesse comportamento, ele acaba perdendo confiança, como ilustrado na Figura 5.2. No caso do Analista, sua confiança chega ao máximo de 80, o que o impede de acessar recursos mais sensíveis. Contudo, ele consegue recuperar sua confiança ao longo do tempo, voltando a acessar os recursos disponíveis para a sua função, como demonstrado na Figura 5.3.

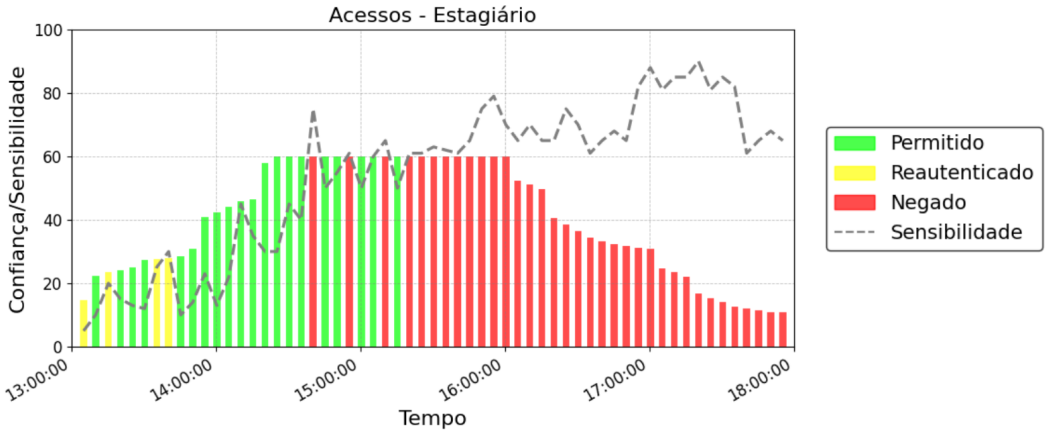

Figura 5.2: Acesso normal - Estagiário

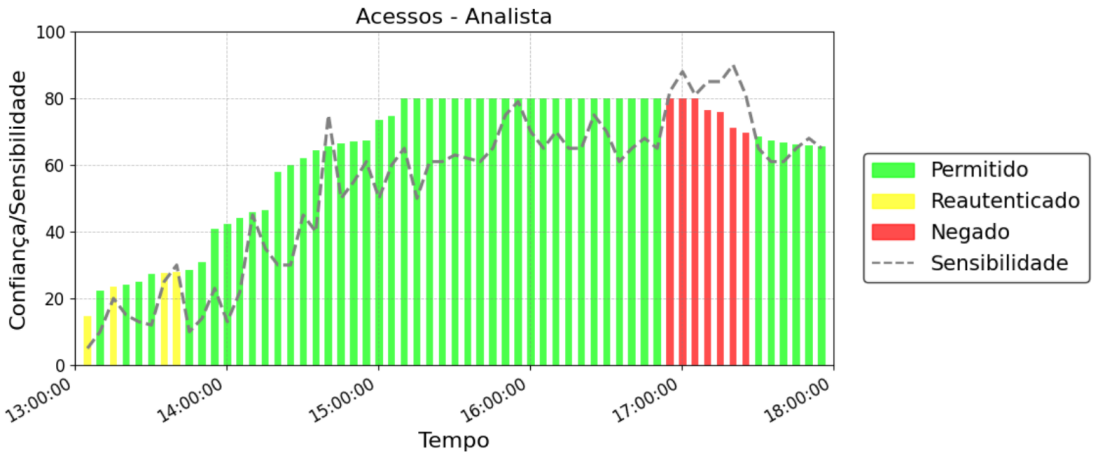

Figura 5.3: Acesso normal - Analista

5.2 Caso 2: Acesso - Administrador

Para lidar com o acesso do Administrador, utilizamos os mesmos recursos do cenário anterior, com o objetivo de demonstrar como um usuário com essa função conseguiria acessar os recursos no sistema.

5.2.1 Caso 2.1: Acesso normal - Administrador

Nesse caso, podemos observar na Figura 5.4 que, devido ao seu nível de confiança mais alto, o Administrador tem permissão para acessar tanto os recursos menos sensíveis quanto aqueles com maior grau de sensibilidade, sem a necessidade de reautenticação. E é importante ressaltar que, conforme mostrado na Tabela 4.1, a confiança do Administrador nunca cai abaixo de 40.

Além disso, vale destacar a nova regra imposta especificamente para os Administradores: a cada 1h30min de uso contínuo do sistema, será necessário realizar o login novamente, o que pode ser observado no gráfico pela cor azul, indicando os momentos que o usuário efetuou novamente o login. Essa medida foi adotada devido ao alto grau de responsabilidade e ao acesso a recursos sensíveis, garantindo maior segurança no controle de acesso.

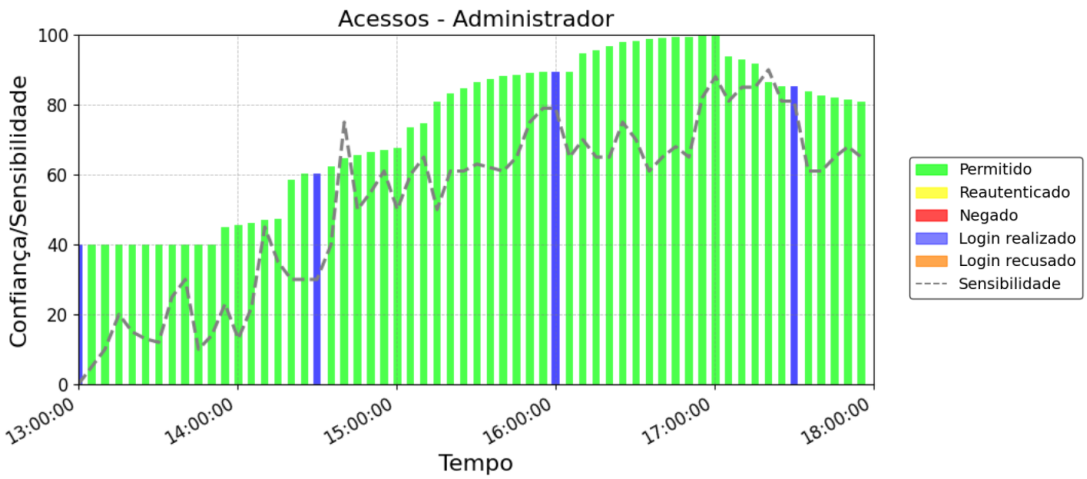

Figura 5.4: Acesso normal - Administrador

5.2.2 Caso 2.2: Roubo de acesso - Administrador

Agora, vamos abordar o caso em que o acesso do Administrador é roubado e um invasor começa a tentar acessar os recursos do sistema. Após 1h30 de uso contínuo, o sistema exige que o usuário realize o login novamente, solicitando o CPF, a senha e o token enviado para o dispositivo do Administrador. Devido a essa validação, o invasor não conseguiu prosseguir no sistema, já que não possuía as credenciais necessárias.

Na Figura 5.5, podemos observar o momento da falha no login, identificado pela cor laranja, o que indica que a tentativa de acesso foi recusada. Após essa tentativa frustrada, o invasor não teve mais acesso a nenhum recurso do sistema, garantindo que a segurança fosse mantida.

5.3 Caso 3: Tentativa de acessar recursos sensíveis

Neste terceiro cenário, analisamos a eficácia do controle de acesso baseado em atributos (ABAC). O caso em questão envolve um estagiário que inicia seu uso no sistema com acessos normais, porém, ao longo de quase uma hora, tenta repetidamente acessar recursos sensíveis sem permissão, como podemos ver na Figura 5.6.

Se observarmos a terceira perspectiva de avaliação da confiança, que se baseia no histórico de comportamento do usuário, podemos identificar dois fatores críticos: a

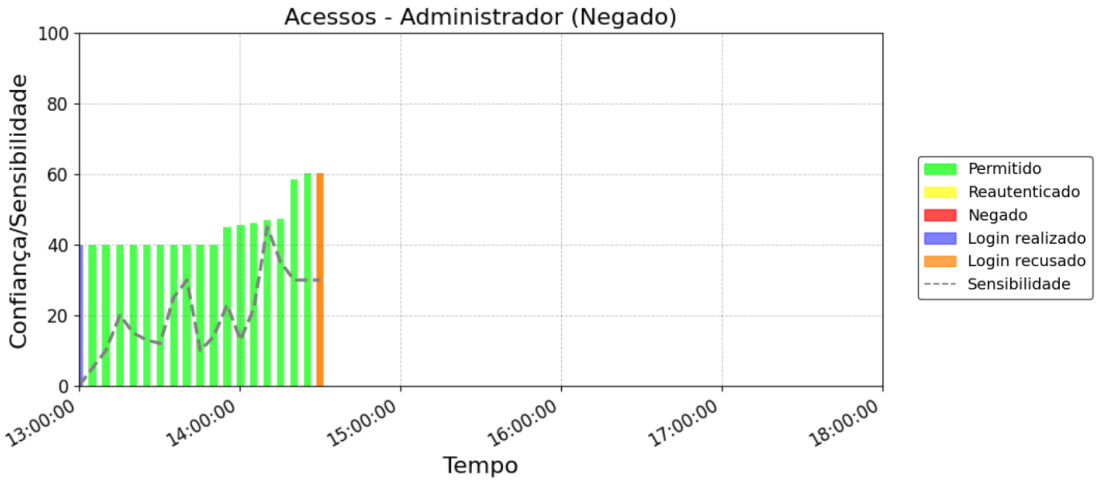

Figura 5.5: Roubo de acesso - Administrador

frequência de tentativas de acesso a recursos altamente sensíveis e o número de requisições negadas consecutivas. Ambos os fatores ocorrem nesse cenário, o que resulta na aplicação de penalidades ao usuário, reduzindo significativamente a confiança que ele havia adquirido até então.

Para recuperar sua confiança dentro do sistema, foi necessário um período de mais de uma hora, durante o qual o usuário precisou acessar apenas recursos de baixa sensibilidade, demonstrando um comportamento mais seguro e confiável ao longo do tempo.

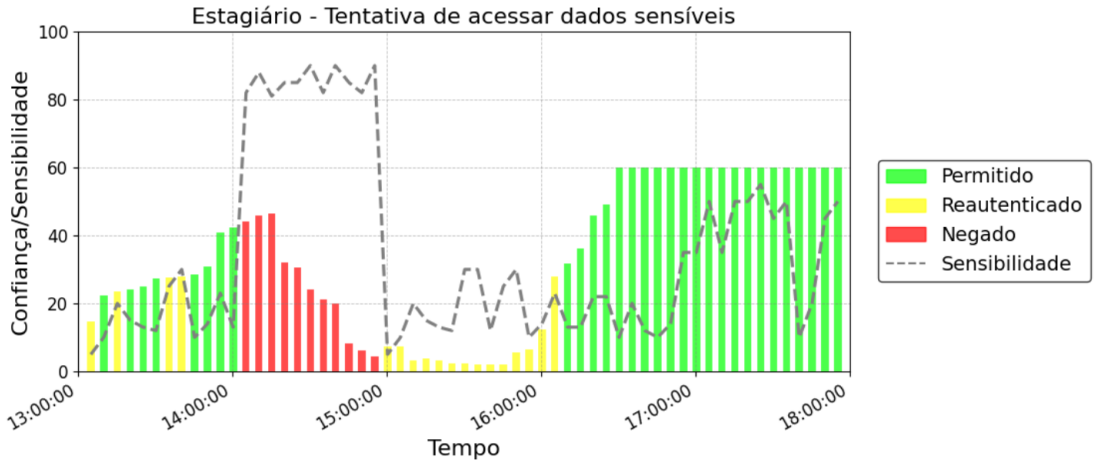

Figura 5.6: Acesso indevido - Estagiário

5.4 Caso 4: Inatividade no sistema

No quarto cenário, analisamos uma das novas regras de segurança do sistema: se um usuário ficar inativo por 1 hora, ele precisará fazer login novamente para continuar acessando os recursos. Essa medida foi implementada para garantir que, caso o usuário se afaste ou esqueça o sistema aberto, ninguém mais consiga utilizar sua sessão sem a devida autenticação.

Na Figura 5.7, temos um exemplo prático usando um usuário com a função de Analista. Podemos ver que entre 14:10 e 15:10, ele não realizou nenhuma ação no sistema, e, ao tentar acessar novamente, precisou refazer o login. O mesmo aconteceu entre 16:00 e 17:00.

Essa regra traz uma camada extra de proteção, evitando que a conta de um usuário fique vulnerável em caso de abandono da sessão, além de reduzir riscos de acessos indevidos.

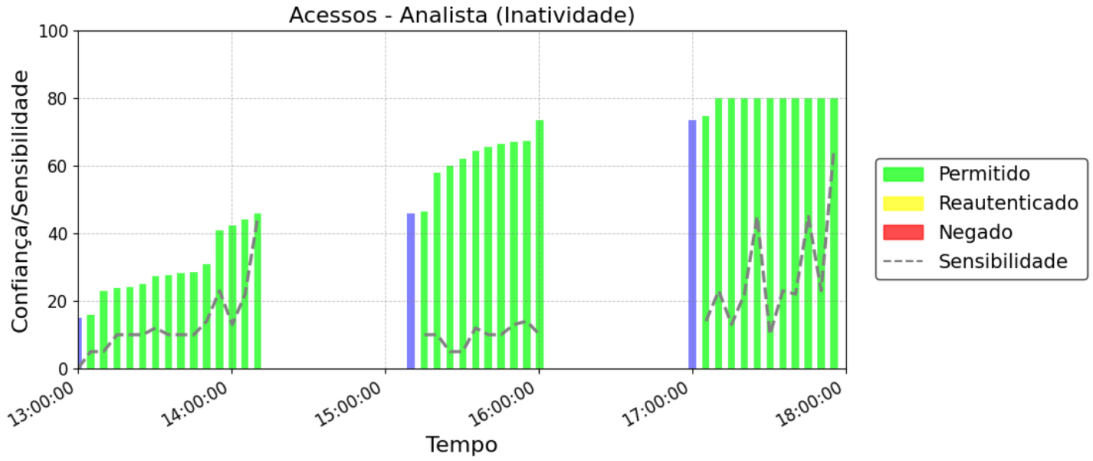

Figura 5.7: Inatividade - Analista

5.5 Caso 5: Mudança repentina de localização

No quinto e último cenário, analisamos um caso clássico de tentativa de acesso suspeito, onde o sistema precisa avaliar se realmente é o usuário legítimo tentando entrar ou se há algo errado. Aqui, usamos o controle de acesso baseado em atributos, focando na confiança do usuário com base no contexto.

Tudo começa com um acesso normal: o usuário está no Brasil, navegando pelo sistema. No entanto, de um momento para o outro, sua localização muda repentinamente para o Japão. Essa verificação acontece por meio dos dados de latitude e longitude coletados a cada acesso. Como essa mudança é extremamente improvável de ocorrer de forma legítima em tão pouco tempo, o sistema identifica o comportamento como suspeito e aplica uma punição severa na confiança do usuário.

O impacto disso é imediato: a confiança do usuário despenca a ponto de ele perder completamente o acesso ao sistema, sem possibilidade de recuperação, como podemos ver na Figura 5.8. Sem conseguir acessar mais nada, ele acaba desistindo. Essa validação é essencial para barrar tentativas de roubo de credenciais e acessos indevidos, garantindo que mesmo que um invasor tenha os dados de login de alguém, ele não consiga utilizá-los caso tente acessar de um local inesperado.

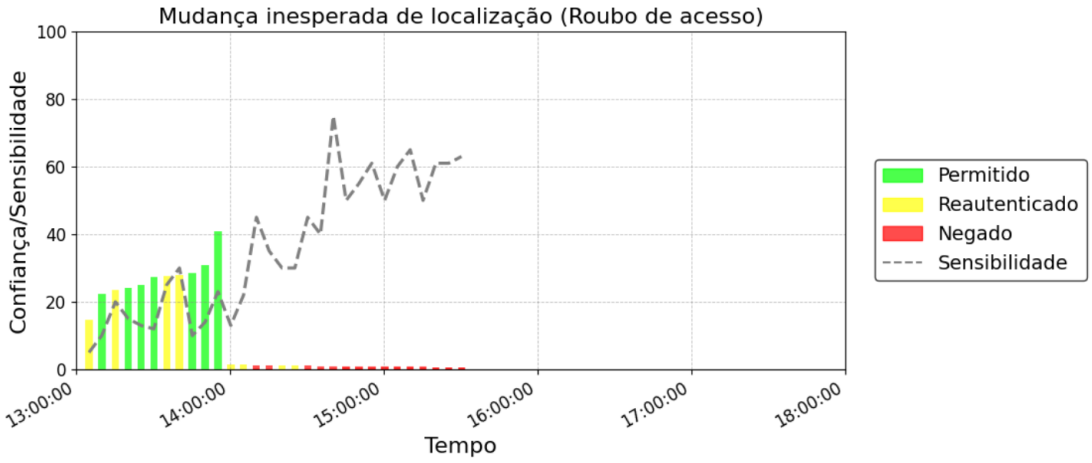

Figura 5.8: Mudança repentina de localização

6 Conclusão e Trabalhos Futuros

Com o avanço da tecnologia e a necessidade crescente de proteger melhor os dados de empresas e usuários, este trabalho teve como objetivo mostrar como o modelo *Zero Trust*, combinado com diferentes formas de controle de acesso, pode aumentar a segurança e a proteção das informações em um sistema.

Os testes realizados deixaram claro que validar constantemente a confiança do usuário e aplicar modelos como ABAC e RBAC ajuda a criar um ambiente mais seguro. Além disso, foi possível ver na prática que um usuário pode ganhar gradualmente mais confiança no sistema e, com isso, acessar recursos mais sensíveis de forma controlada.

Também ficou evidente que o sistema funciona bem em situações indesejadas, como tentativas de invasão ou acessos não autorizados. Nesses casos, a perda de confiança do usuário e as restrições aplicadas ajudaram a evitar possíveis violações de segurança.

Para os trabalhos futuros, há várias possibilidades de aprimoramento. Um dos primeiros passos seria refinar os atributos utilizados no sistema e ajustar melhor as penalidades para comportamentos suspeitos, tornando o controle de acesso ainda mais preciso e eficaz. Além disso, seria essencial desenvolver um mecanismo mais detalhado para monitorar cada acesso de usuário, garantindo uma análise mais transparente e confiável.

Outra melhoria importante seria ampliar as permissões dos administradores, permitindo que eles tenham um controle mais amplo sobre o sistema, podendo atribuir novas funções e validar acessos de forma mais dinâmica e segura. Além disso, uma definição mais clara das funções dentro do sistema poderia ser implementada, garantindo que cada usuário visualize apenas os recursos compatíveis com sua função. Isso evitaria não apenas tentativas de acesso indevidas, mas também reduziria riscos ao limitar a exposição a informações que não estão dentro do seu nível de confiança.

Bibliografia

ANDREWS, A. A. anda Sampath Kumar Venkatachary anda L. J. B. Augmenting zero trust network architecture to enhance security in virtual power plants. In: *Energy Reports*. [S.l.: s.n.], 2022. p. 1309–1320.

ATLAM, H. F.; AZAD, M. A.; ALASSAFI, M. O.; ALSHDADI, A. A.; ALENEZI, A. Risk-based access control model: A systematic literature review. In: . [S.l.: s.n.], 2020. p. 1 – 23.

BANSAL, P. Zero trust security: Is it optional? In: . [S.l.: s.n.], 2024. v. 9, p. 3336–3339.

CHEN, X.; FENG, W.; GE, N.; ZHANG, Y. Zero trust architeture for 6g security. In: *Cornell University*. [S.l.: s.n.], 2022. (Lecture Notes in Computer Science, v. 1), p. 1–7.

COYNE, E.; WEIL, T. R. Abac and rbac: Scalable, flexible, and auditable access management. In: . [S.l.]: IEEE, 2013. v. 15, p. 14 – 16.

DUMITRU, I.-A. Zero trust security. In: . [S.l.: s.n.], 2022. v. 9, p. 99 – 104.

FATIMA, A.; GHAZI, Y.; SHIBLI, M. A.; ABASSI, A. G. Towards attribute-centric access control: an abac versus rbac argument. In: . [S.l.]: Wiley Online Library, 2016. v. 9, p. 3152 – 3166.

FERRAIOLO, D. F.; SANDHU, R.; GAVRILA, S.; KUHN, D. R.; CHANDRAMOULI, R. Proposed nist standard for role-based access control. In: *International Journal of Computer Applications*. New York, NY, USA: Association for Computing Machinery, 2001. v. 4, n. 3, p. 222–274.

FILHO, W. L. R. The role of zero trust architecture in modern cybersecurity: Integration with iam and emerging technologies. In: . [S.l.: s.n.], 2025. v. 11, p. 1–11.

FREITAS, L.; COELHO, K.; NOGUEIRA, M.; VIEIRA, A.; NACIF, J.; SILVA, E. Controle de acesso sensível ao contexto e zero trust para a segurança em e-health. In: *Anais do XLII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*. Porto Alegre, RS, Brasil: SBC, 2024. p. 770–783. ISSN 2177-9384. Disponível em: ⟨https://sol.sbc.org.br/index.php/sbrc/article/view/29834⟩.

FREITAS, L. L. do C. Zero trust como ferramenta de segurança para ambientes e-health. In: . [S.l.: s.n.], 2023. p. 1–60.

HU, V. C.; KUHN, D. R.; FERRAIOLO, D. F. Attribute-based access control. In: . [S.l.]: IEE, 2015. v. 48, p. 85–88.

JIMMY, F. Zero trust security: Reimagining cyber defense for modern organizations. In: . [S.l.: s.n.], 2022. v. 10, p. 887 – 905.

LONG, S.; YAN, L. Racac: An approach toward rbac and abac combining access control. In: . [S.l.]: IEEE, 2019. p. 1609 – 1616.

NGOC, N.; LEE, H. Contextual risk-based access control. In: . [S.l.: s.n.], 2007. p. 1 – 7.

RAJPOOT, Q. M.; JENSEN, C. D.; KRISHNAN, R. Integrating attributes into role-based access control. In: . [S.l.]: Proceedings of the 29th Annual IFIP WG 11.3 Working Conference on Data and Applications Security and Privacy, 2015. p. 242 – 249.

ROSE, S.; BORCHERT, O.; MITCHELL, S.; CONNELLY, S. Zero trust architecture. In: *National Institute of Standards and Technology*. [S.l.]: US, 2020. p. 1–50.

SAMARATI, P.; VIMERCATI, S. de Capitani di. Access control: Policies, models, and mechanisms. In: . [S.l.: s.n.], 2021. p. 137 – 197.

TEERAKANOK, S.; UEHARA, T.; INOMATA, A. Migrating to zero trust architecture: Reviews and challenges. In: *Security and Communication Networks*. [S.l.: s.n.], 2021. v. 2021, p. 1–10.

TSAI, M.; LEE, S.; SHIEH, S. W. Strategy for implementing of zero trust architecture. In: . [S.l.]: IEEE, 2024. v. 73, p. 93 – 100.

VANICKIS, R.; JACOB, P.; DEHGHANZADEH, S. Access control policy enforcement for zero-trust networking. In: . [S.l.]: IEEE, 2018. p. 1–6.

XIAO, S.; YE, Y.; KANWAL, N.; NEWE, T.; LEE, B. Sok: Context and risk aware access control for zero trust systems. In: . [S.l.: s.n.], 2022. p. 1–20.

YAO, Q.; ZHANG, X.; WANG, Q.; FEI, J. Dynamic access control and authorization system based on zero-trust architecture. In: *Journal of Computer and Communications*. New York, NY, USA: Association for Computing Machinery, 2021. v. 3, p. 123 – 127.