INSTITUTO FEDERAL
Goiano

MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL GOIANO - CAMPUS TRINDADE

MODELO DE CONTROLE DE ACESSO MULTIEMPRESA

Multi-Company access control model

Igor Rosa dos Santos [1], **Adson Silva Rocha** [2]

PALAVRAS CHAVE:

Controle de acesso;
Autorização;
Gerenciamento de Recursos;
Recursos;
Empresas;

***KEYWORDS*:**

Access Control;
Authorization;
Resource Management;
Resources;
Companies;

RESUMO: O controle de acesso é requisito essencial para sistemas que comportam usuários. A comunidade de tecnologia da informação compreende a relevância do controle de acesso. No entanto, a implementação dessa medida pode se revelar desafiadora, especialmente em contextos específicos, como em sistemas de empresas de grande porte, onde a governança de recursos é crítica. A complexidade associada à elaboração de um sistema de controle de acesso eficiente pode resultar em custos substanciais. Portanto, esse trabalho busca contribuir propondo um modelo de controle de acesso multi-empresa generalizado. Esse modelo possibilita criar sistemas com organizações interdependentes gerenciando os acessos de forma granular. Espera-se que ao final o modelo seja uma alternativa viável e simplificada para implementar sistemas que requisitam um controle de acesso em ambientes com muitas organizações.

ABSTRACT: *Access control is an essential requirement for systems that accommodate users. The information technology community understands the relevance of access control. However, the implementation of this measure can prove challenging, especially in specific contexts, such as in large-scale enterprise systems, where resource governance is critical. The complexity associated with developing an efficient access control system can result in substantial costs. Therefore, this work seeks to contribute by proposing a generalized multi-company access control model. This model enables the creation of systems with interdependent organizations managing access in a granular way. It is hoped that, in the end, the model will be a viable and simplified alternative for implementing systems that require access control in environments with multiple organizations.*

*** Contato com os autores:**

[1] **e-mail: s.igorrosa@gmail.com (I. R. Santos)**
Eng. de Computação, Graduando, Estudante, Instituto Federal Goiano, s.igorrosa@gmail.com

[2] **e-mail: adson.rocha@ifgoiano.edu.br (A. S. Rocha)**
Eng. de Computação, Doutor, Professor do Curso de Engenharia de Computação, Instituto Federal Goiano, adson.rocha@ifgoiano.edu.br

1. INTRODUÇÃO

O aumento da complexidade e especificidade dos sistemas contemporâneos destaca a necessidade premente de controles ainda mais sofisticados para a gestão de recursos sensíveis e o acesso a dados. Conforme salientado por O'Connor e Loomis (2010), a atribuição, modificação ou encerramento de permissões pode parecer trivial à primeira vista, mas é, na verdade, uma das atividades mais cruciais no âmbito do gerenciamento central da Tecnologia da Informação.

No universo dinâmico da segurança cibernética, a governança de usuários em sistemas de software desempenha um papel vital na preservação da integridade e segurança das informações. O controle de acesso, portanto, emerge como um componente fundamental, definindo políticas que autorizam e regulamentam o acesso a dados e funções sensíveis. Nas palavras de Langaliya e Aluvalu (2015), o controle de acesso aumenta a segurança de um sistema e fornece acesso predefinido aos recursos. Nesse contexto, Langaliya e Aluvalu (2015) ainda destacam que o controle de acesso é parte muito importante nos data centers de governos e empresas, pois limitam e monitoram o acesso de usuários a recursos e serviços.

No panorama atual, a comunidade dedicada ao desenvolvimento de software reconhece a importância do controle de acesso em sistemas. Entretanto, a implementação dessa medida pode se apresentar como um desafio, especialmente em cenários específicos, como nos sistemas de grandes empresas, onde a gestão eficaz dos recursos é fundamental. Para Mendes (2014), conforme os sistemas de software se tornam maiores e mais complexos, o desafio do projeto vai além das estruturas de dados e dos algoritmos de computação. Isto é, é preciso levar em conta o projeto da arquitetura (ou modelo geral) do sistema. Nesse enquadro, a complexidade associada à elaboração de um sistema de controle de acesso eficiente pode resultar em custos substanciais. Além disso, a ausência de um modelo que concilie eficiência e simplicidade pode dificultar ainda mais esse processo.

É nesse contexto desafiador que este trabalho busca contribuir, apresentando um modelo de controle de acesso multiempresa com atribuição de níveis de acesso de forma granular e hierárquica. Esse modelo busca superar as barreiras associadas à implementação desse recurso em ambientes complexos, permitindo a generalização de entidades e incorporando restrições de acesso de forma abrangente, considerando mais de uma instituição e níveis de subordinação entre entidades. Ao aliar eficiência e simplicidade, esta proposta visa oferecer uma solução adaptável e viável para os desafios enfrentados pelas organizações na gestão de acesso a recursos sensíveis em sistemas de software.

2. OBJETIVOS

Este trabalho tem como objeto desenvolver um modelo de controle de acesso capaz de satisfazer ambientes com escopo de multiempresas. Além do que, apresenta-se um esquema básico do modelo contemplando 3 entidades principais (**empresa**, **unidade**, **departamento**). Dessa forma, visa-se apresentar a implementação do modelo em um cenário que expõe como esse pode ser aplicado em ambientes multiempresas. Ao final, discute-se os resultados obtidos e a relevância para esse estudo.

3. METODOLOGIA

O presente trabalho propõe um modelo especializado de controle de acesso em ambientes multiempresas. A estrutura do artigo abrange a apresentação dos conceitos fundamentais do controle de acesso, a explanação do modelo de controle de acesso multiempresa com suas nuances teóricas e técnicas, os resultados da implementação do modelo e a conclusão.

O modelo foi efetivamente implementado e executado por meio de uma plataforma web, facilitando a verificação dos acessos dos usuários aos recursos. A tecnologia escolhida para o

desenvolvimento do front-end foi o React (REACT, 2023), uma biblioteca que agrega agilidade à implementação do modelo, proporcionando a criação de páginas web de forma eficiente. Adicionalmente, foi empregada a tecnologia Next.Js (NEXT.JS, 2023) para a integração do backend. Nesse contexto, diversas ferramentas do Next.Js foram utilizadas no projeto, incluindo o roteamento das páginas, a renderização em servidor e o carregamento otimizado, entre outros.

A infraestrutura de backend foi suportada por uma plataforma especializada chamada Supabase (SUPABASE, 2023). O Supabase (SUPABASE, 2023) oferece recursos adequados para a implementação do modelo, incluindo o Supabase Auth, uma API para gerenciamento de autenticação. Além disso, o banco de dados dessa plataforma foi empregado para a execução do modelo, utilizando o recurso de rows-level-security (RLS) para impor restrições de acesso. Portanto, esse recurso foi essencial na implementação das políticas de controle de acesso.

4. CONTROLE DE ACESSO

O termo controle de acesso refere-se a política de uma determinada organização para autorizar o acesso a determinados recursos. No cenário de desenvolvimento de software o controle de acesso é um componente fundamental do Gerenciamento de Identidade e Acesso (IAM). De acordo com Boff (2023) o Gerenciamento de Identidade e Acesso abrange uma variedade de processos, incluindo a autenticação, a autorização, o gerenciamento de identidades e o provisionamento de usuários. Nesse contexto, Mohammed (2011) destaca que IAM é o conceito que simplifica esses processos e permite o gerenciamento de acesso granular e auditoria em sistemas locais e em um sistema. Logo, compreende-se, também, as autorizações dos usuários, isto é, o que o usuário tem permissão para acessar.

4.1 AUTENTICAÇÃO E AUTORIZAÇÃO

Entende-se como autenticação o processo de verificar a identidade dos usuários, assegurando-se de que o usuário é quem afirma ser. Para Indu, Anand e Bhaskar (2018), a autenticação é um método usado para confirmar a identidade de uma pessoa ou aplicativo, assegurando se eles têm o direito de acessar ou reivindicar algo. Este processo envolve a verificação da autenticidade de uma entidade por outra. Em muitas organizações, a prática comum é solicitar um conjunto de dados do indivíduo que normalmente é o nome de usuário e senha. Sendo assim, espera-se validar a identidade do usuário. Ademais, atualmente, o mercado já se dotou de tecnologias mais avançadas, como autenticação biométrica (que utiliza varreduras de retina ou impressões digitais) e tokens de segurança (que modificam partes de senhas em intervalos regulares), também estão se tornando populares.

Por outro lado, a autorização envolve determinar as permissões de um usuário e aplicá-las em contextos com restrição de acesso baseados em atribuições. Indu, Anand e Bhaskar (2018) definem a autorização como sendo o processo que determina quais usuários ou aplicativos estão habilitados para operar em um sistema. Essa decisão é baseada nas informações de identidade do usuário ou do aplicativo. Ou seja, após a autenticação, que permite aos usuários acesse o sistema, ao validar sua identidade, a autorização entra em cena para especificar quais recursos o usuário pode acessar e quais operações ele pode realizar. Desse modo, Golightly et al. (2023) enquadra o controle de acesso como uma solução de autorização para evitar problemas relacionados à segurança de dados, cumprindo requisitos de segurança específicos para impedir o acesso não autorizado a diferentes recursos.

4.2 ESTRATÉGIAS DE AUTORIZAÇÃO

É conhecida diferentes abordagens projetadas para satisfazer a implementação de um sistema de controle de acesso. De acordo com AFTAB et al. (2022) existem diferentes modelos e mecanismos de controle de acesso, que podem ser classificados tradicionalmente em obrigatório (MAC), discricionário (DAC), baseado em funções (RBAC) ou baseado em atributos (ABAC). Langaliya e Aluvalu (2015) destacam que essas quatros abordagens são as mais tradicionais. Além das abordagens tradicionais destacam-se as muitas abordagens híbridas que nas palavras de AFTAB et al. (2022) são extensões das abordagens tradicionais.

O mecanismo de controle de acesso obrigatório (MAC) concede permissões através do sistema. Isto é, nesse mecanismo o sistema é responsável por controlar os direitos de acesso aos usuários. Nesse contexto, utiliza-se rótulos como “secreto” ou “ultrassecreto” para controlar o acesso dos usuários aos recursos. De acordo com Langaliya e Aluvalu (2015), por proporcionar maior segurança, a abordagem MAC é utilizada sobretudo em aplicações militares e governamentais. Contudo, a manutenção dos rótulos é complexa a longo prazo. Por outro lado, o mecanismo de controle de acesso discricionário (DAC) dá ao proprietário de um recurso a possibilidade de atribuir acesso a outro usuário ou a um grupo de usuários. Nesse caso, o usuário tem mais flexibilidade em controlar o acesso ao recurso. No entanto, é uma abordagem mais suscetível a falhas pela administração humana explícita.

O mecanismo de controle de acesso RBAC atribui acessos com base nos papéis dos usuários, o ABAC toma decisões com base em atributos específicos dos usuários, recursos e contexto. O RBAC é eficaz em ambientes com funções claramente definidas, enquanto o ABAC oferece flexibilidade granular, sendo mais adequado para contextos dinâmicos. A escolha entre essas estratégias depende das necessidades específicas de controle de acesso, estrutura organizacional e características do ambiente. Em alguns casos, a combinação de ambas pode ser adotada para atender a requisitos específicos de segurança.

5. MODELO DE CONTROLE DE ACESSO MULTIEMPRESA

Vista a necessidade da implementação de um mecanismo para executar políticas de controle de acesso, de forma simplificada, propõe-se um modelo baseado na estratégia RBAC ajustado para conceder permissões em organizações e suas entidades subordinadas. Isto é, nesse modelo observa-se principalmente a necessidade que se tem em gerenciar o acesso de usuários em múltiplas organizações e suas cadeias de atribuições hierarquizadas. Assim, usuários que têm permissão para acessar um recurso de uma organização devem poder executar ações e visualizar dados de acordo com seu cargo dentro desta e para além disso nos recursos subordinados.

Chama-se esse modelo de controle de acesso de multiempresa, pois é possível gerenciar o acesso na entidade raiz - o qual chama-se de empresa - e, para além disso, nas suas ramificações. Por sua vez, essas ramificações nem sempre são empresas subordinadas. Pode-se considerar, também, ramificações de uma empresa como sendo suas unidades. Ademais, as unidades podem ser dotadas, também, de ramificações: seus departamentos, por exemplo.

5.1 ESTRUTURA DO MODELO

Cada recurso representa uma organização, sendo assim, o recurso é dotado de funções, pessoas e dados. Isto é, os recursos possuem suas próprias propriedades. Para acessar as propriedades de um recurso, o usuário deve receber permissão para acesso naquele recurso. Aliás, dependendo do papel definido na permissão que o usuário recebe em um recurso, o usuário terá acesso a funções e dados restritos no

recurso. Nesse contexto, as definições de acessos para cada papel é determinado por meio das políticas de controle de acesso.

A disposição de recursos no modelo é elaborada para que todo recurso - se precisar - possua seu recurso subordinado. Ou seja, o recurso é capaz de abranger um grupo de recursos. Deste modo, usuários têm a possibilidade de acessar os recursos subordinados ou ramificações do recurso primário. Contudo, no modelo pode haver papéis que não satisfaz a possibilidade do usuário acessar os recursos subordinados. Isso é possível dado o contexto de atribuir diferentes papéis aos usuários ao definir permissões. A caraterística de atribuir papéis com acessos específicos dá-se o nome de *Controle Granular*. Além disso, a possibilidade, em alguns papéis, dos usuários acessarem os recursos subordinados dá ao modelo a característica de *Acesso Hierárquico*. A figura 1 apresenta o esquema geral dos recursos.

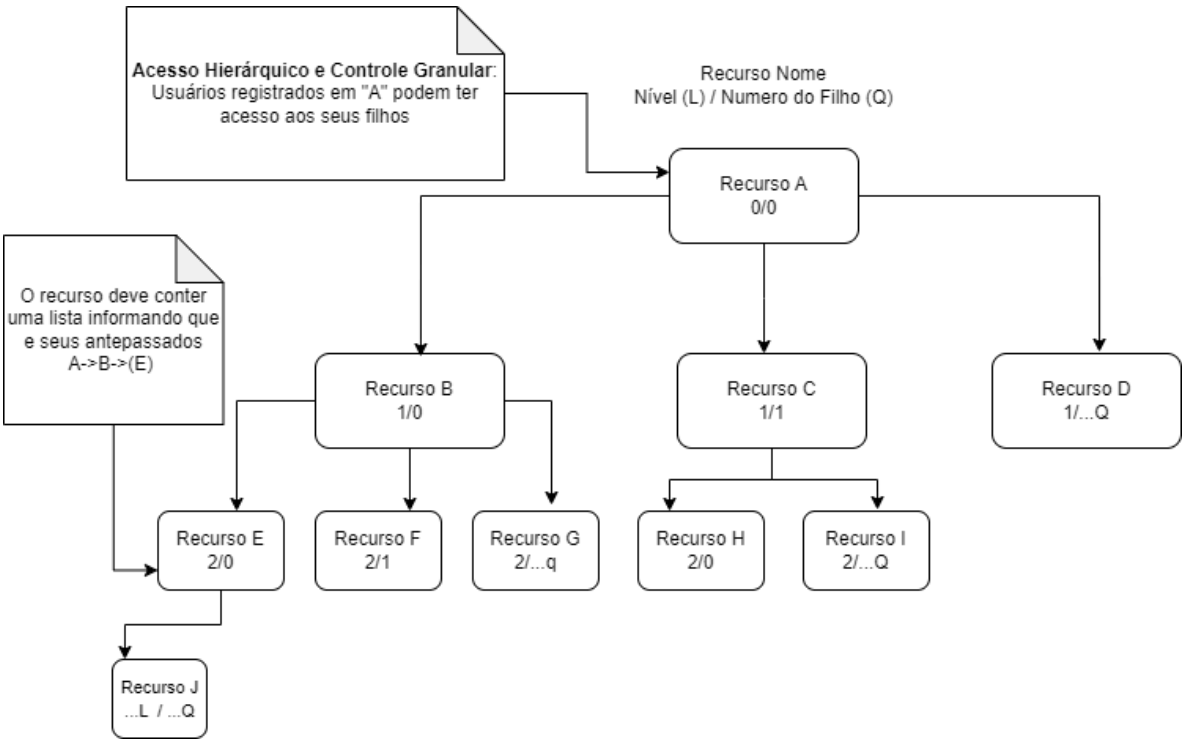

FIGURA 1: Esquema que representa as disposições dos recursos e seus relacionamentos.
FONTE: Elaborado pelos autores.

Nota-se na figura 1 o recurso “A” abrangendo vários outros recursos filhos ou ramificações. Nesse enquadro, “Q” representa o número de ramificações subordinadas incrementado ao recurso superior. Além do mais, “L” representa o nível do recurso, isto é, a cada incremento vertical é somado um nível. Desta maneira, observa-se um grafo dotado de recursos interligados hierarquicamente. Efetivamente, no cenário cujas organizações são representadas por recurso, o controle de acesso define como os usuários acessam esse sistema hierarquizado.

5.2 APLICAÇÃO

Para fins de demonstração do modelo, a terminologia **empresa**, **unidade** e **departamento** será adotada neste trabalho. Toda empresa, unidade e departamento são tipos de recursos que requerem permissões para o acesso. Os recursos são representações das entidades, que por sua vez, são os elementos centrais que demandam controle de acesso. Analogamente a figura 1, representa-se um esquema da estrutura adotada na figura 2.

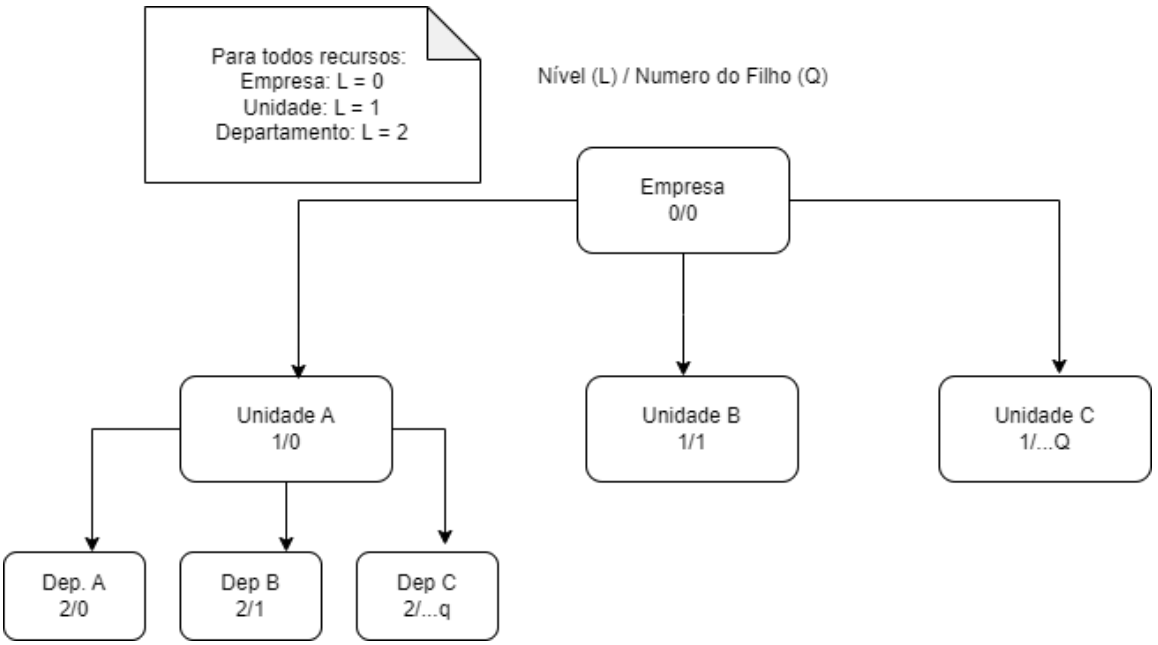

FIGURA 2: Visão conceitual do modelo de controle de acesso multi-empresa.
FONTE: Elaborado pelos autores.

Observa-se na figura 2 a aplicação da terminologia **empresa**, **unidade** e **departamento**. Nesse contexto, empresa sempre será o nível 0 da hierarquia, unidade sempre será o nível 1 e departamento sempre o nível 2. Essa terminologia busca aplicar a condição sistemática de uma empresa. As unidades representam nesse aspecto ramificações independente uma da outra, porém subordinada diretamente a empresa. Assim também se aplica o relacionamento entre departamentos subordinados à unidade.

O acesso dos usuários a empresa fica restrito àquele recurso, isso pois o recurso “empresa” não é subordinado a nenhum outro recurso, logo, não há possibilidade de um acesso de um usuário herdado de um outro recurso. Entretanto, o acesso dos usuários em “unidade” ou “departamento” pode ser atribuído através de uma permissão no recurso atual ou superior. Ademais, para acesso de dados e funções desses recursos cabe uma política de controle de acesso definida conforme os tipos de papéis.

Ao definir-se uma permissão ao usuário para ele ter acesso a um recurso, sempre deve-se atribuir um papel. O papel indica um conjunto de privilégios que o usuário tem naquele recurso e seus subordinados. O acesso a pontos sensíveis do recurso é definido na política de controle de acesso para aquele papel específico. É no tipo de papel, também, que se define quais deles podem ter acesso hierárquico no sistema, isto é, acesso aos recursos subordinados. Para nossa terminologia adotaremos 3 tipos de papéis possíveis nos recursos: **gestor**, **editor**, e **leitor**. Sendo que todos eles têm acesso aos recursos subordinados, além do atual. Cada recurso é criado por um usuário. Esse deverá ter permissão de criação de subordinados em um recurso pai.

A figura 3 apresenta um diagrama de classe que descreve a modelagem do controle de acesso multiempresa. A classe de Permissao aponta quais recursos um usuário pode acessar e quais ações ele pode executar. Através do campo “papel” que define-se qual seu nível de acesso no recurso. Por sua vez, na classe Recurso registra-se seu nível através do campo de mesmo nome (nível). Deve-se registrar para cada recurso os recursos superiores, se houver, o qual o atual é subordinado. Para isso, cada elemento criado na classe Hierarquia representa um superior do recurso atual. Isto é, o elemento de hierarquia cria a relação do recurso subordinado com recurso superior.

Efetivamente, Recurso também se dispõe do campo “ref_tabela“ que especifica qual é o tipo daquele recurso, ou seja, qual tabela (empresa, unidade ou departamentos) o recurso faz referência. Por sua vez, o atributo “nível” indica qual a posição hierárquica do recurso em relação aos seus superiores e/ou

inferiores. Um “nível” igual a 0 indica que aquele recurso é raiz e não tem níveis superiores para ele, um “nível” igual a 2 indica que não há níveis inferiores após aquele recurso.

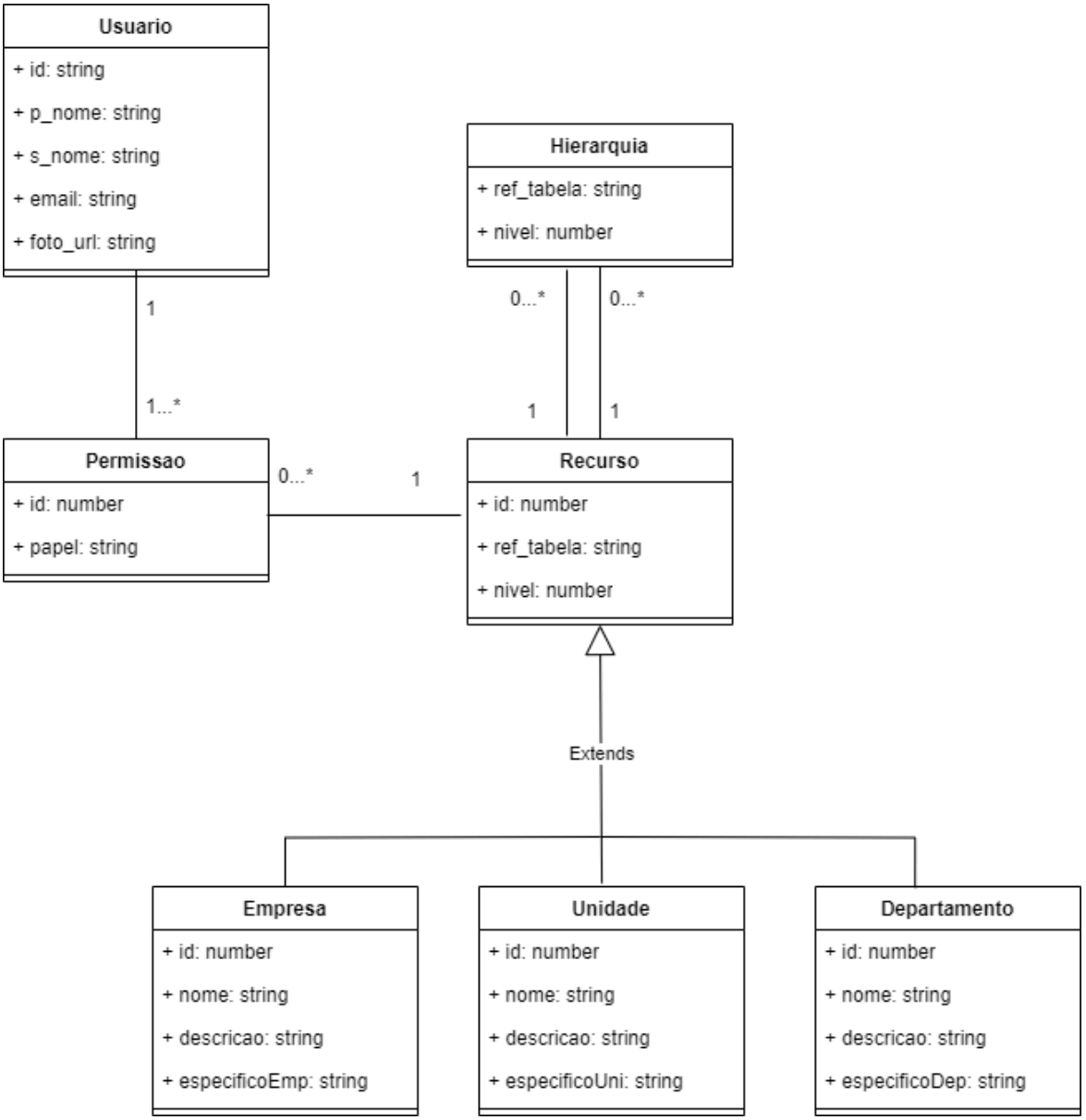

FIGURA 3: Visão conceitual do modelo de controle de acesso multi-empresa.

FONTE: Elaborado pelos autores.

Nesse cenário, as tabelas **empresas**, **unidades** e **departamentos** são necessárias pois guardam as informações específicas de cada tipo de recurso, isto é, considerando cada entidade diferente, podem haver informações distintas para serem arquivadas, por esse motivo há a herança de classes. Sendo assim, a informação específica de cada classe é representada por pelos campos “especificoEmp”, “especificoUni” e “especificoDep” para empresa, unidade e departamento respectivamente. Além disso, guardam as informações de “nome” e “descrição”.

Para fins de demonstração, o quadro 1 apresenta permissões aos usuários com base nos três cargos/papéis: *gestor*, *editor* e *leitor*. Através dos cargos que dentro dos recursos pode-se definir políticas de controle de acesso para cada um deles. A política de controle de acesso indica e define as permissões de cada cargo em relação a execução de ações do sistema e visualização de dados. Embora no modelo proposto tenham sido definidos três cargos, pode-se facilmente estender e definir outros níveis e lhes atribuir uma política de controle de acesso específica.

No presente modelo a política de controle de acesso foi ajustada para que o **gestor** detivesse maiores responsabilidades nos recursos em que foi atribuído, podendo executar tarefas críticas (como a exclusão e atribuição de outros usuários) e acessar dados sensíveis. Por conseguinte, esse nível de acesso dispõe das mesmas atribuições nos recursos subordinados. A atribuição de **editor** também executa tarefas e visualiza dados sensíveis no recurso de registro e nos subordinados. Contudo, não pode atribuir permissão em nenhum caso e nem criar novos recursos subordinados. O **leitor** tem permissão de visualizar dados triviais da organização de registro e de suas subordinadas, sem, no entanto, permissão para editar dados.

QUADRO 1: Política de controle de acesso no modelo multi-empresa

	Empresa	**Unidade**	**Departamento**
Gestor	- Editar dados ; - Excluir registro; - Atribuir e revogar permissões; - Criar unidades; - Ver dados e informações;	- Editar dados ; - Excluir registro; - Atribuir e revogar permissões; - Criar unidades;. - Ver dados e informações;	- Editar dados; - Excluir registro; - Atribuir e revogar permissões; - Criar unidades; - Ver dados e informações;
Editor	- Editar dados; - Ver dados e informações;	- Editar dados ; - Ver dados e informações;	- Editar dados; - Ver dados e informações;
Leitor	- Ver dados e informações;	- Ver dados e informações;	- Ver dados e informações;

FONTE: Elaborado pelos autores.

Nota-se que as permissões dada a cada cargo se estendem também aos recursos subordinados (unidade ou departamento) do recurso superior (empresa ou unidade) em que a permissão foi registrada. Para além disso, pode-se remodelar as políticas de controle de acesso adicionando outros cargos que não estendam suas permissões para os recursos filhos. É possível dessa forma adaptar e alinhar o esquema de acordo com a governança da empresa.

6. IMPLEMENTAÇÃO (PROVA DE CONCEITO)

Foi utilizado para a execução do modelo de controle de acesso a plataforma BaaS (Backend as a service) chamada Supabase (SUPABASE, 2023). Essa plataforma, baseada em Postgres SQL dispõe de algumas ferramentas interessantes utilizadas na implementação do modelo. Com ela, pode-se fazer todo gerenciamento de identidade usando a aplicação de autenticação. Ademais, para definir as políticas de controle de acesso usa-se uma ferramenta integrada chamada Row-Level-Security (RLS).

6.1 ROW LEVEL SECURITY (RLS)

Row Level Security (RLS) é uma ferramenta do banco de dados Postgres (POSTGRES, 2023) que controla quais usuários têm permissão para executar comandos SELECT/INSERT/UPDATE/DELETE. Nela, é possível restringir o acesso a determinadas linhas da tabela de Recursos, permitindo que o usuário (que está autenticado) só acesse um determinado dado se existir uma linha na tabela de permissões que atribui acesso para aquele usuário. Nesse contexto, o Supabase Auth (SUPABASE, 2023) é especialmente projetado

para funcionar em conjunto com o Postgres e, por consequência, com o RLS. Isso permite a criação de políticas de controle de acesso, utilizando regras SQL refinadas, chamadas *policies*, para atender a necessidades de negócios.

O controle de acesso dos recursos é gerido por meio das *policies* de RLS com regras específicas para cada linha de registro da tabela. Considerando a política de controle de acesso dada no Quadro 1, um recurso do tipo **unidade** ou **departamento** só pode ser criado se o usuário tiver o cargo de **gestor** na **empresa** ou **unidade** que recebe o recurso a ser criado. Por outra forma, a RLS executa uma consulta na tabela permissões em que deve haver uma linha que estabelece o relacionamento entre um recurso e o usuário que quer acessar o recurso como gestor.

6.2 RESULTADO DA IMPLEMENTAÇÃO

Criou-se uma empresa (E1) e dela criou-se uma unidade (U1). Da unidade criou-se um departamento (D1). Como usuários, dispõe-se de quatro pessoas (P1, P2, P3 e P4) com níveis de acesso diferentes entre os recursos (E1, U1 e D1). Essas pessoas acessaram o sistema com controle de acesso multi-empresa. Nota-se que P1 tem permissão com cargo de gestor no recurso E1, P2 tem permissão com cargo de editor em U1, P3 tem permissão com cargo de leitor em D1 e P4 não teve permissão atribuída. Obtém-se então o seguinte resultado de acesso dos recursos de acordo com o quadro 2.

QUADRO 2: Acesso e capacidades de cada pessoa em cada recurso

	E1	**U1**	**D1**
P1	- Editar dados; - Excluir registro; - Atribuir e revogar permissões; - Criar unidades; - Ver dados e informações;	- Editar dados; - Excluir registro; - Atribuir e revogar permissões; - Criar unidades; - Ver dados e informações;	- Editar dados; - Excluir registro; - Atribuir e revogar permissões; - Criar unidades; - Ver dados e informações;
P2	- Sem acesso;	- Editar dados; - Ver dados e informações;	- Editar dados; - Ver dados e informações;
P3	- Sem acesso;	- Sem acesso;	- Ver dados e informações;
P4	- Sem acesso;	- Sem acesso;	- Sem acesso;

FONTE: Elaborado pelos autores

7. CONCLUSÃO

Este estudo aborda o desafio de desenvolver um modelo de controle de acesso, que não apenas atende aos requisitos de escalabilidade e modularidade, mas também se destaca por sua simplicidade e eficiência, crucial em sistemas que exigem autenticação e autorização granulares. A solução proposta integra com habilidade elementos de hierarquia e generalização, adaptando-se a ambientes multiempresariais.

Ao contemplar as necessidades específicas de diferentes tipos de organizações, o modelo abre novos horizontes para a personalização e ajuste de permissões de acesso. Este aspecto é particularmente relevante em cenários onde os requisitos de segurança e acesso diferem substancialmente entre departamentos e unidades, isto é, há demandas distintas para esses dois tipos de recursos. A extensibilidade do modelo para incorporar um número ilimitado de níveis hierárquicos e uma variedade de cargos de usuários é uma direção interessante, permitindo uma representação mais precisa e detalhada das complexas estruturas organizacionais.

Além disso, o modelo oferece um tecnologias robustas para a implementação de políticas de segurança mais sofisticadas, alinhando-se às práticas e teorias de segurança contemporâneas. A adaptabilidade do modelo a diferentes contextos organizacionais o torna uma ferramenta versátil para o gerenciamento de acesso.

A realização de estudos de caso em ambientes multiempresariais será crucial para testar a eficácia do modelo, identificar áreas de melhoria e ajustar as políticas de controle de acesso de acordo com as necessidades reais das organizações. Esses estudos também permitirão avaliar a aplicabilidade do modelo em diferentes cenários, contribuindo para uma compreensão mais profunda de como sistemas de controle de acesso podem ser otimizados para eficiência e segurança.

Finalmente, espera-se que este trabalho não apenas forneça uma solução prática para os desafios atuais enfrentados no campo do controle de acesso em ambientes multiempresariais, mas também inspire pesquisadores e profissionais a explorar novas direções e possibilidades na concepção de sistemas de controle de acesso mais avançados e adaptáveis.

8. REFERÊNCIAS BIBLIOGRÁFICAS

AFTAB, Muhammad Umar; HAMZA, Ali; OLUWASANMI, Ariyo; NIE, Xuyun; SARFRAZ, Muhammad Shahzad; SHEHZAD, Danish; QIN, Zhiguang; RAFIQ, Ammar. **Traditional and Hybrid Access Control Models: A Detailed Survey**. Security and Communication Networks, v. 2022, 2022. Disponível em: https://doi.org/10.1155/2022/1560885. Acesso em: 23 dez. 2023.

BOFF, Giovani de Souza et al. **Serviço para gerenciamento de identidades e acessos baseado em Arquitetura Limpa e Microsserviços**. 2023.

GHAZAL, Rubina et al. **Intelligent role-based access control model and framework using semantic business roles in multi-domain environments**. IEEE Access, v. 8, p. 12253-12267, 2020

GOLIGHTLY, L. et al. **Securing Distributed Systems: A Survey on Access Control Techniques for Cloud, Blockchain, IoT and SDN**. Cyber Security and Applications, p. 100015, mar. 2023.

INDU, I.; ANAND, P.M.R.; BHASKAR, V. **Identity and access management in cloud environment: Mechanisms and challenges**. Engineering Science and Technology, an International Journal, v. 21, n. 4, p. 675-683, 2018. Disponível em: <https://doi.org/10.1016/j.jestch.2018.05.010 />. Acesso em: 23 dez. 2023.

JIN, Gangzeng et al. **Role and object domain-based access control model for graduate education information system. Procedia Computer Science**, v. 176, p. 1241-1250, 2020.JIN, Gangzeng et al. Role and object domain-based access control model for graduate education information system. Procedia Computer Science, v. 176, p. 1241-1250, 2020.

LANGALIYA, Chirag; ALUVALU, Rajanikanth. **Enhancing cloud security through access control models: A survey**. International Journal of Computer Applications, v. 112, n. 7, 2015.

MENDES, A. **Desenvolvimento de Software requer Processo e Gestão**. Revista Espaço Acadêmico, v. 11, n. 123, p. 46–57, 2014.

MOHAMMED, Ishaq Azhar. **Identity and Access Management System: a Web-Based Approach for an Enterprise**. 2011. Disponível em: < https://www.researchgate.net/publication/353887611 />. Acesso em: 23 dez. 2023

Next.js. **Docs**. Disponível em: https://nextjs.org/docs. Acesso em: 01 Jun. 2023

O'CONNOR, Alan; LOOMIS, Ross. **Economic analysis of role-based access control**. RTI International, 2010.

POSTGRESQL. Documentation: 16: 5.8. **Row Security Policies**. Disponível em: <https://www.postgresql.org/docs/current/ddl-rowsecurity.html/> Acesso em: 30 nov. 2023.

React. **Documentação do React**. Disponível em: https://react.dev/learn. Acesso em: 01 Jun. 2023

SANDHU, Ravi S. et al. Role-based access control: A multi-dimensional view. In: **Tenth annual computer security applications conference**. IEEE, 1994. p. 54-62.

SUPABASE. **Supabase**. Disponível em: <https://supabase.com/> 2. Acesso em: 30 out. 2023.

UDDIN, Mumina; ISLAM, Shareeful; AL-NEMRAT, Ameer. **A dynamic access control model using authorising workflow and task-role-based access control**. Ieee Access, v. 7, p. 166676-166689, 2019.