MODELOS DE CONTROLE DE ACESSO EM BANCOS DE DADOS NA NUVEM: UMA ANÁLISE COMPARATIVA

Felipe Silencio Silva[1]

Ieda De Oliveira[2]

Maria Beatriz Carvalho Da Silva[3]

Luciano Gonçalves De Carvalho[4]

Resumo

Este artigo tem como objetivo analisar e comparar diferentes modelos de controle de acesso em bancos de dados na nuvem, considerando o crescimento da computação em nuvem e a consequente necessidade de segurança dos dados. A justificativa para o estudo se baseia na importância de proteger a integridade, disponibilidade e autenticidade das informações armazenadas na nuvem. A metodologia adotada incluiu uma pesquisa exploratória em bases de dados como IEEE, ACM e Google Acadêmico, utilizando palavras-chave específicas para identificar literatura relevante, resultando na seleção de 16 documentos para análise detalhada. Os resultados destacam a comparação entre os modelos de controle de acesso Discricionário (DAC), Obrigatório (MAC) e Baseado em Papéis (RBAC), enfatizando suas vantagens, desvantagens e aplicabilidade em diferentes cenários. A pesquisa conclui que a escolha do modelo de controle de acesso mais adequado varia conforme as necessidades específicas de cada organização e seu perfil de risco, não havendo um modelo universalmente ideal. O estudo ressalta a importância do treinamento e da conscientização para a efetividade das políticas de controle de acesso, além de enfatizar a necessidade de adaptação contínua às evoluções da computação em nuvem. Este trabalho contribui significativamente para o campo da segurança de dados em nuvem, oferecendo insights valiosos para a implementação de estratégias de controle de acesso eficazes em diversos ambientes organizacionais.

Palavras-chave: Banco de Dados. Gestão de Acesso. Modelo. Nuvem.

Abstract

This article aims to analyze and compare different access control models in cloud databases, considering the growth of cloud computing and the consequent need for data security. The justification for the study is based on the importance of protecting the integrity, availability, and authenticity of information stored in the cloud. The adopted methodology included exploratory research in databases, such as IEEE, ACM, and Google Scholar, using specific keywords to identify relevant literature,

[1] Graduando em Análise e Desenvolvimento de Sistemas pela Fatec Mogi das Cruzes – Mogi das Cruzes/SP. Endereço eletrônico: felipe.silva403@fatec.sp.gov.br

[2] Graduanda em Análise e Desenvolvimento de Sistemas pela Fatec Mogi das Cruzes – Mogi das Cruzes/SP. Endereço eletrônico: ieda.oliveira@fatec.sp.gov.br

[3] Graduanda em Análise e Desenvolvimento de Sistemas pela Fatec Mogi das Cruzes – Mogi das Cruzes/SP. Endereço eletrônico: maria.silva263@fatec.sp.gov.br

[4] Mestre em Ciências pela Universidade de São Paulo – Mogi das Cruzes/SP. Endereço eletrônico: luciano.carvalho@fatec.sp.gov.br

resulting in the selection of 14 documents for detailed analysis. The results highlight the comparison between Discretionary (DAC), Mandatory (MAC), and Role-Based (RBAC) access control models, emphasizing their advantages, disadvantages, and applicability in different scenarios. The research concludes that the choice of the most appropriate access control model varies according to the specific needs of each organization and its risk profile, with no universally ideal model. The study underscores the importance of training and awareness for the effectiveness of access control policies, as well as emphasizing the need for continuous adaptation to the evolutions of cloud computing. This paper contributes significantly to the field of cloud data security, offering valuable insights for the implementation of effective access control strategies in various organizational environments.

Keywords: *Access Management. Database. Cloud. Models.*

1 Introdução

A evolução tecnológica trouxe consigo a computação em nuvem, uma inovação que transformou profundamente a interação de empresas e indivíduos com a Tecnologia da Informação (TI). Esta modalidade de serviço, que opera sob demanda, tem seu custo atrelado ao consumo, beneficiando desde grandes corporações até usuários individuais. A computação em nuvem visa ser global, atendendo desde o usuário que armazena documentos pessoais na web até empresas que externalizam toda sua infraestrutura de TI (Sousa et al., 2010).

No entanto, a crescente adoção da computação em nuvem, especialmente no que tange aos bancos de dados, trouxe consigo desafios significativos em termos de segurança da informação. A proteção de dados e informações, que engloba sistemas computacionais, informações eletrônicas e métodos mecânicos de armazenamento, tornou-se primordial. As propriedades de confiabilidade, integridade, disponibilidade e autenticidade são essenciais para garantir a segurança das informações (Silva e Rosa, 2017).

Dentro deste contexto, o Sistema de Gerenciamento de Banco de Dados (SGBD) assume um papel central. Estes sistemas, buscam oferecer uma visão de armazenamento e escalabilidade quase infinitos (Sousa et al., 2010). No entanto, enfrentam o desafio de provisionar recursos em um ambiente com múltiplos usuários, diversos SGBDs e grandes data centers. A gestão de acesso, que envolve medidas de controle para garantir que apenas indivíduos autorizados tenham acesso a sistemas e documentos, torna-se um pilar fundamental nesse cenário (ELMASRI E NAVATHE,2011).

Este artigo tem como objetivo apresentar e comparar diferentes modelos de controle de acesso em bancos de dados em nuvem, destacando seus pontos fortes e fracos para que seja possível tirar conclusões sobre o modelo mais eficaz para o gerenciamento de banco de dados em ambiente de nuvem.

2 Referencial teórico

2.1 Computação em Nuvem

A computação em nuvem, conforme definida pelo National Institute of Standards and Technology (NIST), é um modelo que permite um acesso conveniente e sob demanda a um conjunto compartilhado de recursos computacionais configuráveis, como servidores, armazenamento, redes, aplicações e serviços. Esses recursos podem ser rapidamente provisionados e liberados com um esforço gerencial mínimo ou interação direta com o provedor de serviços.

A evolução da computação em nuvem remonta ao final dos anos 60, com a ideia de vender poder computacional e aplicações específicas através de um modelo de negócios utilitário. No entanto, esta ideia foi abandonada na década de 70 devido às limitações tecnológicas da época. Foi apenas com a virada do milênio que o conceito de computação em nuvem foi revitalizado e começou a emergir nos círculos de tecnologia como um modelo de provisionamento de recursos computacionais e de armazenamento como serviço.

2.2 Segurança De Dados

A segurança dos dados em Sistemas de Informação (SI) é essencial, englobando a proteção de arquivos, contas e bancos de dados (BD). Este processo envolve considerar a sensibilidade dos dados, ameaças ao banco de dados e mecanismos de segurança. A conscientização dos usuários é crucial, pois eles desempenham um papel ativo na segurança dos dados, como destacado por Kruger e Kearney (2008), que enfatizam a importância de educar os usuários sobre os efeitos negativos de falhas de segurança.

A integridade e confidencialidade das informações são garantidas avaliando a sensibilidade dos dados, o que influencia o nível de acesso dos usuários. Alves (2006) ressalta a necessidade de proteger as informações para garantir a continuidade dos negócios, enquanto Sêmola (2003) destaca a importância de proteger os dados com base no seu grau de sigilo.

As vulnerabilidades nos SIs, que podem expor os sistemas a ataques, são definidas pela ISO/IEC (2004) como fragilidades que podem ser exploradas por ameaças. Os usuários frequentemente são a fonte de ameaças e vulnerabilidades, conforme observado por Furnell & Thomson (2009) e Pimenta & Quaresma (2016), destacando a necessidade de uma cultura de segurança e práticas seguras.

Em resumo, a segurança dos dados em SI é multifacetada e requer uma abordagem holística que abrange desde a educação do usuário até medidas técnicas de proteção, assegurando a integridade, confidencialidade e disponibilidade das informações.

2.3 Controle De Acesso em Banco de Dados na Nuvem

O controle de acesso em bancos de dados na nuvem é vital para a segurança das informações armazenadas. Como destacado por Hu, Ferraiolo e Kuhn, “...O controle de acesso é responsável por determinar atividades permitidas de usuários legítimos, interpondo-se a cada tentativa de acesso a um recurso no sistema. A tecnologia da informação (TI) pode implementar tais sistemas em diversos contextos e níveis.” Em ambientes de nuvem, onde os dados são acessíveis globalmente, garantir que apenas usuários autorizados tenham acesso e proteger contra intrusões não autorizadas é essencial. Assim, todas as operações devem ser rigorosamente monitoradas e verificadas.

A complexidade do controle de acesso na nuvem é acentuada devido à natureza distribuída e ao volume de dados e recursos. Srivastava e Kumar (2015) destacam a importância de se ter um "framework de controle de segurança" robusto para gerenciar tais desafios em ambientes de nuvem. Eles sugerem que um controle eficaz na nuvem deve abranger desde a segurança física dos data centers até camadas lógicas e metodológicas de segurança.

Srivastava e Kumar (2015) também enfatizam a importância do monitoramento e auditoria contínua das atividades de acesso na nuvem. Essas práticas não apenas detectam e previnem acessos não autorizados, mas também fornecem registros detalhados de atividades, essenciais para a conformidade regulatória e investigações de segurança.

Em resumo, o controle de acesso em ambientes de nuvem é uma área complexa que exige uma abordagem abrangente. A implementação eficaz de controle de acesso na nuvem, seguindo as orientações de Srivastava e Kumar (2015), protege contra ameaças externas e internas, mantendo a integridade e confidencialidade dos dados

3 Material e Métodos

A abordagem utilizada neste trabalho se baseou em uma pesquisa exploratória qualitativa, utilizando as palavras-chave “Banco de Dados”, “Gestão de Acesso”, “Modelo” e “Nuvem”, para identificar literatura relevante nas bases de dados da IEEE, ACM e Google Acadêmico. Esta estratégia foi adotada com o objetivo de obter uma visão abrangente dos modelos de controle de acesso mais eficazes para bancos de dados em nuvem.

Para a seleção dos artigos, estabelecemos critérios que incluíam relevância para o tema central, qualidade acadêmica (avaliada pelo impacto e citações do trabalho), e atualidade, priorizando estudos publicados nos últimos cinco anos. A busca foi realizada no dia 13 de agosto de 2023, resultando na identificação de 14 trabalhos considerados relevantes.

Posteriormente, foi adotada uma abordagem de análise de conteúdo qualitativa, na qual os elementos-chave de cada modelo de acesso e métodos de gestão foram extraídos, categorizados e comparados. Esta análise permitiu-nos responder à pergunta de pesquisa, destacando as características, vantagens e limitações de cada modelo.

4 Modelos De Controle De Acesso

Os principais modelos de controle de acesso aplicados a banco de dados em nuvem e que serão abordados neste trabalho são: discricionário, obrigatório, acesso baseado em papéis, segurança baseada em rótulos e controle de acesso em nível de linha.

4.1 Modelo De Controle De Acesso Discricionário

O controle de acesso discricionário (discretionary access control - DAC) é um modelo de acesso com concessão e revogação de privilégios, o usuário que cria um objeto no banco de dados tem todos os privilégios sobre o objeto. O SGBD monitora os privilégios, as revogações e o administrador, que tem autorização para conceder privilégios a outros usuários com operações para leitura, alteração ou exclusão do objeto.

Apesar de ser um modelo acesso muito flexível e eficaz, se destaca como ponto negativo a vulnerabilidade. De acordo com Ramakrishnan e Gehrke (2008) este tipo de modelo está suscetível a esquemas tipo cavalo de Tróia, onde um usuário não autorizado pode enganar usuários privilegiado e ter acesso a dados sensíveis ou sigilosos.

Segundo Elmasri e Navathe (2011, p. 570), as técnicas de controle de acesso discricionário, concedendo e revogando privilégios em relações, tem sido a maneira tradicionalmente utilizada como mecanismo de segurança em sistemas de banco de dados relacional. Porém para algumas aplicações é necessário incorporar uma política de segurança adicional para classificar objetos e usuários de acordo com o nível de segurança.

4.2 Modelo De Controle De Acesso Obrigatório

O Controle de Acesso Obrigatório (Mandatory Access Control—MAC) trata das brechas no controle de acesso discricionário e ter por base a classificação de sujeitos, que são usuários e programas, e objetos, que são tabelas, linhas e colunas.

Cada sujeito no sistema possui um nível de habilitação e cada objeto possui um nível de classificação que pode ser definida a partir de 4 níveis de sensibilidade, definidas com: Não-Classificado, Confidencial, Secreto e Ultrassecreto.

Para Ramakrishnan e Gehrke (2008, p. 600) o controle de acesso obrigatório é baseado em políticas em nível de sistema que não podem ser alteradas por usuários individuais. Desta forma cada objeto do banco de dado está atribuído a uma classe de segurança e a liberação de usuários é compatível com uma dessas classes de segurança que são organizadas da classe mais segura para a menos segura.

Uma característica deste modelo são as regras para que usuários possam realizar leitura e gravação de dados no BD, de forma a garantir que dados sensíveis sejam compartilhados com usuários que não deveriam ter acesso.

O SGBD define se determinado usuário pode ler ou gravar certo objeto, com base em certas regras que envolvem o nível de segurança do objeto e a liberação do usuário. Essas regras procuram garantir que dados sigilosos nunca possam ser “passados” para um usuário sem a liberação necessária. O padrão SQL não inclui nenhum suporte para controle de acesso obrigatório. (RAMAKRISHNAN; GEHRKE, 2008, p. 600)

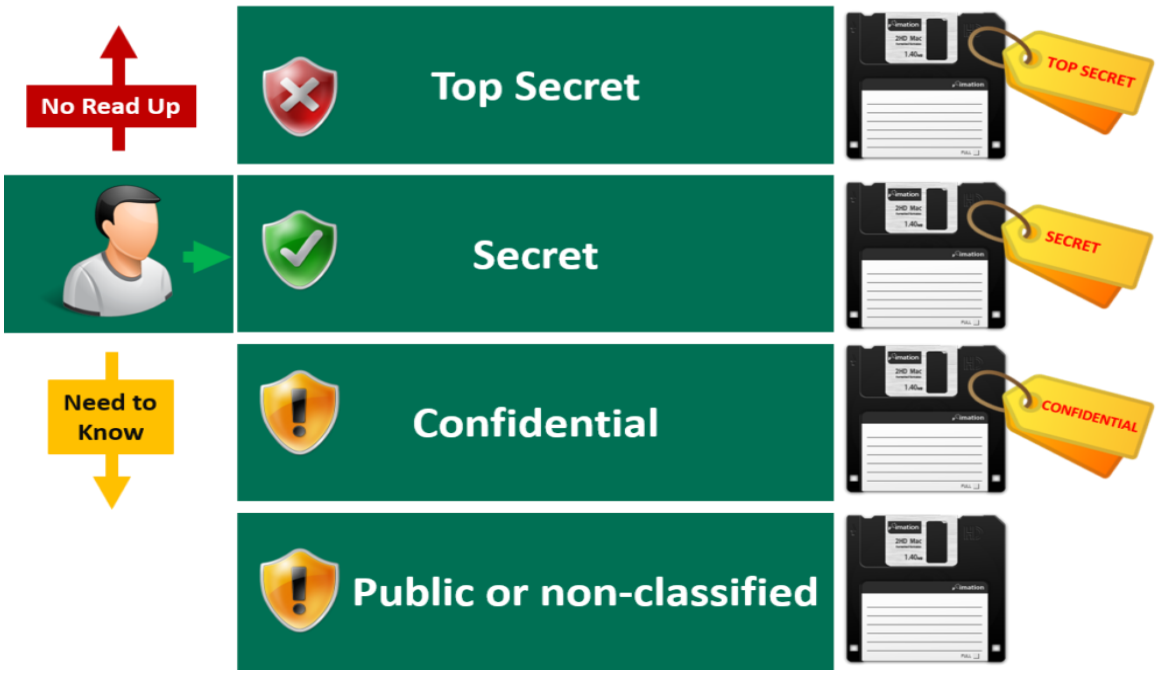
O modelo mais comum de controle de acesso obrigatório chamado modelo de Bell-LaPadula determina duas restrições em todas as leituras e gravações de objetos do banco de dados.

A primeira restrição, denominada de propriedade de segurança simples, indica que um sujeito poderá ter o acesso para leitura, somente se a classe do sujeito foi inferior ou igual a classe do objeto (figura 1). A segunda restrição, denominada de propriedade estrela, está relaciona a permissão de gravar o objeto (figura 2), onde o sujeito poderá realizar a ação somente se a classe do sujeito for superior ou igual a classe do objeto.

Elmasri e Navathe (2011, p. 571) afirmam que a primeira restrição é intuitiva e impõe a regra óbvia de que nenhum sujeito pode ler um objeto cuja classificação de segurança é maior do que a autorização de segurança do sujeito. A segunda restrição é menos intuitiva. Ela proíbe um sujeito de gravar um objeto em uma classificação de segurança inferior do que a autorização de segurança do sujeito.

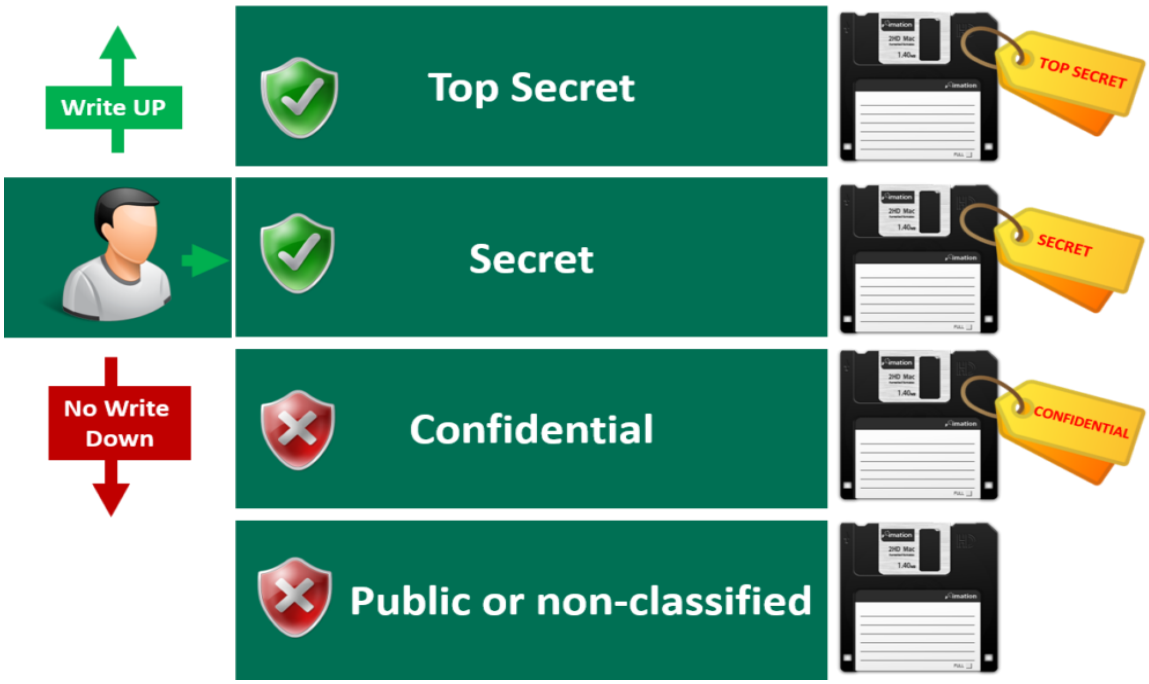
ISSN: 2595-5942

Figura 1 - segurança simples



Fonte: DONDONA, Daniel. 2020. Disponível em: <https://danieldonda.com/modelo-de-seguranca-biba/>. Acesso em: 12 dez. 2023.

Figura 2 - segurança estrela



Fonte: DONDONA, Daniel. 2020. Disponível em: <https://danieldonda.com/modelo-de-seguranca-biba/>. Acesso em: 12 dez. 2023.

A maior diferença do controle de acesso obrigatório em comparação com o controle de acesso discricionário está no controle de segurança proposto para o objeto, uma vez que no modelo discricionário a segurança está direcionada apenas aos usuários e no modelo de acesso obrigatório tanto o objeto quanto o sujeito possuem níveis de segurança.

O DAC por ter muita flexibilidade e ser mais fácil para escolha entre segurança e aplicabilidade, tem utilização em situações mais práticas e é indicado quando se tem uma grande variedade de domínios de aplicação. O MAC, por possuir um alto nível de segurança se aplica em poucos ambientes, como aplicações militares, organizações governamentais e de inteligência.

4.3 Modelo De Controle De Acesso Baseado Em Papéis

O conceito de controle de acesso baseado em papéis (role-based access control - RBAC) apareceu junto com os primeiros sistemas computacionais multiusuários interativos e está baseado em papéis que se aplicam por toda a empresa e permite o gerenciamento e segurança para sistemas de grande escala.

Ao invés de permissões individuais por usuário (utilizadas nos modelos DAC e MAC) no modelo de controle de acesso baseados em papéis, os privilégios são associados a papéis organizacionais e vários usuários podem ser atribuídos aos papéis. Por exemplo, uma empresa pode ter papéis como gerente de conta de vendas, agente de compras, funcionário de entrega, gerente de dependência, e assim por diante (ELMASRI; NAVATHE, 2011 p. 571).

O RBAC permite a facilidade de associar usuários a um mesmo grupo e dar permissão para objetos através dos grupos ao invés de permitir individualmente cada usuário. Para Ackermann (2003) a principal característica de uso de papéis é a flexibilidade, que provê para a administração de grandes números de privilégios em objetos, reduzindo o esforço para definir e administrar políticas de segurança complexas.

Para Baldwin (1990), um papel está definido pelo conceito de domínio de proteção nomeado (NPD). Neste modelo, um papel é uma explícita representação de uma coleção de privilégios que estão definidos e usados pelos administradores de sistemas e usuários e de acordo com Elmasri e Navathe (2011, p.572) os privilégios

de segurança comuns a um papel são concedidos ao nome dele, e qualquer indivíduo designado para esse papel automaticamente teria esses privilégios concedidos.

A separação de tarefas, importante na maioria dos SGBDs comerciais, impede que um usuário realize o trabalho que requer o envolvimento de duas ou mais pessoas. No RBAC o método de exclusões de papéis é responsável pela separação de tarefas. Dois papéis são considerados mutuamente exclusivos se ambos não puderem ser usados simultaneamente pelo usuário (ELMASRI; NAVATHE, 2011 p. 573).

Existem dois tipos de exclusões múltiplas, exclusão em tempo de autorização (estática) e exclusão em tempo de execução (dinâmica) (ELMASRI; NAVATHE, 2011 p. 573). A primeira o usuário não pode ter autorização, ao mesmo tempo, a dois papéis que foram especificados como exclusivos. Enquanto no segundo tipo, o usuário pode ter autorização a dois papéis exclusivos, mas os papéis não podem ser ativados pelo usuário ao mesmo tempo.

A hierarquia de papéis de acordo com Elmasri e Navathe (2011, p.573) é um modo natural de organizar papéis para refletir as linhas de autoridade e responsabilidade da organização. Por convenção, os papéis júniores no final estão conectados a papéis progressivamente sênior à medida que um deles sobe na hierarquia. Sendo assim, quando um usuário tem autorização de um papel, automaticamente tem autorização a papéis inferiores da hierarquia.

Outro fator importante no RBAC está relacionado as possíveis restrições temporais que podem existir nos papéis, como tempo e duração da ativação dos papéis e a ativação temporária de um papel quando ativado por outo papel.

Elmasri e Navathe (2011, p. 573) destacam que os papéis podem ser designados a tarefas de fluxo de trabalho, de modo que um usuário com qualquer um dos papéis relacionados a uma tarefa pode ser autorizado a executá-la e pode desempenhar certo papel somente por determinada duração. O modelo RBAC conta com os recursos que não constam nos modelos DAC e MAC, como, neutralidade de política e melhor suporte para gerenciamento e administração de segurança. A utilização mais comum é para desenvolvimentos de aplicações seguras na web. O RBAC oferece mecanismos para resolver as questões de segurança relacionadas à execução de tarefas e fluxos de trabalho, e para especificar políticas definidas pelo usuário e específicas da organização. (ELMASRI; NAVATHE, 2011 p. 573).

4.4 Modelo De Segurança Baseada Em Rótulos E Controle De Acesso Em Nível De Linha

O controle de acesso em linha oferece mais detalhamento de segurança uma vez cada linha do dado recebe um rótulo que armazena a informação, ao invés das tabelas ou colunas, os rótulos são para impedir que usuários não autorizados tenham acesso à informação. Se esse rótulo não for dado a uma linha, um rótulo de linha é automaticamente atribuído a ele, dependendo do rótulo de sessão do usuário (ELMASRI; NAVATHE, 2011 p. 574).

O administrador pode definir políticas de rótulos de segurança para que sempre que um dado é acessado. Quando uma política é implementada, uma nova coluna é acrescentada a cada linha no esquema. A coluna adicionada contém o rótulo para cada linha que reflete a sensibilidade da linha quanto à política (ELMASRI; NAVATHE, 2011 p. 574). Para um usuário acessar o conteúdo da linha, a identidade do usuário é comparada com o rótulo da linha, os requisitos de segurança do rótulo são aplicados sob os requisitos do DAC, desta forma o usuário precisa atingir os requisitos do DAC e em seguida atingir os requisitos da segurança do rótulo.

Conforme Elmasri e Navathe (2011, p.574) os requisitos do DAC garantem que o usuário é legalmente autorizado a executar essa operação no esquema. Nem todas as aplicações utilizam a segurança baseada em rótulos, para a maioria a proteção DAC é suficiente. Geralmente as políticas de segurança são criadas por gerentes ou responsáveis do setor de recursos humanos, por serem consideradas de alto nível e não dependem diretamente da tecnologia. Elmasri e Navathe (2011, p. 574) explicam que as políticas são um resultado das instruções da gerência para especificar procedimentos organizacionais, princípios de orientação e cursos de ação considerados ágeis, prudentes ou vantajosos. Tais políticas costumam ser acompanhadas por uma definição de penalidades e contramedidas se a política for transgredida.

5 Resultados e Discussão

A escolha de um modelo de controle de acesso adequado é fundamental para garantir a segurança dos dados em ambientes de nuvem. A norma ISO/IEC 27017

fornece diretrizes específicas sobre controles de segurança para serviços de computação em nuvem, destacando a importância de gerenciar e controlar o acesso a recursos na nuvem. Esta norma reforça a necessidade de se adotar um modelo de controle de acesso que esteja alinhado com as necessidades e o perfil de risco da organização. Os modelos de controle de acesso variam consideravelmente em termos de complexidade, segurança e flexibilidade. Na tabela a seguir, discutimos os quatro modelos mais comuns, suas vantagens, desvantagens e aplicabilidade:

Tabela 1 - Comparação entre os quatro modelos de controle de acesso mais comuns: vantagens, desvantagens e aplicabilidade.

Modelo	Vantagens	Desvantagens	Aplicabilidade	Referências
Discricionário	É um modelo flexível, onde o controle é majoritariamente nas mãos do proprietário do recurso.	Ele é vulnerável a ameaças provenientes de atores internos, pois depende do discernimento dos usuários.	É mais adequado para startups e pequenas empresas, onde a estrutura organizacional é menos complexa e a necessidade de flexibilidade é maior.	ELMASRI, Ramez; NAVATHE, Shamkant B. **Sistemas de Banco de Dados.** 6.ed. São Paulo: Pearson, 2011, p. 567
Obrigatório	É um modelo altamente seguro, baseando-se principalmente em classificações predefinidas.	Sua natureza restritiva pode dificultar a colaboração entre diferentes departamentos ou unidades.	Ideal para organizações que estão sob regulamentações rigorosas e necessitam de um controle estrito sobre o acesso a dados.	ELMASRI, Ramez; NAVATHE, Shamkant B. **Sistemas de Banco de Dados.** 6.ed. São Paulo: Pearson, 2011, p. 570 - 571).
Baseado em rótulos	Une segurança e uma flexibilidade controlada, tendo uma hierarquia clara de acessos.	Pode ser um desafio gerenciar, especialmente em organizações maiores com muitos rótulos e classificações.	Organizações que lidam com informações sensíveis e necessitam de uma estrutura clara de controle são as mais beneficiadas por este modelo.	ELMASRI, Ramez; NAVATHE, Shamkant B. **Sistemas de Banco de Dados.** 6.ed. São Paulo: Pearson, 2011, p. 584)
Baseado em Papéis	Altamente escalável e baseado em funções organizacionais.	Sua implementação pode ser complexa, necessitando de uma compreensão clara das funções e responsabilidades.	Empresas de médio e grande porte, onde as funções são bem definidas, se beneficiam mais deste modelo.	ELMASRI, Ramez; NAVATHE, Shamkant B. **Sistemas de Banco de Dados.** 6.ed. São Paulo: Pearson, 2011, p.572 - 573)

Fonte: Elaborado pelo autor.

Em conclusão, a escolha do modelo de controle de acesso não é trivial e deve ser feita após uma avaliação cuidadosa das necessidades e perfil de risco da organização. A norma ISO/IEC 27017 serve como um guia útil neste processo, reforçando a importância de um controle de acesso robusto em ambientes de nuvem. Além disso, é essencial considerar a abordagem estruturada, ágil e elástica para a segurança em nuvem, destacada no documento 'Congresso Internacional Software Livre e Governo Eletrônico III CONSEGI'. Esta abordagem enfatiza a necessidade de proteção e segurança dos serviços e dados, em conformidade com padrões nacionais e internacionais. A resiliência operacional e a segurança como serviço são conceitos cruciais no contexto de controle de acesso, pois um modelo robusto deve ser capaz de se adaptar e responder a ameaças e mudanças no ambiente de segurança. Portanto, ao escolher um modelo de controle de acesso, é fundamental considerar como eles se integram em uma estratégia de segurança mais ampla, incluindo a capacidade de se adaptar a padrões de segurança em evolução, garantindo a segurança dos dados em ambientes de nuvem de forma eficaz e em conformidade com as expectativas regulatórias e de segurança.

Considerações Finais

A evolução da computação em nuvem trouxe consigo uma série de vantagens, desde escalabilidade até a redução de custos operacionais. No entanto, com esses benefícios, surgiram desafios significativos, especialmente no que diz respeito à segurança dos dados.

O controle de acesso é um componente fundamental para garantir a integridade, disponibilidade e autenticidade das informações armazenadas na nuvem. Ao longo deste artigo, exploramos diferentes modelos de controle de acesso, cada um com suas próprias vantagens e desvantagens.

O modelo discricionário, por exemplo, oferece flexibilidade, mas pode ser vulnerável a ameaças internas. Por outro lado, o modelo obrigatório, embora mais seguro, pode ser percebido como restritivo em ambientes dinâmicos. Já o modelo baseado em papéis, que se concentra em funções e responsabilidades, é escalável, mas sua implementação pode ser desafiadora.

A escolha do modelo adequado depende em grande parte do tipo de organização, da natureza dos dados e das regulamentações específicas a que uma empresa pode estar sujeita. Além disso, é essencial que as organizações não apenas escolham o modelo correto, mas também invistam em treinamento e conscientização para garantir que as políticas de controle de acesso sejam efetivamente implementadas e seguidas.

Em última análise, à medida que a computação em nuvem continua a evoluir e a se tornar ainda mais integrada em nossas operações diárias, a necessidade de gestão de acesso robusta e eficaz aumentará. As organizações devem, portanto, ser proativas, não apenas em sua seleção de modelos de controle de acesso, mas também em sua abordagem geral à segurança na nuvem.

Referências Referências

ACKERMANN, Marcelo A. **Aderência de Controles de Acesso em SGBDs Relacionais às Políticas de Segurança de Aplicações**. 2003. 117 f. Dissertação (Mestrado em Ciência da Computação) – Programa de Pós-graduação em Ciência da Computação, Universidade Federal de Santa Catarina, Florianópolis, 2003. Disponível em: <https://repositorio.ufsc.br/bitstream/handle/123456789/85913/203180.pdf?sequence=1>.

BALDWIN R. W. **Naming and Grouping Privileges to Simplify Security Management in Large Databases**. in Proceedings of 1990 IEEE Symposium on Research in Security and Privacy, IEEE Computer Society Press, May 1990.

BREITMAN, Karin; VITERBO, Jose; MARTINS, Adriano; TUJAL, Luis Claudio Pereira; SOARES, Luiz Fernando Gomes. Amãpytuna Computação em Nuvem: serviços livres para a sociedade do conhecimento. III Congresso Internacional Software Livre e Governo Eletrônico, p. 174, 2010.

DONDA, Daniel. Modelo de Segurança Biba. Disponível em: https://danieldonda.com/modelo-de-seguranca-biba/. Acesso em: 11 de dez.2023.

ELMASRI, Ramez; NAVATHE, Shamkant B. **Sistemas de Banco de Dados.** 6.ed. São Paulo: Pearson, 2011.

FURNELL, S., THOMSON, K.-L. (2009). **From Culture to disobedience: recognising the varying user acceptance of IT security**. Computer Fraud & Security, 2009.

GIURI, Luigi; IGLIO, Pietro. **Role templates for content-based access control**. Proceedings of the second ACM workshop on Role-based access control. November 1997.

ISO/IEC. ISO/IEC 13335-1:2004 - Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management. [S.l.], 2004.

KRUGER, A. Hennie; KEARNEY, W. D. (2008). **Consensus Ranking - An ICT security awareness case study.** Computers & Security. p. 1-7, 9 nov. 2021.

QUARESMA, Rui Filipe Cerqueira. A segurança dos sistemas de informação e o comportamento dos usuários. **Journal Of Information Systems and Technology Management**, [S.L.], v. 13, n. 3, p. 1-20, 30 dez. 2016. TECSI.

RAMAKRISHNAN, Raghu; GEHRKE, Johannes. **Sistema de gerenciamento de banco de dados**. 3ª ed. São Paulo: Editora McGraw-Hill, 2008.

R. C. SOUSA, Flávio; O. MOREIRA, Leonardo; F. DE MACÊDO, José Antônio; C. MACHADO, Javam. Gerenciamento de Dados em Nuvem: Conceitos, Sistemas e Desafios. Gerenciamento de Dados em Nuvem: Conceitos, Sistemas e Desafios, **Universidade Federal do Ceará (UFC)**, p. 1-40, 2012.

R. C. SOUSA, Flávio; O. MOREIRA, Leonardo; F. DE MACÊDO, José Antônio; C. MACHADO, Javam. QUALITY OF SERVICE FOR DATABASE IN THE CLOUD. **Departament of Computer Science, Federal University of Ceara**, p. 1-6, 2021.

SILVA, Thaynára; ROSA, Paulo Roberto. SEGURANÇA EM BANCO DE DADOS. **Instituto Federal de Educação, Ciência e Tecnologia de São Paulo**, Presidente Epitácio, p. 1-7, 3 nov. 2021.

WORKMAN, M., BOMMER, W. H., & STRAUB, D. (2008). **Security lapses and the omission of information security measures: A threat control model and empirical test**. Computers in Human Behavior.

SRIVASTAVA, Harshit; KUMAR, Sathish Alampalayam. **Control Framework for Secure Cloud Computing.** Journal of Information Security. p. 12-23, jan. 2015. Disponível em: < https://www.scirp.org/journal/paperinformation?paperid=52951> Acesso em: 12 de dez.2023.