Faculdade de Tecnologia Adib Moisés Dib

Implementação de RBAC no SAP: Estudo de Caso

Amanda Moreira da Silva
Isabela Soeltl Borges
Yasmin Monteiro dos Santos Sousa
Esp. Anderson Valentino Bozzo

RESUMO

Este estudo nasce da necessidade de olhar para a segurança digital além das barreiras técnicas, focando na proteção do coração das grandes empresas: o sistema ERP. O objetivo central é analisar como a transição para o modelo de Controle de Acesso Baseado em Papéis (RBAC) transforma a segurança em um ambiente SAP, utilizando como base a experiência real de uma empresa do setor de tecnologia. Para atingir este objetivo, adotou-se uma abordagem pragmática, associando a revisão teórica ao estudo de caso qualitativo. Na discussão, fica evidente que o antigo modelo de gestão manual gerava um "emaranhado" de permissões excessivas, criando riscos de fraudes e falhas de conformidade com a LGPD. Os resultados mostram que ao adotar o RBAC, a organização deixou de lado o caos das autorizações individuais para adotar uma governança inteligente, baseada em funções de negócio. Essa mudança não apenas reduziu as vulnerabilidades internas ao aplicar o Princípio do Mínimo Privilégio, mas também trouxe agilidade operacional e uma estrutura muito mais transparente e segura para os dados da companhia.

Palavras-chave

Controle de Acesso Baseado em Papéis. ERP. LGPD. SAP. Segurança da Informação.

ABSTRACT

This study arises from the need to look at digital security beyond technical barriers, focusing on protecting the heart of large companies: the ERP system. The central objective is to analyze how the transition to the Role-Based Access Control (RBAC) model transforms security in an SAP environment, using as a basis the real experience of a company in the technology sector. To achieve

this objective, we developed a pragmatic approach, combining a theoretical review with a qualitative case study. In the discussion, it becomes clear that the old manual management model generated a "tangle" of excessive permissions, creating risks of fraud and failures to comply with the LGPD. The results show that by adopting RBAC, the organization put aside the chaos of individual authorizations to adopt intelligent governance, based on business functions. This change not only prevented international vulnerabilities by applying the Principle of Least Privilege, but also brought operational agility and a much more transparent and secure structure for the company's data.

Keywords

Role-Based Access Control. ERP. LGPD. SAP. Information Security.

INTRODUÇÃO

Este artigo apresenta os resultados e discussões decorrentes da pesquisa realizada para atender aos requisitos do Trabalho de Conclusão de Curso da Fatec SBC.

O objetivo geral deste projeto é analisar um caso de aplicação do modelo RBAC (*Role-Based Access Control*) em um sistema SAP de uma empresa de tecnologia, a fim de apresentar sua relevância prática como mecanismo de garantia e aprimoramento da segurança da informação.

A importância deste estudo decorre da necessidade de fortalecer a segurança de sistemas corporativos, que concentram dados essenciais para as organizações, além de examinar, na prática, como a aplicação do modelo RBAC pode gerar benefícios concretos para a proteção de informações confidenciais.

Este projeto respalda-se nos Objetivos de Desenvolvimento Sustentável (ODS) propostos pela Organização das Nações Unidas, especificamente ao ODS 16 (Paz, Justiça e Instituições Eficazes), que aponta a importância de estimular instituições responsáveis e transparentes.

FUNDAMENTAÇÃO TEÓRICA

Em sua essência, um ERP (*Enterprise Resource Planning* ou Planejamento de Recursos Empresariais) é uma solução de software criada para eliminar as barreiras de informação que tradicionalmente fragmentam as empresas, integrando todos os processos de negócio em um único repositório de dados e uma única fonte confiável (IBM, 2025).

Dentro deste universo, a solução criada pela empresa alemã SAP SE (*Systeme, Anwendungen und Produkte in der Datenverarbeitung Societas Europaea*) consolidou-se como o padrão de excelência e líder indiscutível de mercado, especialmente em médias e grandes corporações. Com uma história que datam em 1972, a SAP foi pioneira no conceito de software

empresarial integrado em tempo real, progredindo de suas primeiras versões para mainframe (SAP R/1 e R/2) até as modernas plataformas cliente-servidor e em nuvem, como o SAP S/4HANA (SAP, 2025).

A arquitetura do SAP ERP é fundamentalmente modular, porém, sua genialidade reside na integração nativa entre esses módulos. Cada módulo é desenhado para atender a uma área de negócio específica — como o *Financial Accounting* (FI) para a contabilidade, o *Materials Management* (MM) para a gestão de estoques e suprimentos, ou o *Sales and Distribution* (SD) para o ciclo de vendas.

Por essa razão, a gestão do acesso ao SAP transcende a esfera da administração de tecnologia da informação e se eleva a um pilar da segurança estratégica e da governança corporativa (Gonçalves, Silva, Almeida, 2020). Uma gestão de permissões inadequada neste ambiente não representa apenas uma falha técnica, mas uma vulnerabilidade direta ao coração do negócio, com potencial para causar fraudes financeiras, vazamentos de dados sensíveis, violando regulamentações como a Lei Geral de Proteção de Dados Pessoais (LGPD), paralisação de operações e danos irreparáveis à reputação da empresa.

Para guardar os ativos de informação que residem em seu núcleo, o sistema SAP foi concebido com um modelo de autorização nativo extremamente poderoso e granular. A segurança é erguida sobre a combinação de três elementos conceituais, que funcionam como os "blocos de construção" do acesso.

As transações representam a porta de entrada para a execução de uma tarefa no sistema. São códigos alfanuméricos (ex: ME21N para criar um pedido de compra, FB01 para lançar um documento contábil) que dão ao usuário a capacidade de iniciar uma atividade de negócio específica. Em termos simples, a transação define o que o usuário pode tentar fazer (SAP Help, 2025).

Já os objetos de autorização são os mecanismos de verificação (*checkpoints*) que atuam dentro das transações. Eles permitem um controle de acesso contextual e detalhado, respondendo não apenas o que o usuário faz, mas sobre quais dados e de que forma. Por exemplo, um usuário pode ter acesso à transação de relatório de vendas, mas um objeto de autorização pode restringir sua visão apenas aos dados de uma filial específica (Centro de Custo ou Organização de Vendas) e permitir apenas a atividade de "Exibir", bloqueando as de "Criar" ou "Modificar" (SAP Help, 2025).

Por sua vez, os perfis de autorização são as estruturas técnicas que agregam um conjunto de objetos de autorização com seus valores preenchidos (ex: permissão para a atividade '03 - Exibir'

no objeto 'F_BKPF_BUK' para a Empresa '1000'). São estes perfis que, ao serem atribuídos ao registro mestre de um usuário, efetivamente concedem as permissões no sistema (SAP Help, 2025).

Teoricamente, essa arquitetura granular oferece a flexibilidade para construir um ambiente de segurança perfeitamente alinhado ao princípio do mínimo privilégio. Contudo, na prática, a gestão manual e reativa desses "blocos" sem uma estratégia de governança bem definida transforma essa fortaleza em um labirinto complexo e vulnerável (Brown, 2018).

O Excesso de Privilégios (*Privilege Creep*) ocorre quando os usuários, ao longo do tempo, acumulam permissões que excedem em muito as necessidades de suas funções atuais. Por conveniência ou urgência, é comum que o acesso de um novo colaborador seja copiado do perfil de um colega mais antigo ou de um gestor, concedendo-lhe privilégios desnecessários "por precaução". Da mesma forma, em promoções ou transferências de área, as permissões antigas raramente são revistas e revogadas. Essa prática cria uma superfície de ataque interna perigosamente ampla, aumentando o risco de erros operacionais e de ações maliciosas. (Gillis e Rosencrance, 2024).

A gestão ineficiente de acessos em um modelo granular e individualizado é um processo reativo, manual e intensivo em mão de obra. A equipe de TI ou de segurança SAP é inundada por solicitações pontuais para criar, modificar e remover acessos, resultando em longos prazos de atendimento. A demora para liberar as permissões de um novo funcionário impacta sua produtividade, enquanto o atraso na revogação do acesso de um colaborador desligado representa uma falha de segurança crítica (Lima e Oliveira, 2019). Essa ineficiência não apenas gera custos operacionais, mas também introduz atritos nos processos de negócio.

A Segregação de Funções é um princípio basilar de controle interno que visa prevenir fraudes e erros, garantindo que nenhum indivíduo possua autoridade para executar etapas conflitantes de um processo crítico (por exemplo, criar um fornecedor, aprovar a fatura deste fornecedor e autorizar o seu pagamento). Em um ambiente onde os perfis de acesso são criados e atribuídos de forma fragmentada e sem uma visão holística, torna-se extremamente difícil identificar e mitigar conflitos de SoD (*Segregation of Duties*) (Singh *et al*., 2019). A concessão de acessos tóxicos pode passar despercebida por anos, expondo a organização a riscos financeiros, operacionais e de conformidade.

Diante do cenário de complexidade, ineficiência e risco apresentado pela gestão granular de acessos em sistemas SAP, emerge a necessidade de uma abordagem metodológica que substitua o caos reativo por uma governança estratégica. A solução consolidada na indústria da segurança da informação para este desafio é o Controle de Acesso Baseado em Papéis, ou RBAC (do inglês,

Role-Based Access Control). Este modelo propõe uma mudança de paradigma fundamental: em vez de gerenciar permissões para cada usuário individualmente, a organização gerencia permissões para papéis (*roles*), que por sua vez são atribuídos aos usuários (Fortinet, 2025).

Formalizado em 1992 por David Ferraiolo e Rick Kuhn e publicado pelo NIST (*National Institute of Standards and Technology)*, surgiu como uma alternativa para reduzir a complexidade da administração de segurança em grandes redes e ambientes organizacionais, tornando-se um dos principais modelos de controle de acesso devido à redução dos custos administrativos relacionados ao gerenciamento de permissões. Posteriormente, o modelo foi adotado como padrão nacional dos Estados Unidos sob a designação ANSI/INCITS 359-2004 pelo Instituto Nacional Americano de Padrões (*American National Standards Institute* - ANSI) e pelo Comitê Internacional para Padrões de Tecnologia da Informação (*International Committee for Information Technology Standards* - INCITS). Em 2012, esse padrão passou por revisão e recebeu a denominação INCITS 359-2012 (NIST, 2026).

A partir de 1994, diferentes empresas do setor de tecnologia da informação passaram a desenvolver soluções fundamentadas no modelo, contribuindo para sua expansão e consolidação no mercado. De acordo com análises realizadas pela RTI International (*Research Triangle Institute*) em 2010, o RBAC já estava presente na maior parte das organizações com 500 ou mais colaboradores, evidenciando sua ampla aceitação como mecanismo de controle de acesso (NIST, 2026).

O Controle de Acesso Baseado em Papéis é uma metodologia de restrição de acesso a redes e sistemas que se baseia na função de um indivíduo dentro de uma organização. O conceito central é uma abstração que desvincula as permissões do indivíduo e as associa a um papel funcional. O acesso de um colaborador não é mais definido por quem ele é (o usuário "João Silva"), mas sim pelo que ele faz (o papel de "Analista Fiscal") (Gillis e Rosencrance, 2024).

Conforme definido pela Cloudflare (2025), o RBAC funciona atribuindo um ou mais papéis a um usuário e concedendo a cada papel um conjunto específico de permissões para executar determinadas tarefas. Um "papel" (ou *role*) é, portanto, uma construção lógica que representa uma função de negócio ou um conjunto de responsabilidades, como "Comprador", "Gerente de RH" ou "Auditor Interno". Quando um novo colaborador assume a função de comprador, ele simplesmente herda o papel "Comprador" e, com ele, todas as permissões pré-aprovadas e necessárias para executar suas atividades, nem mais, nem menos.

Essa abordagem estruturada se sustenta em dois pilares fundamentais da segurança da informação, que são aplicados essencialmente pelo modelo, sendo eles o Princípio do Mínimo Privilégio e a Segregação de Funções.

O Princípio do Mínimo Privilégio (PoLP - *Principle of Least Privilege*) determina que um usuário deve ter apenas os níveis de acesso essenciais para executar suas tarefas designadas. O RBAC é a materialização deste conceito (Armo, 2025). Ao projetar um papel, a organização é forçada a definir explicitamente quais transações, relatórios e dados são estritamente necessários para aquela função. Isso combate diretamente o problema do excesso de privilégios discutido anteriormente. O ponto de partida deixa de ser um acesso amplo que é restringido para ser um acesso nulo que é incrementado apenas com o necessário.

Como visto, a concessão de permissões conflitantes é um dos maiores riscos em ambientes ERP. O RBAC transforma a segregação de funções, um exercício reativo de auditoria, em uma prática proativa de design. A metodologia força a criação de papéis que são, por definição, livres de conflitos internos. Por exemplo, o papel "Gestor de Contas a Pagar" não irá conter permissões para criar fornecedores. O controle de SoD é elevado do nível do usuário para o nível de design dos papéis. A análise de risco passa a ser "quais combinações de papéis atribuídas a um mesmo usuário podem gerar um conflito?", o que é uma análise exponencialmente mais simples e gerenciável do que analisar milhares de permissões individuais (Gillis e Rosencrance, 2024).

Ao aplicar o princípio do mínimo privilégio de forma sistemática, o RBAC reduz drasticamente a superfície de ataque interna. Um usuário com permissões excessivas representa uma porta de entrada para o comprometimento de dados, seja por erro ou por intenção maliciosa. A centralização das políticas de acesso em um catálogo de papéis bem definido elimina as inconsistências e erros da gestão manual, garantindo que as diretrizes de segurança sejam aplicadas uniformemente em toda a organização (IBM, 2025).

A LGPD procura regimentar o uso adequado desses dados, englobando não somente a privacidade das informações e dos indivíduos a qual elas dizem respeito, mas também como deve ser feito o tratamento desses dados pelas organizações (Brasil, 2018, art. 1º).

METODOLOGIA

A metodologia adotada para o desenvolvimento deste Trabalho de Conclusão de Curso consiste em uma pesquisa aplicada, com abordagem qualitativa e caráter descritivo e explicativo, concebida a partir do método hipotético-dedutivo. A redação do documento baseia-se nas normas

da ABNT, obtidas a partir do Manual de Normalização de Projeto de Trabalho de Graduação da Fatec SBC (Duarte, 2023).

Esse estudo tem como finalidade analisar a implementação de controle de acesso baseado em papéis (RBAC) no sistema utilizado pelo Grupo Multilaser, visando à otimização da segurança e da eficiência dos processos em um ambiente ERP SAP. A autorização para a citação do nome da empresa, utilização de dados e participação dos especialistas foi formalmente concedida pelo departamento jurídico, mediante assinatura do Termo de Consentimento Livre e Esclarecido (Apêndice B).

A pesquisa contempla levantamento bibliográfico e um estudo de caso único. Para a coleta de dados para o estudo, foi utilizada a técnica de entrevistas semiestruturadas, guiadas por um roteiro de 18 questões (Apêndice A). O roteiro abordou desde o cenário legado anterior à implementação do modelo RBAC até os resultados obtidos após a adoção, além das perspectivas futuras da companhia. Essa abordagem permitiu a obtenção de relatos detalhados sobre as percepções e experiências dos profissionais envolvidos no projeto.

Por fim, os dados coletados foram tratados por meio da Análise de Conteúdo (Bardin, 2016), seguindo rigorosamente as fases de pré-análise, exploração do material e tratamento dos resultados. Essa técnica permitiu categorizar as evidências em três eixos fundamentais para o desenvolvimento deste estudo: a vulnerabilidade do cenário legado, com foco na análise das falhas de segurança e ineficiência operacional do modelo manual, o processo de transição técnica, que descreve o mapeamento de funções e o desenho dos papéis, e o impacto na governança de riscos, abrangendo a avaliação da maturidade digital, a segregação de funções (SoD) e a conformidade regulatória.

ESTUDO DE CASO

O desenvolvimento do estudo, que realizado entre fevereiro e maio de 2026, teve início com a coleta de dados nas entrevistas com os três especialistas diretamente envolvidos no projeto de transição para o modelo RBAC no sistema SAP do Grupo Multilaser: Frederico Almeida (visão técnica do processo), Arthur Ferreira (foco operacional e funcional) e Gabriela Moitinho (foco em governança e processos). Por meio dos relatos obtidos, foi possível levantar informações sobre o cenário anterior de gestão de acessos, os problemas enfrentados, as motivações para a adoção do novo modelo, o processo de implementação adotado pela empresa e os benefícios percebidos após a conclusão do projeto.

Após a leitura flutuante das entrevistas, foram identificadas unidades de sentido relacionadas à implementação do RBAC. Essas unidades foram agrupadas em quatro categorias temáticas: cenário pré-RBAC e riscos, estratégia de implementação, processo atual de aprovação e ganhos/resultados percebidos. A Figura 1 apresenta as evidências extraídas dos depoimentos e as interpretações construídas a partir da análise dos dados.

Figura 1 – Síntese da categorização temática das entrevistas com base na análise de conteúdo de Bardin

Categoria	Evidências encontradas nas entrevistas	Síntese interpretativa
Cenário pré-RBAC e riscos	Permissões excessivas, cópia de perfis, usuários privilegiados, ausência de padronização	O ambiente anterior apresentava fragilidades de segurança e governança decorrentes do crescimento não controlado das permissões.
Estratégia de implementação	Pacotes de acesso, associação ao cargo, segregação de funções, controles preventivos	A implementação do RBAC ocorreu por meio da padronização dos perfis e da formalização das responsabilidades.
Processo atual de aprovações	Fluxos formais, validação técnica, análise de riscos e participação das áreas de negócio	O modelo atual estabelece controles compartilhados que reduzem riscos de concessão inadequada de acessos.
Ganhos e resultados	Redução de chamados, agilidade operacional, auditorias simplificadas e maior rastreabilidade	Os entrevistados convergem na percepção de que o RBAC aumentou a eficiência operacional e a maturidade da governança de acessos.

(Fonte: Autoria própria, 2026)

Conforme os depoimentos dos especialistas, o projeto de transição para o RBAC no Grupo Multilaser foi estruturado com o objetivo de converter um cenário de gestão reativa em uma governança proativa e estratégica.

No modelo anterior, o processo de solicitação de acessos era conduzido de forma manual, por meio de chamados abertos na plataforma JIRA. Isso resultava em um fluxo no qual a equipe de TI (*Basis*) era constantemente sobrecarregada por demandas pontuais e sem padronização, o que gerava ineficiência e longos prazos de atendimento.

Foi observado que a falta de documentação e de governança rigorosa permitia a ocorrência frequente de excesso de privilégios. Nesse contexto, novos colaboradores acumulavam acessos de cargos antigos ou ganhava permissão de "super usuário" após promoções e transferências de setor.

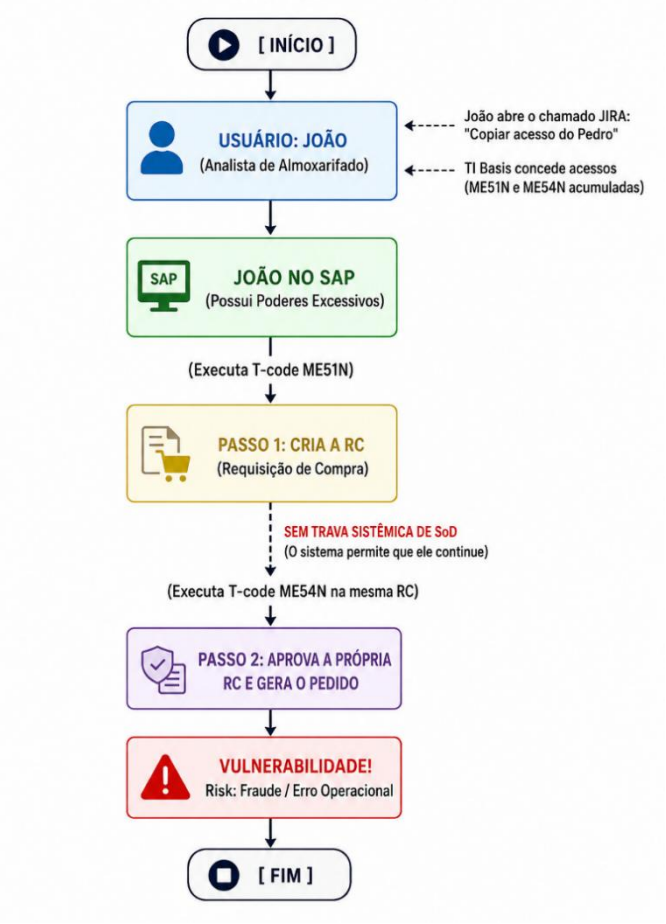
Esse cenário criava uma estrutura de permissões excessivas, que ampliava a superfície de ataque interna e elevava os riscos de fraudes financeiras e vazamento de dados.

A necessidade de implementação do RBAC surgiu, portanto, para substituir o cenário descrito por uma estrutura automatizada e ágil, fundamentada no Princípio do Mínimo Privilégio, garantindo que cada usuário possua apenas o acesso estritamente necessário para o exercício de sua função de negócio.

Antes da implementação do modelo RBAC (*Role-Based Access Control*), a gestão de acessos era caracterizada por um fluxo reativo e artesanal. As solicitações via JIRA careciam de uma matriz de referência, o que forçava a equipe de *Basis* a configurar acessos de forma individualizada para cada usuário. Esse cenário propiciava o fenômeno do *Privilege Creep* (Excesso de Privilégios). O especialista Frederico Almeida destacou que era prática comum copiar os acessos de outros colaboradores ("faz igual ao do João"), o que propagava erros sistematicamente. Como resultado, usuários acumulavam transações desnecessárias ou enfrentavam travamentos em processos críticos por falta de autorizações específicas.

Nesse período, a Segregação de Funções (SoD) era inexistente no nível de sistema, baseando-se apenas na confiança mútua entre *key users*, sem travas automáticas que impedissem, por exemplo, que um mesmo colaborador fizesse uma solicitação e aprovasse o pagamento, conforme representado abaixo na Figura 2. A transição para o RBAC marcou, na visão dos entrevistados, a mudança da gestão focada na subjetividade do indivíduo para a objetividade da função de negócio.

Figura 2 – Exemplo de cenário antes da implementação do RBAC



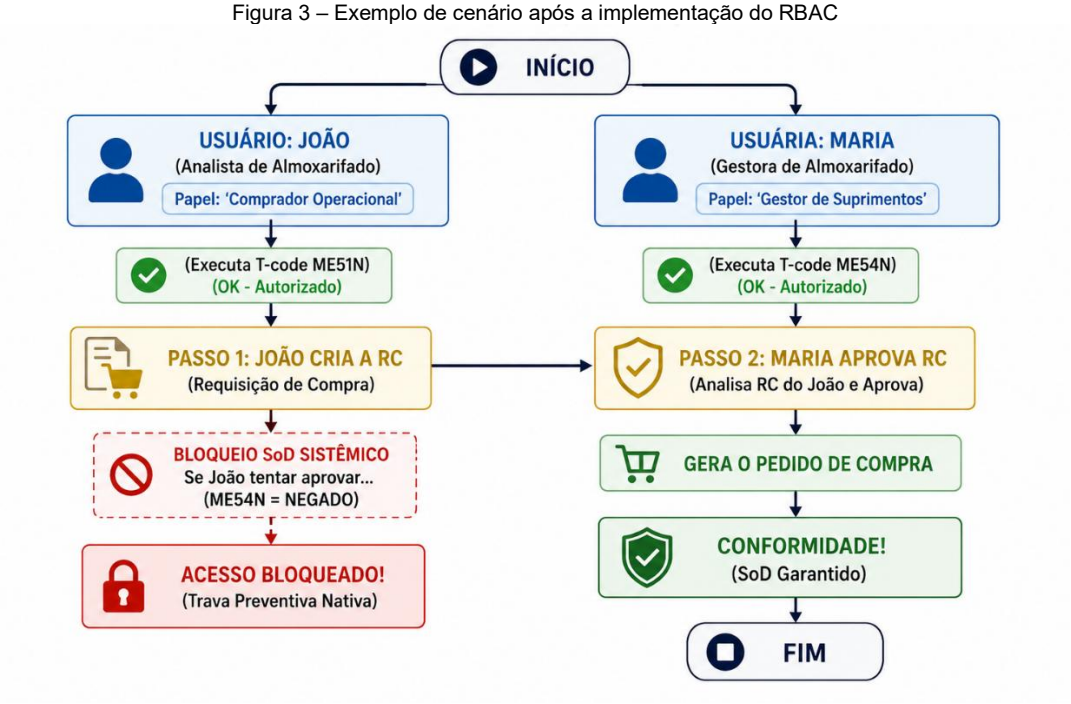
(Fonte: Autoria própria, 2026)

Segundo os especialistas, o projeto foi estruturado em uma parceria entre o time de *Basis* e os líderes setoriais (*key users*). A estruturação dos papéis seguiu critérios de granularidade mínima, baseando-se em três pilares fundamentais:

- **Mapeamento de Processos:** Criação de "pacotes de acesso" baseados na rotina de cada cargo em vez de transações soltas.
- **Princípio do Mínimo Privilégio:** Foco em garantir apenas o acesso essencial, eliminando excessos.
- **SoD Nativo:** A segregação de funções foi embutida no desenho dos papéis, garantindo que a segurança passasse a ser preventiva.

A Figura 3 mostra como passou a ser o processo exemplificado na Figura 2 após a implementação do RBAC.

Figura 3 – Exemplo de cenário após a implementação do RBAC



(Fonte: Autoria própria, 2026)

Para sintetizar a evolução alcançada, a Figura 4 apresenta o comparativo entre o cenário anterior e o atual modelo de governança.

Figura 4 - Comparativo dos Cenários de Governança: Pré-RBAC vs. Pós-RBAC

Indicador	Cenário Pré-RBAC (Manual)	Cenário Pós-RBAC (Governança)
Padronização	Inexistente; perfis exclusivos por usuário.	Total; novos colaboradores recebem perfis em minutos.
Responsabilidade	Difusa; o Basis decidia as transações.	Compartilhada; aprovação técnica e do key user.
Auditoria	Dificultosa; sem trilhas claras.	Rígida e transparente; evidências sistêmicas.

(Fonte: Autoria própria, 2026, baseado nos relatos de Frederico Almeida e Arthur Ferreira)

Os resultados práticos dessa mudança foram mensurados por meio de indicadores de suporte (KPIs - *Key Performance Indicator* ou Indicador-Chave de Desempenho). Observou-se uma redução de aproximadamente 58% no volume mensal de chamados abertos na plataforma JIRA

relacionados a erros de autorização ou solicitações de novos perfis. Além disso, foi informado que a organização instituiu uma revisão periódica de acessos, validando semestralmente a permanência de privilégios e garantindo conformidade com a LGPD.

O processo de implementação do RBAC no sistema SAP do Grupo Multilaser foi consolidado por meio de fases metodológicas fundamentais. A primeira fase consistiu no diagnóstico e levantamento, realizado por meio de entrevistas com *key users* e administradores SAP, para mapear o fluxo de solicitações via JIRA e identificar falhas de documentação nos papéis existentes.

Na segunda fase, foi feita a estruturação de papéis, passando da gestão de "transações soltas" e individuais para a criação de papéis funcionais baseados em processos de negócio e nas responsabilidades específicas de cada colaborador.

A terceira fase definiu o fluxo de trabalho, estabelecendo um fluxo formal de governança que compreende as etapas de abertura de chamado, alinhamento técnico, análise de impacto, aprovação por gestores e concessão final do acesso.

Já a quarta e última fase concluiu o projeto de implementação por meio da mitigação de conflitos, na qual ocorreu a identificação e o tratamento dos riscos de SoD diretamente no desenho dos papéis, garantindo que funções conflitantes não sejam atribuídas a um único perfil.

A análise das entrevistas permite concluir que o sucesso do RBAC reside no apoio da área de negócio, sendo evidenciado pela redução no volume de chamados, conforme citado pelos especialistas, e no retrabalho da equipe de *Basis*.

A principal lição destacada é que a gestão de acessos é um organismo vivo que exige manutenção constante, consolidando um modelo que continua evoluindo para abranger módulos complexos e para garantir a conformidade contínua com regulamentações. Como enfatizou Gabriela Moitinho: *“Ter tudo padronizado e documentado dá trabalho para montar, mas depois você colhe os frutos de um dia a dia tranquilo”*.

Ainda em relação à conformidade legal, o modelo RBAC apresenta aderência à LGPD, especialmente no que tange ao controle de acesso a dados pessoais. Essa relação mostra-se particularmente relevante em módulos como HCM (*Human Capital Management*) e CRM (*Customer Relationship Management*), os quais concentram informações sensíveis.

A aplicação do RBAC contribui para o atendimento ao princípio da necessidade (art. 6º, inciso III), ao restringir o acesso com base nos papéis e responsabilidades de cada usuário, bem como ao princípio da segurança (art. 6º, inciso VII), ao reduzir os riscos de acessos indevidos. Ademais, o modelo favorece a rastreabilidade e a auditabilidade das operações, alinhando-se, assim, ao princípio da responsabilização e da prestação de contas.

A análise do modelo em relação à segurança da informação revela que a adoção do RBAC foi um passo essencial para regimentar o tratamento adequado de dados e proteger a privacidade das informações corporativas. Atualmente, o sistema oferece transparência e inteligência ao vincular permissões a funções lógicas, dificultando ações maliciosas e erros operacionais.

A principal contribuição deste estudo é demonstrar que a transição para o RBAC no Grupo Multilaser não foi apenas uma mudança técnica, mas uma transformação na governança, que trouxe agilidade e segurança estratégica ao coração digital da companhia.

Como proposta para trabalhos futuros, identifica-se a oportunidade de implementar mecanismos de aceite eletrônico de termos de uso diretamente no SAP, bem como o aprimoramento de portais de autoatendimento para que os usuários possam consultar a finalidade do tratamento de seus dados.

CONSIDERAÇÕES FINAIS

Este estudo buscou analisar a transição do modelo de gestão de acessos manual para o Controle de Acesso Baseado em Papéis (RBAC) em um ambiente SAP, tendo como objeto de estudo o sistema do Grupo Multilaser. O objetivo central foi demonstrar, com base na percepção dos especialistas envolvidos, como essa mudança impacta a segurança e a governança corporativa. Acredita-se que este propósito foi alcançado por meio de uma análise qualitativa baseada nos relatos de profissionais que vivenciaram a implementação.

A escolha deste tema justificou-se pela importância crítica do sistema ERP como núcleo digital da empresa. O estudo evidenciou que a ausência de uma estratégia de governança resulta em vulnerabilidades severas, como o *Privilege Creep* (Excesso de Privilégios) e a falta de uma Segregação de Funções (SoD) sistêmica. Tais falhas não apenas podem aumentar os riscos de fraudes financeiras e vazamento de dados, mas também dificultar a conformidade com exigências regulatórias rigorosas, como a Lei Geral de Proteção de Dados Pessoais.

Os resultados relatados indicam que a adoção do RBAC trouxe benefícios operacionais e estratégicos imediatos. Destacam-se a redução de mais de 50% volume de chamados por falta de autorização, a diminuição do retrabalho da equipe de *Basis* e o aumento da transparência por meio de fluxos de aprovação compartilhados entre a TI e os *key users*. A implementação transformou a segurança de um modelo reativo e artesanal para um processo preventivo e automatizado.

A principal contribuição deste trabalho consiste em demonstrar, por meio de um caso real, como os conceitos de segurança da informação e governança podem ser aplicados na resolução de problemas operacionais recorrentes. Ao descrever a transição de um modelo de gestão de

acessos com baixa padronização para uma abordagem estruturada, este estudo contribui como uma referência prática para outras organizações que ainda operam com modelos manuais de autorização em sistemas ERP. A pesquisa evidencia que a implementação do RBAC transcende a área técnica da Tecnologia da Informação, consolidando-se como um elemento estratégico para a prevenção de fraudes, o aumento da eficiência organizacional e a conformidade com a legislação de proteção de dados.

Por fim, é importante reconhecer as limitações deste estudo. Por tratar-se de um estudo de caso único fundamentado em relatos específicos, os achados refletem a realidade particular da organização analisada, bem como a percepção dos entrevistados. Como recomendação para trabalhos futuros, sugere-se a ampliação da pesquisa para outros setores da indústria, visando investigar se os benefícios de governança observados se mantêm em diferentes contextos organizacionais e culturas corporativas.

REFERÊNCIAS

ARMO. What are RBAC Tools?. Armo, 2025. Disponível em: https://www.armosec.io/blog/rbac-tools/. Acesso em: 29 out. 2025.

BARDIN, Laurence. Análise de conteúdo. Tradução: Luís Antero Reto e Augusto Pinheiro. São Paulo: Edições 70, 2016.

BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, e dá outras providências. Diário Oficial [da] República Federativa do Brasil: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. 03 nov. 2025.

BROWN, A. Implementing ERP Systems: Challenges and Strategies. Business Science Reference, 2018.

CASTRO, M. D.; OLIVEIRA, F. M. A entrevista semiestruturada na pesquisa qualitativa-interpretativa: um guia de análise processual. Entretextos, Londrina, v. 22, n. 1, p. 1-25, 2022. Disponível em: https://ojs.uel.br/revistas/uel/index.php/entretextos/article/view/46089. Acesso em: 23 nov. 2025.

CLOUDFLARE. O que é o controle de acesso baseado em função (RBAC)?. Cloudflare, 2025. Disponível em: https://www.cloudflare.com/pt-br/learning/access-management/role-based-access-control-rbac/. Acesso em: 29 out. 2025.

FORTINET. O que é o controle de acesso baseado em função (RBAC)?. Fortinet, 2025. Disponível em: https://www.fortinet.com/br/resources/cyberglossary/role-based-access-control. Acesso em: 29 out. 2025.

GERRING, John. Pesquisa de estudo de caso: princípios e práticas. Petrópolis: Vozes, 2019.

GILLIS, Alexander S.; ROSENCRANCE, Linda. What is Role-Based Access Control (RBAC)?. TechTarget, 2024. Disponível em: https://www.techtarget.com/searchsecurity/definition/role-based-access-control-RBAC. Acesso em: 27 nov. 2025.

GONÇALVES, R.; SILVA, M.; ALMEIDA, J. Governança de dados em sistemas ERP: uma revisão sistemática. Revista Brasileira de Sistemas de Informação, p. 45–58, 2020.

IBM. Controle de acesso baseado em função (RBAC). IBM, 2025. Disponível em: https://www.ibm.com/br-pt/think/topics/rbac. Acesso em: 29 out. 2025.

IBM. O que é ERP (Enterprise Resource Planning)?. IBM, 2025. Disponível em: https://www.ibm.com/br-pt/think/topics/enterprise-resource-planning. Acesso em: 29 out. 2025.

LIMA, A.; OLIVEIRA, B. Gestão de Projetos de Tecnologia: Práticas Eficazes para Implementação de Sistemas ERP. Editora Independente, 2019.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Role Based Access Control (RBAC). NIST Computer Security Resource Center, 2026. Disponível em: https://csrc.nist.gov/Projects/Role-Based-Access-Control. Acesso em: 14 jun. 2026.

SAP. A história da SAP: mais de 50 anos de inovação. SAP, 2025. Disponível em: https://www.sap.com/about/company/history.html. Acesso em: 29 out. 2025.

SAP. O que é a SAP?. SAP Brasil, 2025. Disponível em: https://www.sap.com/brazil/about/what-is-sap.html. Acesso em: 29 out. 2025.

SAP. SAP NetWeaver 7.31 BW ABAP – Online Help. Disponível em: https://help.sap.com/docs/SAP_ERP_SPV/3fea17d5446849b3bca91fea91b0f003/4f4decf806b02892e10000000a42189b.html. Acesso em: 26 nov. 2025.

SEVERINO, Antônio Joaquim. Metodologia do trabalho científico. 24.ed. São Paulo: Cortez, 2016.

SINGH, A. *et al*. Risks and challenges of ERP system customization: a systematic literature review. Journal of Enterprise Information Management, 2019.

APÊNDICE A – TRANSCRIÇÃO DAS ENTREVISTAS

Entrevistado 1: Frederico Almeida

1. Como funcionava o pedido de acesso antes do RBAC?
   R: Era tudo via chamado no JIRA. O processo era bem manual: você abria o chamado, um *key user* da área autorizava e o time de *Basis* tinha que configurar o acesso para o usuário quase que do zero.
2. Rolavam muitos problemas de acessos errados ou exagerados?
   R: Sim, acontecia bastante. Como as funções não eram bem documentadas, na hora de liberar o acesso para alguém, acabava indo coisa a mais ou faltava o que a pessoa realmente precisava. Era um "ajusta daqui, tira dali" constante.
3. E como vocês cuidavam dos conflitos de funções (SoD) nessa época?
   R: Era na base da conversa e do alinhamento manual. A gente abria o chamado, falava com o *key user* da área e tentava definir o que podia ou não, mas não tinha uma trava automática para evitar que alguém tivesse funções conflitantes.
4. Por que decidiram mudar para o modelo RBAC?
   R: O time de *Basis* perdia muito tempo criando acessos manuais, um por um, sem um padrão. A ideia do RBAC foi organizar a casa: trazer agilidade, automatizar o que dava e parar de "apagar incêndio" toda vez que alguém entrava na empresa ou mudava de cargo.
5. Quem ajudou a colocar o projeto de pé?
   R: Eu não estava lá no dia a dia do projeto, mas sei que foi um trabalho conjunto: o time de *Basis* cuidou da parte técnica e os *key users* de cada setor ajudaram a explicar o que cada função precisava fazer.
6. Como descobriram o que cada papel (*role*) deveria acessar?
   R: Foi feito um mapeamento de quem faz o quê. Em vez de liberar transações soltas, eles olharam para o dia a dia de cada cargo e montaram pacotes de acesso que fazem sentido para aquela função específica.
7. O que foi levado em conta na hora de criar esses perfis?
   R: O foco foi dar o acesso exato para o trabalho da pessoa. Nem mais, nem menos. A ideia era garantir que o catálogo de acessos batesse com o que a empresa realmente precisava operacionalmente.
8. E como ficaram os conflitos de funções (SoD) na montagem do modelo?

R: Na hora de desenhar os papéis, já foi pensado em separar quem faz de quem aprova. O objetivo foi criar travas para que um único perfil não tivesse permissões que pudessem gerar riscos de segurança.

9. E hoje, como é o caminho para conseguir um acesso?

   R: O fluxo ficou mais organizado: o chamado é aberto, passa por um alinhamento técnico, uma análise de riscos, e só depois da aprovação do consultor e do *key user* é que o acesso é liberado.

10. Como esses "papéis" ajudam a organizar o SAP na prática?

    R: Mudou a lógica. Antes o *Basis* decidia as transações; agora, o acesso é baseado no processo de negócio. O papel já vem "empacotado" com tudo o que a função precisa, sem bagunça.

11. Tem alguém que assina e se responsabiliza por esses acessos?

    R: Com certeza. Existe uma hierarquia: o pedido passa por uma análise técnica (de um consultor funcional do módulo, como o EWM) e pela palavra final do *key user* da área.

12. Como vocês mantêm esses papéis atualizados?

    R: Sempre que um processo da empresa muda, a gente revisa o papel. Não é algo estático; se a operação mudou, o acesso no SAP acompanha essa mudança através de uma revisão técnica.

13. Vocês revisam de tempos em tempos quem tem acesso ao quê?

    R: Sim, existe uma limpeza periódica. Os gestores olham para suas equipes e confirmam se todo mundo ainda precisa daqueles acessos. Se alguém mudou de área ou saiu, o acesso é cortado para manter o sistema limpo.

14. Diminuiu a correria e o excesso de chamados?

    R: Com certeza! Mesmo não estando mais no dia a dia do módulo, dá para notar que as cobranças diminuíram muito. O processo ficou mais "redondo" e previsível.

15. O RBAC deixou o sistema mais seguro?

    R: Sem dúvida. Quando você limita o acesso apenas ao que a pessoa realmente precisa, você evita erros e problemas de segurança. É muito mais fácil controlar quem faz o quê agora.

16. E para as auditorias, melhorou?

    R: Muito. O processo hoje é mais rígido e transparente. Quando sou chamado para analisar algo como funcional de EWM, vejo que os pedidos e as aprovações estão muito mais organizados do que antigamente.

17. O modelo continua evoluindo ou parou por aí?

    R: Ele continua evoluindo. A ideia é sempre buscar ferramentas que automatizem ainda mais essas análises de risco e tragam mais agilidade para o dia a dia.

18. O que você aprendeu de mais importante com tudo isso?

    R: Que não adianta ter uma ferramenta boa se a área de negócio não apoiar. Manter a documentação em dia e ter processos padronizados é o único jeito de não deixar a gestão de acessos virar uma bagunça de novo.

Entrevistado 2: Arthur Ferreira (Especialista Operacional)

1. Como era o esquema de pedir acesso antigamente?

   R: Era aquele fluxo básico: abria o ticket no JIRA e esperava. O problema é que o *Basis* recebia o pedido e quase tinha que "adivinhar" o que o cara precisava. O *key user* dava o OK, mas era um processo muito manual e artesanal.

2. O pessoal tinha muito acesso sobrando ou faltava coisa?

   R: Direto! Como não tinha um padrão, a gente copiava o acesso de um colega ("faz igual ao do João"), e aí o erro ia passando pra frente. O cara acabava com um monte de transação que nem sabia pra que servia.

3. E como vocês barravam o que não podia ser misturado (SoD)?

   R: Era no "olhômetro" e na base da confiança. A gente conversava com o *key user* e confiava que ele sabia quem podia fazer o quê. Não tinha um sistema que apitava se tivesse algo errado.

4. O que fez a empresa finalmente adotar o RBAC?

   R:O time de *Basis* estava sufocado. Era muito tempo gasto criando acesso "na mão" e corrigindo erro de permissão que não acabava mais. Chegou num ponto onde ou a gente padronizava, ou o suporte ia virar um gargalo eterno.

5. Quem realmente botou a mão na massa no projeto?

   R: O *Basis* puxou a frente técnica, mas quem deu o Norte foram os *key users*. Sem o pessoal que entende do dia a dia de cada setor, não teria como desenhar os papéis.

6. Como decidiram o que ia em cada perfil?

   R: A gente parou de olhar para a "pessoa" e começou a olhar para a "cadeira". Foi um trabalho de entender quais ferramentas cada cargo precisava para trabalhar.

7. Qual foi o critério para montar esses grupos?

R: O foco foi a simplicidade e a segurança. A ideia era: "O que é o mínimo que esse cara precisa para não travar a operação?".

7. E como resolveram aquela bagunça dos conflitos de funções?

R: No desenho dos papéis, a gente já separou as águas. Tipo: quem lança nota não pode ser o mesmo perfil que aprova o pagamento.

8. E hoje, como é o caminho das pedras para ganhar um acesso?

R: Ficou bem mais profissional. Tem o chamado, mas agora ele passa por um filtro técnico de verdade. Antes de chegar no *Basis*, um funcional e o *key user* garantem que o pedido faz sentido.

9. O que mudou na estrutura do SAP com esses novos papéis?

R: Acabou aquela história de "transação solta". Agora o acesso é um espelho do processo da empresa. Se você é do EWM, seu papel já vem com o kit completo do armazém.

10. Quem é que "carimba" a autorização agora?

R: Tem dono. O processo é formal: passa pelo consultor do módulo e o *key user* assina embaixo. Ficou muito mais difícil alguém conseguir um acesso que não deveria ter.

11. E se o processo mudar? Como atualizam tudo?

R: A gente trata a *role* como um produto. Se a empresa muda o jeito de trabalhar, a gente vai lá no ambiente de desenvolvimento, mexe na *role*, testa e sobe para produção.

12. Vocês dão uma geral nos acessos de tempos em tempos?

R: Com certeza, a famosa "limpeza de primavera". Periodicamente os gestores dão um *check* nas equipes. Se o cara mudou de função e esqueceu o acesso antigo aberto, o sistema corta.

13. Sentiu que o volume de reclamação diminuiu?

R: Nossa, da água pro vinho! Quando o acesso é padronizado, o cara entra na empresa e já sai trabalhando. Aquela chuva de chamados de "falta autorização" quase sumiu.

14. O sistema está mais seguro de verdade?

R: Muito mais. O risco de alguém fazer uma besteira caiu absurdamente, porque as cercas estão bem montadas.

15. E o pessoal da auditoria, parou de pegar no pé?

R: Agora a gente tem argumentos. Quando eles chegam, a gente mostra o fluxo e quem aprovou. O processo está tão consolidado que a auditoria flui muito mais rápido.

16. Esse modelo ainda vai mudar muito?

R: O céu é o limite. A ideia é automatizar cada vez mais, talvez até com IA no futuro para prever riscos.

17. Qual o maior aprendizado disso tudo?

R: Que organização paga o preço no começo, mas dá lucro no final. Ter o apoio dos gestores e manter tudo bem documentado evita que o time de TI viva em pânico constante.

Entrevistado 3: Gabriela Moitinho (Especialista em Governança)

1. Como vocês pediam acesso no começo?

R: Era aquele esquema de abrir chamado e torcer. Como não tinha um padrão, cada usuário acabava com um perfil "exclusivo". Era bem difícil de gerenciar.

2. Tinha muito problema de gente com acesso a coisa que não devia?

R: Com certeza. O pessoal ia acumulando acessos de cargos antigos ou ganhava permissão de "super usuário" sem precisar. Isso bagunçava o sistema.

3.Como vocês evitavam que uma pessoa fizesse tudo sozinha no sistema?

R: Na base da conversa e do "policiamento" manual. Não tinha uma trava real no sistema que impedisse isso de acontecer.

4. Por que decidiram organizar tudo com o RBAC?

R: Porque o time técnico não aguentava mais tanto retrabalho e o pessoal da operação vivia parado esperando acesso. A gente precisava de um jeito de dar o acesso certo de primeira.

5. Quem realmente ajudou a definir essas novas regras?

R: Foi uma parceria. O pessoal da TI montou a estrutura, mas quem disse o que o estoque precisava foram os líderes de cada setor.

6. Como vocês decidiram o que entra em cada "pacotinho" de acesso?

R: A gente parou de olhar para o que a "pessoa" queria e olhou para o que a "função" exigia. Isso tirou o achismo da jogada.

7. Qual foi o foco na hora de criar esses perfis?

R: Simplicidade. A ideia foi dar o feijão com arroz bem feito: garantir o necessário para trabalhar sem sobrar nada que causasse erro de segurança.

8. E as travas de segurança, como ficaram?

R: Elas já foram "embutidas" nos perfis. Quando desenhamos as funções, já deixamos separado quem faz e quem confere.

9. Como está o processo de pedir acesso hoje em dia?

R: Ficou bem mais fluido. O pedido entra, a gente dá uma olhada técnica rápida, o gestor aprova e o acesso já cai na conta do cara.

10. O que mudou de verdade no sistema com esses papéis?

R: Padronização. Se entrarem 10 funcionários novos para a mesma área, os 10 vão ter exatamente os mesmos acessos em minutos.

11. Quem é que dá a palavra final agora?

R: O processo é compartilhado. Um especialista do módulo vê se o pedido faz sentido técnico e o *key user* da área dá o carimbo final.

12. E se o trabalho mudar, como vocês ajustam os acessos?

R: A gente mexe no "molde". Se o setor mudar o jeito de trabalhar, a gente atualiza o papel principal e todo mundo recebe a atualização de uma vez.

13. Vocês conferem se ainda tem gente com acesso sobrando?

R: Sim, fazemos um pente-fino de vez em quando. Os chefes de cada área dão uma olhada na lista e dizem quem ainda precisa do quê.

14. Diminuiu a quantidade de gente reclamando de acesso?

R: Muito! Hoje o pessoal quase não me para no corredor para reclamar de erro de autorização. Isso tira um peso enorme das costas de quem dá suporte.

15. O SAP ficou mais seguro de verdade?

R: Com certeza. Agora a gente sabe exatamente onde começa e onde termina o poder de cada um no sistema.

16. E as auditorias? Estão mais tranquilas?

R: Estão ótimas. Agora, quando perguntam algo, a gente tem a resposta na ponta da língua e a prova no sistema. Passa muito mais confiança.

18. O que vem pela frente agora?

R: O plano é deixar tudo cada vez mais automático. Queremos que o sistema identifique riscos na hora, sem a gente precisar intervir tanto.

19. Qual a maior lição que ficou desse projeto?

R: Que organização salva vidas (e o humor do time!). Ter tudo padronizado e documentado dá trabalho para montar, mas depois você colhe os frutos de um dia a dia tranquilo.

APÊNDICE B – TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO (TCLE)

SÃO PAULO
GOVERNO DO ESTADO

Faculdade de Tecnologia Adib Moisés Dib
TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO (TCLE)

O Sr.(a) está sendo convidado(a) a participar come voluntário(a) da pesquisa Implementação RBAC no SAP - Estudo de Caso 01.

Está pesquisa está sob a responsabilidade do(s) pesquisador(es) Esp. Anderson Valentino Bozzo.

Nesta pesquisa pretendemos analisar um caso de aplicação do modelo RBAC (Role-Based Access Control) em um sistema SAP de uma empresa do setor de tecnologia, a fim de apresentar aua relevância práfica como mecanismo de garantia e aprimoramento da segurança da informação.

Declaro que foi entregue/enviado fisicamente/digitalmente todas as informações relativas à pesquisa, sendo elas: objetivos, justificativa, metodologia, riscos, benefícios, garantia de sigilo e privacidade e explicitação da garantia a ressarcimento.

Sei que a qualquer momento poderei salicitar novas informações sobre a pesquisa e me retirar sem prejuizo ou penalidade.

Declaro que concordo em participar. Recebi uma cópia deste termo de consentimento livre e esclarecido e me foi dada a oportunidade de ler sobre a pesquisa e esclarecer as minhas dúvidas.

São Paulo, de 15 de outubro de 2025.

Diogo Lopes
Assinatura do(a) participante

*No caso de o TCLE ser produzido digitalmente, o participante deve indicar consentimento (ou não) por meio de uma das alternativas abaixo:

(X) Sim, aceito participar da pesquisa.

( ) Não, recuso participar da pesquisa.