INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO AMAPÁ
CURSO DE TECNOLOGIA EM REDES DE COMPUTADORES

FRANCISCO MATHEUS FRANKLIN ALVES ROCHA

GERENCIAMENTO DE IDENTIDADE E ACESSO NOS DADOS COMERCIAIS PARA COMBATER VIOLAÇÃO DE DIREITOS

MACAPÁ-AP
2025

FRANCISCO MATHEUS FRANKLIN ALVES ROCHA

GERENCIAMENTO DE IDENTIDADE E ACESSO NOS DADOS COMERCIAIS PARA COMBATER VIOLAÇÃO DE DIREITOS

Trabalho de Conclusão de Curso apresentado a Coordenação do curso de Tecnologia em Redes de Computadores como requisito avaliativo para obtenção do título de Tecnólogo em Redes de Computadores.

Orientador: Prof. Esp. Francisco Sanches da Silva Junior

MACAPÁ-AP

2025

Biblioteca Institucional - IFAP
Dados Internacionais de Catalogação na Publicação (CIP)

R672g Rocha, Francisco Matheus Franklin Alves
Gerenciamento de identidade e acesso nos dados comerciais para combater violação de direitos / Francisco Matheus Franklin Alves Rocha - Macapá, 2025.
50 f.

Trabalho de Conclusão de Curso (Graduação) -- Instituto Federal de Educação, Ciência e Tecnologia do Amapá, Campus Macapá, Tecnologia em Redes de Computadores, 2025.

Orientador: Francisco Sanches da Silva Junior.

1. Gerenciamento de identidade e acesso. 2. Segredo comercial. 3. Segurança da informação. I. Silva Junior, Francisco Sanches da , orient. II. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica do IFAP
com os dados fornecidos pelo(a) autor(a).

FRANCISCO MATHEUS FRANKLIN ALVES ROCHA

GERENCIAMENTO DE IDENTIDADE E ACESSO NOS DADOS COMERCIAIS PARA COMBATER VIOLAÇÃO DE DIREITO

Trabalho de Conclusão de Curso apresentado a Coordenação do curso de Tecnologia em Redes de Computadores como requisito avaliativo para obtenção do título de Tecnólogo em Redes de Computadores.

BANCA EXAMINADORA

gov.br
Documento assinado digitalmente
FRANCISCO SANCHES DA SILVA JUNIOR
Data: 19/02/2026 13:59:19-0300
Verifique em https://validar.iti.gov.br

Prof. Esp. Francisco Sanches da Silva Junior

Orientador

Instituto Federal do Amapá

gov.br
Documento assinado digitalmente
HILTON PRADO DE CASTRO JUNIOR
Data: 19/02/2026 14:03:30-0300
Verifique em https://validar.iti.gov.br

Prof. Me Hilton Prado de Castro Júnior

Instituto Federal do Amapá

gov.br
Documento assinado digitalmente
SHIRLEY DA COSTA MONTEIRO
Data: 19/02/2026 14:33:21-0300
Verifique em https://validar.iti.gov.br

Prof. Esp. Shirley da Costa Monteiro

Instituto Federal do Amapá

Apresentado em: 18 / 12 / 2025.

Conceito/Nota: 8,8

Dedico aos meus familiares e amigos pelos esforços, experiências e conhecimentos que obtive com as minhas relações.

AGRADECIMENTOS

Somente preciso agradecer por chegar a este momento de agora a qual me encontro, sempre me sentir à deriva das coisas do mundo, mas só recentemente com apoio, conversas e experiências, ao menos um pouco, conseguir melhorar, e a conclusão disso é esse Trabalho de Conclusão de Curso, prova que estou a um milésimo a mais de ser decente e competente. Agradeço a todos que me acompanharam e que interagiram comigo até o presente momento para eu chegar e consumar essa parte necessária à minha vida.

O pensamento lógico-verbal faz uso dos códigos da língua e exige uma capacidade intelectual complexa. Seu desenvolvimento possibilita ao sujeito ultrapassar os limites da percepção sensorial imediata e assim estabelecer relações complexas, formar conceitos, refletir conexões, etc.

(VYGOTSKY, Luria, 1967).

RESUMO

O compartilhamento de informações estratégicas em parcerias empresariais voltadas ao desenvolvimento de soluções tecnológicas amplia a exposição de segredos comerciais em ambientes digitais colaborativos. Embora acordos de confidencialidade estabeleçam deveres jurídicos entre as partes, sua efetividade depende da adoção de mecanismos técnicos capazes de restringir acessos e assegurar a rastreabilidade das ações realizadas sobre os ativos informacionais. Este trabalho teve como objetivo analisar a aplicação de mecanismos de Gerenciamento de Identidade e Acesso como apoio à proteção de segredos comerciais em um cenário organizacional simulado de parceria empresarial. A pesquisa caracteriza-se como aplicada, de abordagem qualitativa e natureza descritiva, desenvolvida por meio de pesquisa bibliográfica e documental, associada à construção de um cenário organizacional simulado. A partir dos requisitos identificados, foi modelado um controle de acesso estruturado nos pilares de identificação, autenticação, autorização e monitoramento. A análise indicou que a integração desses mecanismos contribui para a limitação adequada de acessos, para a responsabilização dos usuários e para a demonstração de medidas razoáveis de proteção do segredo comercial. Conclui-se que o Gerenciamento de Identidade e Acesso constitui instrumento relevante para fortalecer a governança sobre informações estratégicas em parcerias empresariais.

Palavras-chave: gerenciamento de identidade e acesso; segredo comercial; controle de acesso; segurança da informação; parcerias empresariais.

ABSTRACT

The sharing of strategic information in business partnerships aimed at developing technological solutions increases the exposure of trade secrets within collaborative digital environments. Although non-disclosure agreements establish legal obligations between the parties, their effectiveness depends on the implementation of technical mechanisms capable of restricting access and ensuring the traceability of actions performed on informational assets. This study aimed to analyze the application of Identity and Access Management mechanisms to support the protection of trade secrets in a simulated organizational scenario of business partnership. The research is characterized as applied, with a qualitative and descriptive approach, developed through bibliographic and documentary research combined with the construction of a simulated organizational scenario. Based on the identified requirements, an access control model was designed around four pillars: identification, authentication, authorization, and monitoring. The analysis indicated that the integration of these mechanisms contributes to proper access restriction, user accountability, and the demonstration of reasonable measures for protecting trade secrets. It is concluded that Identity and Access Management represents a relevant instrument to strengthen governance over strategic information in business partnerships.

Keywords: identity and access management; trade secrets; access control; information security; business partnerships.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

A intensificação das parcerias empresariais voltadas ao desenvolvimento conjunto de produtos, serviços e soluções tecnológicas tem ampliado, de forma significativa, a necessidade de compartilhamento de informações estratégicas entre organizações. Nesse contexto, passam a circular entre as partes dados técnicos, comerciais e operacionais que, muitas vezes, se enquadram na categoria de segredos comerciais, por estarem diretamente associados à vantagem competitiva e ao posicionamento estratégico das empresas.

Paralelamente a esse movimento, observa-se a consolidação de ambientes computacionais baseados em serviços em nuvem e em plataformas colaborativas, nos quais usuários internos, parceiros externos e prestadores de serviço acessam, de maneira remota, recursos informacionais distribuídos. Esse cenário impõe novos desafios à proteção da informação, sobretudo no que se refere ao controle sobre quem pode acessar determinados ativos, em quais condições e para quais finalidades. De acordo com o *National Institute of Standards and Technology* (NIST), o gerenciamento de identidades digitais e de acessos constitui um dos elementos centrais da arquitetura de segurança da informação em ambientes organizacionais, por viabilizar a identificação dos sujeitos, a autenticação de suas credenciais e a aplicação de políticas de autorização sobre recursos computacionais (NIST, 2020; NIST, 2022).

Sob a perspectiva da gestão da segurança da informação, normas internacionais também destacam a importância de mecanismos formais de controle de acesso como requisito fundamental para a proteção de ativos organizacionais. A norma ISO/IEC 27001 estabelece que as organizações devem definir e implementar controles capazes de assegurar que o acesso à informação seja concedido de acordo com necessidades de negócio e princípios de segregação de funções, reduzindo a exposição a usos indevidos e a acessos não autorizados (ABNT, 2022).

No campo jurídico, a proteção de informações confidenciais e de segredos comerciais é reconhecida como elemento essencial para a preservação da competitividade das organizações. O Acordo sobre Aspectos dos Direitos de Propriedade Intelectual Relacionados ao Comércio (TRIPS) estabelece que informações não divulgadas devem ser protegidas contra aquisição, uso ou divulgação não autorizados, desde que possuam valor comercial e sejam objeto de medidas razoáveis de proteção por parte de seus detentores (WTO, 1994). No ordenamento jurídico brasileiro, a Lei nº 9.279/1996 reconhece a tutela dos segredos industriais e comerciais,

enquadrando a divulgação ou utilização indevida dessas informações como prática de concorrência desleal (BRASIL, 1996).

Diante desse panorama, observa-se que a proteção de segredos comerciais em ambientes digitais compartilhados não pode ser compreendida apenas a partir de instrumentos legais ou contratuais. Torna-se necessário articular mecanismos técnicos de controle, capazes de materializar, no nível operacional, as restrições e responsabilidades estabelecidas entre as partes. Nesse sentido, o Gerenciamento de Identidade e Acesso apresenta-se como uma abordagem estruturante para apoiar a proteção da informação em cenários colaborativos, ao integrar processos de identificação, autenticação, autorização e monitoramento de atividades sobre recursos corporativos (NIST, 2020).

1.1 Problema de pesquisa

Embora acordos de confidencialidade e instrumentos contratuais sejam amplamente utilizados para regular o compartilhamento de informações entre organizações, esses mecanismos, por si só, não garantem a efetiva aplicação de restrições de acesso em ambientes digitais. A literatura técnica aponta que falhas nos processos de gerenciamento de identidades, na definição de privilégios e na supervisão das atividades dos usuários constituem fatores recorrentes associados a incidentes de segurança da informação, especialmente em contextos de acesso remoto e ambientes em nuvem (NIST, 2022; ABNT, 2022).

Além disso, a própria proteção jurídica dos segredos comerciais, conforme previsto no acordo TRIPS e na legislação brasileira, pressupõe que o titular da informação adote medidas razoáveis para preservar o seu sigilo. Tais medidas não se limitam a cláusulas contratuais, mas abrangem práticas organizacionais e técnicas de controle que evidenciem o esforço sistemático para impedir acessos e usos não autorizados (WTO, 1994; BRASIL, 1996).

Nesse contexto, considerando um ambiente organizacional no qual empresas parceiras compartilham informações estratégicas por meio de plataformas digitais, formula-se o seguinte problema de pesquisa: de que forma mecanismos de Gerenciamento de Identidade e Acesso podem contribuir para a proteção de segredos comerciais em parcerias empresariais, considerando um cenário organizacional simulado de compartilhamento de informações?

1.2 Justificativa e relevância

A relevância deste estudo decorre, inicialmente, da crescente dependência das organizações em relação a ambientes digitais distribuídos para a condução de atividades estratégicas e projetos colaborativos. A exposição indevida de segredos comerciais pode gerar impactos econômicos, jurídicos e reputacionais, além de comprometer a sustentabilidade dos negócios, uma vez que tais informações representam ativos intangíveis de elevado valor para as organizações (WIPO, 2016).

Do ponto de vista organizacional, o uso de mecanismos estruturados de gerenciamento de identidade e acesso contribui para a redução de riscos associados à atuação de usuários legítimos que, em função de suas atribuições, necessitam acessar recursos sensíveis. Segundo o NIST, a correta definição de identidades digitais, aliada à aplicação consistente de políticas de autorização e à manutenção de registros de auditoria, constitui uma das principais estratégias para mitigar incidentes relacionados a abuso de privilégios e comprometimento de credenciais (NIST, 2020).

Sob a perspectiva normativa, a adoção de controles de acesso alinhados a padrões reconhecidos internacionalmente também representa um requisito para a conformidade com sistemas de gestão da segurança da informação, como os previstos na ISO/IEC 27001, que enfatiza a necessidade de mecanismos técnicos e administrativos capazes de sustentar as políticas de segurança definidas pela organização (ABNT, 2022).

No âmbito acadêmico, observa-se que ainda são limitados os estudos que integram, de forma sistemática, os aspectos técnicos do Gerenciamento de Identidade e Acesso com os requisitos jurídicos e organizacionais relacionados à proteção de segredos comerciais em parcerias empresariais. Assim, este trabalho justifica-se pela contribuição ao debate interdisciplinar entre segurança da informação, gestão organizacional e proteção da propriedade intelectual, ao analisar um modelo conceitual de controle de acesso aplicado a um cenário simulado de cooperação entre empresas.

1.3 Objetivos

1.3.1 Objetivo Geral

O objetivo geral deste trabalho é analisar a aplicação de mecanismos de Gerenciamento de Identidade e Acesso como apoio à proteção de segredos comerciais em um cenário simulado de parceria empresarial.

1.3.2 Objetivos Específicos

- Caracterizar os conceitos de Gerenciamento de Identidade e Acesso, segredo comercial e apropriação indevida de informações a partir da literatura;
- Identificar requisitos organizacionais e normativos aplicáveis à proteção de segredos comerciais em parcerias empresariais;
- Definir um cenário organizacional simulado de compartilhamento de informações entre empresas parceiras;
- Levantar os requisitos de identificação, autenticação, autorização e monitoramento no cenário definido;
- Modelar um conjunto de mecanismos de Gerenciamento de Identidade e Acesso aderente aos requisitos levantados;
- Analisar o modelo proposto no contexto do cenário simulado.

1.4 Estrutura do trabalho

Este trabalho está organizado em sete capítulos. O primeiro apresenta a contextualização do tema, o problema de pesquisa, a justificativa, os objetivos e a organização do estudo. O segundo reúne a fundamentação teórica, abordando o Gerenciamento de Identidade e Acesso, o segredo comercial, a apropriação indevida de informações e os acordos de confidencialidade. O terceiro capítulo descreve os procedimentos metodológicos adotados. O quarto apresenta o cenário organizacional simulado que fundamenta a análise. O quinto descreve o modelo proposto de controle de acesso baseado nos pilares de identificação, autenticação, autorização e monitoramento. O sexto realiza a análise do modelo à luz dos requisitos definidos no cenário.

Por fim, o sétimo capítulo apresenta as considerações finais e indica possibilidades para pesquisas futuras.

2 FUNDAMENTAÇÃO TEÓRICA

A compreensão dos mecanismos de proteção de segredos comerciais em ambientes digitais colaborativos exige a articulação de referenciais teóricos provenientes da segurança da informação, da propriedade intelectual e da gestão organizacional. Nesse contexto, este capítulo reúne os fundamentos conceituais que sustentam a análise desenvolvida ao longo do estudo, abordando o Gerenciamento de Identidade e Acesso como elemento estruturante do controle de acesso a recursos informacionais, a caracterização jurídica e doutrinária do segredo comercial, os riscos associados à apropriação indevida de informações e o papel dos acordos de confidencialidade em parcerias empresariais. A organização dos tópicos busca estabelecer uma base teórica integrada, permitindo compreender de que forma requisitos técnicos, organizacionais e jurídicos convergem para a proteção de informações estratégicas compartilhadas entre organizações.

2.1 Gerenciamento de identidade e acesso

O Gerenciamento de Identidade e Acesso constitui um conjunto de processos, políticas e mecanismos tecnológicos voltados à administração das identidades digitais e ao controle de acesso aos recursos de informação de uma organização. No contexto da segurança da informação, esse conjunto de práticas é responsável por assegurar que apenas usuários devidamente identificados e autenticados possam realizar ações previamente autorizadas sobre sistemas e dados corporativos. No Brasil, esse entendimento está alinhado às diretrizes apresentadas pela ABNT NBR ISO/IEC 27001, que estabelece a necessidade de definição de controles formais de acesso como parte integrante de um sistema de gestão da segurança da informação, associando identidade, autenticação e autorização à proteção dos ativos organizacionais (ABNT, 2022).

Sob a perspectiva operacional, o Gerenciamento de Identidade e Acesso permite à organização administrar de forma estruturada o ciclo de vida das identidades digitais, vinculando usuários, serviços e dispositivos a perfis compatíveis com suas responsabilidades organizacionais. A literatura técnica aponta que a gestão adequada dessas identidades é fundamental para mitigar riscos relacionados ao uso indevido de credenciais e à concessão excessiva de privilégios, constituindo elemento central da governança de segurança da informação (NIST, 2020; ABNT, 2022).

No contexto brasileiro, a Cartilha de Segurança para Internet destaca que o controle de acesso, a gestão de contas e a revisão periódica de privilégios são medidas essenciais para a prevenção de incidentes em ambientes corporativos (CERT.br, 2023). Essa orientação reforça que o gerenciamento de identidades integra um conjunto mais amplo de práticas organizacionais voltadas à proteção dos ativos informacionais.

A literatura técnica e normativa aponta que o Gerenciamento de Identidade e Acesso é estruturado, de forma geral, a partir de quatro funções principais: identificação, autenticação, autorização e auditoria ou monitoramento das atividades realizadas pelos usuários. A identificação está associada ao reconhecimento único de cada entidade no sistema, enquanto a autenticação tem como finalidade comprovar a identidade declarada. A autorização, por sua vez, define quais ações podem ser executadas por cada identidade, e o monitoramento viabiliza a rastreabilidade das atividades executadas nos sistemas, permitindo a realização de auditorias e investigações posteriores (ABNT, 2022; NIST, 2020).

No contexto organizacional, o uso integrado dessas funções contribui diretamente para a aplicação do princípio do menor privilégio e para a redução da exposição a acessos não autorizados. Segundo a norma brasileira ABNT NBR ISO/IEC 27002, os controles de acesso devem ser definidos de acordo com as necessidades do negócio e revisados periodicamente, considerando mudanças no ambiente organizacional, no vínculo dos usuários com a instituição e na sensibilidade dos ativos de informação (ABNT, 2022). Dessa forma, o Gerenciamento de Identidade e Acesso passa a assumir papel estratégico na proteção de informações críticas, especialmente em ambientes colaborativos e de múltiplos usuários.

2.2 Segredo comercial

O segredo comercial é compreendido como um tipo de ativo intangível que reúne informações estratégicas de natureza técnica, comercial ou organizacional, não acessíveis ao público e que conferem vantagem competitiva à empresa que as detém. No campo da propriedade intelectual, Denis Borges Barbosa (2010) define o segredo empresarial como um conjunto de conhecimentos e informações confidenciais que possuem valor econômico justamente em razão de não serem de conhecimento público, sendo protegidos pelo ordenamento jurídico desde que seu titular adote medidas razoáveis para preservar o seu sigilo.

No contexto brasileiro, a tutela jurídica do segredo comercial encontra respaldo na Lei nº 9.279/1996, que regula os direitos e obrigações relativos à propriedade industrial. A referida lei enquadra como prática de concorrência desleal a divulgação, exploração ou utilização, sem

autorização, de informações confidenciais obtidas por meio de relação contratual ou de emprego, quando essas informações possuem caráter reservado e valor econômico para seu titular (BRASIL, 1996). Assim, a proteção do segredo comercial não decorre de registro formal, mas da própria condição de confidencialidade e do esforço do titular em preservar o sigilo.

Do ponto de vista doutrinário, observa-se que o segredo comercial pode abranger fórmulas, métodos de produção, estratégias de mercado, listas de clientes, modelos de negócio, códigos-fonte e outras informações relevantes ao funcionamento da empresa. Segundo Barbosa (2010), a principal característica desse tipo de proteção é a sua dependência direta da adoção de mecanismos organizacionais, contratuais e técnicos capazes de impedir o acesso indiscriminado às informações sensíveis. A ausência dessas medidas pode fragilizar a própria possibilidade de reconhecimento jurídico do segredo.

Nesse sentido, a Organização Mundial da Propriedade Intelectual ressalta que a proteção dos segredos empresariais está condicionada à demonstração de práticas efetivas de segurança da informação, incluindo políticas internas, controle de acesso e restrição de circulação de documentos sensíveis. Tais medidas evidenciam que o titular da informação adota esforços razoáveis para manter o caráter confidencial dos dados, requisito indispensável para sua proteção jurídica (WIPO, 2016).

2.3 Apropriação indevida de informações

A apropriação indevida de informações, no contexto empresarial, está associada ao uso, divulgação ou exploração de dados confidenciais por parte de indivíduos que tiveram acesso legítimo a essas informações, mas que passaram a utilizá-las em desacordo com as finalidades previamente estabelecidas. No direito brasileiro, essa conduta é frequentemente relacionada às práticas de concorrência desleal previstas na Lei da Propriedade Industrial, especialmente quando envolve segredos comerciais obtidos em razão de vínculo contratual, profissional ou de confiança (BRASIL, 1996).

De acordo com Capez (2022), a violação de deveres de lealdade e de confidencialidade, quando vinculada à obtenção de vantagem econômica indevida ou à produção de prejuízo a terceiros, caracteriza conduta ilícita que pode gerar responsabilidade civil e, em determinadas circunstâncias, repercussões na esfera penal. No ambiente corporativo, essa situação ocorre, com frequência, quando empregados, prestadores de serviço ou parceiros utilizam informações estratégicas para beneficiar concorrentes ou para desenvolver atividades próprias em prejuízo do titular da informação.

Sob a perspectiva da gestão da informação, a apropriação indevida apresenta elevada complexidade de detecção, uma vez que, diferentemente dos bens físicos, a cópia ou o acesso não autorizado a dados digitais não implica, necessariamente, a subtração perceptível do ativo original. Segundo a Cartilha de Segurança para Internet, incidentes envolvendo vazamento de informações e uso indevido de dados internos figuram entre os principais eventos de segurança registrados em organizações brasileiras, sendo frequentemente associados à ausência de controles adequados de acesso e de monitoramento das atividades dos usuários (CERT.br, 2023).

Nesse contexto, a literatura nacional sobre segurança da informação enfatiza que a prevenção da apropriação indevida depende não apenas de instrumentos contratuais, como acordos de confidencialidade, mas também da implementação de mecanismos técnicos capazes de restringir acessos, registrar ações e apoiar processos de auditoria. Conforme orienta a ABNT NBR ISO/IEC 27002, o uso de trilhas de auditoria, registros de eventos e segregação de funções constitui prática essencial para a detecção de comportamentos anômalos e para a produção de evidências em processos de apuração de incidentes (ABNT, 2022).

2.4 Acordos de confidencialidade no contexto da proteção de segredos comerciais em parcerias empresariais

No contexto das parcerias empresariais, o compartilhamento de informações estratégicas é normalmente formalizado por meio de acordos de confidencialidade, que têm como finalidade disciplinar o uso, a guarda e a limitação da divulgação de dados sensíveis entre as partes. No direito brasileiro, tais instrumentos decorrem da autonomia privada e da função social dos contratos, previstas no Código Civil, sendo amplamente utilizados como mecanismo jurídico para a proteção do conhecimento empresarial, especialmente em relações de cooperação tecnológica e de transferência de informações sensíveis (Tartuce, 2023).

A utilização de acordos de confidencialidade apresenta relação direta com a tutela jurídica dos segredos comerciais estabelecida pela Lei nº 9.279/1996, sobretudo quando se trata de informações obtidas em razão de vínculo contratual, profissional ou de cooperação entre empresas. Conforme destaca Barbosa (2010), a presença de cláusulas de sigilo constitui elemento relevante para demonstrar que determinada informação é tratada como segredo empresarial, reforçando a intenção do titular de preservar o seu caráter reservado.

A doutrina nacional de propriedade intelectual destaca que o segredo comercial não se caracteriza apenas pelo conteúdo da informação, mas principalmente pela adoção de medidas

concretas para restringir o seu acesso e a sua circulação. Nesse sentido, Pimentel e Basso (2019) ressaltam que a proteção jurídica do segredo depende da demonstração de diligência por parte do titular, o que envolve, necessariamente, a utilização de instrumentos contratuais e organizacionais capazes de limitar o acesso às informações sensíveis apenas às pessoas diretamente envolvidas na atividade econômica.

Os acordos de confidencialidade também exercem a função de delimitar, no plano organizacional, quais informações podem ser compartilhadas, quem são os sujeitos autorizados a acessá-las e quais finalidades justificam esse acesso. Para Kasznar (2018), a definição contratual do escopo das informações e das responsabilidades das partes é indispensável para a adequada gestão de riscos em contratos de cooperação tecnológica, especialmente em ambientes nos quais há circulação intensiva de conhecimento entre empresas.

Entretanto, a literatura jurídica nacional aponta que a formalização contratual, embora necessária, não é suficiente para assegurar, na prática, a proteção das informações em ambientes digitais. Conforme observa Barbosa (2010), o contrato estabelece deveres jurídicos, mas não cria, por si só, mecanismos técnicos de controle de acesso, de rastreabilidade de ações ou de prevenção de usos indevidos, o que torna indispensável a adoção de práticas organizacionais e tecnológicas complementares.

Essa compreensão encontra respaldo nas normas técnicas brasileiras de segurança da informação. A ABNT NBR ISO/IEC 27001 estabelece que os controles de acesso devem considerar, entre outros aspectos, os requisitos legais e contratuais aplicáveis à organização, de modo que as obrigações assumidas em instrumentos formais, como os acordos de confidencialidade, sejam refletidas em políticas, procedimentos e mecanismos tecnológicos de proteção dos ativos de informação (ABNT, 2022).

De forma complementar, a ABNT NBR ISO/IEC 27002 orienta que as regras de concessão, revisão e revogação de acessos devem estar alinhadas às responsabilidades atribuídas aos usuários e às restrições estabelecidas por acordos formais firmados com parceiros e prestadores de serviço, incluindo contratos de confidencialidade, de forma a garantir que o acesso à informação ocorra exclusivamente dentro dos limites definidos pela organização (ABNT, 2022).

Dessa forma, no contexto deste trabalho, os acordos de confidencialidade são compreendidos como requisitos organizacionais que orientam a definição das políticas de acesso aos sistemas de informação em parcerias empresariais que envolvem o compartilhamento de segredos comerciais. Esses instrumentos delimitam, no plano jurídico e organizacional, quais informações devem ser protegidas e quais usuários podem ter acesso a

elas, servindo como base para a modelagem dos mecanismos de Gerenciamento de Identidade e Acesso analisados no cenário simulado adotado neste estudo.

3 METODOLOGIA

A presente pesquisa caracteriza-se como um estudo de natureza aplicada, uma vez que busca analisar a utilização de mecanismos de Gerenciamento de Identidade e Acesso no contexto de um problema organizacional concreto, relacionado à proteção de segredos comerciais em parcerias empresariais. Quanto à abordagem, trata-se de uma pesquisa qualitativa, pois não se fundamenta em mensurações estatísticas, mas na interpretação de conceitos, normas, documentos técnicos e referenciais teóricos voltados à segurança da informação e à proteção da propriedade intelectual, conforme classificação apresentada por Prodanov e Freitas (2013).

Do ponto de vista dos objetivos, a pesquisa possui caráter descritivo, pois procura descrever e analisar características, propriedades e relações entre mecanismos de controle de acesso, requisitos organizacionais e instrumentos de proteção da informação. Segundo Gil (2019), pesquisas descritivas têm como principal finalidade a caracterização de fenômenos e o estabelecimento de relações entre variáveis, sem a interferência direta do pesquisador sobre o objeto investigado, o que se adequa ao propósito deste trabalho.

Em relação aos procedimentos técnicos, o estudo foi desenvolvido a partir de pesquisa bibliográfica e documental. A pesquisa bibliográfica foi utilizada para o levantamento de obras, artigos científicos, normas técnicas e publicações institucionais relacionadas ao Gerenciamento de Identidade e Acesso, à segurança da informação, aos segredos comerciais e à apropriação indevida de informações. Já a pesquisa documental foi empregada na análise de legislações, acordos internacionais e documentos normativos que tratam da proteção da informação e da propriedade intelectual no contexto organizacional. De acordo com Marconi e Lakatos (2017), a combinação de fontes bibliográficas e documentais possibilita maior consistência teórica e melhor compreensão do fenômeno estudado.

Adicionalmente, este trabalho adota a estratégia de construção de um cenário organizacional simulado como base para a análise proposta. O uso de cenários constitui um recurso metodológico amplamente empregado em estudos aplicados na área de gestão e tecnologia da informação, por permitir a representação de situações reais de forma controlada, facilitando a análise de soluções sem a necessidade de intervenção direta em ambientes produtivos. Segundo Godet (2000), a utilização de cenários favorece a compreensão de contextos complexos e a avaliação de alternativas de solução diante de situações organizacionais específicas.

O desenvolvimento da pesquisa foi estruturado em etapas sequenciais conforme Tabela 1, alinhadas aos objetivos específicos definidos neste estudo. Inicialmente, realizou-se a caracterização conceitual dos temas Gerenciamento de Identidade e Acesso, segredo comercial e apropriação indevida de informações, a partir da literatura técnico-científica e normativa. Em seguida, foram identificados os requisitos organizacionais e normativos relacionados à proteção de informações confidenciais em parcerias empresariais, com base na legislação vigente, em normas de segurança da informação e em documentos institucionais.

Tabela 1 - Etapas metodológicas da pesquisa

ETAPA	DESCRIÇÃO	BASE TEÓRICA
1	Caracterização conceitual dos temas centrais	Barbosa (2010); ABNT (2022); NIST (2020)
2	Identificação de requisitos organizacionais e normativos	BRASIL (1996); WTO (1994); ABNT (2022)
3	Definição do cenário organizacional simulado	Godet (2000)
4	Levantamento dos requisitos técnicos de controle de acesso	ABNT (2022); NIST (2020)
5	Modelagem do controle de acesso	Fundamentação teórica consolidada
6	Análise de aderência do modelo ao cenário	Barbosa (2010); ABNT (2022)

Fonte: Elaborado pelo autor

Na etapa seguinte, foi definido um cenário organizacional simulado que representa uma parceria empresarial envolvendo o compartilhamento de informações classificadas como segredos comerciais, em ambiente digital colaborativo. A partir desse cenário, foram levantados os requisitos de identificação, autenticação, autorização e monitoramento necessários para o controle de acesso aos ativos informacionais. Conforme Prodanov e Freitas (2013), a delimitação clara do contexto de análise constitui elemento fundamental para garantir a consistência dos resultados em pesquisas de natureza qualitativa.

Posteriormente, foi elaborado um modelo conceitual de controle de acesso baseado em Gerenciamento de Identidade e Acesso, estruturado nos pilares de identificação, autenticação, autorização e monitoramento, de modo a atender aos requisitos levantados no cenário simulado. Essa etapa corresponde à fase de modelagem da solução, na qual se buscou organizar, de forma sistemática, os mecanismos técnicos descritos na literatura e nos referenciais normativos. Segundo Marconi e Lakatos (2017), a modelagem conceitual permite a abstração dos elementos essenciais do fenômeno estudado, favorecendo a análise de suas relações e implicações.

Por fim, o modelo proposto foi analisado à luz dos requisitos definidos para o cenário simulado, considerando suas contribuições para a proteção dos segredos comerciais e suas limitações no contexto organizacional estudado. Essa análise foi conduzida de forma interpretativa, confrontando os mecanismos propostos com os objetivos de proteção da informação estabelecidos na fundamentação teórica. De acordo com Gil (2019), a análise qualitativa baseada na confrontação entre teoria e evidências documentais constitui procedimento adequado para estudos descritivos e aplicados na área de ciências sociais aplicadas e tecnologia

4 CENÁRIO ORGANIZACIONAL SIMULADO DE COMPARTILHAMENTO DE SEGREDOS COMERCIAIS EM PARCERIAS EMPRESARIAIS

O cenário considerado neste estudo corresponde a uma parceria empresarial voltada ao desenvolvimento conjunto de soluções tecnológicas, na qual uma organização detentora de conhecimento técnico especializado compartilha informações estratégicas com uma empresa parceira responsável por atividades complementares do projeto. Esse tipo de cooperação é recorrente em ambientes de inovação e de desenvolvimento colaborativo, nos quais o intercâmbio de dados técnicos, especificações, códigos e informações comerciais é condição necessária para a execução das atividades, especialmente em iniciativas que envolvem compartilhamento de conhecimento entre organizações distintas (Kasznar, 2018; WIPO, 2016).

No contexto simulado, as informações compartilhadas entre as empresas são classificadas como segredos comerciais, por apresentarem valor econômico, caráter confidencial e relevância estratégica para a competitividade da organização detentora. Conforme discutem Barbosa (2010) e Pimentel e Basso (2019), a caracterização do segredo empresarial está associada não apenas ao conteúdo da informação, mas também à adoção de medidas organizacionais e técnicas voltadas à preservação do sigilo, o que reforça a necessidade de mecanismos formais de controle sobre o acesso aos ativos informacionais.

Considerando a realidade contemporânea das organizações, o cenário pressupõe a utilização de ambientes digitais colaborativos baseados em infraestrutura de computação em nuvem, nos quais usuários internos e parceiros externos acessam recursos de forma remota. A utilização desse tipo de ambiente amplia a superfície de exposição das informações e exige mecanismos mais rigorosos de controle de acesso e de rastreabilidade das ações realizadas sobre os ativos informacionais. De acordo com a ABNT NBR ISO/IEC 27001, ambientes distribuídos e compartilhados demandam a definição clara de políticas de acesso, responsabilidades e controles técnicos capazes de assegurar a confidencialidade, a integridade e a disponibilidade das informações organizacionais (ABNT, 2022).

No cenário proposto, os usuários envolvidos na parceria são classificados em diferentes perfis organizacionais conforme Quadro 2, compreendendo colaboradores da empresa detentora do segredo comercial, profissionais da empresa parceira e usuários temporários eventualmente envolvidos em atividades de suporte técnico, auditoria ou consultoria. Essa segmentação está diretamente relacionada à aplicação do princípio do menor privilégio, segundo o qual cada usuário deve possuir apenas os acessos estritamente necessários para o desempenho de suas atribuições. A literatura nacional e normativa aponta que a ausência de

definição adequada de perfis e privilégios constitui um dos fatores mais recorrentes associados a incidentes de segurança da informação em ambientes corporativos (ABNT, 2022; CERT.br, 2023).

Tabela 2 - Perfis de usuários no cenário simulado

PERFIL	EMPRESA	TIPO DE ACESSO	INFORMAÇÃO SENSÍVEL	NÍVEL DE RISCO
Desenvolvedor interno	Detentora	Leitura/Escrita	Código-fonte	Alto
Analista parceiro	Parceira	Leitura	Documentação técnica	Médio
Consultor externo	Terceiro	Acesso temporário	Logs e relatórios	Médio

Fonte: Elaborado pelo autor

Além da definição dos perfis de usuários, o cenário considera como requisitos centrais a existência de mecanismos capazes de identificar de forma única cada usuário, autenticar adequadamente suas credenciais, autorizar ações de acordo com suas responsabilidades e registrar as atividades executadas sobre os recursos compartilhados. Tais requisitos estão alinhados às diretrizes de controle de acesso e de auditoria previstas nas normas brasileiras de segurança da informação, que recomendam a adoção de mecanismos formais de rastreamento de eventos, investigação de incidentes e produção de evidências digitais em situações de uso indevido da informação (ABNT, 2022).

Por fim, o cenário simulado parte do pressuposto de que as obrigações de sigilo, de limitação de uso e de proteção das informações compartilhadas são formalmente estabelecidas por meio de acordos de confidencialidade firmados entre as empresas participantes da parceria. Conforme ressaltam Tartuce (2023) e Barbosa (2010), tais instrumentos contratuais delimitam deveres jurídicos entre as partes, mas dependem da existência de controles organizacionais e tecnológicos capazes de assegurar sua efetiva aplicação no ambiente operacional. Dessa forma, o cenário apresentado fornece a base organizacional necessária para a modelagem do controle de acesso fundamentado em mecanismos de Gerenciamento de Identidade e Acesso, desenvolvida no capítulo seguinte.

5 MODELO PROPOSTO DE CONTROLE DE ACESSO BASEADO EM GERENCIAMENTO DE IDENTIDADE E ACESSO

O modelo proposto neste trabalho tem como finalidade estruturar, em nível conceitual, um conjunto de mecanismos de controle de acesso orientados à proteção de segredos comerciais no contexto de parcerias empresariais, considerando o cenário organizacional simulado apresentado no capítulo anterior. A modelagem parte dos requisitos organizacionais, jurídicos e técnicos identificados ao longo da fundamentação teórica, especialmente aqueles relacionados à necessidade de restrição de acesso, rastreabilidade das ações e preservação da confidencialidade das informações estratégicas compartilhadas entre as organizações envolvidas (ABNT, 2022; Barbosa, 2010).

A concepção do modelo está alinhada às diretrizes de controle de acesso previstas nas normas brasileiras de segurança da informação, que recomendam a adoção de mecanismos formais para identificação de usuários, autenticação de identidades, autorização de operações e registro das atividades realizadas sobre os ativos de informação, de modo a garantir a adequada proteção dos recursos organizacionais em ambientes colaborativos e distribuídos (ABNT, 2022). Adicionalmente, tais mecanismos são compatíveis com as recomendações técnicas amplamente consolidadas na literatura de segurança da informação, que tratam o gerenciamento de identidades como elemento estruturante para a aplicação de políticas de acesso e para a produção de evidências em processos de auditoria e investigação de incidentes (NIST, 2020).

Dessa forma, o modelo é estruturado a partir de quatro pilares fundamentais do Gerenciamento de Identidade e Acesso — identificação, autenticação, autorização e monitoramento — os quais são analisados de maneira integrada, considerando as características do ambiente de parceria empresarial e os requisitos decorrentes dos acordos de confidencialidade. Cada pilar é apresentado nas subseções a seguir, descrevendo-se sua função no modelo proposto e sua contribuição para a proteção dos segredos comerciais no cenário organizacional simulado.

5.1 Identificação das identidades

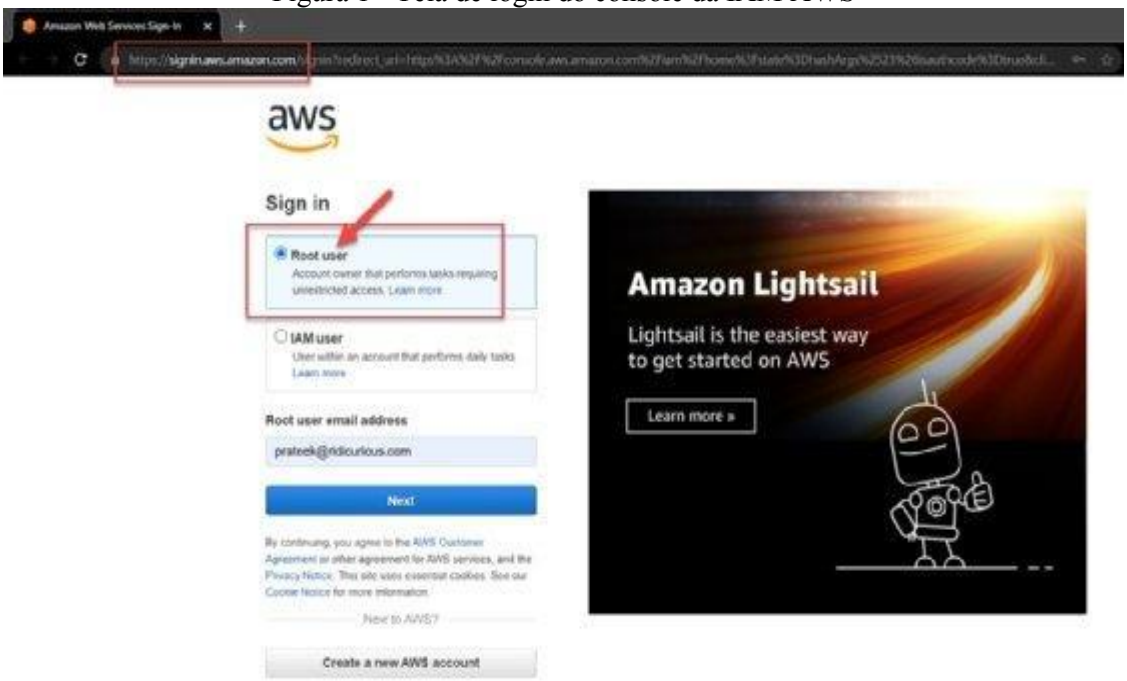
No modelo proposto, a identificação das identidades corresponde ao processo de estabelecimento de uma representação digital única para cada entidade que interage com os recursos compartilhados no contexto da parceria empresarial, sejam elas pessoas, serviços ou aplicações. Essa identificação constitui a base para a aplicação das políticas de controle de

acesso, pois permite associar cada identidade a responsabilidades organizacionais, perfis de atuação e restrições previamente definidas no ambiente da parceria.

No contexto do cenário organizacional simulado, a identificação é estruturada de forma a diferenciar usuários pertencentes à empresa detentora do segredo comercial, usuários da empresa parceira e usuários temporários, eventualmente vinculados a atividades de suporte, auditoria ou consultoria. Essa distinção é essencial para a definição de políticas de acesso compatíveis com as atribuições de cada grupo e para a aplicação do princípio do menor privilégio, garantindo que cada identidade possua apenas os acessos necessários ao desempenho de suas funções.

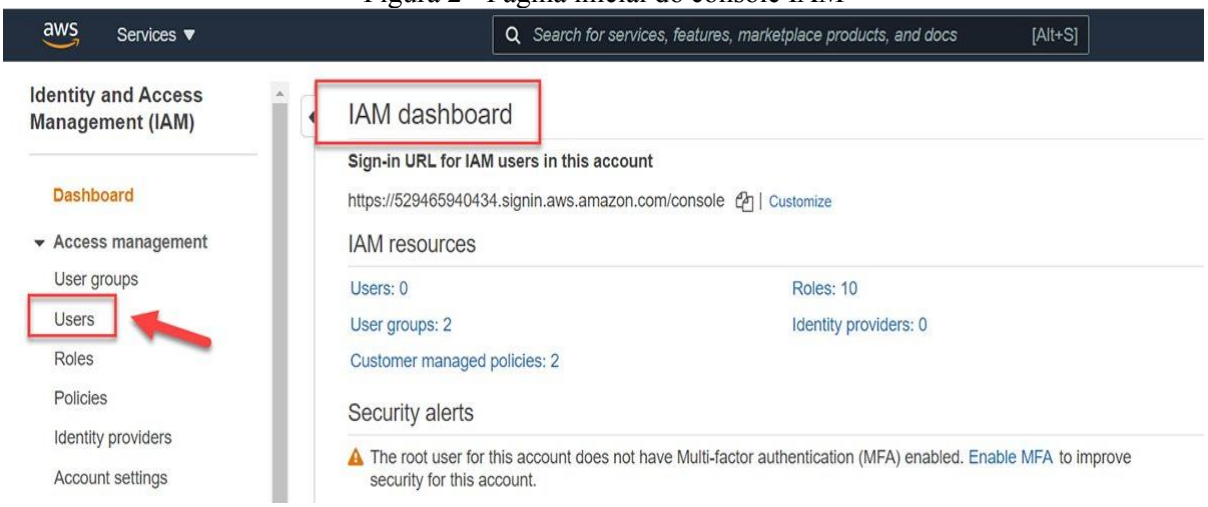
Além da criação formal das identidades, o modelo prevê a vinculação de informações descritivas associadas a cada usuário, tais como função organizacional, vínculo com a empresa de origem e finalidade de acesso aos recursos compartilhados. Essas informações são utilizadas como elementos de apoio à organização das identidades e à posterior aplicação de políticas de autorização, permitindo maior controle sobre a concessão de privilégios no ambiente colaborativo.

Figura 1 - Tela de login do console da IAM AWS



Fonte: Adaptado pelo autor.

Figura 2 - Página inicial do console IAM

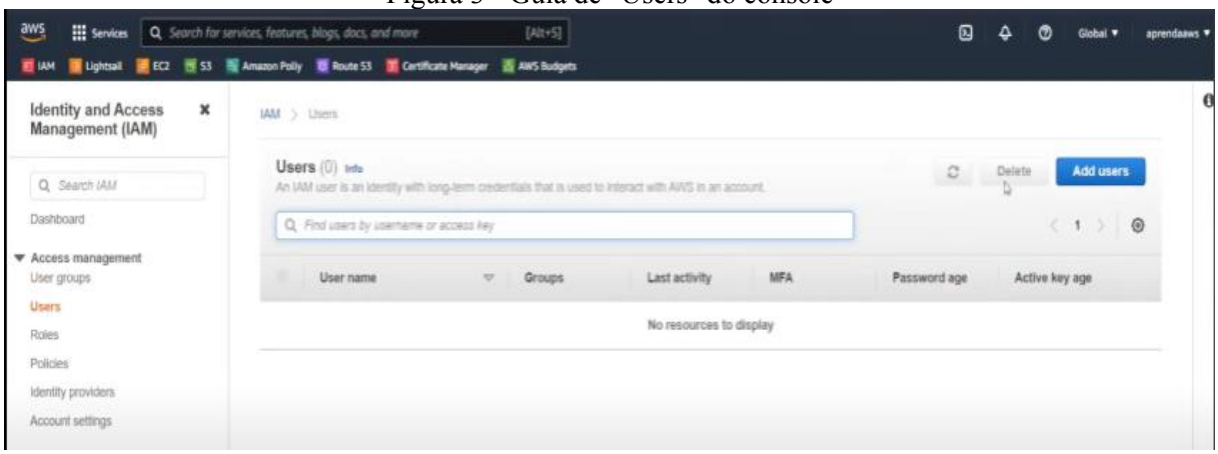


Fonte: Elaborado pelo autor.

A criação das identidades no modelo proposto é realizada de forma centralizada pela área responsável pela gestão do ambiente tecnológico da parceria, garantindo que somente usuários previamente autorizados e formalmente vinculados às empresas participantes possam ser registrados no sistema. Essa centralização reduz o risco de criação indevida de contas e facilita os processos de auditoria e de revisão periódica de acessos.

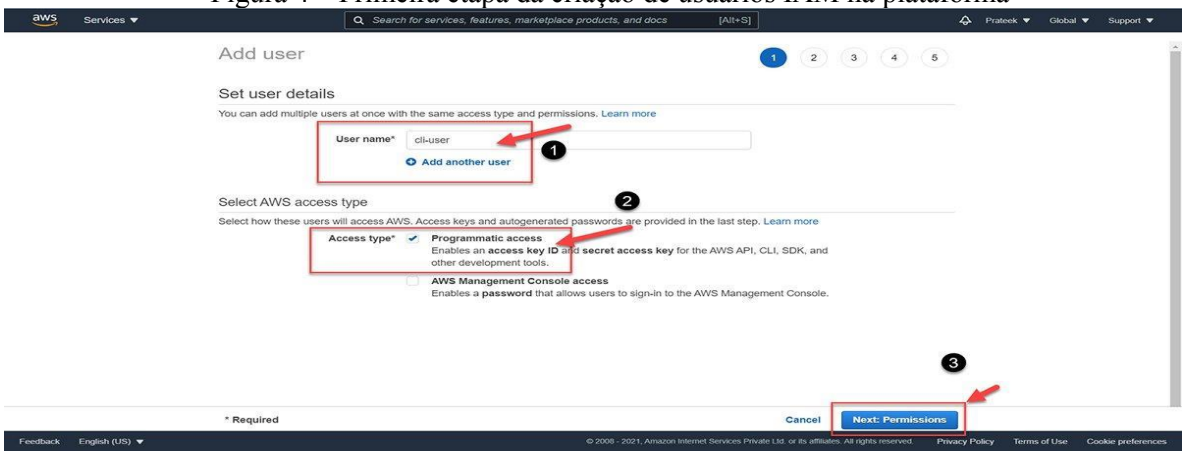
Cada identidade criada passa a representar, no ambiente digital, o vínculo organizacional do usuário com a parceria, permitindo que todas as solicitações de acesso aos recursos compartilhados sejam avaliadas a partir dessa identificação. Dessa forma, a identidade digital torna-se o elemento inicial de todo o processo de autenticação, autorização e monitoramento previsto no modelo, conforme Figura 3.

Figura 3 - Guia de "Users" do console



Fonte: Elaborado pelo autor.

Figura 4 – Primeira etapa da criação de usuários IAM na plataforma

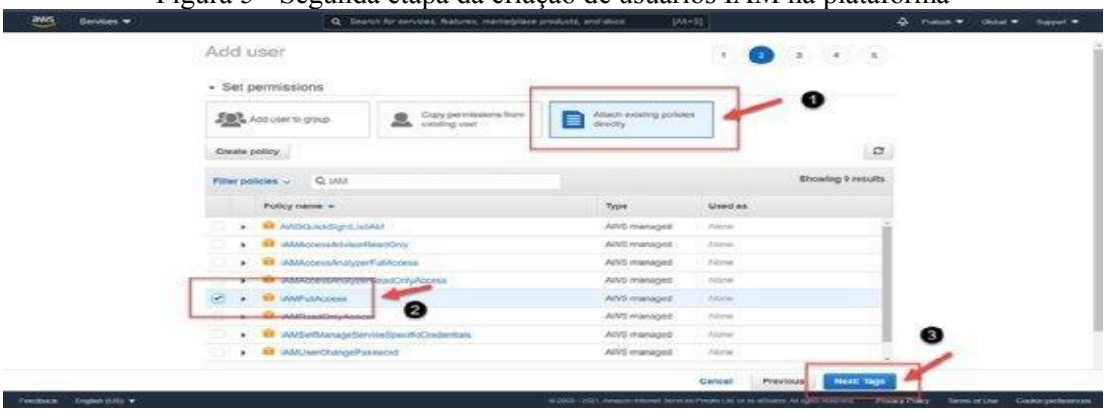


Fonte: Elaborado pelo autor.

No modelo adotado, as identidades são organizadas de forma a permitir sua associação posterior a políticas de acesso e a atributos organizacionais. Essa organização facilita a administração de ambientes com múltiplos usuários e diferentes perfis, além de reduzir a complexidade na concessão e na revogação de acessos ao longo do ciclo de vida da parceria empresarial.

A definição de convenções de nomenclatura e de identificação interna das contas também é considerada parte do modelo, pois contribui para a rastreabilidade das ações executadas no ambiente e para a correta identificação dos responsáveis por acessos e operações realizadas sobre os ativos informacionais.

Figura 5 - Segunda etapa da criação de usuários IAM na plataforma



Fonte: Elaborado pelo autor.

Além da identificação básica do usuário, o modelo proposto prevê o uso de informações complementares associadas às identidades, como atributos organizacionais (tags), que indicam o papel do usuário no contexto da parceria, sua empresa de origem ou sua finalidade de acesso.

Esses atributos passam a integrar a identidade digital e são utilizados posteriormente como referência para a aplicação de políticas de controle de acesso mais flexíveis.

O uso de atributos associados às identidades possibilita a aplicação de políticas baseadas em características organizacionais, favorecendo a escalabilidade do modelo e a adaptação a mudanças no quadro de usuários, especialmente em parcerias que envolvem equipes multidisciplinares e temporárias.

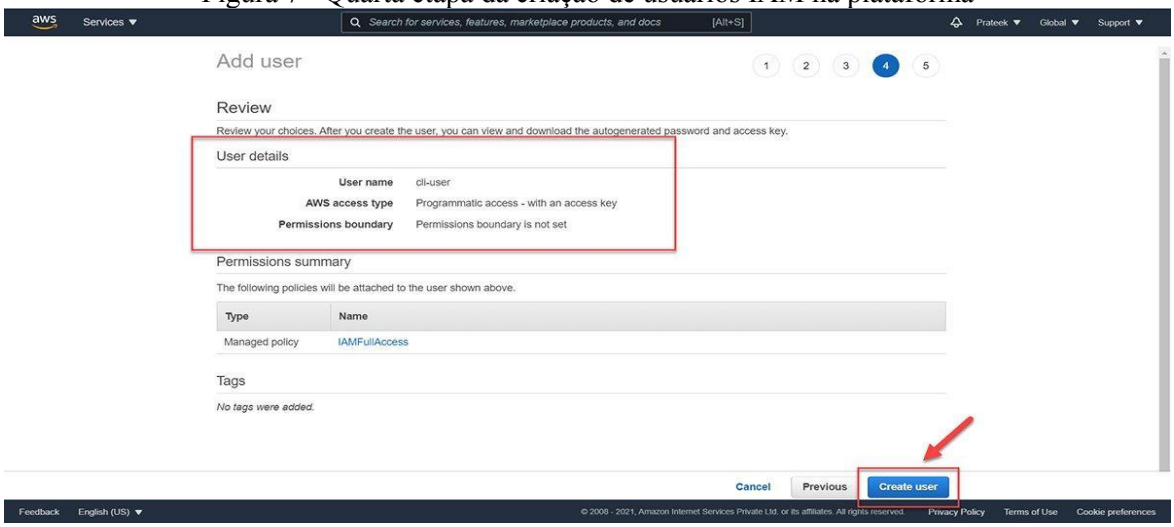
Figura 6 — Terceira etapa da criação de usuários IAM na plataforma.

Fonte: Elaborado pelo autor.

Após a definição das informações de identificação e dos atributos organizacionais, o modelo prevê a validação das configurações da identidade antes de sua disponibilização para acesso ao ambiente colaborativo. Essa etapa permite verificar se os dados de identificação, os vínculos organizacionais e as informações de apoio estão de acordo com as regras estabelecidas pela parceria empresarial.

Essa validação contribui para reduzir falhas de cadastro que possam resultar em concessões indevidas de acesso ou dificuldades de rastreamento posterior das atividades executadas pelos usuários.

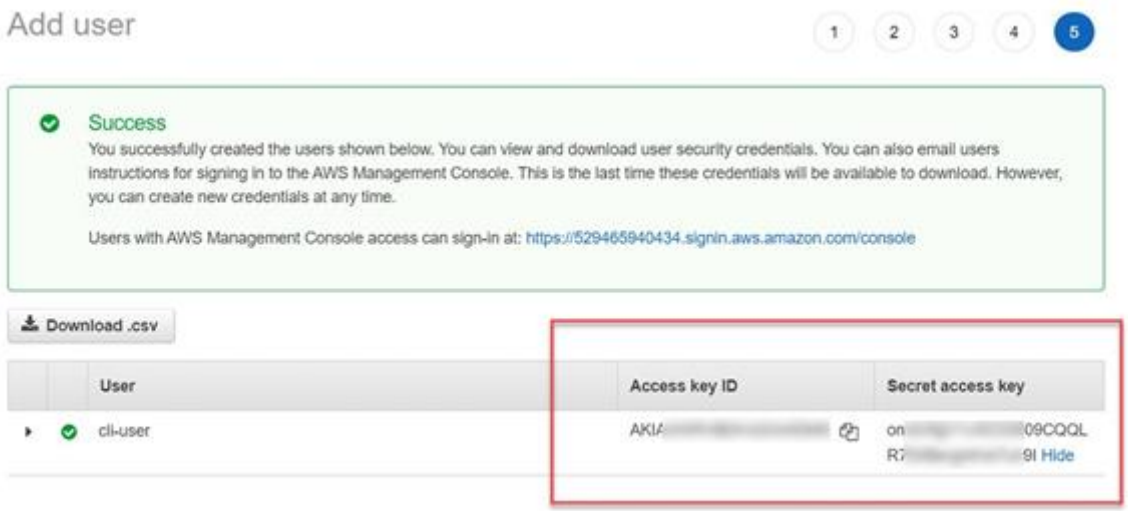
Figura 7 - Quarta etapa da criação de usuários IAM na plataforma



Fonte: Elaborado pelo autor.

Concluído o processo de identificação, as informações de credenciais e de acesso inicial são disponibilizadas aos respectivos usuários, observando-se os procedimentos organizacionais de entrega segura dessas informações. No modelo proposto, essa etapa representa o encerramento do ciclo de identificação da identidade digital, a partir do qual o usuário passa a estar apto a submeter solicitações de acesso aos recursos compartilhados, que serão posteriormente tratadas pelos mecanismos de autenticação e autorização.

Figura 8 - Quinta etapa da criação de usuários IAM na plataforma.



Fonte: Elaborado pelo autor.

5.2 Autenticação dos usuários

No modelo proposto, a autenticação corresponde ao mecanismo responsável por validar se a identidade digital previamente cadastrada no sistema realmente pertence ao usuário que solicita acesso aos recursos compartilhados no contexto da parceria empresarial. Enquanto a identificação estabelece a existência da identidade no ambiente, a autenticação tem a função de confirmar essa identidade por meio da verificação de credenciais, reduzindo o risco de uso indevido de contas e de acesso não autorizado a informações classificadas como segredos comerciais.

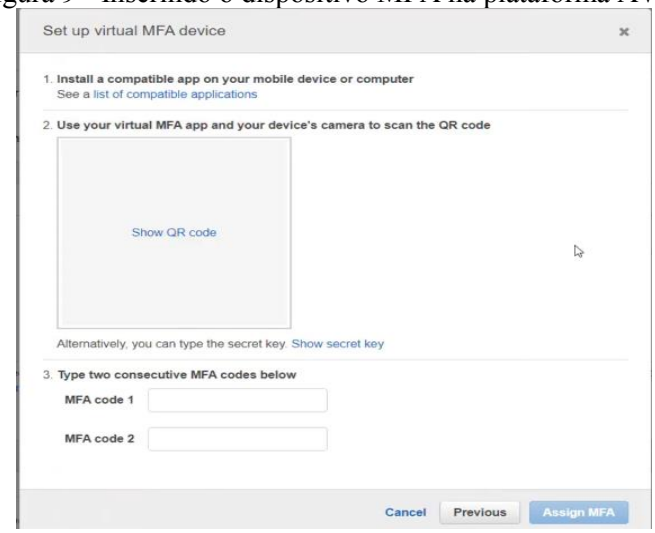
As boas práticas de segurança da informação indicam que mecanismos de autenticação devem ser estruturados a partir de fatores distintos de verificação, tradicionalmente classificados como algo que o usuário sabe, algo que o usuário possui e algo que o usuário é. A adoção combinada desses fatores, especialmente em ambientes que tratam informações sensíveis, é recomendada por diretrizes técnicas e normas de segurança como medida para mitigar riscos associados a comprometimento de credenciais (ABNT, 2022; NIST, 2022).

Considerando o cenário organizacional simulado, no qual há compartilhamento de informações estratégicas entre empresas distintas por meio de ambiente digital colaborativo, o modelo adota a autenticação multifator como mecanismo prioritário de validação das identidades. A autenticação multifator exige a combinação de dois ou mais fatores independentes para liberar o acesso, reduzindo significativamente a probabilidade de que o simples conhecimento de uma senha seja suficiente para comprometer o ambiente.

A utilização de múltiplos fatores de autenticação mostra-se particularmente relevante em ambientes de computação em nuvem e acesso remoto, nos quais as credenciais podem ser alvo de ataques de força bruta, phishing ou engenharia social. Conforme orienta a ABNT NBR ISO/IEC 27002, a adoção de mecanismos adicionais de verificação é recomendada para acessos privilegiados ou para sistemas que processam informações críticas, reforçando a proteção contra acessos não autorizados (ABNT, 2022).

No modelo proposto, a autenticação multifator pode envolver o uso combinado de senha pessoal e dispositivo adicional de verificação, como aplicativo autenticador virtual ou token associado individualmente à identidade do usuário. Essa associação fortalece o vínculo entre o usuário e sua identidade digital, tornando mais difícil a exploração indevida das credenciais.

Figura 9 - Inserindo o dispositivo MFA na plataforma AWS.



Fonte: Elaborado pelo autor.

Além da ativação do mecanismo multifator, o modelo prevê que a gestão dos dispositivos de autenticação esteja sujeita a regras organizacionais previamente definidas, incluindo procedimentos para ativação, substituição e revogação de dispositivos em caso de perda, comprometimento ou desligamento do usuário da parceria empresarial. A manutenção desse controle é essencial para evitar que dispositivos vinculados a identidades inativas permaneçam habilitados no ambiente.

Figura 10 – Política de gerenciamento de dispositivos virtuais do AWS

```
        "Sid": "AllowManageOwnVirtualMFADevice",
        "Effect": "Allow",
        "Action": [
            "iam:CreateVirtualMFADevice"
        ],
        "Resource": "arn:aws:iam::*:mfa/*"
    },
    {
        "Sid": "AllowManageOwnUserMFA",
        "Effect": "Allow",
        "Action": [
            "iam:DeactivateMFADevice",
            "iam:EnableMFADevice",
            "iam:ListMFADevices",
            "iam:ResyncMFADevice"
        ],
        "Resource": "arn:aws:iam::*:user/${aws:username}"
```

Fonte: Elaborado pelo autor.

Ao estruturar a autenticação como etapa obrigatória e robusta no processo de acesso aos recursos compartilhados, o modelo proposto contribui para reduzir riscos associados ao uso indevido de credenciais e reforça a proteção dos segredos comerciais no ambiente colaborativo.

A autenticação, portanto, funciona como barreira intermediária entre a identificação da identidade digital e a autorização das ações solicitadas, garantindo que apenas usuários devidamente validados possam prosseguir para as etapas seguintes do controle de acesso.

5.3 Autorização de acessos

No modelo proposto, a autorização corresponde ao mecanismo responsável por definir quais ações cada identidade autenticada pode executar sobre os recursos compartilhados no ambiente da parceria empresarial. Enquanto a identificação estabelece quem é o usuário e a autenticação confirma sua identidade, a autorização determina o alcance efetivo de suas permissões, vinculando cada identidade a um conjunto específico de privilégios previamente definidos.

A definição adequada das permissões é elemento central para a proteção dos segredos comerciais no cenário simulado, pois permite restringir o acesso às informações estratégicas exclusivamente aos usuários que necessitam delas para o desempenho de suas funções. A norma ABNT NBR ISO/IEC 27002 recomenda que os direitos de acesso sejam concedidos de acordo com as necessidades do negócio e revisados periodicamente, observando-se o princípio do menor privilégio e a segregação de funções (ABNT, 2022).

No contexto do modelo adotado, as permissões são estruturadas por meio de políticas formais de acesso, que especificam quais recursos podem ser utilizados, quais operações são permitidas e sob quais condições essas ações podem ser executadas. Essas políticas funcionam como regras lógicas aplicadas às identidades autenticadas, permitindo ou negando operações de acordo com critérios previamente estabelecidos.

A utilização de políticas formais de autorização possibilita maior controle sobre o ambiente colaborativo, especialmente quando há múltiplos perfis de usuários pertencentes a organizações distintas. Ao associar políticas específicas a grupos ou a identidades individuais, o modelo permite a diferenciação clara entre usuários com acesso administrativo, usuários com acesso restrito a determinados documentos e usuários com permissões temporárias vinculadas a atividades específicas.

Além das permissões baseadas em perfis, o modelo proposto contempla a utilização de atributos organizacionais associados às identidades como elementos adicionais de controle. Essa abordagem, conhecida como controle de acesso baseado em atributos (ABAC), permite que decisões de autorização considerem características como função do usuário, empresa de origem ou classificação da informação acessada. Conforme indicado na literatura técnica e em

diretrizes normativas, a utilização de atributos favorece maior flexibilidade e escalabilidade na gestão de acessos, especialmente em ambientes dinâmicos (NIST, 2020).

Figura 11 - Política ABAC AWS.

Fonte: Elaborado pelo autor.

No modelo, os atributos associados às identidades são utilizados para estabelecer condições específicas nas políticas de autorização, de modo que o acesso a determinados recursos seja concedido apenas quando houver correspondência entre o perfil do usuário e a classificação da informação. Essa estratégia contribui para reforçar o controle sobre segredos comerciais, evitando que informações sensíveis sejam acessadas por usuários que, embora autenticados, não possuam vínculo adequado com o contexto da atividade.

Figura 12 - Condição de Igualdade de etiqueta

```
        "Sid": "AllActionsSecretsManagerSameProjectSameTeam",
        "Effect": "Allow",
        "Action": "secretsmanager:*",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:ResourceTag/access-project": "${aws:PrincipalTag/access-
project}",
                "aws:ResourceTag/access-team": "${aws:PrincipalTag/access-
team}",
                "aws:ResourceTag/cost-center": "${aws:PrincipalTag/cost-center}"
            },
```

Fonte: Elaborado pelo autor.

A estruturação das políticas de autorização no modelo proposto também prevê a revisão periódica das permissões concedidas, especialmente em situações de alteração de função,

encerramento de contrato ou conclusão de etapas do projeto. Essa prática está alinhada às recomendações das normas de segurança da informação, que enfatizam a necessidade de atualização contínua dos direitos de acesso para evitar privilégios excessivos ou obsoletos (ABNT, 2022).

Ao integrar políticas formais de autorização, controle baseado em atributos e revisão periódica de privilégios, o modelo fortalece a proteção dos segredos comerciais no ambiente colaborativo simulado. A autorização, nesse contexto, funciona como o mecanismo decisório central do controle de acesso, traduzindo as obrigações contratuais e os requisitos organizacionais em regras técnicas aplicáveis às identidades autenticadas.

5.4 Monitoramento das atividades

No modelo proposto, o monitoramento das atividades corresponde ao mecanismo responsável por registrar e armazenar as ações realizadas pelas identidades autenticadas sobre os recursos compartilhados no ambiente da parceria empresarial. Essa etapa complementa os mecanismos preventivos de identificação, autenticação e autorização, permitindo a rastreabilidade das operações executadas e a responsabilização dos usuários em caso de utilização inadequada das informações classificadas como segredos comerciais.

A manutenção de registros de eventos é recomendada pelas normas de segurança da informação como prática essencial para ambientes que tratam informações sensíveis. A ABNT NBR ISO/IEC 27002 orienta que os registros de eventos relevantes — como tentativas de acesso, operações realizadas e alterações em configurações críticas — sejam devidamente coletados, protegidos contra modificações indevidas e mantidos por período compatível com as necessidades organizacionais e legais (ABNT, 2022). No contexto do modelo proposto, tais registros são associados às identidades digitais previamente cadastradas, permitindo que cada ação realizada no ambiente colaborativo seja vinculada a um usuário específico.

A geração de logs vinculados às identidades possibilita a visualização detalhada das operações executadas, incluindo o tipo de ação realizada e o recurso acessado. Conforme ilustrado na Figura 13, é possível observar o registro de um evento associado a determinada identidade, evidenciando informações como a operação solicitada e o contexto em que ela ocorreu. Esse tipo de registro reforça a rastreabilidade das ações e permite que a organização mantenha histórico auditável das atividades realizadas no ambiente.

Figura 13 - Politica no IAM AWS.


```
"eventVersion": "1.09",
"userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE:Role-Session-Name",
    "arn": "arn:aws:sts::111122223333:assumed-role/Role-Name/Role-Session-Name",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
        "sessionIssuer": {
            "type": "Role",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:iam::111122223333:role/Admin",
            "accountId": "111122223333",
            "userName": "Admin"
```


Fonte: Elaborado pelo autor.

A Figura 14 apresenta a continuidade do detalhamento desse tipo de registro, evidenciando informações complementares relacionadas à identidade envolvida, ao recurso acessado e aos parâmetros da operação executada. A visualização estruturada desses dados demonstra como o monitoramento pode ser utilizado para identificar comportamentos atípicos ou acessos que não estejam alinhados às responsabilidades atribuídas ao usuário no contexto da parceria empresarial.

Figura 14 - Continuação de politica no IAM AWS.


```
"eventTime": "2024-09-09T17:51:44Z",
"eventSource": "iam.amazonaws.com",
"eventName": "GetUserPolicy",
"awsRegion": "us-east-1",
"sourceIPAddress": "192.0.2.101",
"userAgent": "aws-cli/1.16.96 Python/2.7.8 Linux/10 botocore/1.12.86",
"requestParameters": {
    "userName": "ExampleIAMUserName",
    "policyName": "ExamplePoliccyName"
```


Fonte: Elaborado pelo autor

A vinculação entre identidade digital e registro de eventos é elemento central para a produção de evidências em casos de investigação de incidentes relacionados à apropriação indevida de informações. Conforme discutido por Barbosa (2010), a proteção jurídica do segredo comercial depende da adoção de medidas concretas de controle e diligência por parte do titular da informação. A existência de registros auditáveis das ações realizadas no ambiente

reforça essa diligência e contribui para demonstrar que a organização adotou mecanismos técnicos compatíveis com a necessidade de preservação do sigilo.

Além de permitir a apuração de incidentes após sua ocorrência, o monitoramento contínuo favorece a detecção preventiva de comportamentos anômalos, como acessos em horários incomuns, tentativas repetidas de leitura de recursos não vinculados ao perfil do usuário ou alterações não previstas em políticas de autorização. A análise periódica desses registros é recomendada pelas normas de segurança da informação como prática de governança e gestão de riscos, contribuindo para a melhoria contínua dos controles implementados (ABNT, 2022).

Assim, no modelo proposto, o monitoramento não é tratado apenas como mecanismo reativo, mas como componente estratégico do controle de acesso, integrando-se aos demais pilares do Gerenciamento de Identidade e Acesso. Enquanto identificação, autenticação e autorização atuam de forma preventiva, o monitoramento acrescenta uma dimensão de supervisão e responsabilização, assegurando que as operações realizadas no ambiente colaborativo possam ser rastreadas, analisadas e, quando necessário, utilizadas como base para medidas corretivas ou jurídicas.

6 ANÁLISE DO MODELO PROPOSTO NO CENÁRIO ORGANIZACIONAL SIMULADO

A análise do modelo proposto tem como objetivo verificar sua aderência aos requisitos organizacionais, jurídicos e técnicos identificados no cenário simulado de compartilhamento de segredos comerciais entre empresas parceiras. Conforme discutido nos capítulos anteriores, a proteção efetiva de informações classificadas como segredos comerciais depende da adoção de medidas concretas que restrinjam o acesso, assegurem a rastreabilidade das ações e demonstrem diligência por parte do titular da informação (Barbosa, 2010; ABNT, 2022).

No cenário organizacional descrito, os principais requisitos de proteção envolvem a identificação formal dos usuários, a validação segura de suas credenciais, a limitação de acesso às informações de acordo com suas atribuições e a capacidade de registrar e auditar as operações realizadas no ambiente colaborativo. Esses requisitos derivam tanto das obrigações contratuais estabelecidas por meio dos acordos de confidencialidade quanto das boas práticas normativas de segurança da informação (ABNT, 2022; PIMENTEL; BASSO, 2019).

6.1 Aderência aos requisitos de identificação

O primeiro requisito identificado no cenário refere-se à necessidade de vincular cada ação executada no ambiente digital a uma identidade única e formalmente cadastrada. O modelo proposto atende a essa exigência ao estruturar o processo de criação e gestão de identidades digitais de forma centralizada, associando cada usuário a um vínculo organizacional específico e a atributos que indicam sua função no contexto da parceria.

Essa estrutura contribui para a responsabilização individual e para a segregação adequada de perfis, permitindo que acessos sejam concedidos ou revogados de maneira controlada. Além disso, a formalização da identidade digital está alinhada às recomendações normativas que exigem procedimentos documentados para criação, alteração e exclusão de contas (ABNT, 2022). Dessa forma, o modelo demonstra aderência ao requisito de identificação inequívoca dos usuários.

6.2 Aderência aos requisitos de autenticação

No que se refere à autenticação, o cenário simulado exige mecanismos capazes de reduzir o risco de uso indevido de credenciais, especialmente em ambiente de computação em

nuvem com acesso remoto. O modelo atende a esse requisito por meio da adoção de autenticação multifator, combinando diferentes fatores de verificação para validação da identidade do usuário.

A utilização de múltiplos fatores fortalece a segurança do acesso, mitigando riscos associados a vazamento de senhas ou ataques de engenharia social, em consonância com as recomendações da ABNT NBR ISO/IEC 27002 e das diretrizes internacionais de identidade digital (ABNT, 2022; NIST, 2022). Assim, o modelo apresenta aderência adequada ao requisito de validação robusta das identidades no ambiente colaborativo.

6.3 Aderência aos requisitos de autorização

O requisito central do cenário organizacional está relacionado à limitação de acesso às informações classificadas como segredos comerciais, de modo que apenas usuários com necessidade legítima possam visualizar ou manipular determinados recursos. O modelo proposto atende a esse requisito por meio da utilização de políticas formais de autorização associadas às identidades e, adicionalmente, pela aplicação de controle baseado em atributos.

A combinação entre políticas explícitas e atributos organizacionais permite maior granularidade na definição das permissões, favorecendo a aplicação do princípio do menor privilégio. Conforme recomendam as normas de segurança da informação, a concessão de direitos de acesso deve estar vinculada às necessidades do negócio e ser periodicamente revisada (ABNT, 2022). Nesse sentido, o modelo demonstra aderência satisfatória ao requisito de restrição controlada de acesso às informações estratégicas.

6.4 Aderência aos requisitos de monitoramento e responsabilização

A proteção dos segredos comerciais, conforme discutido anteriormente, depende da adoção de medidas que permitam demonstrar diligência na preservação do sigilo (Barbosa, 2010). No cenário analisado, isso implica a capacidade de registrar e auditar as ações realizadas pelos usuários sobre os ativos informacionais. O modelo proposto incorpora mecanismos de monitoramento capazes de registrar eventos associados às identidades autenticadas, permitindo a rastreabilidade das operações executadas. Essa capacidade favorece tanto a investigação de incidentes quanto a demonstração de conformidade com obrigações contratuais e normativas. De acordo com a ABNT NBR ISO/IEC 27002, a manutenção de registros de eventos constitui

prática essencial para a gestão de incidentes e para a produção de evidências (ABNT, 2022). Assim, o modelo apresenta aderência ao requisito de monitoramento e responsabilização.

A análise da aderência do modelo aos requisitos identificados no cenário simulado evidencia que a proteção dos segredos comerciais não pode ser compreendida de forma fragmentada, restrita a controles isolados. A efetividade do modelo decorre da integração sistêmica entre seus pilares, de modo que identificação, autenticação, autorização e monitoramento atuem de forma complementar e encadeada. Conforme orientam as normas de gestão da segurança da informação, a ausência ou fragilidade de um desses componentes compromete o equilíbrio do sistema de proteção, uma vez que a segurança da informação depende da coerência entre políticas, processos e mecanismos técnicos (ABNT, 2022; NIST, 2020). Assim, a robustez do modelo não reside apenas na adoção de controles específicos, mas na articulação estruturada entre eles.

Além disso, sob a perspectiva jurídica, a análise demonstra que o modelo contribui para atender ao requisito de adoção de "medidas razoáveis de proteção", elemento central para o reconhecimento da tutela dos segredos comerciais tanto no âmbito do TRIPS quanto na legislação brasileira (WTO, 1994; BRASIL, 1996). A implementação de mecanismos formais de controle de acesso, autenticação multifator e registros auditáveis reforça a demonstração de diligência por parte da organização, elemento frequentemente destacado pela doutrina como condição para a manutenção do status jurídico do segredo empresarial (BARBOSA, 2010; PIMENTEL; BASSO, 2019). Dessa forma, o modelo analisado não apenas atende a requisitos técnicos de segurança da informação, mas também contribui para sustentar a proteção jurídica dos ativos intangíveis compartilhados no contexto da parceria empresarial.

Tabela 3 – Síntese de aderência do modelo aos requisitos do cenário

REQUISITO IDENTIFICADO NO CENÁRIO	**PILAR DO MODELO**	**MECANISMO ESTRUTURANTE ADOTADO**	**CONTRIBUIÇÃO PARA A PROTEÇÃO DO SEGREDO COMERCIAL**
Identificação formal e inequívoca dos usuários	Identificação	Cadastro centralizado de identidades digitais com vínculo organizacional definido	Permite vincular cada ação a um usuário específico, reforçando responsabilização individual
Validação segura das credenciais de acesso	Autenticação	Autenticação multifator associada à identidade digital	Reduz riscos de comprometimento de contas e acesso indevido por terceiros
Restrição de acesso conforme necessidade funcional	Autorização	Políticas formais de permissão e controle baseado em atributos (ABAC)	Assegura aplicação do princípio do menor privilégio e limita exposição de informações sensíveis

Registro e rastreabilidade das ações realizadas	Monitoramento	Geração e armazenamento de logs vinculados às identidades autenticadas	Possibilita auditoria, investigação de incidentes e demonstração de diligência na proteção do sigilo

Fonte: Elaborado pelo autor

O Quadro 3 sintetiza a relação entre os requisitos identificados no cenário organizacional simulado e os mecanismos estruturantes do modelo de controle de acesso proposto. Observa-se que cada exigência derivada das obrigações contratuais e normativas encontra correspondência em um dos pilares do Gerenciamento de Identidade e Acesso, evidenciando a coerência interna da modelagem adotada.

A estrutura apresentada demonstra que o modelo não se limita à adoção isolada de mecanismos técnicos, mas integra identificação, autenticação, autorização e monitoramento de forma articulada, assegurando que as obrigações de confidencialidade estabelecidas na parceria empresarial sejam traduzidas em controles operacionais efetivos. Essa correspondência reforça a aderência do modelo aos princípios de proteção da informação previstos nas normas de segurança e na legislação relacionada aos segredos comerciais (ABNT, 2022; Barbosa, 2010).

Além disso, a organização dos requisitos e mecanismos em formato sintético permite visualizar de maneira clara como cada componente do modelo contribui para a redução de riscos associados à apropriação indevida de informações estratégicas. Dessa forma, o modelo apresenta consistência lógica e alinhamento com as boas práticas de governança de acesso em ambientes colaborativos.

6.5 Contribuições e limitações do modelo

A análise realizada indica que o modelo proposto apresenta aderência consistente aos requisitos identificados no cenário organizacional simulado, integrando os quatro pilares do Gerenciamento de Identidade e Acesso de forma coerente com as exigências contratuais e normativas relacionadas à proteção de segredos comerciais.

Como contribuição, destaca-se a integração entre dimensões jurídica, organizacional e técnica, permitindo que obrigações contratuais sejam traduzidas em mecanismos concretos de controle de acesso. A utilização de autenticação multifator e de políticas baseadas em atributos amplia a robustez do modelo e favorece sua aplicação em ambientes com múltiplos perfis e diferentes níveis de sensibilidade informacional.

Entretanto, é importante reconhecer que o modelo foi analisado a partir de um cenário simulado, não tendo sido submetido a validação empírica em ambiente organizacional real.

Dessa forma, aspectos relacionados à usabilidade, impacto operacional e custos de implementação não foram avaliados de maneira prática. Estudos futuros poderiam contemplar a aplicação do modelo em contexto real de parceria empresarial, permitindo avaliação mais abrangente de sua efetividade.

7 CONSIDERAÇÕES FINAIS

O presente trabalho teve como objetivo analisar a aplicação de mecanismos de Gerenciamento de Identidade e Acesso como apoio à proteção de segredos comerciais em um cenário organizacional simulado de parceria empresarial. A fundamentação evidenciou que a proteção jurídica do segredo comercial depende não apenas da formalização de obrigações contratuais, mas também da adoção de medidas organizacionais e técnicas capazes de restringir o acesso às informações estratégicas e de demonstrar diligência na preservação do sigilo.

A análise realizada evidenciou que a estruturação do controle de acesso com base nos quatro pilares do Gerenciamento de Identidade e Acesso, identificação, autenticação, autorização e monitoramento, o que permite a tradução das exigências contratuais e normativas em mecanismos técnicos concretos. A identificação formal das identidades digitais favorece a responsabilização individual, a autenticação multifator reduz o risco de uso indevido de credenciais; as políticas de autorização baseadas em perfis e atributos viabilizam a aplicação do princípio do menor privilégio e o monitoramento das atividades assegura rastreabilidade e suporte à auditoria, conforme recomendado pelas normas de segurança da informação.

No cenário organizacional simulado, observou-se que o modelo proposto apresenta aderência consistente aos requisitos de proteção identificados, especialmente no que se refere à limitação de acesso às informações classificadas como segredos comerciais e à capacidade de registrar as ações realizadas no ambiente colaborativo. A integração entre dimensões jurídica, organizacional e técnica constitui uma das principais contribuições do estudo, ao demonstrar que acordos de confidencialidade e controles tecnológicos devem atuar de forma complementar para garantir a efetiva proteção da informação.

Entretanto, é necessário reconhecer as limitações do trabalho. A análise foi conduzida a partir de um cenário simulado, não tendo sido realizada validação empírica em ambiente organizacional real. Dessa forma, aspectos relacionados à implementação prática, desempenho operacional, custos e impactos na usabilidade não foram avaliados de forma aplicada. A ausência de experimentação em contexto real limita a generalização dos resultados, embora não comprometa a consistência conceitual do modelo apresentado.

Como possibilidade de continuidade da pesquisa, recomenda-se a aplicação do modelo em parceria empresarial real, permitindo avaliar sua efetividade operacional, identificar ajustes necessários e mensurar impactos sobre a governança da informação. Estudos futuros também podem explorar a integração do modelo com outras práticas de segurança, como classificação da informação, gestão de riscos e programas formais de conformidade.

Concluo este estudo, portanto, evidenciando que o gerenciamento de identidade e acesso, quando estruturado de maneira alinhada às obrigações contratuais e às normas de segurança da informação, constitui instrumento relevante para a proteção de segredos comerciais em ambientes colaborativos. A adoção integrada de mecanismos de identificação, autenticação, autorização e monitoramento fortalece a governança sobre o acesso às informações estratégicas e contribui para a mitigação de riscos associados à apropriação indevida de conhecimento empresarial.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIR DE NORMAS TÉCNICA - ABNT. **NBR ISO/IEC 27001**:2022 – Tecnologia da informação – Técnicas de segurança – Sistemas de gestão da segurança da informação – Requisitos. Rio de Janeiro: ABNT, 2022.

ASSOCIAÇÃO BRASILEIR DE NORMAS TÉCNICA – ABNT. **NBR ISO/IEC 27002**:2022 – Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação. Rio de Janeiro: ABNT, 2022.

BARBOSA, Denis Borges. **Uma introdução à propriedade intelectual**. 2. ed. Rio de Janeiro: Lumen Juris, 2010.

BRASIL. Lei nº 9.279, de 14 de maio de 1996. Regula direitos e obrigações relativos à propriedade industrial. **Diário Oficial da União**: seção 1, Brasília, DF, 15 maio 1996.

CAPEZ, Fernando. **Curso de direito penal** – parte especial. 21. ed. São Paulo: Saraiva, 2022.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL - CERT. **Cartilha de Segurança para Internet**. São Paulo: NIC.br, 2023.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. 7. ed. São Paulo: Atlas, 2019.

GODET, Michel. **A caixa de ferramentas da prospectiva estratégica**. Lisboa: Publicações Dom Quixote, 2000.

KASZNAR, Elisabeth. **Transferência de tecnologia e contratos empresariais**. São Paulo: Atlas, 2018.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de metodologia científica**. 8. ed. São Paulo: Atlas, 2017.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). *Digital Identity Guidelines*. Special Publication 800-63. Gaithersburg: NIST, 2022.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **Security and Privacy Controls for Information Systems and Organizations. Special Publication**. Rev. 5. Gaithersburg: NIST, 2020. 800-53

PIMENTEL, Luiz Otávio; BASSO, Maristela. **Direito da propriedade intelectual aplicado**. São Paulo: Revista dos Tribunais, 2019.

PRODANOV, Cleber Cristiano; FREITAS, Ernani Cesar de. **Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico**. 2. ed. Novo Hamburgo: Feevale, 2013.

TARTUCE, Flávio. **Manual de direito civil: volume único**. 13. ed. São Paulo: Método, 2023.

WORLD INTELLECTUAL PROPERTY ORGANIZATION (WIPO). **Protecting trade secrets: a practical guide for businesses.** Geneva: WIPO, 2016.

WORLD TRADE ORGANIZATION (WTO). **Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)**. Geneva: WTO, 1994.