v7.n11.2026

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

PROTEÇÃO DE DADOS EM NUVEM PRIVADA: DESAFIOS, BOAS PRÁTICAS E ANÁLISE COMPARATIVA ENTRE NEXTCLOUD, OWNCLOUD E SEAFILE

DATA PROTECTION IN PRIVATE CLOUD: CHALLENGES, BEST PRACTICES, AND A COMPARATIVE ANALYSIS OF NEXTCLOUD, OWNCLOUD, AND SEAFILE

PROTECCIÓN DE DATOS EN NUBE PRIVADA: DESAFÍOS, BUENAS PRÁCTICAS Y ANÁLISIS COMPARATIVO ENTRE NEXTCLOUD, OWNCLOUD Y SEAFILE

Anderson Strack[1], Ricardo Tombesi Macedo[2], Roberto Franciscatto[3]

e7119224
https://doi.org/10.47820/recima21.v7i11.9224

PUBLICADO: 11/2026

RESUMO

A crescente adoção de serviços em nuvem transformou a maneira como organizações armazenam e processam seus dados, mas também trouxe desafios significativos à segurança da informação. Este artigo analisa os desafios e as boas práticas de proteção de dados em ambientes de armazenamento em nuvem privada. Adotou-se revisão narrativa de literatura, análise qualitativa de conteúdo e estudo comparativo em ambiente virtualizado entre as soluções Nextcloud, ownCloud e Seafile, avaliadas quanto a autenticação e controle de acesso, criptografia, proteção contra ataques de força bruta, auditoria e registro de atividades, atualizações e integração com ferramentas externas de segurança. A revisão identificou vulnerabilidades específicas, como compartilhamento não autorizado, configurações incorretas e escalonamento de privilégios, bem como riscos à confidencialidade, integridade e disponibilidade dos dados, e reuniu estratégias de autenticação, criptografia, monitoramento e resposta a incidentes. Nos testes, as três soluções apresentaram recursos essenciais, como autenticação de dois fatores e criptografia em trânsito e em repouso, e o Nextcloud apresentou a maior cobertura entre os recursos avaliados, especialmente em auditoria e registro de atividades e na integração nativa com antivírus. Os resultados restringem-se às versões testadas e não constituem avaliação de desempenho sob ataque.

PALAVRAS-CHAVE: Segurança da informação. Nuvem privada. Proteção de dados. Nextcloud.

ABSTRACT

The growing adoption of cloud services has transformed how organizations store and process their data, but it has also introduced significant information security challenges. This article analyzes the challenges and best practices for data protection in private cloud storage environments. The study combined a narrative literature review, qualitative content analysis, and a comparative study in a virtualized environment of Nextcloud, ownCloud, and Seafile, assessed in terms of authentication and access control, encryption, protection against brute-force attacks, auditing and activity logging, updates, and integration with external security tools. The review identified specific vulnerabilities, such as unauthorized sharing, misconfigurations, and privilege escalation, as well as risks to data confidentiality, integrity, and availability, and gathered strategies for authentication, encryption, monitoring, and incident response.

[1] Especialista em Gestão de Tecnologia da Informação pela Universidade Federal de Santa Maria - RS (UFSM).
[2] Doutor em Ciência da Computação pela Universidade Federal do Paraná (UFPR). Professor na Universidade Federal de Santa Maria - RS (UFSM).
[3] Doutor em Informática na Educação pela Universidade Federal do Rio Grande do Sul (PPGIE/UFRGS) Professor na Universidade Federal de Santa Maria - RS (UFSM).

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

In the tests, all three solutions provided essential features, such as two-factor authentication and encryption in transit and at rest, while Nextcloud showed the broadest coverage of the assessed features, particularly in auditing and activity logging and in native antivirus integration. The results are limited to the tested versions and do not constitute a performance assessment under attack.

KEYWORDS: *Information security. Private cloud. Data protection. Nextcloud.*

RESUMEN
La creciente adopción de servicios en la nube ha transformado la forma en que las organizaciones almacenan y procesan sus datos, pero también ha planteado desafíos significativos en materia de seguridad de la información. Este artículo analiza los desafíos y las buenas prácticas de protección de datos en entornos de almacenamiento en nube privada. Se adoptó una revisión narrativa de la literatura, un análisis cualitativo de contenido y un estudio comparativo en entorno virtualizado entre las soluciones Nextcloud, ownCloud y Seafile, evaluadas en cuanto a autenticación y control de acceso, cifrado, protección contra ataques de fuerza bruta, auditoría y registro de actividades, actualizaciones e integración con herramientas externas de seguridad. La revisión identificó vulnerabilidades específicas, como el intercambio no autorizado, las configuraciones incorrectas y la escalada de privilegios, así como riesgos para la confidencialidad, integridad y disponibilidad de los datos, y reunió estrategias de autenticación, cifrado, monitoreo y respuesta a incidentes. En las pruebas, las tres soluciones presentaron recursos esenciales, como la autenticación de dos factores y el cifrado en tránsito y en reposo, y Nextcloud mostró la mayor cobertura entre los recursos evaluados, especialmente en auditoría y registro de actividades y en la integración nativa con antivirus. Los resultados se limitan a las versiones probadas y no constituyen una evaluación de desempeño bajo ataque.

PALABRAS CLAVE*: Seguridad de la información. Nube privada. Protección de datos. Nextcloud.*

1. INTRODUÇÃO

A rápida evolução da tecnologia tem redefinido a maneira como organizações de todos os setores gerenciam e armazenam seus dados. A adoção crescente de serviços em nuvem emergiu como um dos pilares dessa transformação, oferecendo flexibilidade, escalabilidade e acessibilidade. No entanto, a computação em nuvem também trouxe à tona uma série de desafios, particularmente no que diz respeito à segurança da informação.

Neste contexto, em que informações confidenciais e ativos corporativos valiosos são armazenados e processados em ambientes virtualizados e distribuídos, a necessidade de garantir a integridade, confidencialidade e disponibilidade desses dados torna-se central. A proteção contra ameaças cibernéticas e o cumprimento de regulamentações tornaram-se requisitos relevantes para a continuidade dos negócios e para a conformidade das organizações.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

O presente trabalho analisa os desafios e as boas práticas de segurança no uso de serviços em nuvem para armazenamento e processamento de dados, com foco em ambientes de nuvem privada. Para tanto, são investigados os principais riscos e vulnerabilidades potenciais que podem comprometer a segurança nesses ambientes, bem como as estratégias recomendadas para mitigá-los.

Diante desse cenário, a pesquisa orienta-se pela seguinte pergunta: quais mecanismos de proteção de dados são oferecidos por soluções de código aberto para nuvem privada e de que forma eles se relacionam com os principais riscos de segurança identificados na literatura? O objetivo geral é analisar os desafios e as boas práticas de proteção de dados em ambientes de armazenamento em nuvem privada, comparando os recursos de segurança das soluções Nextcloud, ownCloud e Seafile. Como objetivos específicos, busca-se: (i) identificar, na literatura, os principais riscos e vulnerabilidades associados à computação em nuvem e à virtualização; (ii) sistematizar boas práticas de autenticação, criptografia, monitoramento e conformidade normativa, incluindo a LGPD e as normas ISO/IEC 27001 e 27002; (iii) implementar as três soluções em ambiente virtualizado controlado; e (iv) comparar seus recursos de segurança segundo critérios previamente definidos. Espera-se, com isso, oferecer subsídios técnicos a organizações que avaliam a adoção de soluções de nuvem privada.

2. REFERENCIAL TEÓRICO

Nas seções a seguir serão exploradas as bases teóricas ligadas à computação em nuvem e seus modelos de implantação e de serviço, desafios de segurança em ambientes de nuvem, autenticação e gerenciamento de identidade, criptografia em nuvem, monitoramento e detecção de intrusões, Lei Geral de Proteção de Dados Pessoais, normas de segurança e práticas complementares de segurança em nuvem privada.

2.1. Computação em nuvem e seus modelos

Nesta seção são apresentados a definição e as características da computação em nuvem, os modelos de implantação e os modelos de serviço.

Segundo o *National Institute of Standards and Technology* (NIST), a computação em nuvem é um modelo que permite o acesso conveniente e sob demanda, pela rede, a um conjunto compartilhado de recursos computacionais configuráveis, como redes, servidores, armazenamento, aplicações e serviços, que podem ser rapidamente provisionados e liberados com mínimo esforço de gerenciamento ou interação com o provedor (MELL; GRANCE, 2011).

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

Essa abordagem elimina a obrigação das empresas de adquirir, configurar ou gerenciar a infraestrutura, permitindo que paguem apenas pelos recursos efetivamente utilizados (GOOGLE CLOUD, 2023).

O NIST define cinco características essenciais da computação em nuvem (MELL; GRANCE, 2011). Autoatendimento sob demanda: o consumidor pode provisionar recursos, como tempo de processamento e armazenamento, de forma automática, sem interação humana com o provedor. Amplo acesso à rede: os recursos estão disponíveis pela rede e são acessados por mecanismos padronizados, a partir de diferentes dispositivos clientes, como computadores, notebooks e dispositivos móveis. Agrupamento de recursos (*resource pooling*): os recursos computacionais são compartilhados entre vários consumidores em modelo multilocatário e atribuídos dinamicamente conforme a demanda. Elasticidade rápida: a infraestrutura em nuvem pode crescer ou diminuir de forma dinâmica, ajustando-se automaticamente à demanda de tráfego, seja aumentando os recursos de uma máquina ou distribuindo a carga em várias máquinas. Serviço medido: o uso dos recursos na nuvem é monitorado e medido, permitindo que os clientes paguem apenas pelo que utilizam, seguindo um modelo de faturamento *pay-as-you-go*.

2.1.2. Modelos de implantação: nuvem pública, privada, comunitária e híbrida

Quanto ao modelo de implantação, o NIST distingue quatro categorias: nuvem pública, privada, comunitária e híbrida (MELL; GRANCE, 2011), cada uma proporcionando benefícios distintos. Frequentemente, as empresas encontram vantagens ao adotar mais de uma dessas categorias.

Nuvem Pública: recursos como servidores e armazenamento são oferecidos pela Internet por provedores como AWS e Microsoft Azure. O provedor gerencia toda a infraestrutura, facilitando o acesso e uso para as empresas. Nuvem Privada: oferece recursos de computação exclusivos para uma organização, o que favorece maior controle sobre a segurança e a privacidade dos dados. Pode ser hospedada internamente ou por um provedor. Nuvem Comunitária: é compartilhada por um grupo de organizações com interesses ou requisitos comuns, como missão, políticas de segurança ou exigências de conformidade. Nuvem Híbrida: combina dois ou mais desses modelos, como nuvens públicas e privadas, permitindo a integração de recursos conforme necessário. Isso oferece flexibilidade, permitindo que empresas aloquem dados sensíveis em nuvens privadas e outros serviços em nuvens públicas.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

2.1.3. Modelos de serviço: IaaS, PaaS e SaaS

Quanto ao modelo de serviço, o NIST define três categorias (MELL; GRANCE, 2011): Infraestrutura como Serviço (IaaS) - o consumidor provisiona processamento, armazenamento e rede e controla sistemas operacionais e aplicações, sem gerenciar a infraestrutura física subjacente. Plataforma como Serviço (PaaS) - oferece os recursos necessários para o desenvolvimento e a implantação de aplicativos, sem a necessidade de gerenciar a infraestrutura. Software como Serviço (SaaS) - fornece aplicativos completos como serviço, com o provedor gerenciando toda a infraestrutura e manutenção.

2.2. Desafios de segurança em ambientes de nuvem

Nesta seção são apresentadas duas partes, uma de ameaças à confidencialidade, integridade e disponibilidade dos dados em ambientes de nuvem e a segunda sobre os riscos de segurança relacionados à virtualização.

2.2.1. Ameaças à confidencialidade, integridade e disponibilidade dos dados em ambientes de nuvem.

A segurança ineficiente na nuvem pode expor usuários e provedores a diversos tipos de ameaças cibernéticas. No levantamento mais recente da Cloud Security Alliance, baseado na consulta a mais de 500 especialistas, as principais ameaças à computação em nuvem são, em ordem de relevância: configurações incorretas e controle inadequado de mudanças; falhas na gestão de identidades e acessos (IAM); interfaces e APIs inseguras; e seleção ou implementação inadequada da estratégia de segurança em nuvem, seguidas por recursos de terceiros inseguros, desenvolvimento inseguro de software, divulgação acidental de dados, vulnerabilidades de sistemas, visibilidade limitada, compartilhamento de recursos sem autenticação e ameaças persistentes avançadas (CSA, 2024). O relatório destaca que várias dessas ameaças estão associadas a erro humano e a falhas de configuração, mais do que a vulnerabilidades dos provedores. De forma complementar, a Kaspersky (2023) agrupa as ameaças em: riscos de infraestrutura baseada na nuvem, incluindo estruturas de TI legadas incompatíveis e interrupções no serviço de armazenamento de dados de terceiros; ameaças internas devido a erro humano, como configuração incorreta dos controles de acesso do usuário; e ameaças externas causadas predominantemente por agentes maliciosos, como *malware*, *phishing* e ataques de DDoS.

Entre as ameaças mais citadas, destaca-se o vazamento de dados, que pode ocorrer devido ao roubo ou à perda acidental de informações, comprometendo a confidencialidade, a

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

disponibilidade e a integridade dos dados. As causas incluem má gestão de credenciais, ameaças como *phishing* e o uso de APIs inseguras (AIQON, 2023; CSA, 2024). A mesma fonte descreve as ameaças a seguir (AIQON, 2023).

Configurações Incorretas: erros humanos, permissões excessivas, contas obsoletas e configurações padrão não alteradas podem levar a exposições de dados, criando vulnerabilidades significativas.

Ameaças Internas: podem ser intencionais ou acidentais, envolvendo funcionários, contratados ou parceiros que acessam dados de forma inadequada. As ameaças incluem abuso de privilégios, dispositivos comprometidos e contas compartilhadas.

Sequestro de Contas: técnicas como quebra de senhas e *phishing* são usadas para roubar credenciais, visando especialmente contas privilegiadas e serviços de assinatura.

Ataques de Negação de Serviço (DoS): DoS e DDoS visam sobrecarregar sistemas com requisições excessivas, tornando-os indisponíveis. Ataques persistentes avançados de negação de serviço (APDoS) combinam múltiplos vetores, incluindo a camada de aplicação, e podem atingir servidores e bancos de dados.

Malware: atacantes induzem usuários a baixar *malware*, que opera em segundo plano para roubar dados de servidores em nuvem, comprometendo a segurança das informações.

2.2.2. Riscos de segurança relacionados à virtualização

O NIST recomenda, para ambientes virtualizados, planejar a segurança da solução antes da sua implantação, proteger todos os seus elementos e manter essa proteção ao longo do tempo, além de restringir e proteger o acesso administrativo ao hipervisor e às ferramentas de gerenciamento (SCARFONE; SOUPPAYA; HOFFMAN, 2011). De forma complementar, o portal Imasters (2015) aponta estratégias que, quando implementadas, podem ajudar a reduzir possíveis ameaças em ambientes virtuais, sem recorrer a processos e soluções dispendiosas e complexas que podem estar fora do alcance de muitas organizações.

Separação: visa estabelecer como e onde separar as máquinas virtuais de desenvolvimento, teste e produção. Imposição do processo: objetiva habilitar processos específicos à TI por meio de portais de autoatendimento para aumentar a eficiência e simplificar o gerenciamento. Gerenciamento de dispersão: permite gerenciar ativamente o ambiente virtual em termos de o que está sendo usado e o que é ou não necessário. Gerenciamento completo da pilha: concentra seu foco em conexões de ponta a ponta no ambiente virtual. Auditoria incorporada: aproveita ferramentas para automatizar verificações de segurança, balanceamentos e processos, sempre que possível. Aplicação de *patches*: implementa um

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

processo de manutenção e gerenciamento de *patches* e programa-o para garantir que os *patches* estejam atualizados tanto em máquinas virtuais *online* quanto *offline*.

Com o conhecimento dos principais riscos de segurança associados à virtualização e um compromisso de seguir as práticas recomendadas de atenuação dos riscos, é possível para qualquer organização encontrar um equilíbrio entre aproveitar as vantagens da virtualização e manter níveis adequados de segurança.

2.3. Autenticação e gerenciamento de identidade

A autenticação é o processo de verificação da identidade de um usuário, processo ou dispositivo, geralmente como pré-requisito para o acesso a recursos de um sistema. As diretrizes do NIST classificam os mecanismos de autenticação em níveis de garantia (AAL1 a AAL3) e recomendam a autenticação multifator para acessos de maior risco, exigindo autenticadores resistentes a *phishing* no nível mais elevado (TEMOSHOK *et al.*, 2025). Em ambientes de nuvem, a autenticação integra a gestão de identidades e acesso (IAM), cujas falhas figuram entre as principais ameaças à computação em nuvem (CSA, 2024). O serviço de autenticação garante que as informações sejam acessadas apenas por usuários autorizados a fazê-lo (CAPTERRA, 2023).

Pequenas e médias empresas (PMEs) podem usar serviços de autenticação para proteger o acesso a aplicativos, *websites* e sistemas de software gerenciados remotamente. Isso é especialmente útil, pois muitos proprietários e gestores de PMEs trabalham fora do escritório. Com a autenticação, as PMEs podem proteger suas informações confidenciais, mesmo quando os funcionários utilizam dispositivos fora da rede empresarial (CAPTERRA, 2023).

2.4. Criptografia em nuvem

A criptografia transforma informações em códigos para proteger dados sensíveis, tornando-os inacessíveis a usuários não autorizados e prevenindo roubos. É amplamente usada por sites, aplicativos e plataformas de armazenamento, como o Google Cloud, para garantir a segurança, confidencialidade e integridade das informações transmitidas e armazenadas *online* (HOSTINGER, 2023). Em ambientes de nuvem, distinguem-se a criptografia em trânsito, que protege os dados durante a comunicação entre cliente e servidor, geralmente por meio do protocolo TLS, e a criptografia em repouso, que protege os dados armazenados.

A criptografia de armazenamento em nuvem pode reduzir significativamente o impacto de invasões ou vazamentos, ao tornar os dados ininteligíveis para quem não possuir as chaves.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

Ela também preserva a privacidade de documentos empresariais valiosos, restringindo o acesso a membros específicos da organização. Além disso, facilita a conformidade com legislações como a LGPD, ajudando as empresas a atender às exigências legais relacionadas à segurança e privacidade de dados (ADTSYS, 2023). Essa proteção, contudo, depende diretamente da gestão das chaves criptográficas: algoritmos robustos perdem efetividade se as chaves forem geradas, armazenadas ou distribuídas de forma inadequada, razão pela qual o NIST recomenda controles para todo o ciclo de vida das chaves, da geração à destruição (BARKER, 2020). Nesse sentido, a criptografia do lado do servidor protege os dados contra o acesso indevido ao meio de armazenamento, mas, em regra, não contra quem administra o servidor que detém as chaves, ao passo que a criptografia de ponta a ponta (E2EE) mantém as chaves sob controle do usuário, distinção relevante para a comparação apresentada na seção 3.

2.5. Monitoramento e detecção de intrusões

Nesta seção são apresentadas duas partes: uma referente às técnicas de monitoramento em ambientes de nuvem e outra referente à importância da detecção de intrusões para identificar atividades suspeitas.

2.5.1. Técnicas de monitoramento em ambientes de nuvem

O monitoramento em nuvem consiste na supervisão contínua da disponibilidade, do desempenho e da segurança dos recursos e fluxos de trabalho em ambiente de nuvem, com base na coleta e análise de métricas, eventos e registros (*logs*) (AUSTER, 2023; CONTACTA, 2023). Do ponto de vista da segurança, o NIST recomenda a gestão estruturada desses registros, com definição dos eventos a serem registrados, proteção da integridade e da confidencialidade dos *logs*, prazos de retenção compatíveis com as necessidades da organização e análise periódica de seu conteúdo (KENT; SOUPPAYA, 2006).

2.5.2. Detecção de intrusões e identificação de atividades suspeitas

Assegurar a segurança na nuvem exige um monitoramento que vá além da simples utilização de ferramentas básicas de rede e da verificação dos tempos de resposta. As ferramentas de monitoramento avançadas são capazes de analisar questões relacionadas à rede, aplicativos, fluxo de dados e, além disso, de identificar a causa raiz de problemas e detectar questões associadas ao sistema operacional (CONTACTA, 2023). Nesse contexto, os sistemas de detecção e prevenção de intrusões (IDS/IPS) monitoram eventos em redes ou em hosts, analisam-nos em busca de sinais de incidentes e, no caso dos IPS, podem bloquear

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

automaticamente atividades maliciosas. Essas soluções dividem-se, entre outros tipos, em baseadas em rede (NIDS) e em host (HIDS), e empregam métodos de detecção por assinaturas, por anomalias ou por análise de protocolos (SCARFONE; MELL, 2007). Em nuvens privadas, IDS/IPS costumam ser implantados no servidor ou na rede que hospeda a aplicação, e não necessariamente integrados a ela, aspecto relevante para a interpretação dos resultados apresentados na seção 3.

2.6. Lei geral de proteção de dados pessoais

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018, é a legislação brasileira que disciplina o tratamento de dados pessoais, inclusive nos meios digitais, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018, art. 1º). A lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, desde que a operação seja realizada no território nacional, tenha por objetivo a oferta de bens ou serviços a indivíduos localizados no Brasil ou envolva dados coletados no país (BRASIL, 2018, art. 3º). Cabe distinguir, contudo, que os titulares protegidos pela lei são sempre pessoas naturais, a quem se referem os dados pessoais (art. 5º, V), ao passo que as pessoas jurídicas podem atuar como agentes de tratamento, na condição de controladoras ou operadoras (art. 5º, VI e VII). Inspirada no Regulamento Geral sobre a Proteção de Dados (RGPD) europeu, a LGPD reconhece a vulnerabilidade dos indivíduos diante do uso de seus dados por terceiros (MICHELETTI, 2021).

No contexto deste estudo, a LGPD relaciona-se diretamente aos controles avaliados. O princípio da segurança impõe a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão, e o princípio da prevenção exige a adoção de medidas para evitar a ocorrência de danos (BRASIL, 2018, art. 6º, VII e VIII). O art. 46 determina que os agentes de tratamento adotem essas medidas desde a fase de concepção do produto ou do serviço até a sua execução, o que abrange recursos como autenticação, controle de acesso e criptografia; o art. 37 exige que controlador e operador mantenham registro das operações de tratamento, aspecto relacionado aos registros de auditoria; e o art. 48 obriga o controlador a comunicar à Autoridade Nacional de Proteção de Dados (ANPD) e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante, o que pressupõe capacidade de monitoramento e de resposta a incidentes (BRASIL, 2018).

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

2.7. Normas de segurança

A segurança da informação é um assunto relevante, e existem diversas normas e padrões que estabelecem orientações e boas práticas para garantir a segurança de dados e sistemas. A seguir, são apresentadas as normas ISO/IEC 27001 e ISO/IEC 27002, complementadas pelas normas ISO/IEC 27017 e ISO/IEC 27018, específicas para serviços em nuvem.

2.7.1. Iso/iec 27001

A ISO/IEC 27001 é um padrão internacional que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação (SGSI) no contexto da organização, incluindo a avaliação e o tratamento de riscos de segurança da informação (ABNT, 2022a). Sua versão vigente apresenta, no Anexo A, 93 controles de referência organizados em quatro temas: organizacionais, de pessoas, físicos e tecnológicos. Este padrão ajuda as organizações a gerenciar a segurança de ativos como informações financeiras, propriedade intelectual, dados de funcionários e informações confiadas a terceiros (27001.PT, 2024).

2.7.2. Iso/iec 27002

A ISO/IEC 27002 é uma norma internacional que fornece orientações para a implementação dos controles de segurança da informação, servindo como referência para a seleção e a aplicação dos controles listados no Anexo A da ISO/IEC 27001. Ela é projetada para ser usada em conjunto com a ISO/IEC 27001, que especifica os requisitos para um Sistema de Gestão de Segurança da Informação (ABNT, 2022b; ISO, 2022).

2.7.3. Normas específicas para serviços em nuvem

Para ambientes de nuvem, a ISO/IEC 27017 complementa a ISO/IEC 27002 com orientações adicionais e controles específicos aplicáveis tanto a provedores quanto a clientes de serviços em nuvem, como a definição de papéis e responsabilidades compartilhadas, a segregação em ambientes de computação virtual e o monitoramento das atividades em nuvem (ISO, 2015). A ISO/IEC 27018, por sua vez, estabelece diretrizes para a proteção de dados pessoais em nuvens públicas que atuam como operadoras desses dados (ISO, 2025). Embora esta última se destine a nuvens públicas, seus princípios de transparência, controle de acesso e proteção de dados pessoais dialogam com as exigências da LGPD também em ambientes de nuvem privada.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

2.8. Práticas complementares e tendências em segurança de nuvem privada

Além dos mecanismos abordados nas seções anteriores, a literatura técnica recente destaca práticas complementares relevantes para a proteção de dados em nuvem privada. A primeira é o modelo de responsabilidade compartilhada, segundo o qual as obrigações de segurança se distribuem entre provedor e cliente conforme o modelo de serviço adotado (ISO, 2015). Em uma nuvem privada auto-hospedada, como as avaliadas neste estudo, a organização concentra a maior parte dessas responsabilidades, incluindo a infraestrutura, o sistema operacional, a aplicação e a configuração dos controles. A segunda é a arquitetura de confiança zero (*zero trust*), que parte do pressuposto de que nenhum usuário ou dispositivo deve ser considerado confiável apenas por sua localização na rede, exigindo autenticação e autorização para cada acesso a recursos (ROSE *et al.*, 2020). Em consonância, o princípio do menor privilégio e o controle de acesso baseado em papéis (RBAC) limitam as permissões de usuários e administradores ao estritamente necessário para o desempenho de suas funções (JOINT TASK FORCE, 2020).

No plano da resiliência, o *ransomware* representa ameaça relevante a repositórios de arquivos, inclusive em nuvens privadas sincronizadas com estações de trabalho, uma vez que arquivos cifrados localmente por um atacante podem ser replicados para o servidor. O NIST recomenda, entre outras medidas, manter cópias de segurança regulares, isoladas da rede de produção e periodicamente testadas (BARKER *et al.*, 2022), orientação que se expressa, no mercado, na estratégia conhecida como 3-2-1-1-0: três cópias dos dados, em dois tipos de mídia, uma fora do local, uma desconectada ou imutável e zero erros na verificação da restauração. Por fim, por se tratar de soluções de código aberto que dependem de componentes de terceiros, como servidor web, banco de dados e interpretadores, a gestão de vulnerabilidades e de *patches* e o endurecimento (*hardening*) do sistema operacional e dos serviços tornam-se essenciais (SOUPPAYA; SCARFONE, 2022), em linha com a inclusão dos recursos de terceiros inseguros entre as principais ameaças à computação em nuvem (CSA, 2024).

3. METODOLOGIA

Esta pesquisa teve como objetivo analisar os desafios de segurança em ambientes de armazenamento em nuvem privada e identificar boas práticas para a proteção de dados nesses contextos, bem como comparar os recursos de segurança oferecidos por três soluções de código aberto. Quanto à natureza, trata-se de pesquisa aplicada; quanto à abordagem,

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

qualitativa, com apoio em verificação experimental; e, quanto aos procedimentos, combina revisão narrativa da literatura e estudo comparativo experimental em ambiente controlado.

Na primeira etapa, realizou-se uma revisão narrativa da literatura, contemplando publicações técnicas de referência, como as do NIST, da Cloud Security Alliance e das normas ISO/IEC, a legislação aplicável e conteúdos especializados em cibersegurança. As fontes foram selecionadas de forma intencional, segundo os critérios de pertinência ao tema da segurança em nuvem privada, atualidade e reconhecimento técnico da fonte. Por não seguir protocolo sistemático de busca, essa etapa não pretende esgotar a produção sobre o tema, o que constitui uma limitação do estudo.

Os dados coletados foram analisados qualitativamente por meio da técnica de análise de conteúdo. Esta abordagem permitiu a identificação de padrões, tendências e abordagens recomendadas para a segurança em nuvem privada. A análise foi realizada em várias etapas, incluindo a codificação dos dados, a categorização dos temas principais e a síntese dos achados. Este processo resultou na definição das categorias de segurança utilizadas na comparação experimental, a saber: autenticação e controle de acesso; criptografia de dados; proteção contra ataques de força bruta e exploração de vulnerabilidades; auditoria e registro de atividades; atualizações e correções; e integração com ferramentas externas de segurança, bem como na formulação de recomendações práticas.

Na segunda etapa, realizou-se um estudo comparativo experimental em ambiente controlado, no qual foram implantadas e testadas três soluções de código aberto para nuvem privada: Nextcloud, ownCloud e Seafile. A escolha dessas soluções justifica-se por serem amplamente difundidas, por disporem de versões gratuitas passíveis de auto-hospedagem e, no caso de Nextcloud e ownCloud, por compartilharem origem comum, o que favorece a comparação. Foram comparados os mecanismos de segurança disponíveis em cada solução, nas versões instaladas, segundo as categorias definidas na etapa anterior.

Optou-se por esse delineamento, em vez de um estudo de caso organizacional, porque o objetivo não foi investigar a adoção dessas ferramentas em uma organização específica, mas comparar, sob condições equivalentes de infraestrutura, os recursos de segurança efetivamente disponíveis em cada solução. O ambiente controlado permite isolar as diferenças entre as ferramentas, embora não reproduza as condições de uso e de ataque de um ambiente de produção.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

3.1. Estudo comparativo experimental: avaliação de segurança de nextcloud, owncloud e seafile

Esta seção descreve as ferramentas, o ambiente e os procedimentos de teste, as configurações das máquinas virtuais e os cenários para avaliação de segurança das soluções escolhidas.

3.1.1.Ferramentas

O ownCloud é uma aplicação de código aberto para compartilhamento e sincronização de arquivos, lançada em junho de 2010. Ela possui duas versões: a versão Server, gratuita e direcionada a um número pequeno de usuários, e a versão Enterprise, paga e direcionada às empresas. O ownCloud é escrito em PHP; portanto, é necessário ter um interpretador PHP instalado no servidor, além de um servidor web e de um banco de dados. A solução possui a parte do servidor, na qual ficam os arquivos dos usuários que possuem conta naquela instância, e a parte do cliente, por meio da qual os usuários enviam e baixam os arquivos da nuvem (servidor). A parte cliente é acessível por meio de um navegador web, mas também é possível instalar aplicativos nas versões desktop (Linux, Mac e Windows) e mobile (Android e iOS) (OWNCLOUD, 2016).

O Nextcloud é uma aplicação de código aberto derivada do ownCloud, criada em 2016 pelo fundador do ownCloud, Frank Karlitschek, com parte da equipe de desenvolvimento do projeto original. Assim como o ownCloud, o Nextcloud possui versões gratuita e paga, é escrito em PHP e possui as mesmas dependências. Além disso, tem funcionamento similar, com partes servidor e cliente, incluindo o acesso via navegador e também possui aplicativos clientes desktop (Linux, Mac e Windows) e mobile (Android e iOS) (NEXTCLOUD, 2017).

O Seafile é uma plataforma de código aberto para sincronização, compartilhamento e colaboração em documentos. Diferentemente do ownCloud e do Nextcloud, seu servidor é desenvolvido principalmente nas linguagens C e Python e não depende de PHP. Além das funcionalidades de sincronização e compartilhamento de arquivos, o Seafile inclui um editor de documentos colaborativo integrado, o SeaDoc, voltado à edição e ao gerenciamento de fluxos de trabalho (SEAFILE, 2024).

3.1.2. Ambiente e procedimentos de teste

A avaliação da segurança das ferramentas ownCloud, Nextcloud e Seafile correspondeu à análise dos parâmetros de segurança definidos na etapa de revisão e agrupados nas seis categorias descritas na seção 2. Os testes foram realizados na

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

infraestrutura de um dos laboratórios de testes de uma empresa privada focada em serviços em nuvem, que dispõe de várias máquinas, *switches* e rede estável, com as três soluções implantadas em condições equivalentes de hardware, sistema operacional e dependências, conforme descrito na seção 2.1.3.

Os recursos passíveis de verificação prática foram ativados e testados diretamente nas máquinas virtuais, a partir da área de administração de cada solução e do acesso como usuário padrão pelo navegador. Os procedimentos consistiram em: (i) ativação da autenticação de dois fatores e realização de login com aplicativo autenticador baseado em TOTP; (ii) criação de usuários e grupos, atribuição de permissões e compartilhamento de arquivos com proteção por senha e data de expiração; (iii) acesso às soluções por HTTPS e conferência do certificado TLS no navegador, para verificação da criptografia em trânsito; (iv) ativação do módulo de criptografia do lado do servidor, no Nextcloud e no ownCloud, e criação de biblioteca criptografada, no Seafile, para verificação da criptografia em repouso; (v) realização de sucessivas tentativas de login com senha incorreta, para observação do mecanismo de bloqueio de IP ou de usuário; (vi) conferência do registro das ações realizadas nos *logs* de auditoria; e (vii) instalação do aplicativo ou *plugin* de antivírus, quando disponível.

Os itens que não podem ser aferidos em laboratório, como a frequência de atualizações, a comunicação de correções de segurança, as auditorias realizadas pela comunidade e a compatibilidade com sistemas IDS/IPS externos, foram avaliados com base na documentação oficial e nos canais de comunicação de cada projeto. Para o registro dos resultados na Tabela 1, adotou-se o seguinte critério: “Sim” indica recurso disponível e verificado na versão instalada; “Não”, recurso inexistente na versão instalada; e as respostas descritivas registram as diferenças observadas entre as soluções. Ressalta-se que os testes verificaram a presença e o funcionamento dos recursos, e não sua resistência a ataques reais, aspecto que não integrou o escopo do estudo. Para a comparação global, os registros foram posteriormente convertidos na escala de pontuação descrita na seção 3.

3.1.3. Configurações das máquinas virtuais

Foram definidas e criadas três máquinas virtuais (VMs), por meio da ferramenta Proxmox Virtual Environment, versão 7.2-5, sendo cada servidor de nuvem privada (ownCloud, Nextcloud e Seafile) implantado em uma VM.

Cada VM foi configurada com 2 vCPU, 4 GB de RAM e 30 GB de disco SSD. O sistema operacional utilizado foi o Ubuntu 22.04.4 LTS. O ownCloud, o Nextcloud e o Seafile exigiram

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

a instalação de algumas dependências à parte: um servidor web, banco de dados, Python e PHP. As seguintes dependências foram instaladas em cada máquina virtual: para o Nextcloud, servidor web Apache 2.4.52, banco de dados MariaDB 10.6.16 e linguagem PHP 8.1.27; para o ownCloud, servidor web Apache 2.4.52, banco de dados MariaDB 10.6.16 e linguagem PHP 7.4.33; e para o Seafile, servidor web Apache 2.4.52, Python 3 e banco de dados MariaDB 10.6.18. Além das dependências acima listadas, foram também instaladas as soluções de nuvem privada nas seguintes versões: ownCloud 10.14.0, Nextcloud 27.1.5 e Seafile 11.0.9. As três ferramentas possuem área do administrador, que deve ser criada pelo primeiro usuário. O administrador é responsável por algumas configurações, como criar outros usuários, definir suas cotas de armazenamento e definir o limite máximo para envio de arquivos. Na área de administrador, foram realizadas algumas configurações como a criação de um usuário padrão. O acesso à nuvem foi realizado por meio do navegador web Mozilla Firefox, versão 124.0.2.

4. RESULTADOS E DISCUSSÃO

As três plataformas oferecem os mecanismos essenciais de segurança avaliados, como senhas fortes, autenticação de dois fatores, controle de permissões e criptografia em trânsito e em repouso. A Tabela 1 apresenta o comparativo dos itens de segurança analisados entre Nextcloud, ownCloud e Seafile, nas versões instaladas, e a Tabela 2, apresentada adiante, sintetiza essa comparação por meio de pontuação.

Tabela 1. Comparativo dos recursos de segurança das soluções avaliadas (ownCloud 10.14.0, Nextcloud 27.1.5 e Seafile 11.0.9)

Recurso	Nextcloud	ownCloud	Seafile
Autenticação e Controle de Acesso			
Senhas Fortes	Sim	Sim	Sim
Autenticação de Dois Fatores (2FA)	Suporte a 2FA com aplicativos autenticadores e dispositivos U2F	Suporte a 2FA com aplicativos autenticadores e dispositivos U2F	Suporte a 2FA com aplicativos autenticadores
Integração com Sistemas de Autenticação Externos	Sim	Sim	Sim

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

Permissões de Usuário e Grupos	Sim	Sim	Sim
Compartilhamento Seguro	Sim	Sim	Sim
Fluxos de Trabalho de Compartilhamento	Fluxos de trabalho automatizados, controle granular	Controles detalhados, menos extensos que *Nextcloud*	Controles detalhados, menos extensos que *Nextcloud* e o*wnCloud*
Criptografia de Dados			
Criptografia em Repouso	Criptografia do lado do servidor, E2EE	Criptografia do lado do servidor	Criptografia do lado do servidor, E2EE
Algoritmos Utilizados	AES-256 e outros algoritmos padrão da indústria	AES-256 e outros algoritmos padrão da indústria	AES-256 e outros algoritmos padrão da indústria
Criptografia em Trânsito	TLS/SSL para comunicação segura	TLS/SSL para comunicação segura	TLS/SSL para comunicação segura
Proteção contra Ataques de Força Bruta e Exploração de Vulnerabilidades			
Limitação de Tentativas de Login	Bloqueio temporário de IP após tentativas falhadas	Bloqueio temporário de IP após tentativas falhadas	Congelamento do usuário após erros de senhas
Educação e Alertas	Sim	Sim	Sim
Certificados SSL/TLS	Sim	Sim	Sim
Compatibilidade com IDS/IPS externos (no servidor)	Sim	Sim	Sim
Logs de Auditoria	Sim	Sim	Sim
Comunidade e Auditorias de Segurança	Sim	Sim	Sim
Auditoria e Registro de Atividades			

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

Registro de Ações de Usuários	Sim	Menos avançado em comparação com *Nextcloud*.	Menos avançado em comparação com o*wnCloud*.
Logs Detalhados	Sim	Menos avançado em comparação com *Nextcloud*.	Menos avançado em comparação com o*wnCloud*.
Monitoramento em Tempo Real	Sim	Menos avançado em comparação com *Nextcloud*.	Menos avançado em comparação com o*wnCloud*.
Relatórios Personalizáveis	Sim	Sim, mas com menos opções de personalização em comparação com *Nextcloud*.	Sim, mas com menos opções de personalização em comparação com o*wnCloud*.
Exportação de Dados	Sim	Sim	Sim
Políticas de Retenção de Logs	Sim	Sim	Sim, embora as opções possam ser menos flexíveis do que no *Nextcloud* e o*wnCloud*.
Auditoria de Segurança	Sim	Sim	Sim
Atualizações e Patching			
Frequência de Atualizações	Frequentes	Regulares	Regulares
Rapidez na Correção de Vulnerabilidades	Sim	Sim	Sim
Comunicação	Informações sobre atualizações e *patches* comunicadas de forma transparente através do blog oficial e canais da comunidade.	Comunicação transparente sobre atualizações e *patches* através do blog oficial e canais da comunidade.	Anúncios de atualizações e *patches* através do blog oficial e canais da comunidade.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

Atualizações Automáticas	Sim	Sim	Não
Notificações	Notificações enviadas aos administradores sobre novas atualizações e *patches*.	Notificações enviadas aos administradores sobre novas atualizações e *patches*.	Notificações sobre atualizações e *patches* são comunicadas, mas podem não ser integradas diretamente ao software.
Integração com Ferramentas de Segurança Externas			
Firewalls	Sim	Sim	Sim
Integração nativa com IDS na aplicação	Não possui integração direta	Não possui integração direta	Não possui integração direta
Antivírus	Integração nativa.	Integração através de *plugins* e *scripts*.	Não

Fonte: elaborado pelo Autor.

Para viabilizar uma comparação objetiva entre as soluções, os registros da Tabela 1 foram convertidos em uma escala ordinal de pontuação, aplicada aos 30 itens avaliados: atribuíram-se 2 pontos ao recurso disponível de forma plena ou nativa; 1 ponto ao recurso disponível com limitação registrada na comparação, como implementação menos avançada, dependente de *plugins*, menos flexível ou de menor frequência; e 0 ponto ao recurso ausente na versão instalada. Todos os itens receberam o mesmo peso, de modo que a pontuação máxima possível é de 60 pontos. A Tabela 2 apresenta o resultado por categoria.

Tabela 2. Pontuação das soluções por categoria de segurança

Categoria (pontuação máxima)	Nextcloud	ownCloud	Seafile
Autenticação e controle de acesso (12)	12	11	10
Criptografia de dados (6)	6	5	6
Proteção contra força bruta e exploração de vulnerabilidades (12)	12	12	12

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

Auditoria e registro de atividades (14)	14	10	9
Atualizações e correções (10)	10	9	6
Integração com ferramentas externas de segurança (6)	4	3	2
Total (60)	**58 (96,7%)**	**50 (83,3%)**	**45 (75,0%)**

Fonte: elaborado pelo Autor, com base na Tabela 1.

Pelo critério adotado, o Nextcloud obteve 58 dos 60 pontos possíveis (96,7%), seguido pelo ownCloud, com 50 pontos (83,3%), e pelo Seafile, com 45 pontos (75,0%). A vantagem do Nextcloud concentra-se na categoria de auditoria e registro de atividades, em que superou o ownCloud em quatro pontos e o Seafile em cinco, e na de atualizações, sobretudo em razão da ausência de atualizações automáticas no Seafile. Os resultados, contudo, não são uniformes entre as categorias: na proteção contra ataques de força bruta, as três soluções empataram, e, na criptografia, o Seafile igualou-se ao Nextcloud e superou o ownCloud, por oferecer criptografia de ponta a ponta, recurso não disponível no ownCloud na versão avaliada. Cabe ressaltar que a pontuação expressa a cobertura dos recursos avaliados, e não um nível absoluto de segurança: a ausência de ponderação entre itens de criticidade distinta e a natureza ordinal da escala constituem limitações dessa análise, que deve ser lida em conjunto com a Tabela 1.

Quanto à integração com ferramentas externas, nenhuma das soluções apresentou integração nativa com IDS, embora as três sejam compatíveis com IDS/IPS instalados no servidor ou na rede, conforme discutido na seção 1.5.2. Na prática, a detecção de intrusões depende de soluções complementares, como HIDS ou NIDS, cuja implantação, configuração e monitoramento ficam a cargo da organização, em consonância com o modelo de responsabilidade compartilhada discutido na seção 1.8. De modo semelhante, a ausência de integração com antivírus no Seafile e a dependência de *plugins* e *scripts* no ownCloud transferem à equipe técnica a tarefa de verificar os arquivos enviados pelos usuários, o que, em repositórios compartilhados e sincronizados, eleva o risco de disseminação de *malware* entre usuários.

Por fim, ressalta-se que os resultados correspondem às versões instaladas (ownCloud 10.14.0, Nextcloud 27.1.5 e Seafile 11.0.9). Como essas plataformas evoluem rapidamente, e parte das versões avaliadas já foi sucedida por novas versões principais, recursos ausentes ou limitados podem ser incorporados ou aprimorados em versões posteriores, o que exige que a comparação seja periodicamente revisitada antes de subsidiar decisões de adoção.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

5. CONSIDERAÇÕES FINAIS

Este estudo analisou os desafios de segurança e as boas práticas de proteção de dados em ambientes de armazenamento em nuvem privada e comparou os mecanismos de proteção oferecidos pelas soluções Nextcloud, ownCloud e Seafile. O estudo comparativo experimental, realizado em ambiente virtualizado no laboratório de testes de uma empresa de serviços em nuvem, permitiu verificar a presença e o funcionamento dos principais recursos de segurança que essas ferramentas podem proporcionar.

Em resposta à pergunta de pesquisa, verificou-se que as três soluções oferecem os mecanismos essenciais associados aos principais riscos identificados na literatura, como a autenticação de dois fatores e o controle de permissões, relacionados às falhas na gestão de identidades e acessos; a criptografia em trânsito e em repouso, relacionada ao vazamento de dados; e o bloqueio de tentativas de login, relacionado ao sequestro de contas. As soluções diferem, contudo, na profundidade dos recursos de auditoria, de atualização e de integração com ferramentas externas de segurança. Vale destacar que cada organização tem suas particularidades, o que exige um estudo detalhado para identificar a solução mais adequada a cada caso específico.

Com base na revisão e nas comparações realizadas, recomenda-se que soluções de nuvem privada destinadas à proteção de dados ofereçam, no mínimo, os seguintes itens: senhas fortes, autenticação de dois fatores (2FA), integração com sistemas de autenticação externos, permissões de usuário e grupos, compartilhamento seguro, fluxos de trabalho de compartilhamento automatizados e com controle granular, criptografia em repouso e em trânsito, limitação de tentativas de login, educação e alertas, certificados SSL/TLS, compatibilidade com IDS/IPS externos e *logs* de auditoria, complementados por práticas organizacionais como gestão de *patches*, cópias de segurança isoladas e monitoramento contínuo.

Pelo critério de pontuação adotado, o Nextcloud apresentou a maior cobertura entre os recursos avaliados (58 de 60 pontos), especialmente em auditoria e registro de atividades e em atualizações, seguido pelo ownCloud (50 pontos) e pelo Seafile (45 pontos), que, por sua vez, se equiparou ao Nextcloud em criptografia. Esse resultado indica maior disponibilidade de recursos de segurança nos parâmetros selecionados, e não que o Nextcloud seja, em termos absolutos, mais seguro, uma vez que a segurança efetiva depende também da configuração, da manutenção e do monitoramento realizados pela organização. O estudo também sistematizou os principais pontos a serem considerados na proteção de dados em nuvem

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

privada, como os modelos de implantação e de serviço, as ameaças mais relevantes, os requisitos da LGPD e das normas ISO/IEC e as práticas complementares de segurança.

O estudo de segurança em nuvem privada envolve múltiplos fatores, como a proteção de dados, *compliance* com regulamentos e a gestão de vulnerabilidades. Analisar de forma abrangente os riscos e propor soluções eficazes para diferentes cenários requer um entendimento profundo de várias tecnologias e práticas de segurança. O desafio reside em garantir que todos os aspectos de segurança sejam cobertos, considerando as particularidades de cada sistema.

A cibersegurança é uma área em constante mudança, com novos tipos de ataques e vulnerabilidades surgindo regularmente. As soluções de segurança que são eficazes hoje podem não ser suficientes amanhã. Por isso, acompanhar essas mudanças e garantir que as práticas e recomendações no trabalho estejam atualizadas é um desafio contínuo.

Entre as limitações do estudo, destacam-se: a comparação de apenas três plataformas, em versões específicas e em um único ambiente laboratorial; o caráter narrativo da revisão, sem protocolo sistemático; a natureza dos testes, que verificaram a presença e o funcionamento dos recursos, sem ensaios adversariais, como testes de intrusão, nem medição de desempenho sob ataque; a ausência de métricas quantitativas de segurança e de ponderação entre itens de criticidade distinta na pontuação adotada; e a inexistência de validação externa das classificações apresentadas. Para pesquisas futuras, sugerem-se a realização de testes de intrusão e de varredura de vulnerabilidades, a inclusão de versões mais recentes e de outras soluções, a validação das classificações por especialistas, a análise de dados de organizações que utilizam nuvens privadas em produção e a investigação de outros cenários de adoção, como as nuvens comunitária e híbrida.

REFERÊNCIAS

27001.PT. O que é a norma ISO 27001? [S. l.], 2024. Disponível em: https://www.27001.pt/. Acesso em: 15 jul. 2024.

ADTSYS. Criptografia de armazenamento em nuvem: muito mais segurança digital. [S. l.], 2023. Disponível em: https://www.adtsys.com.br/criptografia-de-armazenamento-em-nuvem-muito-mais-seguranca-digital/. Acesso em: 5 nov. 2023.

AIQON. As 6 principais ameaças na computação em nuvem e como mitigá-las. [S. l.], 2023. Disponível em: https://aiqon.com.br/blog/as-6-principais-ameacas-na-computacao-na-nuvem-e-como-mitiga-las/. Acesso em: 29 out. 2023.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). ABNT NBR ISO/IEC 27001: segurança da informação, segurança cibernética e proteção à privacidade: sistemas de gestão da segurança da informação: requisitos. Rio de Janeiro: ABNT, 2022a.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). ABNT NBR ISO/IEC 27002: segurança da informação, segurança cibernética e proteção à privacidade: controles de segurança da informação. Rio de Janeiro: ABNT, 2022b.

AUSTER. Monitoramento em nuvem: o que é e como fazer para a sua empresa em Uberlândia. Uberlândia, 2023. Disponível em: https://austercontabil.com.br/monitoramento-em-nuvem/. Acesso em: 5 nov. 2023.

BARKER, E. Recommendation for key management: part 1 – general. NIST Special Publication 800-57 Part 1, Revision 5. Gaithersburg: NIST, 2020. DOI: https://doi.org/10.6028/NIST.SP.800-57pt1r5.

BARKER, W. *et al.* Ransomware risk management: a cybersecurity framework profile. NIST Interagency Report 8374. Gaithersburg: NIST, 2022. DOI: https://doi.org/10.6028/NIST.IR.8374.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, p. 59, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 5 out. 2026.

CAPTERRA. Serviço de autenticação. [S. l.], 2023. Disponível em: https://www.capterra.com.br/glossary/742/authentication-service. Acesso em: 4 nov. 2023.

CLOUD SECURITY ALLIANCE (CSA). Top threats to cloud computing 2024. [S. l.]: CSA, 2024. Disponível em: https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2024. Acesso em: 5 out. 2026.

CONTACTA. Monitoramento em nuvem: tudo o que você precisa saber. [S. l.], 2023. Disponível em: https://www.contacta.com.br/monitoramento-em-nuvem-tudo-o-que-voce-precisa-saber/. Acesso em: 5 nov. 2023.

GOOGLE CLOUD. Definição da computação em nuvem. [S. l.], 2023. Disponível em: https://cloud.google.com/learn/what-is-cloud-computing. Acesso em: 11 ago. 2023.

HOSTINGER. O que é criptografia: entenda como ela funciona, quais os diferentes tipos e mais informações. [S. l.], 2023. Disponível em: https://www.hostinger.com.br/tutoriais/o-que-e-criptografia. Acesso em: 4 nov. 2023.

IMASTERS. Virtualização e segurança: superando os riscos. [S. l.], 2015. Disponível em: https://imasters.com.br/devsecops/virtualizacao-e-seguranca-superando-os-riscos. Acesso em: 29 out. 2023.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). ISO/IEC 27017:2015: information technology: security techniques: code of practice for information security controls based on ISO/IEC 27002 for cloud services. Geneva: ISO, 2015.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). ISO/IEC 27002:2022: information security, cybersecurity and privacy protection: information security controls. Geneva: ISO, 2022. Disponível em: https://www.iso.org/standard/75652.html. Acesso em: 15 jul. 2024.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). ISO/IEC 27018:2025: information security, cybersecurity and privacy protection: guidelines for protection of personally identifiable information (PII) in public clouds acting as PII processors. Geneva: ISO, 2025.

JOINT TASK FORCE. Security and privacy controls for information systems and organizations. NIST Special Publication 800-53, Revision 5. Gaithersburg: NIST, 2020. DOI: https://doi.org/10.6028/NIST.SP.800-53r5.

KASPERSKY. O que é segurança na nuvem? [S. l.], 2023. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-cloud-security. Acesso em: 14 ago. 2023.

KENT, K.; SOUPPAYA, M. Guide to computer security log management. NIST Special Publication 800-92. Gaithersburg: NIST, 2006. DOI: https://doi.org/10.6028/NIST.SP.800-92.

MELL, P.; GRANCE, T. The NIST definition of cloud computing. NIST Special Publication 800-145. Gaithersburg: NIST, 2011. DOI: https://doi.org/10.6028/NIST.SP.800-145.

MICHELETTI, M. Lei Geral de Proteção de Dados: o abismo entre a teoria e a prática. [S. l.]: CDL Jundiaí, 2021. Disponível em: https://cdljundiai.com.br/wp-content/uploads/2021/09/LGPD-O-ABISMO-ENTRE-A-TEORIA-E-A-PRATICA_202102231600.pdf. Acesso em: 12 jul. 2024.

NEXTCLOUD. You should control your data. [S. l.], 2017. Disponível em: https://nextcloud.com/about/. Acesso em: 11 abr. 2024.

OWNCLOUD. A safe home for all your data. [S. l.], 2016. Disponível em: https://owncloud.org. Acesso em: 11 abr. 2024.

ROSE, S.; BORCHERT, O.; MITCHELL, S.; CONNELLY, S. Zero trust architecture. NIST Special Publication 800-207. Gaithersburg: NIST, 2020. DOI: https://doi.org/10.6028/NIST.SP.800-207.

SCARFONE, K.; MELL, P. Guide to intrusion detection and prevention systems (IDPS). NIST Special Publication 800-94. Gaithersburg: NIST, 2007. DOI: https://doi.org/10.6028/NIST.SP.800-94.

SCARFONE, K.; SOUPPAYA, M.; HOFFMAN, P. Guide to security for full virtualization technologies. NIST Special Publication 800-125. Gaithersburg: NIST, 2011. DOI: https://doi.org/10.6028/NIST.SP.800-125.

SEAFILE. Who we are. [S. l.], 2024. Disponível em: https://www.seafile.com/en/about/. Acesso em: 9 jul. 2024.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

SOUPPAYA, M.; SCARFONE, K. Guide to enterprise patch management planning: preventive maintenance for technology. NIST Special Publication 800-40, Revision 4. Gaithersburg: NIST, 2022. DOI: https://doi.org/10.6028/NIST.SP.800-40r4.

TEMOSHOK, D. *et al.* Digital identity guidelines: authentication and authenticator management. NIST Special Publication 800-63B-4. Gaithersburg: NIST, 2025. DOI: https://doi.org/10.6028/NIST.SP.800-63B-4.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.