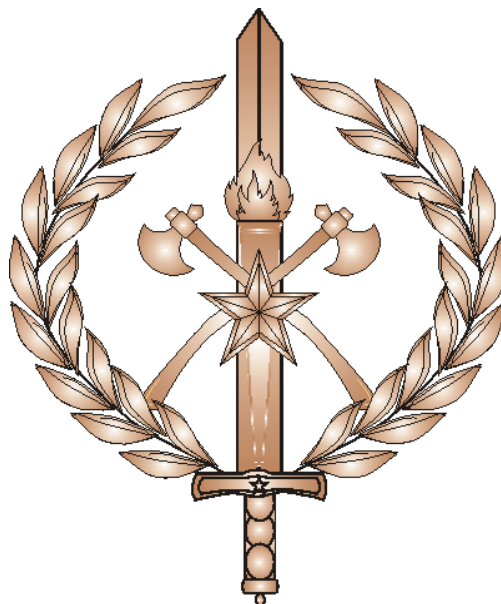


**CORPO DE BOMBEIROS MILITAR DO DISTRITO FEDERAL
DEPARTAMENTO DE ENSINO, PESQUISA, CIÊNCIA E TECNOLOGIA
DIRETORIA DE ENSINO
CENTRO DE ESTUDOS DE POLÍTICA, ESTRATÉGIA E DOCTRINA
CURSO DE ALTOS ESTUDOS PARA OFICIAIS**

MAJ QOBM/Compl. ANDERSON **FERREIRA** DA SILVA



**NUVEM PRIVADA NO CBMDF: UMA ALTERNATIVA PARA
ARMAZENAMENTO E COMPARTILHAMENTO DE ARQUIVOS,
GARANTINDO A LEGALIDADE, SEGURANÇA E PRIVACIDADE**

**BRASÍLIA
2025**

MAJ QOBM/Compl. ANDERSON **FERREIRA** DA SILVA

**NUVEM PRIVADA NO CBMDF: UMA ALTERNATIVA PARA
ARMAZENAMENTO E COMPARTILHAMENTO DE ARQUIVOS,
GARANTINDO A LEGALIDADE, SEGURANÇA E PRIVACIDADE**

Artigo científico apresentado à disciplina Metodologia Científica como requisito para conclusão do Curso de Altos Estudos para Oficiais do Corpo de Bombeiros Militar do Distrito Federal.

Orientador: TEN-CEL QOBM/Comb. ÍCARO **MACEDO** DE SOUZA

BRASÍLIA
2025

MAJ QOBM/Compl. ANDERSON FERREIRA DA SILVA

**NUVEM PRIVADA NO CBMDF: UMA ALTERNATIVA PARA
ARMAZENAMENTO E COMPARTILHAMENTO DE ARQUIVOS,
GARANTINDO A LEGALIDADE, SEGURANÇA E PRIVACIDADE**

Artigo científico apresentado à disciplina Metodologia Científica como requisito para conclusão do Curso de Altos Estudos para Oficiais do Corpo de Bombeiros Militar do Distrito Federal.

Aprovado em: ____/____/____.

BANCA EXAMINADORA

André Telles Campos – Cel QOBM/Comb.
Presidente

Igor **Muniz** da Silva – Ten-Cel QOBM/Comb.
Membro

Lucas Araújo Pereira – Ten-Cel QOBM/Compl.
Membro

Ícaro **Macedo** de Souza – Ten-Cel QOBM/Comb.
Orientador

TERMO DE AUTORIZAÇÃO PARA PUBLICAÇÃO

AUTOR: Maj. QOBM/Compl. Anderson Ferreira da Silva

TÍTULO: Nuvem Privada no CBMDF: Uma alternativa para armazenamento e compartilhamento de arquivos, garantindo a legalidade, segurança e privacidade.

DATA DE DEFESA: 13/10/2025.

| | | |
|--|--|---|
| Acesso ao documento | | |
| <input type="checkbox"/> Texto completo | <input type="checkbox"/> Texto parcial | <input type="checkbox"/> Apenas metadados |
| Em caso de autorização parcial, especificar a(s) parte(s) que deverá(ão) ser disponibilizadas: | | |

| |
|--|
| Licença |
| <p>DECLARAÇÃO DE DISTRIBUIÇÃO NÃO EXCLUSIVA</p> <p>O referido autor:</p> <p>a) Declara que o documento entregue é seu trabalho original, e que detém o direito de conceder os direitos contidos nesta licença. Declara também que a entrega do documento não infringe, tanto quanto lhe é possível saber, os direitos de qualquer outra pessoa ou entidade.</p> <p>b) Se o documento entregue contém material do qual não detém os direitos de autor, declara que obteve autorização do detentor dos direitos de autor para conceder ao CBMDF os direitos requeridos por esta licença, e que esse material cujos direitos são de terceiros está claramente identificado e reconhecido no texto ou conteúdo do documento entregue.</p> <p>Se o documento entregue é baseado em trabalho financiado ou apoiado por outra instituição que não o CBMDF, declara que cumpriram quaisquer obrigações exigidas pelo respectivo contrato ou acordo.</p> <p>LICENÇA DE DIREITO AUTORAL</p> <p>Na qualidade de titular dos direitos de autor da publicação, autorizo a Biblioteca da Academia de Bombeiro Militar disponibilizar meu trabalho por meio da Biblioteca Digital do CBMDF, com as seguintes condições: disponível sob Licença Creative Commons 4.0 International, que permite copiar, distribuir e transmitir o trabalho, desde que seja citado o autor e licenciante. Não permite o uso para fins comerciais nem a adaptação desta.</p> <p>A obra continua protegida por Direito Autoral e/ou por outras leis aplicáveis. Qualquer uso da obra que não o autorizado sob esta licença ou pela legislação autoral é proibido.</p> |

Anderson **Ferreira** da Silva

Maj. QOBM/Compl.

RESUMO

Este artigo propõe um modelo de nuvem privada para o Corpo de Bombeiros Militar do Distrito Federal - CBMDF para garantir o armazenamento e compartilhamento legal, seguro e privado de arquivos institucionais, alinhando-se à Política de Segurança da Informação e Comunicação - POSIC do Governo do Distrito Federal - GDF. A pesquisa aborda a dependência atual do CBMDF em serviços gratuitos de nuvem pública e as limitações da nuvem governamental existente, ambas as quais representam riscos significativos à integridade dos dados e à conformidade com as políticas. Foi utilizada uma metodologia aplicada e qualitativa, utilizando o raciocínio indutivo de desafios específicos do CBMDF para propor uma solução geral. Os procedimentos técnicos incluíram pesquisa bibliográfica e documental, entrevistas com profissionais de TI do GDF, e análise de documentos internos do CBMDF. Uma solução básica de nuvem privada de código aberto, *Nextcloud*, foi implementada para fins de análise em "nuvem.cbm.df.gov.br". Os resultados confirmam que um modelo de nuvem privada oferece uma solução viável e econômica para garantir a legalidade, a segurança e a privacidade dos dados, ao mesmo tempo em que aborda desafios operacionais e técnicos. Esta solução permite ao CBMDF alinhar as suas atividades institucionais com os requisitos da POSIC do GDF, proporcionando um ambiente seguro e privado com controle aprimorado sobre sua infraestrutura, particularmente através da adoção de tecnologias de código aberto.

Palavras-chave: CBMDF, Código aberto, POSIC, Nuvem privada, Segurança da informação.

ABSTRACT

This article proposes a private cloud model for the Military Fire Department of the Federal District (CBMDF) to ensure the legal, secure, and private storage and sharing of institutional files, aligning with the Information and Communication Security Policy (POSIC) of the Federal District Government (GDF). The research addresses the CBMDF's current reliance on free public cloud services and the limitations of the existing governmental cloud, both of which pose significant risks to data integrity and policy compliance. An applied and qualitative methodology was utilized, employing inductive reasoning from specific CBMDF challenges to propose a general solution. Technical procedures included bibliographic and documentary research, interviews with GDF IT professionals, and analysis of internal CBMDF documents. A basic open-source private cloud solution, Nextcloud, was implemented for demonstration purposes at "nuvem.cbm.df.gov.br". The results confirm that a private cloud model offers a viable and economical solution for ensuring data legality, security, and privacy, while addressing operational and technical challenges. This solution allows the CBMDF to align its institutional activities with the GDF's POSIC requirements, providing a secure and private environment with enhanced control over its infrastructure, particularly through the adoption of open-source technologies.

Keywords: CBMDF, Open source, POSIC, Private cloud, Information security.

1 INTRODUÇÃO

A crescente demanda por armazenamento e compartilhamento de arquivos digitais transformou a maneira como organizações e indivíduos gerenciam suas informações. No contexto corporativo, essa realidade é ainda mais latente, impulsionando a busca por soluções eficientes e seguras. No entanto, o uso indiscriminado de serviços de nuvem pública e gratuita, muitas vezes por meio de contas pessoais, tem se revelado uma prática arriscada, especialmente para instituições onde normativos proíbem esse procedimento, como o Corpo de Bombeiros Militar do Distrito Federal - CBMDF.

No âmbito do Governo do Distrito Federal - GDF, a Política de Segurança da Informação e Comunicação - POSIC, por meio da Resolução nº 01, de 29 de abril de 2024 (Distrito Federal, 2024a), estabelece diretrizes claras e mandatórias, que incluem a obrigatoriedade de utilização de recursos de rede e armazenamento em nuvem fornecidos pela área de Tecnologia da Informação e Comunicação - TIC do órgão e a proibição explícita do uso de serviços de e-mail e armazenamento gratuitos para atividades institucionais. Essa determinação coloca o CBMDF diante do desafio de buscar alternativas que garantam a legalidade, a segurança e a privacidade de suas informações, ao mesmo tempo em que otimizam custos e processos.

Diferente dos modelos de nuvem pública, que podem apresentar vulnerabilidades inerentes ao compartilhamento de infraestrutura com múltiplos usuários, a nuvem privada oferece um ambiente dedicado e controlado, permitindo à corporação gerenciar seus próprios recursos de armazenamento e compartilhamento de arquivos. Isso não apenas assegura a conformidade com a POSIC do GDF, mas também mitiga os riscos associados à segurança da informação, privacidade dos dados e acesso não autorizado. Adicionalmente, a disponibilidade de soluções de código aberto e de baixo custo no mercado torna a nuvem privada, em alguns casos, uma opção acessível e eficiente, que se alinha às restrições orçamentárias da instituição, demandando investimentos apenas em contratos de manutenção e aquisição de equipamentos. Assim, como o CBMDF pode implementar uma solução de armazenamento e compartilhamento de arquivos

em nuvem que garanta a legalidade, segurança e privacidade dos dados institucionais, em conformidade com a POSIC do GDF, buscando evitar o uso de nuvens públicas gratuitas e superando as restrições de nuvem governamental, tecnologicamente e financeiramente viável?

Dessa forma, este estudo tem como objetivo principal analisar a viabilidade de uma nuvem privada para o Corpo de Bombeiros Militar do Distrito Federal (CBMDF) com foco no armazenamento e compartilhamento de arquivos, explorando como essa abordagem pode garantir a legalidade, a segurança e a privacidade das informações. A pesquisa buscará responder a questões cruciais, e para isso tem como objetivos específicos analisar os requisitos do CBMDF, identificar os riscos e as limitações das soluções de nuvem pública e governamental, propor uma solução de nuvem privada de baixo custo, realizar uma análise de viabilidade econômica e discutir os desafios operacionais e técnicos para a adoção e a sustentabilidade da solução proposta.

2 DESENVOLVIMENTO

2.1 Revisão de literatura

De acordo com Macson (2023), a computação em nuvem (em inglês, *Cloud Computing*) é uma das tecnologias que mais crescem e se espalham atualmente, impulsionada pela necessidade das corporações de renovar seus parques tecnológicos e pela drástica redução inicial nos custos de implementação.

Segundo o National Institute of Standards and Technology - NIST (MELL, 2011), a computação em nuvem é definida como um modelo que permite o acesso onipresente, conveniente e sob demanda à rede compartilhada com um conjunto de recursos, e possuindo cinco características essenciais: autoatendimento sob demanda, amplo acesso à rede, agrupamento de recursos (*resource pooling*), elasticidade rápida e serviço medido (*pay-per-use*). Além disso, a nuvem é categorizada por modelos de serviço e de implantação:

2.1.1 Modelos de Serviço

- **Software como Serviço (SaaS):** Aplicações de software são fornecidas ao usuário final como um serviço através da internet, sem a necessidade de instalação ou gerenciamento local (ex: *e-mails* baseados em web). Esse é um modelo mais abrangente, onde o cliente apenas configura o software e o provedor de serviços cuida de todo o restante, incluindo hospedagem, manutenção e infraestrutura. O acesso geralmente é feito pela internet através de um navegador, sem a necessidade de instalação
- **Plataforma como Serviço (PaaS):** Oferece uma plataforma para o desenvolvimento, execução e gerenciamento de aplicações, incluindo sistemas operacionais, linguagens de programação, bancos de dados, etc., sem o controle da infraestrutura subjacente. Esse modelo fica entre o SaaS e o IaaS (descrito logo a seguir) em termos de controle. O cliente é responsável por seus aplicativos e dados, mas o provedor oferece um ambiente completo para desenvolvimento, teste e implantação, cuidando de toda a infraestrutura (servidores, redes, etc.). Este geralmente é um modelo adotado por desenvolvedores e equipes que desejam se concentrar na criação de aplicativos sem gerenciar a complexidade da infraestrutura.
- **Infraestrutura como Serviço (IaaS):** Fornece recursos computacionais básicos, como servidores virtuais, armazenamento e redes, permitindo ao usuário maior controle sobre o ambiente, mas exigindo o gerenciamento do sistema operacional e das aplicações. É um modelo que oferece mais controle ao cliente. O provedor de serviços cuida apenas da infraestrutura física (servidores, armazenamento, rede), e o cliente é responsável por tudo o que está acima, como sistemas operacionais e aplicativos. O cliente aluga a infraestrutura conforme a necessidade e paga pelo uso. É a escolha ideal para equipes que precisam de alto controle e têm a expertise para gerenciar a infraestrutura.

2.1.2 Modelos de Implantação

- **Nuvem Pública:** Os recursos são disponibilizados por um provedor terceiro para o público em geral via internet. Caracteriza-se pelo compartilhamento de infraestrutura entre múltiplos usuários (*multi-tenancy*) e pela alta escalabilidade.
- **Nuvem Híbrida:** Combina dois ou mais tipos de nuvens distintas (públicas, privadas ou comunitárias) que permanecem como entidades únicas, mas são unidas por tecnologia padronizada ou proprietária que permite a portabilidade de dados e aplicações.
- **Nuvem Comunitária:** A infraestrutura é compartilhada por diversas organizações com interesses comuns, geralmente governada por uma ou mais dessas organizações.
- **Nuvem Privada:** A infraestrutura de computação é operada exclusivamente para uma única organização. Este modelo, de foco principal deste estudo, será detalhado a seguir.

2.1.3 A Nuvem Privada: Controle, Segurança e Exclusividade

A nuvem privada é um modelo de implantação de computação em nuvem onde a infraestrutura é provisionada para uso exclusivo por uma única organização. Isso significa que a organização tem controle total sobre os recursos, a segurança e a privacidade dos dados, seja a infraestrutura gerenciada internamente pela própria organização ou por um terceiro. Strack (2024), em sua monografia sobre desafios e melhores práticas para a proteção de dados em ambientes de armazenamento em nuvem privada, reforça a importância desse modelo para a segurança e o controle dos dados.

As principais características da nuvem privada incluem:

- **Exclusividade:** Os recursos são dedicados a uma única entidade, eliminando as preocupações com compartilhamento com outros órgãos

que podem estar causando ineficiente no serviço usado, e assim garantindo maior isolamento.

- **Controle Total:** A organização detém o controle completo sobre a infraestrutura, desde a camada física até o software, permitindo personalizar configurações de segurança, rede e armazenamento de acordo com suas políticas internas e requisitos regulatórios.
- **Segurança Aprimorada:** Dada a exclusividade e o controle, é possível implementar medidas de segurança mais rigorosas e adaptadas às necessidades específicas da organização, o que é crucial para dados sensíveis.
- **Conformidade:** Facilita o atendimento a regulamentações específicas de setores ou governos, como a Lei Geral de Proteção de Dados - LGPD (BRASIL, 2018) e, no caso do CBMDF, a POSIC do GDF, uma vez que a organização mantém a soberania sobre seus dados.
- **Customização:** A infraestrutura pode ser adaptada para atender a requisitos de desempenho, escalabilidade e integração com sistemas legados, o que nem sempre é possível em nuvens públicas.
- **Custos:** Embora o investimento inicial possa ser maior que em nuvens públicas (devido à aquisição de *hardware* e *software*, e a necessidade de equipe especializada), a longo prazo, pode ser mais custo-efetiva, especialmente com a adoção de soluções de código aberto.

2.1.4 Segurança da Informação e Privacidade de Dados em Ambientes de Nuvem

A segurança da informação é um pilar fundamental em qualquer ambiente de Tecnologia da Informação, e na computação em nuvem não é diferente. No entanto, o modelo de nuvem introduz desafios e responsabilidades compartilhadas. Subashini (2011), aponta a importância da segurança nas questões de entrega de serviço em modelos de computação em nuvem, onde em ambientes de nuvem, a segurança abrange múltiplos domínios: segurança da rede, segurança da aplicação, segurança de dados, gerenciamento de identidade e acesso, e segurança física. Para nuvens privadas, a responsabilidade pela segurança recai predominantemente

sobre a própria organização, o que exige um alto nível de maturidade em gestão de segurança.

A privacidade de dados é intrinsecamente ligada à segurança, mas se refere especificamente ao controle sobre o acesso, uso e divulgação de informações pessoais e sensíveis. Com a LGPD, a garantia da privacidade tornou-se uma exigência legal e um diferencial competitivo.

A POSIC do GDF, no contexto deste trabalho, reforça a necessidade de que o armazenamento e compartilhamento de dados institucionais estejam em conformidade com rígidos padrões de segurança e privacidade. Isso significa que a solução de nuvem adotada pelo CBMDF deve oferecer mecanismos robustos de controle de acesso, criptografia de dados em trânsito e em repouso, monitoramento de atividades e trilhas de auditoria para garantir a inviolabilidade e a confidencialidade das informações.

2.1.5 Soluções de Código Aberto para Nuvem Privada e Gerenciamento de Arquivos

A busca por soluções de nuvem privada de baixo custo tem impulsionado a adoção de tecnologias de código aberto (*open source*). Essas soluções oferecem a vantagem de reduzir significativamente os custos com licenciamento de software, permitindo que o investimento seja direcionado para *hardware*, infraestrutura de rede, treinamento e suporte.

Diversas plataformas de código aberto permitem a construção de uma nuvem privada, oferecendo funcionalidades comparáveis às soluções comerciais. Para armazenamento e compartilhamento de arquivos, destacam-se:

- **Nextcloud/OwnCloud:** São plataformas robustas que oferecem funcionalidades completas de sincronização e compartilhamento de arquivos, calendários, contatos, tarefas e colaboração online. São altamente customizáveis e podem ser integradas com sistemas de autenticação existentes, como LDAP/Active Directory. A flexibilidade e o controle sobre os dados são pontos fortes (NEXTCLOUD, 2025) (OWNCLOUD, 2025).

- **OpenStack:** Embora mais complexo, o OpenStack é um conjunto de *software* de código aberto que fornece um sistema operacional para a nuvem, controlando grandes *pools* de recursos de computação, armazenamento e rede. Ele pode ser usado para construir uma infraestrutura IaaS de nuvem privada, sobre a qual outras soluções de compartilhamento de arquivos podem ser implementadas (OPENSTACK, 2025).

A adoção dessas tecnologias open source não se limita apenas à redução de custos. Ela também promove maior flexibilidade, evita a dependência de fornecedores e permite que a organização tenha um controle mais granular sobre o desenvolvimento e a evolução de sua infraestrutura, segundo Macson (2023).

2.1.6 Gerenciamento e Compartilhamento de Arquivos em Nuvem

O armazenamento e compartilhamento de arquivos são funcionalidades essenciais em qualquer ambiente corporativo moderno. Em nuvem, essas funcionalidades ganham em escalabilidade, acessibilidade e flexibilidade. No entanto, é fundamental que sejam acompanhadas de mecanismos robustos de controle de acesso, versionamento, auditoria e capacidade de recuperação de desastres.

A transição de um ambiente de servidores de arquivos tradicionais para uma nuvem privada de compartilhamento de arquivos exige um planejamento cuidadoso. Nesse sentido, segundo Strack (2024), é necessário considerar:

Migração de dados: Estratégias para transferir grandes volumes de dados de forma segura e com o mínimo de interrupção.

Integração com sistemas existentes: Conexão com sistemas de autenticação (como *Active Directory* ou *LDAP*) para gerenciar permissões de acesso de forma centralizada.

Treinamento de usuários: Capacitação dos militares para utilizar a nova plataforma de forma eficiente e segura.

Backup e Recuperação: Definição de políticas de backup e planos de recuperação de desastres para garantir a continuidade dos serviços e a integridade dos dados.

Uma nuvem privada bem implementada para compartilhamento de arquivos não apenas atende às exigências regulatórias e de segurança, mas também otimiza a colaboração e a produtividade da equipe, fornecendo uma plataforma centralizada e confiável para o trabalho diário.

2.1.7 Repatriação de Nuvem

Repatriação de Nuvem ou *Cloud Repatriation* é o processo de mover dados, cargas de trabalho (*workload*) ou infraestrutura de TI para fora de uma nuvem pública, parcial ou totalmente. O ambiente de destino para hospedagem de serviços em nuvem é o próprio ambiente da organização, numa infraestrutura local (*on-premises*) ou um *data center* localizado que oferece serviço de *colocation* (Räisänen, 2025).

Os custos elevados e imprevisíveis na nuvem pública tem sido um dos principais motivos para a repatriação de nuvem. A empresa Dropbox transferiu grande parte da sua infraestrutura da AWS para seus próprios servidores, alcançando uma economia de aproximadamente US\$ 75 milhões em dois anos (Krazit, 2018). A GEICO percebendo um aumento de mais de 2,5 vezes nos custos de nuvem, a empresa repatriou grande parte das suas cargas de trabalho (Targett, 2024).

No estudo de Jewargi (2023), o autor acrescenta ainda outros fatores para a repatriação de nuvem, como a segurança de dados, à regulamentação, ao desempenho de aplicativos, à independência de fornecedores e ao tempo de inatividade. Em seu trabalho, Jewargi descreve o exemplo de um ex-funcionário da Amazon Web Service - AWS acusado de roubar dados referentes à empresa Capital One que possuía serviços de nuvem na AWS em 2019.

Em um caso específico do CBMDF sobre a contratação de Software como Serviço - SaaS, a análise da possível aquisição do Microsoft 365 por meio de ata de

registro de preço revelou desafios importantes. A principal preocupação foi o alto custo e a dependência gerada pelo fornecedor.

A contratação, caso fosse realizada em março de 2023, visava adquirir o pacote Microsoft Office 365 Enterprise E3, que incluía o MS Office, 1 TB de armazenamento no OneDrive e acesso ao Microsoft Teams, com licenças individuais e um contrato de três anos. A compra inicial de 541 licenças tinha o valor de R\$ 2.431.578,06. Conforme o Estudo Técnico Preliminar - ETP, a quantidade total prevista era de 2.301 licenças, o que elevaria o custo total para R\$ 10.342.074,06.

Além do custo, a análise, detalhada no Memorando 44 (Distrito Federal, 2022a), destacou o risco de dependência. A não renovação do contrato resultaria em um grande prejuízo operacional e financeiro, pois a migração e padronização dos dados armazenados na nuvem exigiriam tempo, custos e esforços significativos.

Portanto, a decisão de adotar uma solução SaaS de grande escala como o Microsoft 365 exige um estudo aprofundado e uma análise de custos e riscos extremamente assertivos. É crucial que o órgão tenha certeza de que a ferramenta atende plenamente às necessidades, considerando o alto investimento e a potencial dependência que pode ser gerada.

2.2 Metodologia

A pesquisa adotou uma metodologia de natureza aplicada, tendo como principal objetivo a proposição de um modelo de nuvem privada para o CBMDF, visando atender às suas necessidades de armazenamento e compartilhamento de arquivos de forma legal, segura e privada. Conforme aponta Gil (2022), a pesquisa aplicada objetiva gerar conhecimentos para aplicação prática, dirigidos à solução de problemas específicos.

Com uma abordagem predominantemente qualitativa, o estudo aprofundou a compreensão do problema e das soluções potenciais. Segundo Marconi (2010) a abordagem qualitativa preocupa-se em analisar e interpretar, de forma aprofundada, os fenômenos e atribuir-lhes significados, o que é fundamental para um projeto de cunho propositivo.

Quanto aos objetivos, a pesquisa se configura inicialmente como exploratória, para levantar informações sobre o tema no contexto do CBMDF, e subsequentemente descritiva, para detalhar as características da solução proposta. De acordo com Cervo e Bervian (2002), a pesquisa exploratória busca proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito, enquanto a descritiva visa a observar, registrar, analisar e correlacionar fatos ou fenômenos (Cervo, 2002). O raciocínio lógico que fundamenta o estudo é o indutivo, partindo da análise das particularidades e desafios do CBMDF para construir e propor uma solução geral e aplicável (Gerhardt, 2009).

Os procedimentos técnicos envolveram principalmente a pesquisa bibliográfica para a fundamentação teórica sobre computação em nuvem, segurança da informação e soluções de código aberto, e a pesquisa documental para análise da Política de Segurança da Informação e Comunicações - POSIC do GDF e de outros documentos institucionais relevantes. Gil (2022) destaca que a pesquisa bibliográfica é desenvolvida a partir de material já elaborado, constituído principalmente de livros e artigos científicos, enquanto a documental utiliza materiais que não receberam ainda um tratamento analítico (Gil, 2022).

Embora não seja um estudo de caso com coleta de dados primários in loco, a pesquisa assume um caráter de estudo de caso propositivo ao focar na problemática específica do CBMDF para desenvolver uma solução concreta e aplicável às suas necessidades.

Assim, ainda na pesquisa documental e coleta de dados, esta pesquisa envolveu entrevista com gestores e profissionais da SETIC/GDF para verificação de limitações, possíveis restrições e serviços oferecidos pela nuvem privada governamental. Também foram utilizadas informações recentes de processos do Sistema de Eletrônico de Informação - SEI, onde constam diversas evidências sobre uso de nuvem públicas e gratuitas por parte do CBMDF, além de resultados e relatórios técnicos sobre uso de nuvem e infraestrutura de rede de computadores, pela Corporação.

Quanto à proposição de uma solução de nuvem privada para o CBMDF, foi implementado de forma básica, uma solução open source de nuvem, para

demonstração de uma possível alternativa para solução do problema descrito nesta pesquisa.

Por fim, ferramentas de Inteligência Artificial foram empregadas para aprimorar a redação do texto, visando clareza e boa leitura, bem como para auxiliar na correção e ajustes durante a implementação da solução do Nextcloud disponibilizado em “nuvem.cbm.df.gov.br” para demonstração de um serviço de nuvem privada.

2.3 Resultados e discussão

2.3.1 Evidências no uso de nuvem gratuita pelo CBMDF e conflito com a POSIC do GDF

Uma pesquisa no Sistema Eletrônico de Informações (SEI) do Distrito Federal, acessível em “<https://www.portalsei.df.gov.br/>”, revela o uso de serviços de nuvem pública gratuita por militares do CBMDF para atividades institucionais, conforme Figuras 1 e 2.

Ao realizar uma “Pesquisa Pública” no SEI, especificando o órgão “CBMDF” e utilizando as palavras-chave “google drive” e “docs.google”, é possível encontrar diversos processos que comprovam essa prática. A análise desses processos demonstra que o armazenamento de informações de estoque de materiais de Unidades e o acompanhamento diário de serviços operacionais são realizados em plataformas como o Google Drive e Google Docs.

A evidência mais contundente é encontrada no processo SEI 00053-00054049/2025-88¹, que trata da solicitação de levantamento sobre a geração e armazenamento de dados. As respostas a essa solicitação, contidas na Circular Nº 204/2025 - CBMDF/GABCG (Distrito Federal, 2025b), incluem relatos de diversas Unidades que confirmam o uso de nuvens gratuitas.

¹ O pedido de acesso às informações do processo 00053-00054049/2025-88 para uso neste artigo, foi solicitado por meio do processo SEI 00053-00065502/2025-81.

Alguns trechos de memorandos do processo SEI 00053-00054049/2025-88 demonstram essa realidade:

“II – Métodos alternativos de armazenamento:

Utilizam-se planilhas armazenadas em nuvem (DRIVE.GOOGLE) com acesso restrito aos militares da seção, como método complementar de controle e organização de dados.” Memorando 554 (Distrito Federal, 2025c).

“I – Sistemas utilizados para geração, armazenamento e manipulação de dados:

....

Planilhas online do google sheets, para controle financeiro de contratos e controle técnico de manutenção de aeronaves.

Painel Lookerstudio google, para acesso rápido as estatísticas operacionais.

.... “ Memorando 144 (Distrito Federal, 2025d).

“I – Sistemas utilizados para geração, armazenamento e manipulação de dados:

...

Para comunicação deste GBM com os militares aqui lotados usa-se, eventualmente, uilizam-se ferramentas como Whatsapp, formulários google.” Memorando 446 (Distrito Federal, 2025e)

Esses relatos deixam claro que o uso de serviços de nuvem gratuita não é um caso isolado, mas uma prática comum em várias Unidades do CBMDF.

Para utilizar os serviços do Google, como o armazenamento de arquivos e a criação de documentos, planilhas e formulários colaborativos, é necessária a criação de uma conta de e-mail do Gmail (GOOGLE, 2025). Essa prática, no entanto, contraria a Política de Segurança da Informação e Comunicações (POSIC) do GDF, que proíbe o uso de e-mails gratuitos para a condução de atividades institucionais. O

uso de nuvens públicas gratuitas, portanto, representa uma violação das normas internas de segurança da informação da instituição.

Figura 1 – Tela de pesquisa no Portal SEI/DF, com a palavra-chave "google drive".

The screenshot shows the search interface of the SEI/DF portal. The search term 'GOOGLE DRIVE' is entered in the search box. The search filters are set to 'Processos' and 'Documentos Gerados'. The search results are displayed in a table with three entries, each showing the document number, date, and unit.

| Nº SEI (protocolo Processual/ Documento): | Texto para Pesquisa: | Pesquisar em: | Interessado / Remetente: | Órgão Gerador: | Unidade Geradora: | Tipo do Processo: | Tipo do Documento: | Data entre: |
|---|----------------------|---|--------------------------|----------------|-------------------|-------------------|--------------------|-------------|
| | GOOGLE DRIVE | <input checked="" type="checkbox"/> Processos <input checked="" type="checkbox"/> Documentos Gerados <input type="checkbox"/> Documentos Externos | | CBMDF | | | | |

| Resultado | Data |
|---|------------------|
| CBMDF - Serviço Administrativo Diário nº 00053-00065408/2025-22 (CBMDF - Livro do dia ao Depósito 1º GBM - 02/08/2025 - ALA CHARLIE) | 177728846 |
| de "Pesquisar" DIGITAR "Depósito Operacional", CLICAR no botão COPY; ABRIR uma planilha no Google... Drive; COLAR (Ctrl + V) na planilha; SELECIONAR no menu Formatar > "Converter para Tabela"; Botão... | |
| Unidade: CBMDF/COMARI/1ºGBM/PRONT | Data: 03/08/2025 |
| CBMDF - Serviço Administrativo Diário nº 00053-00065408/2025-22 (CBMDF - Livro do dia ao Depósito 1º GBM - 01/08/2025 - ALA BRAVO) | 177720156 |
| de "Pesquisar" DIGITAR "Depósito Operacional", CLICAR no botão COPY; ABRIR uma planilha no Google... Drive; COLAR (Ctrl + V) na planilha; SELECIONAR no menu Formatar > "Converter para Tabela"; Botão... | |
| Unidade: CBMDF/COMARI/1ºGBM/PRONT | Data: 02/08/2025 |
| CBMDF - Serviço Administrativo Diário nº 00053-00065408/2025-22 (CBMDF - Livro do dia ao Depósito 1º GBM - 31/07/2025 - ALA ALFA) | 177604628 |
| de "Pesquisar" DIGITAR "Depósito Operacional", CLICAR no botão COPY; ABRIR uma planilha no Google... Drive; COLAR (Ctrl + V) na planilha; SELECIONAR no menu Formatar > "Converter para Tabela"; Botão... | |
| Unidade: CBMDF/COMARI/1ºGBM/PRONT | Data: 01/08/2025 |

Fonte: Captura de tela realizada em 25 de julho de 2025 no site <https://www.portalsei.df.gov.br/>.

Figura 2 – Tela de pesquisa no Portal SEI/DF, com a palavra-chave "docs.google".

The screenshot shows the SEI/DF search interface. At the top, there is a search bar with the text "docs.google" entered. Below the search bar, there are several filters: "Pesquisar em:" with checkboxes for "Processos" (checked), "Documentos Gerados" (checked), and "Documentos Externos" (unchecked); "Interessado / Remetente:" with a text input field; "Órgão Gerador:" with a dropdown menu set to "CBMDF"; "Unidade Geradora:" with a text input field; "Tipo do Processo:" with a dropdown menu; and "Tipo do Documento:" with a dropdown menu. Below the filters, there are four search results displayed as cards. Each card contains the following information: "CBMDF - Serviço Operacional nº 00053-00024808/2024-05 (CBMDF - Livro do dia ao Depósito ALA B - 01/08/2025) 177721892"; a URL starting with "https://docs.google.com/forms/d/e/1FAIpQLScdO540xnayGkv90ko94wxIPNEQhXHyjBdxzhYM21o2A5qpw/viewform"; "Unidade: CBMDF/GPRAMP/PRONT"; and "Data: 02/08/2025".

Fonte: Captura de tela realizada em 25 de julho de 2025 no site <https://www.portalsei.df.gov.br/>.

2.3.2 Orçamento do CBMDF para custeio e investimento em TIC

A gestão dos recursos de TIC no CBMDF tem sido orientada pelo Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) há mais de 15 anos. A obrigatoriedade desse plano foi reforçada pelo Decreto nº 40.015, de 14 de agosto de 2019, que o tornou uma condição indispensável para todas as aquisições e contratações de bens e serviços de TIC na Administração Pública do Distrito Federal, em seu Art. 1º do referido Decreto.

Apesar da importância do PDTIC, a análise dos últimos dois planos (quando a validade mudou de quatro para dois anos) revela uma execução orçamentária consistentemente baixa em TIC na Corporação. A Tabela 1, por exemplo, demonstra

que no período do PDTIC 2021-2022, a execução orçamentária foi de apenas 17% do valor total previsto de R\$ 35.714.600,00.

Além da baixa execução, a distribuição do orçamento também é notável. A maior parte dos recursos, mais de 90%, foi direcionada para investimento (equipamentos de redes), e não para custeio. É importante ressaltar que serviços como o SaaS, que é um modelo comum de contratação de soluções de software, se enquadram na natureza de custeio.

Tabela 1 – Avaliação da execução orçamentária do PDTIC 2021-2022

| Meta | Descrição da Necessidade | Processo SEI | Valor |
|---------------|------------------------------------|------------------------|-------------------------|
| M14 | Telefonia Fixa | 0053-046372/2016 | R\$ 411.621,19 |
| M14 | Telefonia Móvel | 053001603/2014 | R\$ 355.604,88 |
| M1 | Conectividade de IP com a Internet | SEI-053-082340/2016 | R\$ 19.276,68 |
| M1 | Equipamentos de redes | 00053-00098149/2020-10 | R\$ 5.136.892,11 |
| TOTAL: | | | R\$ 5.923.394,86 |

Fonte: Relatório 15 do processo SEI 00053-00193932/2022-40 (Distrito Federal, 2022b).

Na Tabela 2, por exemplo, percebe-se o mesmo cenário da tabela anterior, onde no PDTIC 2023-2024, a execução orçamentária foi de apenas 5,92% do valor total previsto de R\$ 28.488.200,00.

Tabela 2 – Avaliação da execução orçamentária do PDTIC 2023-2024

| Descrição | Processo SEI | Valor |
|-------------------------------|------------------------|------------------|
| Capacitação – Curso Alura | 00053-00063254/2022-91 | R\$ 44.880,00 |
| Tablets | 00053-00163137/2021-46 | R\$ 252.999,54 |
| Baterias Estacionárias | 00053-00175585/2022-73 | R\$ 9.760,00 |
| No-break – DITIC | 00053-00129830/2023-51 | R\$ 15.463,63 |
| Subscrição Sistema Singular | 00053-00167439/2021-93 | R\$ 288.236,99 |
| Telefonia – VoIP | 00053-00050868/2023-94 | R\$ 63.154,80 |
| Telefonia – móvel – renovação | 00053-00038695/2020-93 | R\$ 996.117,59 |
| Certificado digital tipo A3 | 00053-00047615/2023-33 | R\$ 7.704,00 |
| Link para o CETOP | 00053-00191100/2022-99 | R\$ 9.200,00 |
| | Utilizado | R\$ 1.687.516,55 |

Fonte: Relatório 2 do processo SEI 00053-00196475/2024-15 (Distrito Federal, 2024b).

Essa baixa execução orçamentária e a concentração em investimentos, com pouca alocação para custeio, levantam questões sobre a capacidade da Corporação em modernizar e manter seus sistemas de TIC de forma eficaz, especialmente numa possível contratação de serviços em nuvem e de softwares online (modalidade SaaS) que ofereçam ferramentas colaborativas.

Ainda, com base nos Relatórios de Gestão Anuais² de 2023 a 2024, o orçamento médio da Corporação, excluindo a folha de pagamento e demais despesas de pessoal, foi de R\$ 51.998.656,77 para custeio e R\$ 17.564.351,69 para investimento. A memória de cálculo sobre os valores médios dos Relatórios de Gestão Anuais estão dispostos no Apêndice B. Ao comparar esses valores com o orçamento médio previsto para os dois últimos PDTICs, observa-se que, em média, 40,95% de todo o orçamento da Corporação deveria ser destinado a gastos com Tecnologia da Informação e Comunicação (TIC). Mesmo considerando a possibilidade de descontos em licitações, se tivéssemos 100% de execução orçamentária dos PDTICs, a alocação de quase metade do orçamento da Corporação seria para área de TIC, o que parece ser excessivamente alta, especialmente para uma instituição com um orçamento total relativamente baixo para cobrir todas as suas despesas de custeio e investimento.

Um exemplo disso, apresentado no tópico 2.1.7 deste artigo, foi análise de aquisição do Microsoft Office 365 Enterprise E3 para o CBMDF, conforme detalhado no Memorando 44 (Distrito Federal, 2022a). O contrato, com um valor total de R\$ 10.342.074,06 por três anos, levanta sérias preocupações. Dado o cenário de baixa execução orçamentária e a alta dependência de recursos para TIC, se este contrato tivesse sido firmado, existiria um risco real de que a Corporação não tivesse orçamento suficiente para garantir a continuidade desses serviços após o término do contrato. E uma vez não renovando o contrato, o fornecedor daria um prazo de até 60 dias para que os usuários retirassem todos seus dados na nuvem ou apresentar um outro ambiente em nuvem ou local para migração dos dados, com o risco de perda total das informações geradas na nuvem durante o período de vigência do contrato.

2.3.3 Limitações na prestação dos serviços da nuvem governamental da SETIC/SEE do GDF

Em 2019, o Corpo de Bombeiros Militar do Distrito Federal (CBMDF) consultou a Secretaria de Estado de Fazenda, Planejamento, Orçamento e Gestão

2

<https://www.cbm.df.gov.br/lai/prestacao-de-contas-anual-uniao/prestacao-de-contas-anual-uniao/>

do Distrito Federal (atual Secretaria de Estado de Economia do DF) sobre a migração de seus recursos e serviços de Data Center. A iniciativa foi tomada em conformidade com o Art. 6º do Decreto nº 40.015, de 14 de agosto de 2019 (Distrito Federal, 2019b).

A consulta foi formalizada através do Ofício 2367 (Distrito Federal, 2019a). Em resposta, a SETIC/GDF, por meio da Nota Técnica 3 (Distrito Federal, 2019c), afirmou que poderia atender à solicitação, detalhando os serviços oferecidos aos órgãos do GDF, conforme ilustrado na Figura 3.

Figura 3 – Serviços ofertados pela SETIC/GDF.

| Colocation | Hosting | Infraestrutura como Serviço (IaaS) | Plataforma como Serviço (PaaS) | Software como Serviço (SaaS) |
|----------------------|----------------------|------------------------------------|--------------------------------|------------------------------|
| Dados | Dados | Dados | Dados | Dados |
| Aplicação | Aplicação | Aplicação | Aplicação | Aplicação |
| Middleware e Runtime | Middleware e Runtime | Middleware e Runtime | Middleware e Runtime | Middleware e Runtime |
| SGBD | SGBD | SGBD | SGBD | SGBD |
| Sistema Operacional | Sistema Operacional | Sistema Operacional | Sistema Operacional | Sistema Operacional |
| Virtualização | Virtualização | Virtualização | Virtualização | Virtualização |
| Servidores | Servidores | Servidores | Servidores | Servidores |
| Storage | Storage | Storage | Storage | Storage |
| Network/Segurança | Network/Segurança | Network/Segurança | Network/Segurança | Network/Segurança |
| Data Center | Data Center | Data Center | Data Center | Data Center |

| |
|--------------------------------|
| Gerido pelo Órgão Cliente |
| Gerido pelo CeTIC - SUTIC/SEEC |

Fonte: Nota Técnica 3 do processo SEI 00053-00100615/2019-92.

Assim, diante da resposta positiva da SETIC/GDF que atenderia à toda a demanda do CBMDF para hospedar os ativos do Data Center do CBMDF, a migração deste ocorreu então no início de 2020.

Durante esses quase 6 anos com uso dos serviços e infraestrutura de Data Center da SUTIC/GDF, os quais podemos chamar de uma nuvem computacional governamental, alguns problemas foram relatados, principalmente nos primeiros anos, como adequação de aplicações, ajustes de aplicações quanto a carga de trabalho, indisponibilidade de serviço de Internet, dentre outros, conforme registros na Central de Serviços do CBMDF (centraldeservicos.cbm.df.gov.br). Ainda assim, a

migração do Data Center local do CBMDF para a SETIC/GDF, mostrou-se vantajosa, especialmente devido à redução de gastos com compra de equipamentos de Data Center, como Storage e Servidores.

Entretanto, algumas questões de segurança ainda não são bem tratadas por parte da SETIC/GDF, no que diz respeito às regras de acesso entre redes dos órgãos do GDF e outras, como pode ser verificado nos incidentes de segurança relatados no processo SEI 00053-00078073/2024-21 no documento Relatório Analítico (Distrito Federal, 2024a).

Em julho de 2025, uma reunião entre CBMDF e SETIC/GDF, trouxe à tona pontos importantes sobre a infraestrutura de Tecnologia da Informação do Governo do Distrito Federal. Entretanto, devido à ausência de assinatura da ata de reunião de todos os membros da reunião, o teor dessa reunião não poderá ser colocado nesta pesquisa.

Ainda assim, em maio de 2025, por meio do processo SEI 00053-00049105/2025-62, foi questionado ao chefe da Seção de Redes do CBMDF diversas informações sobre a infraestrutura de data center usada pela Corporação. Neste processo, ficou detalhado informações sobre o armazenamento de dados, onde volume total de dados armazenados pelo CBMDF é de 106.56 terabytes. E que a SERED monitora o servidor de arquivos principal com ferramenta de deduplicação para evitar superlotação, mas o ambiente virtualizado é totalmente controlado pela SETIC/GDF. E que quando um novo disco de armazenamento para uma máquina virtual é solicitado, a SETIC analisa e aprova o pedido. Mas solicitações para discos maiores que 200GB devem ser enviadas por meio do sistema SEI. A SERED não tem conhecimento de um limite máximo de armazenamento disponível para o CBMDF, pois a SETIC gerencia o armazenamento entre os diversos órgãos que compartilham o equipamento (Distrito Federal, 2025f).

A SERED informou ainda que o backup do ambiente virtualizado é feito diariamente, com retenção de 30 dias. Já os discos externos anexados às Máquinas Virtuais têm um backup diário com retenção mínima de 15 dias. O ambiente de produção/crítico do CBMDF está hospedado na SETIC e é acessado através da

GDFnet CLOUD. A SERED não tem acesso à plataforma de software de backup utilizada pela SETIC.

Ainda com informações do processo 00053-00049105/2025-62, solicitou à SETIC/GDF informações atualizadas sobre a infraestrutura de TI que utilizam. Em resposta, a SETIC informou que as máquinas virtuais (VMs) do CBMDF estão em um ambiente de cluster compartilhado da plataforma VMware. Este ambiente usa recursos de alta disponibilidade e balanceamento automático de carga, e que não há servidores físicos dedicados exclusivamente ao CBMDF. Os recursos computacionais são otimizados e compartilhados entre diversas Secretarias. A SETIC esclareceu que não possui informações detalhadas sobre os sistemas e aplicativos em execução nessas VMs, sendo essa uma responsabilidade do próprio CBMDF, que deve manter o controle e inventário dessas aplicações (Distrito Federal, 2025g).

Quanto à solução de software de escritório colaborativo, não foi constatado que a SETIC/GDF possui tal solução para oferecer aos órgãos do GDF. Entretanto, no PDTIC³ da SETIC/GDF para o período de 2023-2026, encontra-se no inventário de necessidade, a N-04 que refere-se ao licenciamento de office 365. Onde ainda neste PDTIC, tem-se o planejamento de aquisição P-09 para o office 365 no valor total de R\$ 300.000,00. Um valor que demonstra ser insuficiente para atender à todos os usuários da Administração Pública do GDF, com base nas informações sobre custo de licenciamento do office 365, do tópico 2.3.2 deste trabalho. Assim, acredita-se que essa N-04 do PDTIC será apenas para uso dos usuários da SETIC/GDF e nenhum outro órgão.

Visto isso, o CBMDF deve adotar uma postura estratégica e cautelosa em relação ao serviço de nuvem governamental da SETIC/GDF. É fundamental que a Corporação realize um planejamento aprofundado para avaliar os riscos e os custos associados a soluções internas e externas. Antes de qualquer decisão, o CBMDF deve buscar garantias claras da SETIC/GDF sobre a capacidade de armazenamento, a eficiência das políticas de backup e a segurança dos dados, a fim de garantir a continuidade e a integridade de seus serviços críticos.

³ <https://www.secti.df.gov.br/documents/d/secti/pdtic-2023-2026-pdf>

2.3.4 Alternativas de nuvem privada para o CBMDF com disponibilidade de várias aplicações

Atualmente várias soluções para aquisição ou implementação de uma nuvem computacional existem. Como já discutido em tópicos anteriores, a Corporação demonstra um baixo orçamento para manter um serviço de nuvem pelos grandes fornecedores, com licença para seus mais de 5 mil militares da ativa. Ainda, verificou-se que a SETIC/GDF demonstra disponibilidade de grande volumes de armazenamento, mas não possui licenças de ferramentas de SaaS, como software de escritório online que possam trabalhar de forma colaborativa como o Microsoft Office 365 ou Google Docs.

Nesse contexto, tem-se alternativas de código aberto (*opensource*) para a implementação de um serviço de nuvem privada. Dentre as opções, como demonstrado no tópico 2.1.5 deste artigo, tem-se Nextcloud, OwnCloud, OpenStack e outras. O Nextcloud foi selecionado por sua facilidade de implementação, segurança e a vasta gama de aplicativos disponíveis.

Para viabilizar a solução, foi solicitado, através do processo SEI 00053-00065729/2025-27 (Distrito Federal, 2025a), permissão e a disponibilização de um servidor na infraestrutura do CBMDF para a instalação do Nextcloud. A implementação foi bem-sucedida, com a instalação e configuração da plataforma. Uma etapa crucial foi a integração do Nextcloud com o serviço de Diretório do CBMDF (o LDAP do MS Active Directory), permitindo que os militares acessem a nuvem privada utilizando suas credenciais de rede corporativa. Após a conclusão das configurações, o serviço foi disponibilizado no endereço “nuvem.cbm.df.gov.br”.

Os testes e o uso prático da solução foram realizados, com foco especial no Nextcloud com suas funcionalidades básicas para um serviço de nuvem, no que diz respeito ao armazenamento e compartilhamento de arquivos, e ao uso de ferramenta de escritório online e colaborativa da plataforma, que no caso foi feito a integração do Onlyoffice com o Nextcloud. O software demonstrou ser capaz de oferecer as funcionalidades essenciais para a edição e o compartilhamento de documentos, planilhas e formulários. A facilidade de compartilhamento de arquivos com múltiplos militares evidenciou a capacidade da solução de atender às

demandas da Corporação de forma segura e econômica, com um conjunto de recursos bastante similar aos oferecidos pelos grandes fornecedores.

Detalhes específicos dos testes de uso e implementação do Nextcloud, assim como integração do Onlyoffice, podem ser verificados no Apêndice A.

3 CONSIDERAÇÕES FINAIS

O estudo identificou a utilização de serviços de nuvem pública gratuita por militares do CBMDF, uma prática que demanda atenção para assegurar a conformidade com a Política de Segurança da Informação e Comunicações (POSIC) do GDF.

Como solução alinhada a essas diretrizes, a implementação de uma nuvem privada baseada no Nextcloud mostrou-se uma alternativa viável e segura. A proposta institucional elimina a necessidade do uso de ferramentas pessoais, centralizando o armazenamento e o compartilhamento de dados em um ambiente controlado.

Reconhece-se que o mercado oferece outras alternativas corporativas, como os pacotes Microsoft 365 e Google Workspace. No entanto, considerando as limitações orçamentárias da Corporação e os custos envolvidos na aquisição dessas soluções comerciais, cabe à instituição avaliar a opção mais adequada ao seu contexto financeiro, de controle e conformidade.

Para consolidar a adoção de qualquer nova solução, são essenciais medidas de capacitação dos usuários, visando facilitar a transição e superar a resistência natural à mudança. Como etapas futuras, recomenda-se a expansão da plataforma para atender toda a corporação, assegurando sua escalabilidade, aliada à definição de políticas robustas de backup e manutenção.

Ao investir em uma infraestrutura tecnológica adequada, o CBMDF fortalece sua segurança digital e avança em direção a uma gestão da informação mais moderna e eficiente.

REFERÊNCIAS

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).** Brasília, DF. 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2025.

CERVO, A. L.; BERVIAN, P. A. **Metodologia científica:** para uso dos estudantes universitários. 5. ed. São Paulo: Prentice Hall, 2002.

CORPO DE BOMBEIROS MILITAR DO DISTRITO FEDERAL. CBMDF. **Relatório de Gestão 2024.** Brasília, DF. 2024. Disponível em: <https://www.cbm.df.gov.br/lai/wp-content/uploads/2025/01/RELATORIO-DE-GESTAO-CBMDF-2024-TCU-VERSAO-7.pdf>. Acesso em: 11 ago. 2025.

CORPO DE BOMBEIROS MILITAR DO DISTRITO FEDERAL. CBMDF. **Relatório de Gestão 2023.** Brasília, DF. 2023. Disponível em: <https://www.cbm.df.gov.br/lai/download/relatorio-de-gestao-2023/?tmstv=1757557462>. Acesso em: 11 ago. 2025.

DISTRITO FEDERAL. Corpo de Bombeiros Militar do Distrito Federal. CBMDF. Diretoria de Tecnologia da Informação e Comunicação (DITIC). **Solicitação de informações - Estudo CAEO - Dados e Infraestrutura de Redes.** Brasília, DF. 2025a. Disponível em: Processo SEI nº 00053-00065729/2025-27, protocolo 174325825.

DISTRITO FEDERAL. Corpo de Bombeiros Militar do Distrito G). **Solicitação de levantamento quanto a geração e armazenamento de dados.** Brasília, DF. 2025b. Disponível em: Processo SEI nº 00053-00054049/2025-88, protocolo 172243337.

DISTRITO FEDERAL. Corpo de Bombeiros Militar do Distrito G). **Solicitação de levantamento quanto a geração e armazenamento de dados.** Brasília, DF. 2025c. Disponível em: Processo SEI nº 00053-00054049/2025-88, protocolo 174180693.

DISTRITO FEDERAL. Corpo de Bombeiros Militar do Distrito G). **Solicitação de levantamento quanto a geração e armazenamento de dados**. Brasília, DF. 2025d. Disponível em: Processo SEI nº 00053-00054049/2025-88, protocolo 174180234.

DISTRITO FEDERAL. Corpo de Bombeiros Militar do Distrito G). **Solicitação de levantamento quanto a geração e armazenamento de dados**. Brasília, DF. 2025e. Disponível em: Processo SEI nº 00053-00054049/2025-88, protocolo 174173695.

DISTRITO FEDERAL. Corpo de Bombeiros Militar do Distrito Federal. CBMDF. Diretoria de Tecnologia da Informação e Comunicação (DITIC). **Informação sobre armazenamento de arquivos - SETIC**. Brasília, DF. 2025f. Disponível em: Processo SEI nº 00053-00049105/2025-62, protocolo 172147859.

DISTRITO FEDERAL. Corpo de Bombeiros Militar do Distrito Federal. CBMDF. Diretoria de Tecnologia da Informação e Comunicação (DITIC). **Informação sobre armazenamento de arquivos - SETIC**. Brasília, DF. 2025g. Disponível em: Processo SEI nº 00053-00049105/2025-62, protocolo 175246690.

DISTRITO FEDERAL. Corpo de Bombeiros Militar do Distrito Federal. CBMDF. Diretoria de Tecnologia da Informação e Comunicação (DITIC). **IRP 08/2022 - SEGES/ME - Licença do Office 365**. Brasília, DF. 2022a. Disponível em: Processo SEI nº 00053-00124560/2022-10, protocolo 109078065.

DISTRITO FEDERAL. Corpo de Bombeiros Militar do Distrito Federal. CBMDF. Diretoria de Tecnologia da Informação e Comunicação (DITIC). **Consulta SUTIC Decreto Nº 40.015**. Brasília, DF. 2019a. Disponível em: Processo SEI nº 00053-00100615/2019-92, protocolo 31687440.

DISTRITO FEDERAL. Corpo de Bombeiros Militar do Distrito Federal. CBMDF. Diretoria de Tecnologia da Informação e Comunicação (DITIC). **Consulta SUTIC Decreto Nº 40.015**. Brasília, DF. 2019c. Disponível em: Processo SEI nº 00053-00100615/2019-92, protocolo 35668190.

DISTRITO FEDERAL. Corpo de Bombeiros Militar do Distrito Federal. CBMDF. Diretoria de Tecnologia da Informação e Comunicação (DITIC). **Medidas para implantação de resposta a incidentes de segurança da informação**. Brasília, DF.

2014. Disponível em: Processo SEI nº 00053-00078073/2024-21, protocolo 138347183.

DISTRITO FEDERAL. Decreto nº 40.015, de 14 de agosto de 2019. **Dispõe sobre a obrigatoriedade de elaboração e publicação dos Planos Diretores de Tecnologia da Informação e Comunicação e sobre a centralização e utilização da rede GDFNet.** Brasília, DF. 2019b. Diário Oficial do Distrito Federal, n. 156, 15 ago. 2019.

DISTRITO FEDERAL. Resolução nº 01, de 29 de abril de 2024. **Aprova a Política de Segurança da Informação e Comunicação (POSIC) do Governo do Distrito Federal.** Brasília, DF. 2024a. Diário Oficial do Distrito Federal, n. 79, 29 abr. 2024.

DISTRITO FEDERAL. Corpo de Bombeiros Militar do Distrito Federal. CBMDF. Diretoria de Tecnologia da Informação e Comunicação (DITIC). **Relatório - PDTIC - 2021-2022 e Cronograma PDTIC 2023-2024.** Brasília, DF. 2022. Disponível em: Processo SEI nº 00053-00193932/2022-40, protocolo 98376655.

DISTRITO FEDERAL. Corpo de Bombeiros Militar do Distrito Federal. CBMDF. Diretoria de Tecnologia da Informação e Comunicação (DITIC). **Relatório de Monitoramento e Avaliação, dos Indicadores, Metas e Ações do PDTIC 2023-2024.** Brasília, DF. 2024b. Disponível em: Processo SEI nº 00053-00196475/2024-15, protocolo 158313614.

GERHARDT, T. E.; SILVEIRA, D. T. **Métodos de pesquisa.** Porto Alegre: Editora da UFRGS, 2009.

GIL, A. C. **Como Elaborar Projetos de Pesquisa.** 7. ed. São Paulo: Atlas, 2022.

GOOGLE. **Usar o Gmail para acessar sua Conta do Google.** 2025. Disponível em: <https://support.google.com/accounts/answer/76194?hl=en>. Acesso em: 14 jul. 2025.

JEWARGI, K. **Public Cloud to Cloud Repatriation Trend.** *Scholars Journal of Engineering and Technology*, v. 11, n. 1, p. 1-3, 2023.

KRAZIT, T. **Dropbox saved almost \$75 million in two years by building its own tech infrastructure.** GeekWire. 23 fev. 2018. Disponível em:

<https://www.geekwire.com/2018/dropbox-saved-almost-75-million-two-years-building-tech-infrastructure/>. Acesso em: 14 jul. 2025.

KUROSE, James F.; ROSS, Keith W. **Redes de Computadores: Uma Abordagem Top-Down**. 8. ed. Tradução de Daniel Vieira. São Paulo: Pearson Education do Brasil, 2020.

MACSON, J. M. M. de A. **Utilização de Serviços em Nuvem por Instituições Militares**. Rio de Janeiro, 2023. Trabalho Acadêmico (Ensaio Acadêmico) – Escola Superior de Guerra (ESG), Rio de Janeiro, 2023.

MARCONI, M. DE A.; LAKATOS, E. M. **Fundamentos de metodologia científica**. 7. ed. São Paulo: Atlas, 2010.

MELL, Peter; GRANCE, Timothy. **The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology**. Special Publication 800-145. Estados Unidos: NIST, 2011.

MICROSOFT. **Visão geral do Active Directory Domain Services**. Microsoft Learn. Disponível em: <https://learn.microsoft.com/pt-br/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>. Acesso em: 13 jun. 2025.

NEXTCLOUD. **Nextcloud latest user manual introduction**. 2025. Disponível em: https://docs.nextcloud.com/server/latest/user_manual/en/. Acesso em: 12 maio 2025.

NIELSEN, Jakob. **10 Heuristics for User Interface Design**. Milpitas, CA: Nielsen Norman Group, 1994. Disponível em: <https://www.nngroup.com/articles/ten-usability-heuristics/>. Acesso em: 9 ago. 2025.

OPENSTACK. **Welcome to OpenStack Documentation**. 2025. Disponível em: <https://docs.openstack.org/2025.1/>. Acesso em: 14 mai. 2025.

OWNCLOUD. **ownCloud Architectural Guide**. 2025. Disponível em: https://oc.owncloud.com/rs/038-KRL-592/images/Whitepaper_Architectural_Guide_EN.pdf. Acesso em: 12 mai. 2025.

RÄISÄNEN, I. **Cloud Repatriation: factors and strategies for successfully and beneficially leaving the public cloud**. 2025.

RED HAT. **O que é Open Source?** Red Hat. Disponível em: <https://www.redhat.com/pt-br/topics/open-source/what-is-open-source>. Acesso em: 21 jun. 2025.

SIDDIQUI, Laiba. **Data Monitoring: Benefits, Best Practices, and Automation Opportunities.** Disponível em: https://www.splunk.com/en_us/blog/learn/data-monitoring.html. Acesso em: 10 jun. 2025.

STRACK, Anderson. **Desafios e Melhores Práticas para a Proteção de Dados em Ambientes de Armazenamento em Nuvem Privada.** Frederico Westphalen, RS, 2024. Monografia (Especialização em Gestão de Tecnologia da Informação) – Universidade Federal de Santa Maria, Frederico Westphalen, RS, 2024.

SUBASHINI, A.; KAVITHA, V. **A survey on security issues in service delivery models of cloud computing.** Journal of Network and Computer Applications, v. 34, n. 1, p. 1-11, 2011.

TARGETT, E. Warren Buffett's Geico repatriates work from the cloud, continues ambitious infrastructure overhaul. **The Stack.** 17 out. 2024. Disponível em: https://www-thestack-technology.translate.google.com/warren-buffetts-geico-repatriates-work-from-the-cloud-continues-ambitious-infrastructure-overhaul/?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt&_x_tr_pto=tc. Acesso em: 14 jul. 2025.

APÊNDICE A

Nextcloud

A instalação do Nextcloud na rede interna da Corporação foi autorizada por meio do processo SEI 00053-00065729/2025-27 (Distrito Federal, 2025a).

O Nextcloud foi implementado em uma máquina virtual, numa infraestrutura de rede com solução de virtualização da VMware⁴, com a seguinte configuração de hardware:

vCPU: 4

RAM: 32 GB

Armazenamento: 150 GB

A máquina virtual recebeu o nome “nuvem” e o endereço FQDN⁵ `nuvem.cbm.df.gov.br`.

A instalação foi realizada utilizando a ferramenta *Snap*, que simplifica a implementação, garantindo os componentes essenciais para um funcionamento adequado. Por ser uma demonstração inicial, o foco principal foi a funcionalidade, sem ajustes personalizados para otimização de performance.

Diversas configurações e ajustes foram realizados no Nextcloud para viabilizar esta pesquisa. Embora o detalhamento de todos os procedimentos esteja fora do escopo deste trabalho, é crucial destacar a integração do Nextcloud com o *Active Directory* Corporativo. Essa configuração, devidamente autorizada, permitiu o acesso à base de dados de usuários e grupos da Corporação, o que foi um requisito essencial para os testes de funcionalidade que serão apresentados.

⁴ <https://www.vmware.com/solutions/app-platform>

⁵ FQDN significa "**Fully Qualified Domain Name**" (ou Nome de Domínio Totalmente Qualificado). É o nome completo e absoluto de um computador ou dispositivo em uma rede, que não deixa nenhuma dúvida sobre a sua localização exata. Ele inclui o nome do host (no caso, `nuvem`) e o nome do domínio ao qual ele pertence (no caso, `cbm.df.gov.br`).

Essa configuração, devidamente autorizada, permitiu o acesso à base de dados de usuários e grupos da Corporação, o que foi um requisito essencial para os testes de funcionalidade que serão apresentados..

Onlyoffice

A ferramenta de escritório Onlyoffice, na rede interna da Corporação também foi autorizada por meio do processo SEI 00053-00065729/2025-27 (Distrito Federal, 2025a) e implementado em uma máquina virtual, numa infraestrutura de rede com solução de virtualização da VMware, com a seguinte configuração de hardware:

vCPU: 4

RAM: 32 GB

Armazenamento: 150 GB

A máquina virtual recebeu o nome “office” e o endereço FQDN office.cbm.df.gov.br.

A instalação do Onlyoffice foi realizada de forma manual e personalizada, por meio de repositórios oficiais da solução. Essa instalação manual foi necessária para garantir algumas funcionalidades e configurações que apresentaram erros quando do uso da instalação com *Snap*.

Após a instalação do Onlyoffice, foi realizado a devida configuração de integração com a ferramenta Nextcloud, permitindo assim que os documentos criados no Nextcloud fizessem uso de toda solução do Onlyoffice.

Critérios de testes quanto às funcionalidades da solução Nextcloud

1. A solução possui um gerenciador de arquivos para criar, compartilhar e sincronizar arquivos?
2. A solução possui alguma ferramenta de chat, videoconferência?

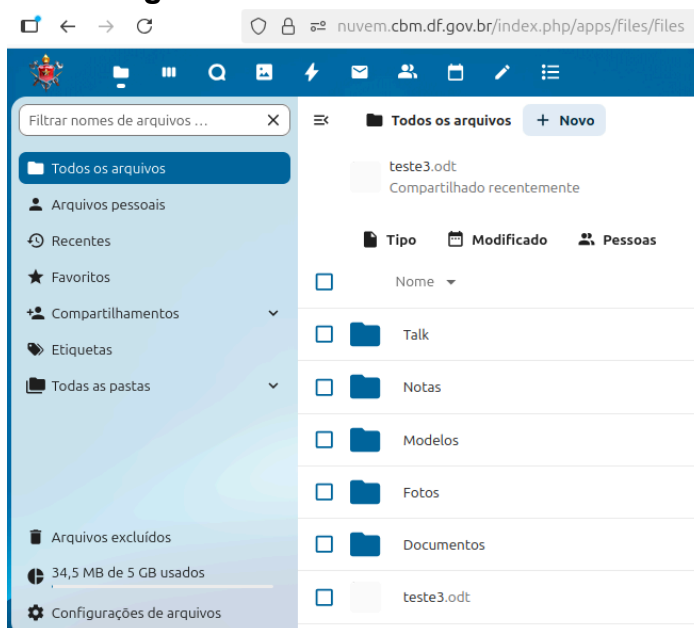
3. A solução possui ferramentas de calendário, contatos e e-mail?
4. A solução possui ferramentas de escritório, como documentos, planilhas, apresentações, criação de formulários e outras?
5. A solução permite atividades de modo colaborativo, ao menos com ferramentas de escritório?
6. A solução possui recursos de Inteligência Artificial - IA e outros?

Para cada critério citado acima, foi constatado que a solução atende à todos os critérios, conforme demonstrado abaixo:

1. A solução possui um gerenciador de arquivos para criar, compartilhar e sincronizar arquivos?

Para este critério, verificou que a solução possui a ferramenta “Nextcloud Files”, similar por exemplo as soluções do Dropbox ou Google Drive, que permite gerenciar todos os arquivos armazenados na conta do usuário, conforme Figura 4.

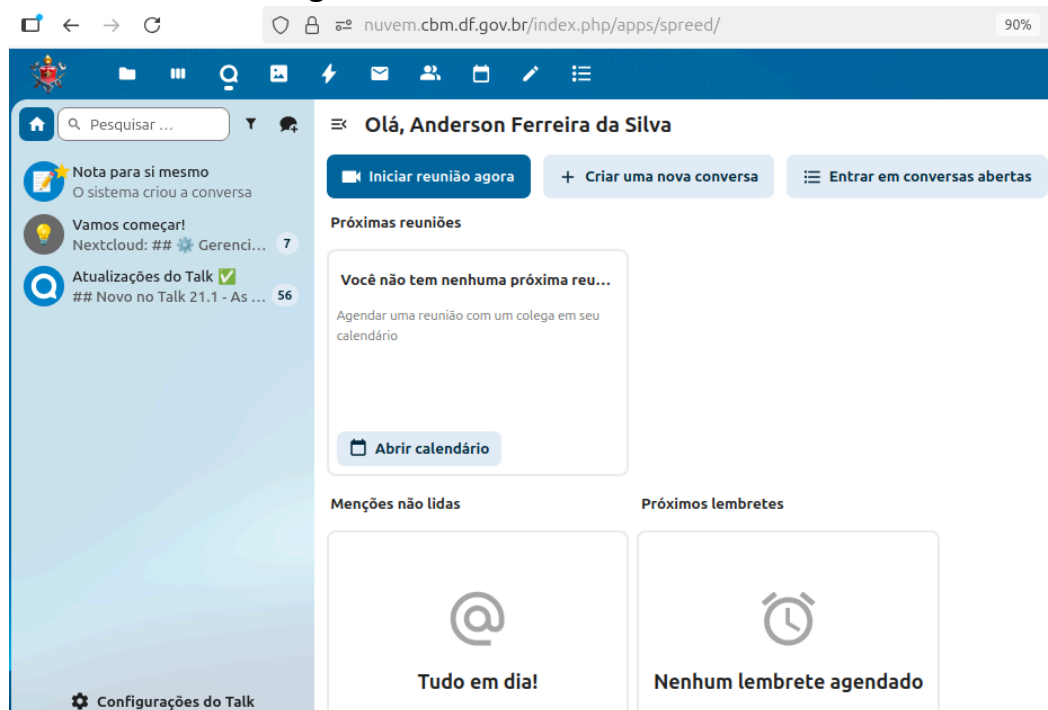
Figura 4 - Interface do Nextcloud Files



2. A solução possui alguma ferramenta de chat, videoconferência?

A solução possui a ferramenta Nextcloud Talk, própria para chat e videoconferência, como um similar das soluções de mercado Zoom ou Teams.

Figura 5 - Interface do Nextcloud Talk

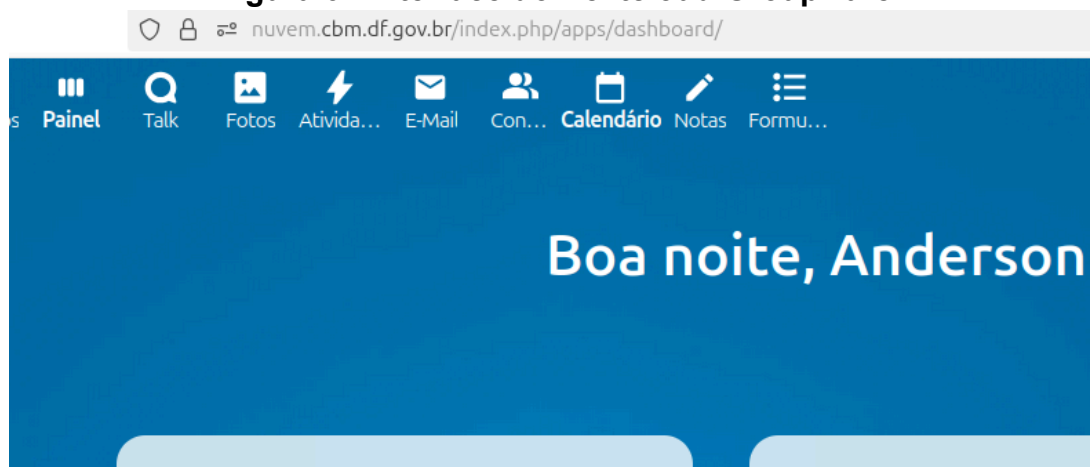


3. A solução possui ferramentas de calendário, contatos e e-mail?

A solução possui a ferramenta Nextcloud Groupware, Calendário, contatos e e-mail integrados, similar as ferramentas básicas encontradas em solução do Google Workspace.

Pode-se verificar que essas ferramentas estão disponíveis no topo da página principal do Nextcloud Groupware, conforme Figura 6 abaixo.

Figura 6 - Interface do Nextcloud Groupware



4. A solução possui ferramentas de escritório, como documentos, planilhas, apresentações, criação de formulários e outras?

O Nextcloud oferece sua própria suíte de escritório, o Nextcloud Office. No entanto, devido a algumas de suas limitações, optou-se pela integração com o Onlyoffice.

Com essa integração, as ferramentas do Onlyoffice garantem todas as funcionalidades encontradas nas principais soluções de escritório em nuvem do mercado, como Google Docs e Microsoft 365. Para provar a potência da plataforma, o Onlyoffice disponibiliza testes de comparação em seu próprio site, para que os usuários possam verificar as vantagens e o potencial da ferramenta.

Foi verificado esses testes e comparações diretamente no link: <https://www.onlyoffice.com/pt/document-editor-comparison.aspx>. Confirmando que de fato Onlyoffice mostra-se como solução ideal para ferramentas de escritório, com todos os recursos encontrados nas diversas ferramentas de mercado e principalmente possibilidade o desenvolvimento e atividades de forma colaborativa.

Figura 7 - Interface do Nextcloud Files com várias opções de criação de documentos

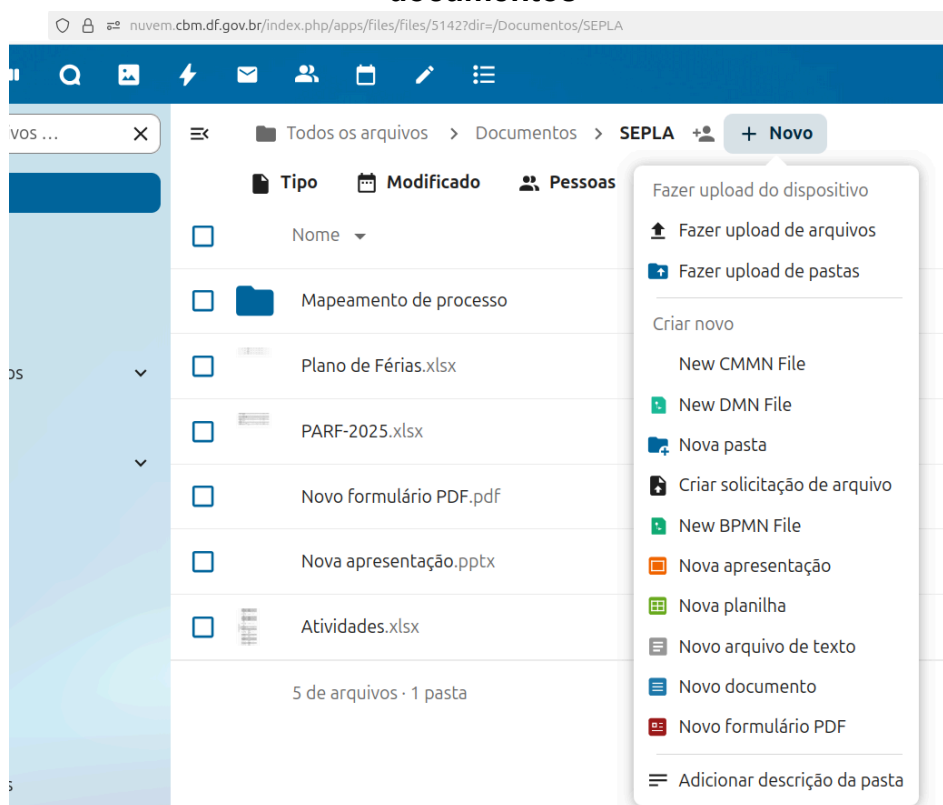
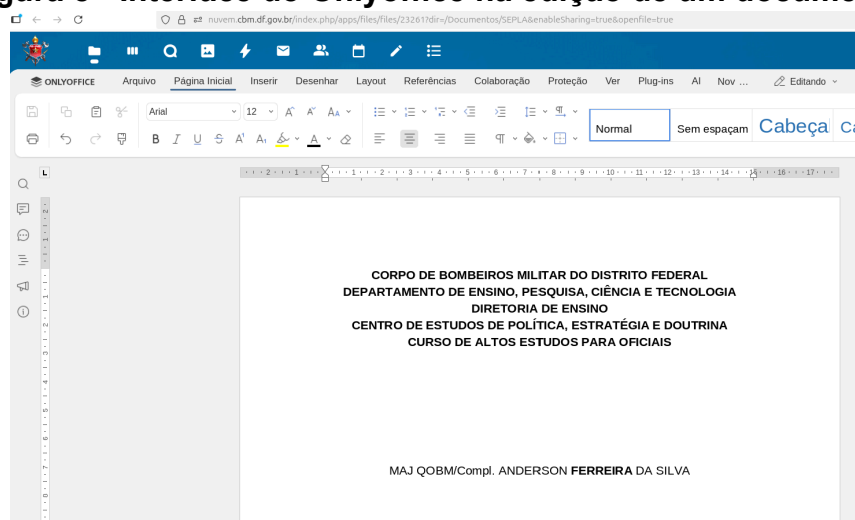


Figura 8 - Interface do Onlyoffice na edição de um documento

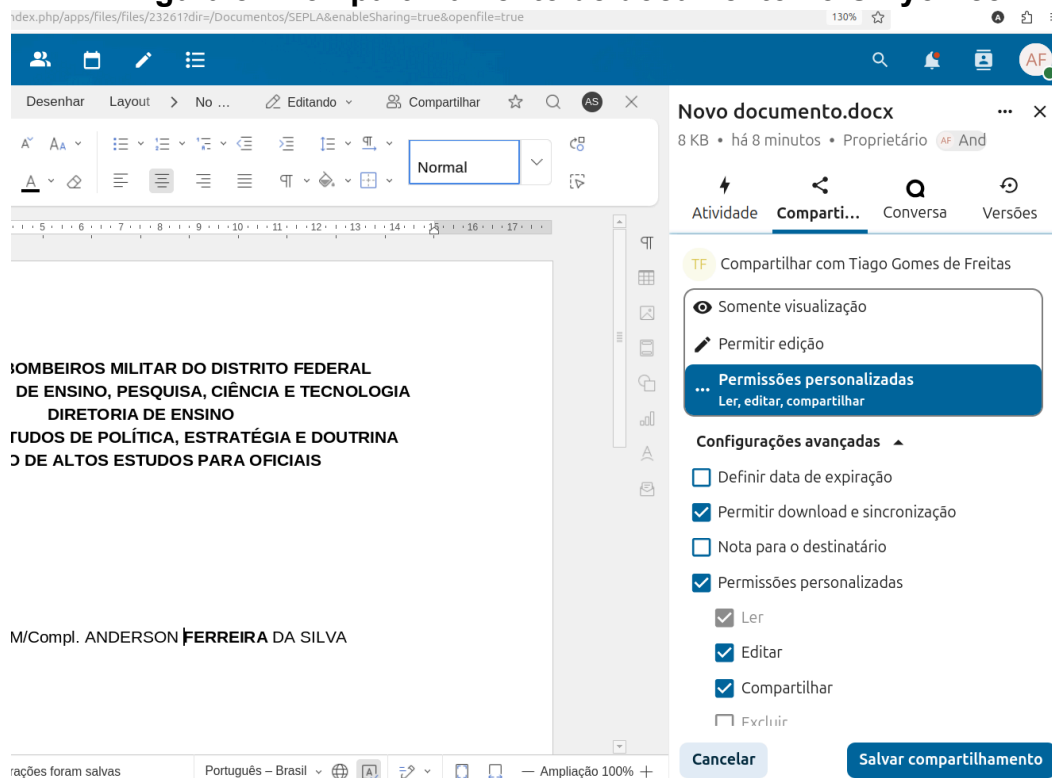


5. A solução permite atividades de modo colaborativo, ao menos com ferramentas de escritório?

A ferramenta Onlyoffice integrada ao Nextcloud possui diversas opções para compartilhar os documentos e permitir a construção do documento de forma colaborativa, no modo como acontece nas diversas ferramentas do mercado, como Google Docs e Microsoft 365.

A Figura 8 abaixo mostra as opções de compartilhamento do documento no Onlyoffice para que possa trabalhado com vários outros usuários.

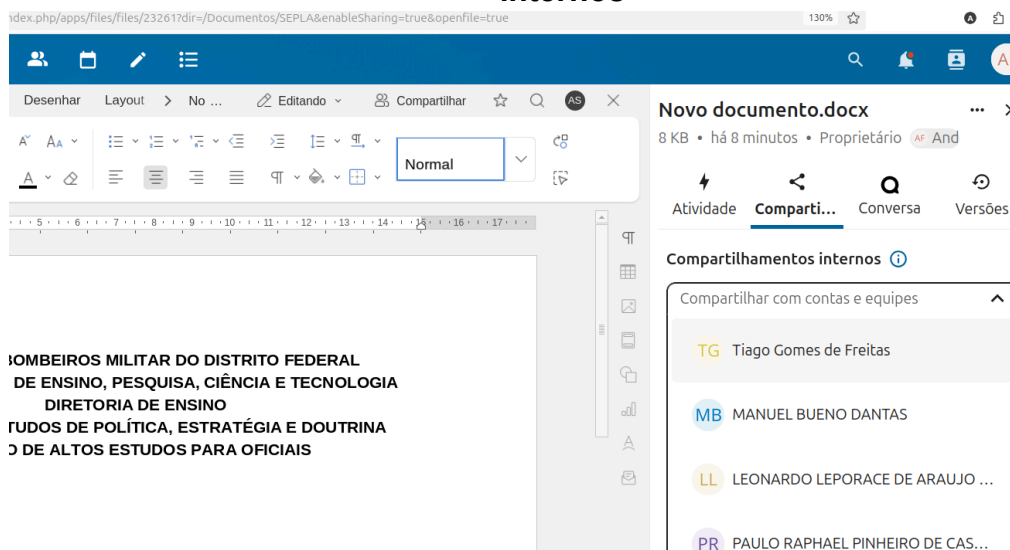
Figura 8 - Compartilhamento de documento no Onlyoffice



Este endereço “<https://nuvem.cbm.df.gov.br/index.php/s/Z9k5Aafdof7CMLx>” trata-se do formato de um link de documento que pode ser disponibilizado para outro usuário acessar determinado documento do Onlyoffice e trabalhar colaborativamente.

A Figura 9 mostra o compartilhamento de documento listando usuários da base do CBMDF do ambiente Active Directory. Todos os militares desta Figura são da SEPLA/DITIC e visualizados automaticamente, sem necessidade de cadastro de usuário na plataforma Nextcloud, apenas da configuração de integração com o AD Corporativo.

Figura 9 - Compartilhamento de documento no Onlyoffice com usuários internos



Ao compartilhar um documento para trabalho colaborativo, o Nextcloud também envia email para o usuário, informando sobre arquivo compartilhado, conforme Figura 10. Este endereço de email do usuário também faz parte das informações que estão cadastradas no AD Corporativo.

Figura 10 - Aviso por email de compartilhamento de documento pelo Nextcloud

Anderson Ferreira compartilhou teste3.odt com você



Anderson Ferreira via Nextcloud <nuvem@cbm.df.gov.br>

Responder a todos | v

dom 20/07, 23:57

Anderson Ferreira da Silva v



Anderson Ferreira compartilhou teste3.odt com você

Abrir teste3.odt

6. A solução possui recursos de Inteligência Artificial - IA e outros?

A solução Nextcloud possui um ecossistema de aplicativos, com variedade grande de aplicativos que podem ser instalados e/ou integrados para expandir as funcionalidades, desde recursos para criação de mapeamento de processos, como ferramentas BPM, leitores de RSS, gerenciadores de senhas até aplicações com mapas.

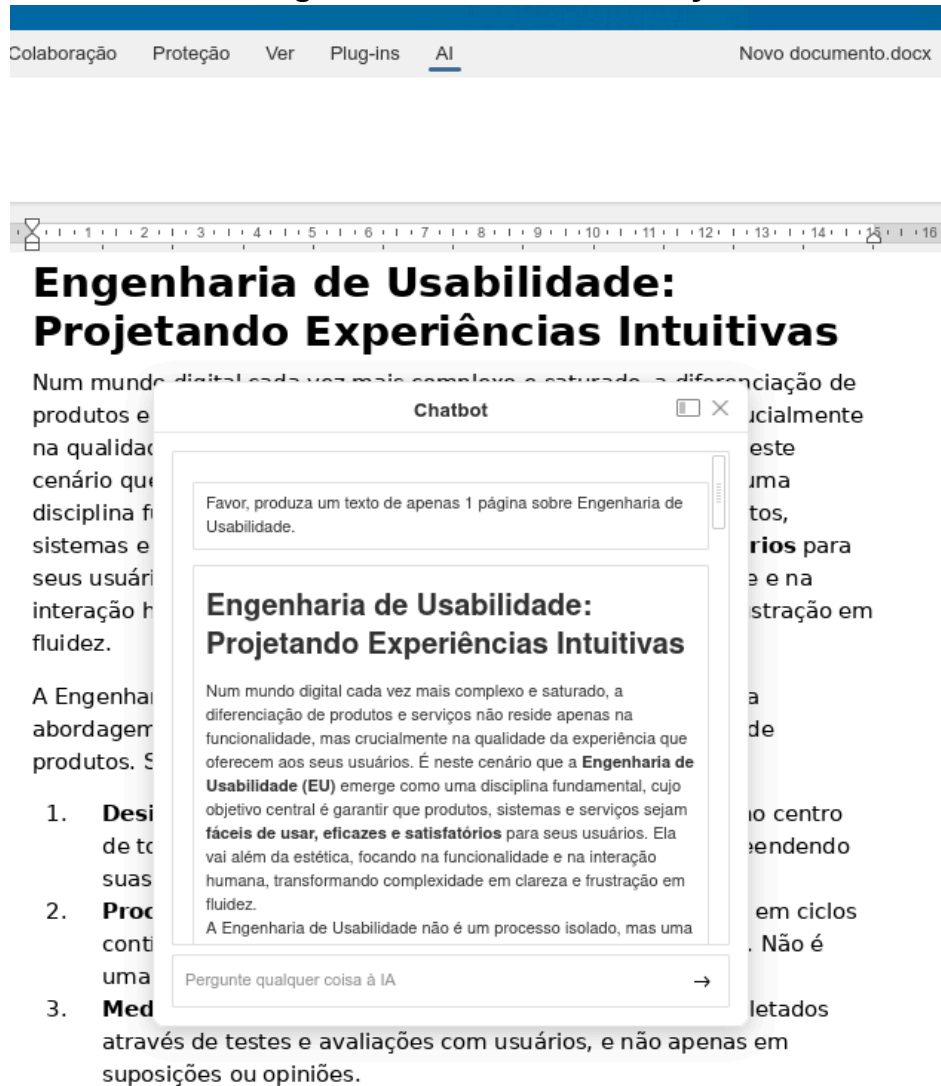
A partir da versão 9.0 Onlyoffice introduziu recentemente uma atualização significativa em seu Recursos de IA, tornando o trabalho mais inteligente. Os usuários agora têm a flexibilidade de conectar qualquer assistente de IA, seja OpenAI, Together AI, Mistral, Anthropic, Groq, Google Gemini, DeepSeek, Ollama, xAI ou até mesmo soluções locais.⁶

A Figura 11, mostra a configuração de ferramentas de IA que realizei no Onlyoffice deste trabalho.

6

<https://www.onlyoffice.com/blog/pt-br/2025/01/principais-ferramentas-de-ia-para-suites-do-office>

Figura 11 - Uso de IA no Onlyoffice



Segue abaixo o comparativo do Onlyoffice com Nextcloud em relação ao Google Docs, com base nas 10 heurísticas de Jakob Nielsen (ou princípios de usabilidade) (Nielsen, 1994) na área de conhecimento da Engenharia de Usabilidade.

1. Visibilidade do Status do Sistema

Google Docs: Mostra claramente se o documento está salvo, quem está editando e onde o cursor de cada pessoa está.

OnlyOffice: Faz o mesmo, com ícones e indicadores claros de salvamento e colaboração. A experiência do usuário nesse quesito é, no mínimo, equivalente.

2. Correspondência entre o Sistema e o Mundo Real

Google Docs: Usa ícones e menus que remetem a conceitos conhecidos de documentos (impressora, pincel, etc.).

OnlyOffice: Vai além, com uma interface que se assemelha muito ao Microsoft Office, que é o padrão de mercado. Isso cria uma correspondência ainda mais forte com o mundo real para a maioria dos usuários, pois eles já têm uma familiaridade prévia.

3. Controle e Liberdade do Usuário

Google Docs: Permite desfazer e refazer ações facilmente.

OnlyOffice: Oferece o mesmo nível de controle. A estrutura de menus e ícones é tão similar à de ferramentas de mercado que a curva de aprendizado para ações básicas é praticamente nula.

4. Consistência e Padrões

Google Docs: Mantém consistência em sua interface.

OnlyOffice: Essa é a grande vantagem do OnlyOffice. Ele adota um padrão de interface (*ribbon*) que é amplamente reconhecido. Demonstra que o OnlyOffice seguiu os padrões que os usuários conhecem em se tratando de softwares de escritório, minimizando a necessidade de um novo aprendizado.

5. Prevenção de Erros

Google Docs: Avisa sobre potenciais perdas de dados e outros erros.

OnlyOffice: Também possui mecanismos de prevenção de erros, como salvamento automático. A similaridade com ferramentas conhecidas reduz a probabilidade de erros de uso.

6. Reconhecimento em vez de Recordação

Google Docs: Os menus e ícones são visíveis, não exigindo que o usuário memorize comandos.

OnlyOffice: Ele é "reconhecível" instantaneamente para quem já usou o Microsoft Office (ex.: Figura 8). O usuário não precisa "recordar" onde estão as funções, pois elas estão onde ele já espera que estejam.

7. Flexibilidade e Eficiência de Uso

Google Docs: É eficiente para usuários que já o dominam, mas a falta de atalhos e funções mais avançadas (em comparação com o MS Office, por exemplo) pode limitar a eficiência de usuários experientes.

OnlyOffice: Oferece uma ampla gama de atalhos de teclado e recursos avançados, como macros e ferramentas de edição de imagens mais robustas. Sua interface, que se assemelha a ferramentas conhecidas, permite que tanto o usuário novato quanto o experiente encontrem o que precisam rapidamente. Isso permite que a ferramenta se adapte a diferentes níveis de habilidade, o que a torna mais flexível e eficiente.

8. Estética e Design Minimalista

Google Docs: Adota um design limpo e minimalista, o que facilita o foco na tarefa.

OnlyOffice: Segue a mesma linha, mantendo a interface visualmente "limpa" mesmo com a barra de ferramentas completa (*ribbon*). Ele evita a poluição visual, apresentando apenas os elementos essenciais para a tarefa atual. O fato de o design ser familiar e não ter elementos supérfluos, como pop-ups de publicidade, faz com que a experiência seja agradável e focada, assim como no Google Docs.

9. Ajuda e Documentação

Google Docs: Possui uma ajuda robusta e integrada, facilmente acessível através do menu.

OnlyOffice: Oferece documentação e tutoriais detalhados, que auxiliam o usuário a aprender e resolver problemas. A comunidade de usuários também contribui com material de ajuda, e a semelhança da interface com outras ferramentas de mercado muitas vezes elimina a necessidade de procurar ajuda para tarefas básicas, pois o usuário já sabe como fazer.

10. Reconhecimento, Diagnóstico e Recuperação de Erros

Google Docs: Apresenta mensagens de erro claras e construtivas. Por exemplo, se a internet cair, ele avisa que está "tentando se reconectar".

OnlyOffice: Se destaca por ter mensagens de erro igualmente claras. Além disso, a ferramenta oferece um histórico de versões e um mecanismo de recuperação de arquivos que permite ao usuário voltar a uma versão anterior do documento, o que minimiza a frustração em caso de perda de dados.

APÊNDICE B

Na Tabela 3 abaixo, segue o cálculo do valor médio das despesas de custeio e investimento do CBMDF para os anos de 2024 e 2023, considerando os Relatórios de Gestão.

Tabela 3 - Valores de custeio e investimento no CBMDF dos anos de 2023 a 2024

| Tipo de despesa | 2024 | 2023 | Valor Médio |
|-----------------|---|--|--------------------------|
| | (Corpo de Bombeiros Militar do Distrito Federal, 2024, p. 55) (Corpo de Bombeiros Militar do Distrito Federal, 2024, p. 57)) | (Corpo de Bombeiros Militar do Distrito Federal, 2023, p. 52) (Corpo de Bombeiros Militar do Distrito Federal, 2023, p. 53) | |
| Custeio | R\$ 52.646.232,73 | R\$ 51.351.080,82 | R\$ 51.998.656,77 |
| Investimento | R\$ 13.519.390,13 | R\$ 21.609.313,25 | R\$ 17.564.351,69 |