aurum
Revista Multidisciplinar

ISSN: 3085-7783

IMPACTOS DE SISTEMAS LEGADOS EM ÓRGÃOS PÚBLICOS: ANÁLISE E PROPOSTA DE MODERNIZAÇÃO

IMPACTS OF LEGACY SYSTEMS IN PUBLIC AGENCIES: ANALYSIS AND MODERNIZATION PROPOSAL

https://doi.org/10.63330/armv1n10-003

Submetido em: 08/12/2025 e Publicado em: 12/12/2025

Carlos Henrique da Gama Marques
Graduando em Engenharia da Computação
Uninorte – Centro Universitário do Norte
E-mail: carlos.marques26@outlook.com

Klaiver Ferreira Araújo
Graduando em Engenharia da Computação
Uninorte – Centro Universitário do Norte
E-mail: klaiverlal@gmail.com

Euler de Azevedo Costa
Pós-graduação em Cloud Computing, Professor Orientador
Uninorte – Centro Universitário do Norte, XP Educação
LATTES: http://lattes.cnpq.br/6931883098604250

Roneuane Grazielle da Gama Araujo
Pós-graduação em Engenharia e Administração de Sistemas de Banco de Dados, Professor Orientador
Uninorte – Centro Universitário do Norte, Universidade Estatual de Campinas
LATTES: http://lattes.cnpq.br/0820708416379517

RESUMO
Com o crescente avanço da tecnologia da informação, surgem métodos mais eficientes para o gerenciamento centralizado de infraestrutura de TI e de dados, desde infraestruturas “on-premise" às plataformas em nuvem. O avanço da tecnologia da informação exige que a administração pública modernize sua infraestrutura para garantir eficiência, segurança e conformidade. No entanto, muitos órgãos ainda dependem de sistemas legados que limitam seu potencial e introduzem riscos significativos. Este trabalho tem como objetivo analisar os impactos de um servidor legado em uma repartição pública, avaliando seu desempenho, segurança e efeitos sobre os usuários, além de propor uma solução de modernização viável. O estudo de caso aborda a incompatibilidade entre um servidor Debian 7 “Wheezy” com Samba 3.6.6 e estações de trabalho Windows 11, demonstrando a necessidade de degradar deliberadamente protocolos de segurança para manter a funcionalidade. As métricas técnicas e a percepção dos usuários destacam como a obsolescência tecnológica prejudica a produtividade e expõe a instituição a riscos, justificando a urgência da migração para sistemas modernos.

Palavras-chave: Sistemas legados; Infraestrutura de TI; Segurança da informação.

ABSTRACT
With the growing advancement of information technology, more efficient methods for the centralized management of IT infrastructure and data are emerging, from on-premise infrastructures to cloud platforms. The progress in information technology requires public administration to modernize its infrastructure to ensure efficiency, security, and compliance. However, many agencies still rely on legacy systems that limit their potential and introduce significant risks. This paper aims to analyze the impacts of a legacy server in a public agency by evaluating its performance, security, and effects on users, as well as proposing a viable modernization solution. The case study addresses the incompatibility between a Debian 7 “Wheezy” server running Samba 3.6.6 and Windows 11 workstations, demonstrating the need to deliberately downgrade security protocols to maintain functionality. Technical metrics and user perception highlight how technological obsolescence impairs productivity and exposes the institution to risks, justifying the urgency of migrating to modern systems.

Keywords: Legacy systems; IT infrastructure; Information security.

1 INTRODUÇÃO

1.1 APRESENTAÇÃO DO TEMA

A administração pública brasileira opera em uma realidade paradoxal: enquanto a legislação contemporânea — em particular a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, a Instrução Normativa IN 04/2023 da Secretaria de Governo Digital, e as exigências de conformidade com frameworks internacionais como o NIST Cybersecurity Framework e a ISO/IEC 27001 — exige rigor na proteção de dados e segurança cibernética, muitos órgãos governamentais permanecem presos a infraestruturas tecnológicas obsoletas, incapazes de suportar esses requisitos.

Os sistemas legados não são meramente "antigos"; são infraestruturas que ultrapassaram seu ciclo de vida útil, chegaram ao status de End-of-Life (EOL). Segundo Sommerville (2011), sistemas legados são sistemas socio-técnicos que continuam a prestar serviços essenciais, mas cuja manutenção se torna progressivamente mais custosa e arriscada devido à obsolescência do hardware e do software de suporte. Portanto, acumulam débito técnico estrutural. Este débito manifesta-se em múltiplas dimensões: vulnerabilidades de segurança não remediáveis, ineficiência operacional, incompatibilidade com tecnologias modernas e dificuldade de atender a regulamentações contemporâneas.

No contexto específico deste estudo, a manutenção de um ambiente legado em uma repartição pública — baseado em um servidor Debian 7 "Wheezy" com Samba 3.6.6 — exemplifica essa condição crítica. O Debian 7, lançado em 2013, teve seu suporte encerrado em maio de 2018. O Samba 3.6.6, por sua vez, nunca foi pensado para interoperar com sistemas operacionais tão modernos quanto o Windows 11, lançado em 2021. A tentativa de manter a compatibilidade entre estas arquiteturas distantes obriga à degradação deliberada da segurança, criando um cenário onde o próprio funcionamento diário da instituição se torna um risco de compliance.

1.2 DELIMITAÇÃO DO PROBLEMA DE PESQUISA

O presente trabalho investiga os impactos de uma infraestrutura legada específica em uma repartição pública, focalizando três dimensões analíticas: técnica, de governança e de experiência do usuário.

Dimensão Técnica: Como um servidor Debian 7 com Samba 3.6.6, em modelo de Controlador de Domínio Primário (PDC) NT4, consegue interoperar com estações Windows 11? Quais protocolos de segurança devem ser deliberadamente desativados para viabilizar essa compatibilidade? Qual é a superfície de ataque resultante?

Dimensão de Governança: Como essa infraestrutura se posiciona face aos requisitos do NIST Cybersecurity Framework 2.0 e da ABNT NBR ISO/IEC 27001:2022? Em que medida a manutenção desse ambiente representa riscos de não-conformidade com a LGPD?

Dimensão de Usabilidade e Produtividade: Qual é o impacto operacional real? Como os servidores públicos percebem e vivenciam a obsolescência? Quais métricas de eficácia, eficiência e satisfação de usuário (conforme ISO 9241-11) podem ser mensuradas?

O problema central é que a manutenção dessa infraestrutura legada, frequentemente justificada por inércia operacional ou restrições orçamentárias, cria custos ocultos que prejudicam a produtividade e expõem a instituição a riscos inaceitáveis de segurança e compliance.

1.3 OBJETIVOS

1.3.1 Objetivo geral

Analisar os impactos técnicos, de segurança, de governança e de produtividade de um servidor legado Debian 7 com Samba 3.6.6 em uma repartição pública, e propor uma solução de modernização de infraestrutura viável, economicamente sustentável e alinhada aos frameworks de governança de TI contemporâneos (NIST CSF 2.0 e ABNT NBR ISO/IEC 27001).

1.3.2 Objetivos específicos

- Realizar diagnóstico técnico detalhado da infraestrutura legada, documentando as configurações de degradação de segurança necessárias para manter a interoperabilidade entre o servidor Debian 7 (Samba 3.6.6) e estações Windows 11, identificando especificamente os protocolos e serviços desativados.
- Analisar as lacunas de segurança e governança da infraestrutura atual à luz dos frameworks NIST Cybersecurity Framework 2.0 e ABNT NBR ISO/IEC 27001:2022, mapeando violações de controles específicos.
- Mensurar o impacto da infraestrutura obsoleta na produtividade e experiência dos servidores públicos, utilizando como base os pilares da usabilidade (eficácia, eficiência e satisfação) da norma ABNT NBR ISO 9241-11.
- Identificar as causas raiz dos gargalos de desempenho diagnosticados, incluindo análise de protocolos de autenticação e suas implicações para o sistema operacional cliente.
- Propor e validar um plano de migração para uma solução moderna de Controlador de Domínio (baseado em Univention Corporate Server), que resolva simultaneamente os problemas técnicos, de segurança, de governança e de usabilidade identificados.

1.4 JUSTIFICATIVA

A relevância científica e prática deste trabalho repousa em múltiplos pilares:

Relevância Regulatória: A Lei Geral de Proteção de Dados (Brasil, Lei nº 13.709/2018) impõe sanções severas em caso de violação de segurança de dados. A manutenção de um sistema sem suporte de segurança (EOL) e com protocolos notoriamente inseguros representa risco direto de não-conformidade regulatória e exposição a sanções administrativas.

Relevância Técnica: A análise da incompatibilidade entre gerações tecnológicas oferece oportunidade para investigar como sistemas modernos (Windows 11) tratam a herança de protocolos legados, contribuindo ao entendimento dos mecanismos de autenticação e segurança em ambientes heterogêneos.

Relevância Prática: O estudo fornece subsídios quantitativos e técnicos para gestores públicos avaliarem o impacto real de sistemas legados, traduzindo questões técnicas abstratas em métricas concretas de produtividade e experiência do usuário, facilitando a justificativa para investimento em modernização.

Relevância Econômica: Demonstrar que o custo oculto da obsolescência tecnológica — em perda de produtividade, retrabalho, e risco regulatório — justifica que investimentos em modernização é essencial em contextos de restrição orçamentária, como é comum na administração pública. A proposta de solução utiliza software com licenciamento gratuito (UCS Core Edition), demonstrando viabilidade econômica.

Relevância de Governança: A pesquisa articula os princípios de governança corporativa (função "Governar" do NIST CSF 2.0) com a realidade operacional, mostrando como a ausência de modernização representa uma falha de supervisão estratégica.

1.5 REVISÃO TEÓRICA

Este estudo se fundamenta na intersecção de três áreas principais: os padrões de governança e segurança (NIST e ISO 27001), a mensuração da experiência do usuário (ISO 9241-11) e a arquitetura de serviços de diretório e autenticação. Esta seção apresenta os conceitos teóricos que sustentam o diagnóstico e a solução proposta.

1.5.1 Governança de TI e gestão de risco em segurança da informação

A modernização de infraestruturas legadas é uma exigência não apenas técnica, mas de governança corporativa. A ABNT NBR ISO/IEC 27001:2022 — norma brasileira que implementa o padrão internacional ISO/IEC 27001 — estabelece na Seção 5 que a "Alta Direção" deve demonstrar "liderança e comprometimento" com o sistema de gestão da segurança da informação, assegurando a "integração dos requisitos do sistema de gestão da segurança da informação nos processos da organização" (ABNT, 2022,

p. 15). Isto significa que decisões sobre manutenção ou modernização de infraestrutura não são questões meramente operacionais de TI, mas responsabilidades estratégicas da administração.

Este princípio é complementado e aprofundado pelo NIST Cybersecurity Framework (CSF) 2.0, lançado em fevereiro de 2024. O CSF 2.0 introduz como pilar central a função "Governar" (GV), que estabelece a "supervisão organizacional, liderança ativa e políticas, planos e processos implementados para permitir uma abordagem coerente à gestão de riscos de cibersegurança em toda a organização" (NIST, 2024, p. 8). Especificamente, a subcategoria GV.PO-04 exige que as organizações "determinem e comuniquem as expectativas de desempenho de cibersegurança para todos os componentes da organização" (NIST, 2024, p. 34). A manutenção de um servidor EOL que compromete a postura de segurança de toda a instituição viola diretamente este princípio.

1.5.2 Mensuração de usabilidade: Eficiência, eficácia e satisfação

Para avaliar o impacto de um sistema legado na experiência e produtividade do usuário final, este estudo utiliza a norma ABNT NBR ISO 9241-11:2018, que define usabilidade como "o grau em que um produto pode ser usado por usuários específicos para atingir objetivos específicos com eficácia, eficiência e satisfação em um contexto de uso específico" (ABNT, 2018, p. 3).

A norma operacionaliza a usabilidade através de três componentes mensuráveis:

- Eficácia: O grau em que os usuários conseguem completar tarefas de forma acurada e completa. É medida pela taxa de sucesso em atingir objetivos, sem erro ou retrabalho necessário.
- Eficiência: Os recursos gastos em relação aos resultados alcançados, frequentemente expressa como tempo investido ou número de passos necessários para completar uma tarefa. Uma tarefa realizada com menos tempo ou passos é mais eficiente.
- Satisfação: A percepção subjetiva, conforto, e atitudes positivas (ou negativas) do usuário em relação ao uso do produto. Inclui frustração, aceitabilidade e disposição de uso continuado.

Estes pilares fundamentam tanto o instrumento de coleta de dados (questionário aplicado aos servidores públicos) quanto a análise de impacto apresentada na Seção 3.

1.5.3 Arquitetura de serviços de diretório: Do modelo NT4 ao Active Directory

A infraestrutura diagnosticada opera dentro de um modelo arquitetural específico de redes Microsoft, cuja história é fundamental para entender tanto os problemas quanto a solução proposta.

1.5.3.1 Domínio NT4 e Protocolo NTLM

O servidor analisado emula um Controlador de Domínio Primário (PDC) do modelo Windows NT4, uma arquitetura que remonta aos anos 1990. Segundo Desmond, Richards, Allen e Lowe-Norris (2013, p.

12), o modelo NT4 baseia-se em uma arquitetura de "mestre único" (Single-Master Architecture), onde apenas o PDC possui uma cópia gravável do banco de dados de diretório. Todos os demais computadores na rede (Backup Domain Controllers, ou BDCs, e estações de trabalho) funcionam como consumidores desse repositório centralizado. Esta arquitetura cria dois problemas estruturais:

1. Ponto único de falha: Se o PDC falha, a rede perde toda capacidade de autenticar novos usuários (embora estações de trabalho já autenticadas possam continuar funcionando com token em cache).
2. Gargalo de desempenho: Todo tráfego de autenticação passa necessariamente pelo PDC, que pode ficar sobrecarregado em ambientes com muitos usuários.

O protocolo de autenticação utilizado é o NTLM (NT LAN Manager), desenvolvido pela Microsoft. De acordo com a Microsoft (2025d), o NTLM utiliza um mecanismo de "desafio-resposta" onde o servidor envia um desafio aleatório ao cliente, que responde com um hash da senha do usuário combinado com o desafio. Este desenho é computacionalmente custoso para o servidor (que deve manter credenciais de todos os usuários em memória ou em banco de dados de rápido acesso) e vulnerável a ataques de retransmissão, nos quais um atacante pode capturar a resposta de desafio-resposta e reutilizá-la para se autenticar sem conhecer a senha original (Microsoft, 2025a).

Conforme detalhado por Terpstra (2003), a arquitetura NT4 baseada em Samba 3 foi, durante muitos anos, o padrão de facto para interoperabilidade entre redes Windows e sistemas baseados em Unix/Linux. No entanto, o Samba 3 nunca foi projetado para interoperar com sistemas operacionais modernos como o Windows 11, e as incompatibilidades resultantes forçam a degradação de segurança descrita na Seção 3 deste trabalho.

1.5.3.2 Active Directory e Protocolo Kerberos

A solução proposta neste trabalho adota o modelo Active Directory (AD), que representa uma evolução fundamental em relação ao NT4. O AD é um serviço de diretório hierárquico e distribuído que utiliza um modelo de replicação "multi-mestre", permitindo que qualquer Controlador de Domínio (DC) processe alterações ao banco de dados de diretório. Esta mudança arquitetural aumenta significativamente a disponibilidade e reduz gargalos de desempenho (Desmond et al., 2013, p. 45).

A principal evolução na segurança, contudo, reside na adoção do Kerberos como protocolo de autenticação padrão. Kerberos é um protocolo de autenticação desenvolvido no MIT (Instituto de Tecnologia de Massachusetts) na década de 1980, baseado em criptografia de chave simétrica. Segundo Lowe-Norris (2013, p. 78), o Kerberos elimina completamente a transmissão de senhas pela rede através do uso de tickets criptografados emitidos por um Key Distribution Center (KDC). O fluxo é o seguinte:

1. Um usuário faz login em uma estação de trabalho, fornecendo sua senha ao sistema operacional cliente.
2. O cliente criptografa essa senha e a envia ao KDC (geralmente o Controlador de Domínio ou um serviço integrado nele).
3. O KDC verifica a credencial, gera um Ticket Granting Ticket (TGT) válido por um período (tipicamente 10 horas), e o envia ao cliente.
4. O cliente armazena este TGT em cache.
5. Quando o usuário acessa um recurso da rede (compartilhamento de arquivos, impressora, etc.), o cliente apresenta seu TGT ao KDC, que emite um Ticket de Serviço específico para aquele recurso.
6. O cliente utiliza o Ticket de Serviço para se comunicar com o recurso, sem nunca transmitir a senha novamente.

Esta arquitetura resolve os principais problemas de segurança do NTLM: não há transmissão de senhas na rede, não há vulnerabilidade a ataques de retransmissão, e a comunicação pode ser assinada e criptografada. Além disso, Kerberos é um padrão amplamente adotado (RFC 4120), permitindo interoperabilidade com sistemas heterogêneos.

1.5.4 Univention Corporate Server (UCS)

O Univention Corporate Server é uma plataforma baseada em Debian que integra serviços de diretório OpenLDAP e serviços de domínio Active Directory via Samba 4 (UNIVENTION, 2025). Esta arquitetura híbrida permite que o UCS atue como um Controlador de Domínio AD completo, fornecendo o KDC para autenticação Kerberos e suporte ao protocolo SMBv3, o que resolve as incompatibilidades de segurança e desempenho diagnosticadas no ambiente legado.

2 METODOLOGIA

2.1 ABORDAGEM E DELINEAMENTO DA PESQUISA

Esta pesquisa caracteriza-se como um estudo de caso exploratório-descritivo de natureza qualitativa-quantitativa, focando em uma infraestrutura legada específica em uma repartição pública. A abordagem qualitativa permite aprofundamento nos fenômenos observados e entendimento contextual, enquanto a quantificação fornece métricas objetivas que fundamentam a tomada de decisão.

2.2 FRAMEWORK METODOLÓGICO: NIST CYBERSECURITY FRAMEWORK 2.0

O pilar metodológico central é a aplicação do NIST Cybersecurity Framework (CSF) 2.0 como instrumento estruturador de análise. Conforme estabelecido na publicação NIST CSWP 29 (NIST, 2024), o CSF 2.0 organiza a gestão de riscos de cibersegurança em seis funções principais:

1. Governar (GV): Supervisão organizacional, liderança e políticas.
2. Identificar (ID): Desenvolvimento da capacidade organizacional de entender riscos de cibersegurança.
3. Proteger (PR): Implementação de salvaguardas para evitar, detectar e conter ataques.
4. Detectar (DT): Análise de atividades para identificar incidentes de cibersegurança.
5. Responder (RS): Ações para conter o impacto de incidentes.
6. Recuperar (RC): Restauração de capacidades normais de operação após incidentes.

Este framework foi escolhido porque: (a) é amplamente adotado internacionalmente e reconhecido em órgãos governamentais; (b) fornece uma taxonomia consistente que permite mapeamento sistemático de deficiências; (c) propõe uma progressão lógica que facilita a estruturação de propostas de melhoria.

Adicionalmente, a análise utiliza a ABNT NBR ISO/IEC 27001:2022 como complemento, estabelecendo correlação entre os controles técnicos exigidos e os problemas diagnosticados.

2.3 COLETA DE DADOS: DUAS FRENTES COMPLEMENTARES

2.3.1 Frente 1: Auditoria técnica e diagnóstico de incompatibilidade

Consistiu em análise direta tanto do servidor legado quanto de estações de trabalho cliente, com foco em:

- Identificação de versões de sistemas operacionais e serviços (utilizando ferramentas como lsb_release, uname, smb --version).
- Análise de arquivos de configuração críticos (smb.conf do servidor, registros do Windows no cliente).
- Coleta de observações de comportamento operacional (uso de disco, CPU, latência de rede).
- Documentação das mudanças de configuração necessárias para manter compatibilidade.

2.3.2 Frente 2: Levantamento quantitativo da percepção de usuários

Um questionário estruturado foi aplicado a 21 servidores públicos que utilizam a infraestrutura diariamente. O instrumento foi desenvolvido conforme os preceitos da ABNT NBR ISO 9241-11, operacionalizando os três pilares da usabilidade:

Eficácia: Perguntas sobre taxa de sucesso na conclusão de tarefas, frequência de travamentos, necessidade de reinicialização.

Eficiência: Perguntas sobre percepção de velocidade, tempo gasto em operações específicas, retrabalho necessário.

Satisfação: Perguntas sobre atitudes negativas (frustração), prioridades em modernização, impacto percebido na produtividade.

As respostas foram tabuladas e convertidas em percentuais, permitindo quantificação de fenômenos subjetivos.

3 DIAGNÓSTICO DA INFRAESTRUTURA LEGADA

3.1 IDENTIFICAÇÃO DA INFRAESTRUTURA LEGADA

A etapa de análise e enumeração de serviços no servidor de arquivos alvo revelou informações cruciais sobre sua superfície de ataque. Foi confirmado que o host opera com o sistema operacional Debian 7 "Wheezy", uma versão que, no contexto atual, é considerada obsoleta e descontinuada (End-of-Life). A Figura 01 detalha a versão do kernel associada, corroborando a antiguidade da plataforma. Além do sistema operacional, o serviço de compartilhamento de arquivos Samba foi identificado em sua versão 3.6.6. Esta iteração do software, também capturada na Figura 01, é notoriamente legada e conhecida por possuir um vasto histórico de vulnerabilidades de segurança já catalogadas. A presença conjunta desses dois componentes (um SO de servidor sem suporte e uma versão de serviço defasada) indica um risco de segurança significativo.

Figura 01: Debian 7 “Wheezy” com Samba versão 3.6.6

```
Linux puraquequara 3.2.0-4-amd64 #1 SMP Debian 3.2.78-1 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Oct 28 19:11:05 2025 from 172.19.6.165
adm_cml@puraquequara:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Debian
Description:    Debian GNU/Linux 7.11 (wheezy)
Release:        7.11
Codename:       wheezy
adm_cml@puraquequara:~$ smbd -V
Version 3.6.6
adm_cml@puraquequara:~$
```

Fonte: Os autores (2025)

O arquivo de configuração smb.conf, detalhado na Figura 02, revela uma configuração de rede anacrônica e de alto risco. O servidor Samba está explicitamente configurado para atuar como um Controlador de Domínio Primário (PDC) através das diretivas security = user e domain logons = yes. Esta

é uma emulação de um domínio estilo NT4, uma tecnologia que antecede o Active Directory e que depende de protocolos de autenticação fundamentalmente quebrados, como o NTLMv1. Conforme alerta a documentação do samba (Samba, 2025), a recomendação para ambientes hardened é desativar completamente o NTLM, exigindo autenticação via Kerberos ou simple-bind.

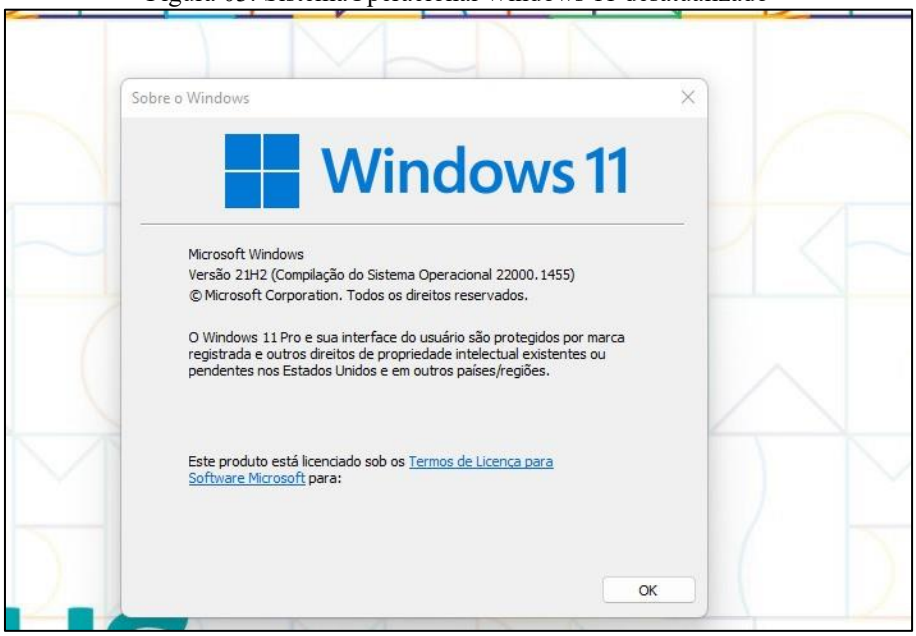
O ponto mais crítico da infraestrutura reside na incompatibilidade de segurança entre o servidor e os clientes. As estações de trabalho (Figura 03) operam com Windows 11 Pro Versão 21H2 encerrado em outubro de 2023. Para que um sistema operacional moderno como o Windows 11 consiga se autenticar em um PDC NT4, é mandatório que protocolos legados e perigosos, como o SMBv1, sejam manualmente habilitados no cliente. O SMBv1 é notório por ser o vetor de ataques como o WannaCry (NHS ENGLAND, 2018)

Figura 02: Arquivo smb.conf do servidor legado

```
adm_cml@puraquequara:/etc/samba$ cat smb.conf
# Parametros Globais
[global]
   # Dominio, Nome e Descricao
        workgroup = MANAUS
        netbios name = puraquequara
        server string = GNU/Linux - SMB

   # Quais interfaces de rede utilizar
        smb ports = 139

   # Quais interfaces de rede utilizar
        interfaces = lo, eth0
        bind interfaces only = yes

   # Nivel de Mensagens
        log level = 3
        log file = /var/log/samba/log.%m
        max log size = 100000
        debug level = 3
        syslog = 1

   # Atuar como um PDC
        security = user
        domain logons = yes
        preferred master = yes
        domain master = yes
        local master = yes
        os level = 100

   # Equivalencia de usuarios Windows X Linux
        username map = /etc/samba/smbusers
        admin users = @"Domain Admins", @"adm_cml"

   # Habilitando Suporte a Wins
        wins support = yes
        wins proxy = yes
        guest account = nobody

   # Evitar o perfil ambulante do Windows NT/XP
        logon path =
        logon drive =
        logon home =
```

Fonte: Os autores (2025)

Figura 03: SistemaOperacional Windows 11 desatualizado

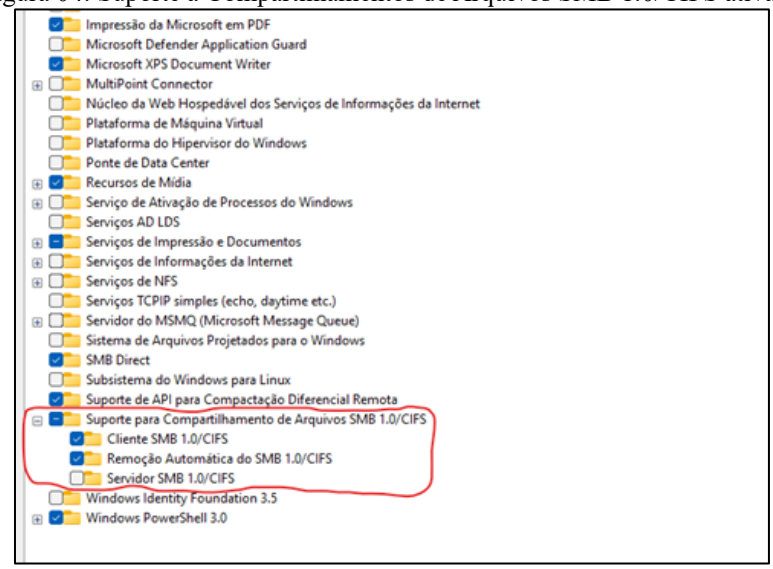


Fonte: Os autores (2025)

3.1.1 Análise das configurações de degradação de segurança no cliente

A auditoria confirmou a necessidade de habilitar manualmente o Suporte para Compartilhamento de Arquivos SMB 1.0/CIFS (Figura 04), um protocolo obsoleto desativado por padrão pela Microsoft por ser um vetor conhecido para ataques de ransomware (Microsoft, 2025; Microsoft, 2020). Além disso, a configuração do servidor (Figura 02) opera na porta 139, o que indica o uso do protocolo NetBIOS para resolução de nomes e sessão. Stallings e Brown (2014) alertam que mecanismos de autenticação obsoletos não oferecem garantias de confidencialidade e integridade adequadas para ambientes modernos, sendo suscetíveis a interceptação e ataques de repetição.

Figura 04: Suporte a Compartilhamentos de Arquivos SMB 1.0/CIFS ativado

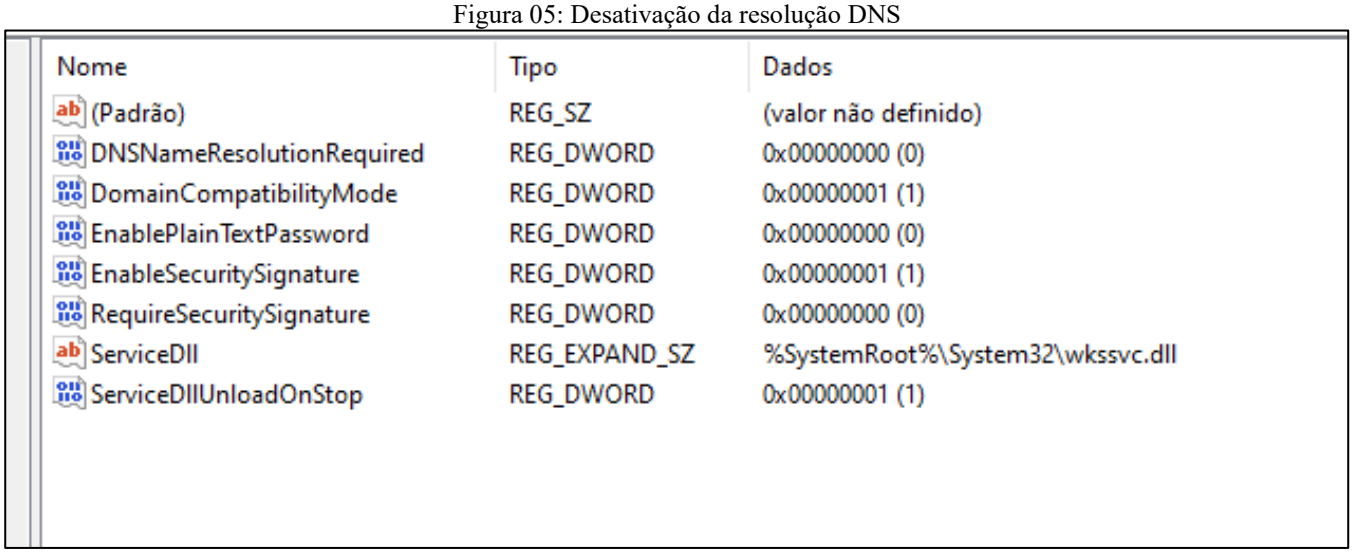


Fonte: Os autores (2025)

3.1.2 Configurações inseguras em registros de Sistema Operacional

Ajustes no registro do Windows 11 foram necessários para rebaixar a segurança do cliente. Conforme a Figura 05, a chave RequireSecuritySignature, do serviço LanmanWorkstation (wkssvc), foi configurada com o valor 0 (zero). Esta alteração desativa a exigência de assinatura de pacotes SMB, tornando a comunicação vulnerável a ataques de "man-in-the-middle" e retransmissão de credenciais (Microsoft, 2025a). Adicionalmente, a chave DNSNameResolutionRequired também foi definida como 0, relaxando as validações de identidade do servidor (Microsoft, 2025b). Embora a Figura 06 mostre que o serviço Netlogon ainda tenta requerer assinatura (RequireSignOrSeal=1), a desativação no LanmanWorkstation já compromete a segurança da sessão de compartilhamento de arquivos.

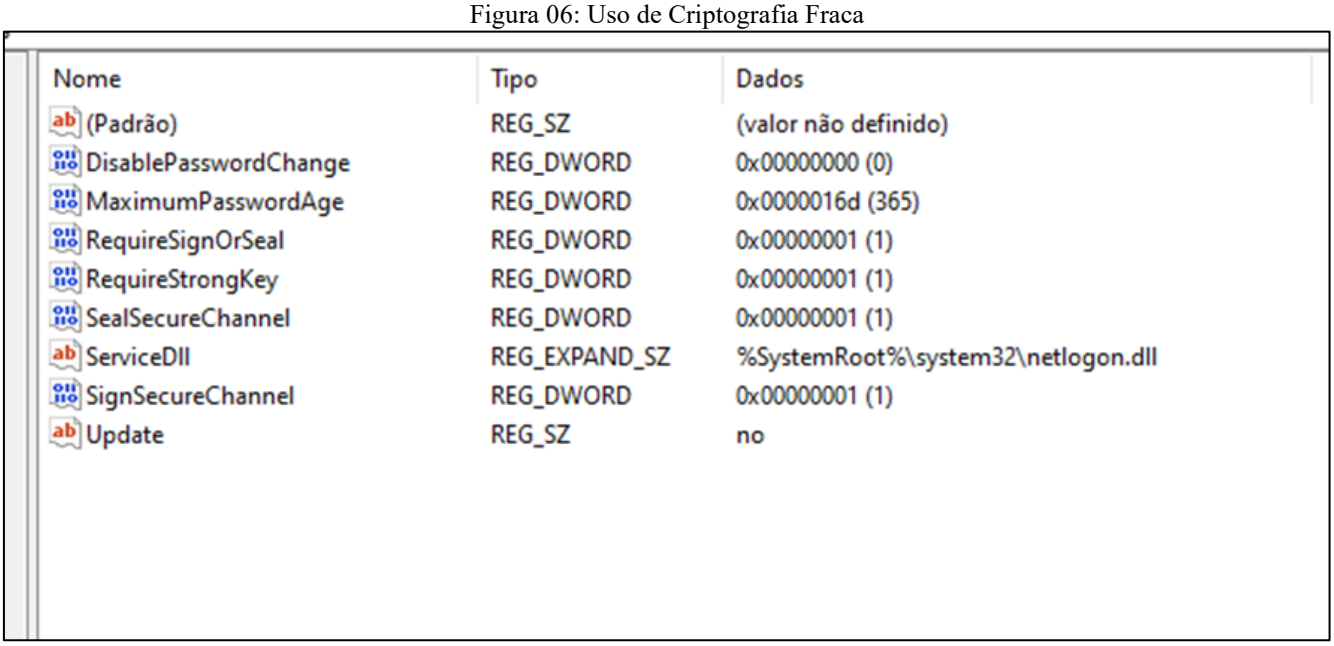
Figura 05: Desativação da resolução DNS



Nome	Tipo	Dados
(Padrão)	REG_SZ	(valor não definido)
DNSNameResolutionRequired	REG_DWORD	0x00000000 (0)
DomainCompatibilityMode	REG_DWORD	0x00000001 (1)
EnablePlainTextPassword	REG_DWORD	0x00000000 (0)
EnableSecuritySignature	REG_DWORD	0x00000001 (1)
RequireSecuritySignature	REG_DWORD	0x00000000 (0)
ServiceDll	REG_EXPAND_SZ	%SystemRoot%\System32\wkssvc.dll
ServiceDllUnloadOnStop	REG_DWORD	0x00000001 (1)

Fonte: Os autores (2025)

Figura 06: Uso de Criptografia Fraca



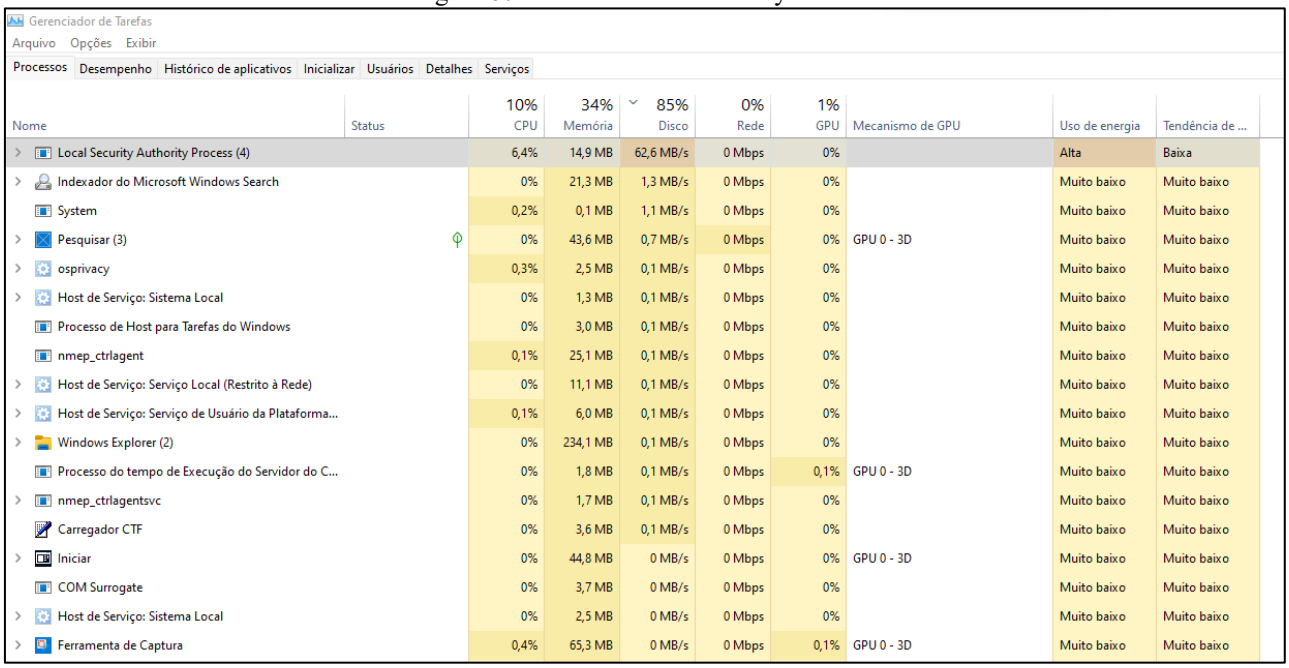
Nome	Tipo	Dados
(Padrão)	REG_SZ	(valor não definido)
DisablePasswordChange	REG_DWORD	0x00000000 (0)
MaximumPasswordAge	REG_DWORD	0x0000016d (365)
RequireSignOrSeal	REG_DWORD	0x00000001 (1)
RequireStrongKey	REG_DWORD	0x00000001 (1)
SealSecureChannel	REG_DWORD	0x00000001 (1)
ServiceDll	REG_EXPAND_SZ	%SystemRoot%\system32\netlogon.dll
SignSecureChannel	REG_DWORD	0x00000001 (1)
Update	REG_SZ	no

Fonte: Os autores (2025)

3.1.3 Análise de desempenho e impacto operacional

Observação de picos de 80% de uso de disco pelo processo Local Security Authority Process (LSASS) nos clientes Windows 11 (Figura 07), este sintoma é causado pela incompatibilidade de protocolos de autenticação, o Windows 11 é projetado para usar Kerberos como método preferencial em domínios Active Directory (Microsoft, 2025c). No entanto, ao falhar em se comunicar com o servidor Samba 3.6.6, o sistema operacional é forçado a um fallback para o protocolo legado NTLM (MICROSOFT, 2025d), gerando um ciclo de tentativas, timeouts e registros de log que sobrecarregam o disco.

Figura 07: Processo Local Security Process



Nome	Status	10% CPU	34% Memória	85% Disco	0% Rede	1% GPU	Mecanismo de GPU	Uso de energia	Tendência de ...
Local Security Authority Process (4)		6,4%	14,9 MB	62,6 MB/s	0 Mbps	0%		Alta	Baixa
Indexador do Microsoft Windows Search		0%	21,3 MB	1,3 MB/s	0 Mbps	0%		Muito baixo	Muito baixo
System		0,2%	0,1 MB	1,1 MB/s	0 Mbps	0%		Muito baixo	Muito baixo
Pesquisar (3)		0%	43,6 MB	0,7 MB/s	0 Mbps	0%	GPU 0 - 3D	Muito baixo	Muito baixo
osprivacy		0,3%	2,5 MB	0,1 MB/s	0 Mbps	0%		Muito baixo	Muito baixo
Host de Serviço: Sistema Local		0%	1,3 MB	0,1 MB/s	0 Mbps	0%		Muito baixo	Muito baixo
Processo de Host para Tarefas do Windows		0%	3,0 MB	0,1 MB/s	0 Mbps	0%		Muito baixo	Muito baixo
nmep_ctrlagent		0,1%	25,1 MB	0,1 MB/s	0 Mbps	0%		Muito baixo	Muito baixo
Host de Serviço: Serviço Local (Restrito à Rede)		0%	11,1 MB	0,1 MB/s	0 Mbps	0%		Muito baixo	Muito baixo
Host de Serviço: Serviço de Usuário da Plataforma...		0,1%	6,0 MB	0,1 MB/s	0 Mbps	0%		Muito baixo	Muito baixo
Windows Explorer (2)		0%	234,1 MB	0,1 MB/s	0 Mbps	0%		Muito baixo	Muito baixo
Processo do tempo de Execução do Servidor do C...		0%	1,8 MB	0,1 MB/s	0 Mbps	0,1%	GPU 0 - 3D	Muito baixo	Muito baixo
nmep_ctrlagentsvc		0%	1,7 MB	0,1 MB/s	0 Mbps	0%		Muito baixo	Muito baixo
Carregador CTF		0%	3,6 MB	0,1 MB/s	0 Mbps	0%		Muito baixo	Muito baixo
Iniciar		0%	44,8 MB	0 MB/s	0 Mbps	0%	GPU 0 - 3D	Muito baixo	Muito baixo
COM Surrogate		0%	3,7 MB	0 MB/s	0 Mbps	0%		Muito baixo	Muito baixo
Host de Serviço: Sistema Local		0%	2,5 MB	0 MB/s	0 Mbps	0%		Muito baixo	Muito baixo
Ferramenta de Captura		0,4%	65,3 MB	0 MB/s	0 Mbps	0,1%	GPU 0 - 3D	Muito baixo	Muito baixo

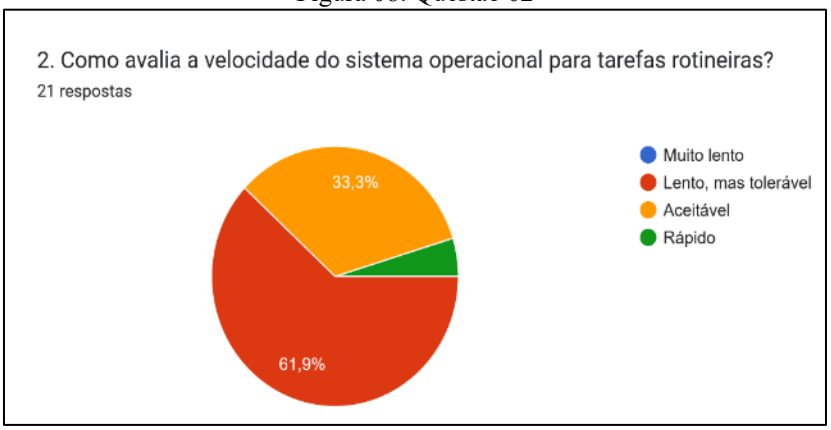
Fonte: Os autores (2025)

Este conjunto de dados técnicos, sob a ótica do NIST Cybersecurity Framework, demonstra uma violação direta dos princípios da função "Proteger" (NIST, Protect). Do ponto de vista da ABNT NBR ISO/IEC 27001:2022, tais configurações contrariam diversos objetivos de controle, como os de Controle de Acesso (A.5.15), Uso de Criptografia (A.8.24) e Segurança de Redes (A.8.20), ao adotar protocolos e configurações que são reconhecidamente fracos.

3.2 EFICIÊNCIA (EFFICIENCY): O DESPERDÍCIO DE TEMPO E RECURSOS

A eficiência, conforme preconiza a norma ABNT NBR ISO 9241-11, não se limita apenas à conclusão de uma tarefa, mas foca na relação entre o nível de eficácia alcançado e a quantidade de recursos despendidos, tais como tempo, esforço mental e custos operacionais. Neste quesito, os dados coletados indicam uma falha severa e sistêmica.

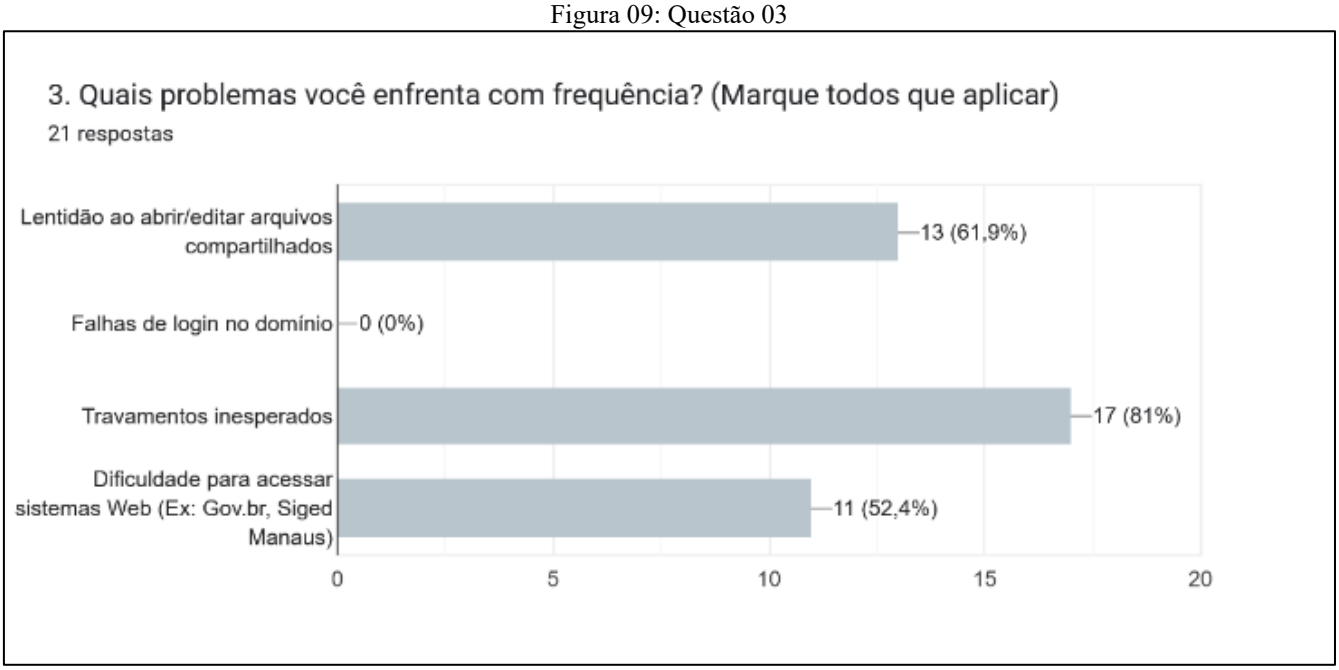
Figura 08: Questão 02



Fonte: Os autores (2025)

- Percepção de Velocidade: 95,2% dos usuários classificam o sistema como "Muito lento" (33,3%) ou "Lento, mas tolerável" (61,9%). Apenas 4,8% (1 respondente) consideram "Aceitável".
- Impacto nas Tarefas: 90,5% dos servidores confirmam que o sistema atrasa suas tarefas diárias, sendo que para 38,1% esse atraso é "significativo".
- Causa Raiz Percebida: A lentidão não é genérica. 61,9% (13 servidores) identificaram especificamente a "Lentidão ao abrir/editar arquivos compartilhados" (Figura 09), como um problema frequente.

Figura 09: Questão 03



Fonte: Os autores (2025)

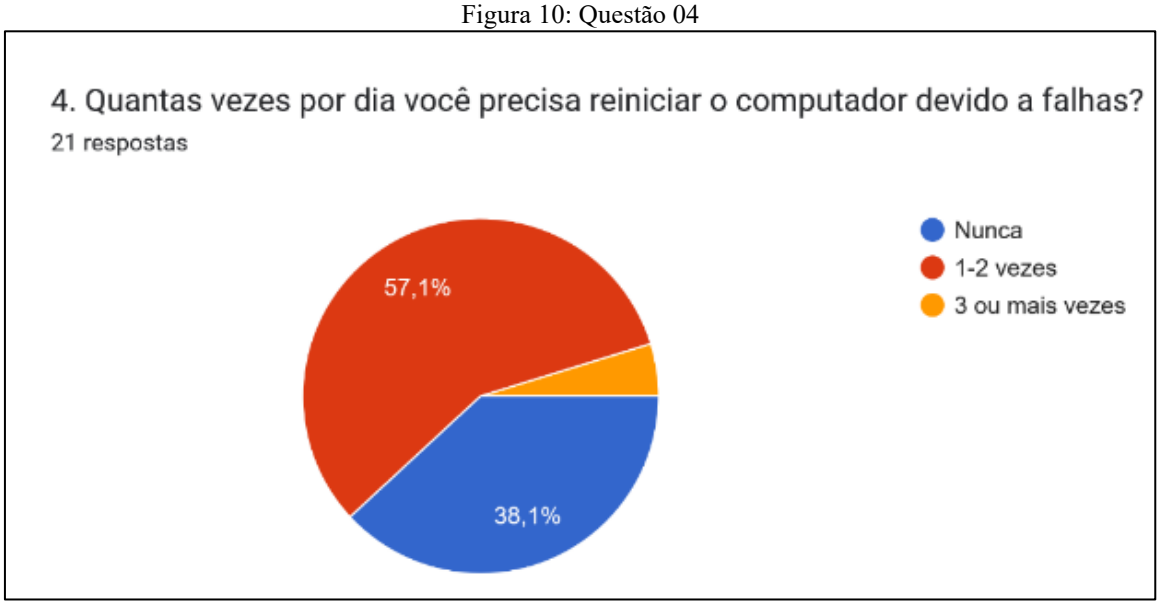
Essa percepção do usuário está em perfeita sincronia com a análise técnica, que diagnosticou os picos de 80% de uso de disco no processo LSASS, causados pelo conflito de protocolos de autenticação (Kerberos vs. NTLM) e pela latência induzida pelo protocolo SMBv1.

3.2.1 - Eficácia (Effectiveness): A incapacidade de concluir o trabalho

A eficácia mede se o usuário consegue completar suas tarefas de forma correta e completa. Os resultados demonstram que a instabilidade do sistema impede ativamente a conclusão do trabalho.

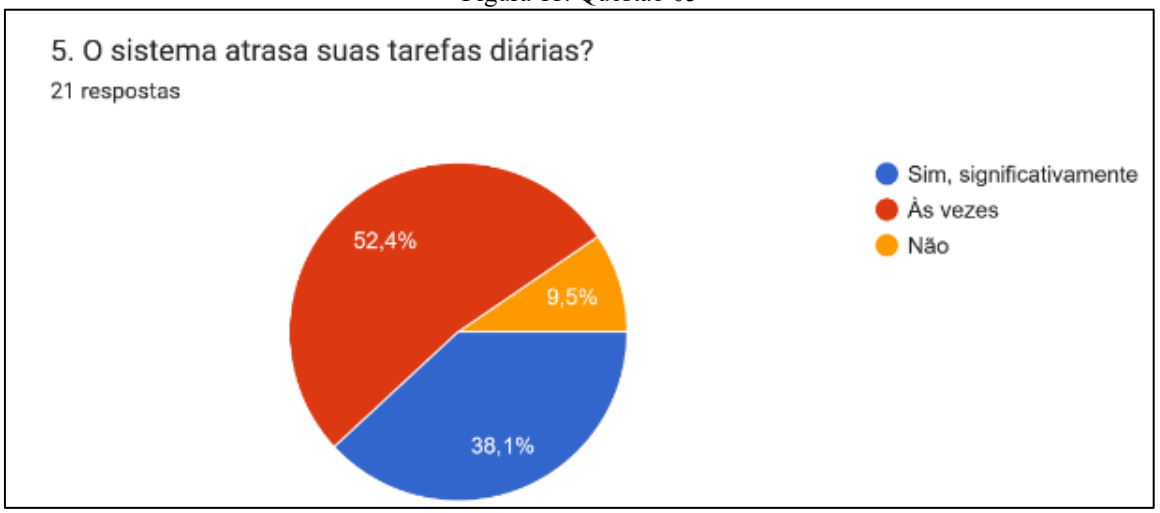
- Travamentos Frequentes: O problema mais relatado pelos usuários foi a instabilidade, com 81% (17 servidores) relatando "Travamentos inesperados" (Figura 09) como um problema frequente.
- Interrupção Completa do Trabalho: A consequência desses travamentos é drástica. Mais da metade dos usuários (57,1%) precisa reiniciar seus computadores de 1 a 2 vezes por dia devido a falhas (Figura 10). Somando-se aos 4,8% que reiniciam 3 ou mais vezes, conclui-se que 61,9% dos servidores perdem tempo reiniciando suas máquinas diariamente.

Figura 10: Questão 04



Fonte: Os autores (2025)

Figura 11: Questão 05



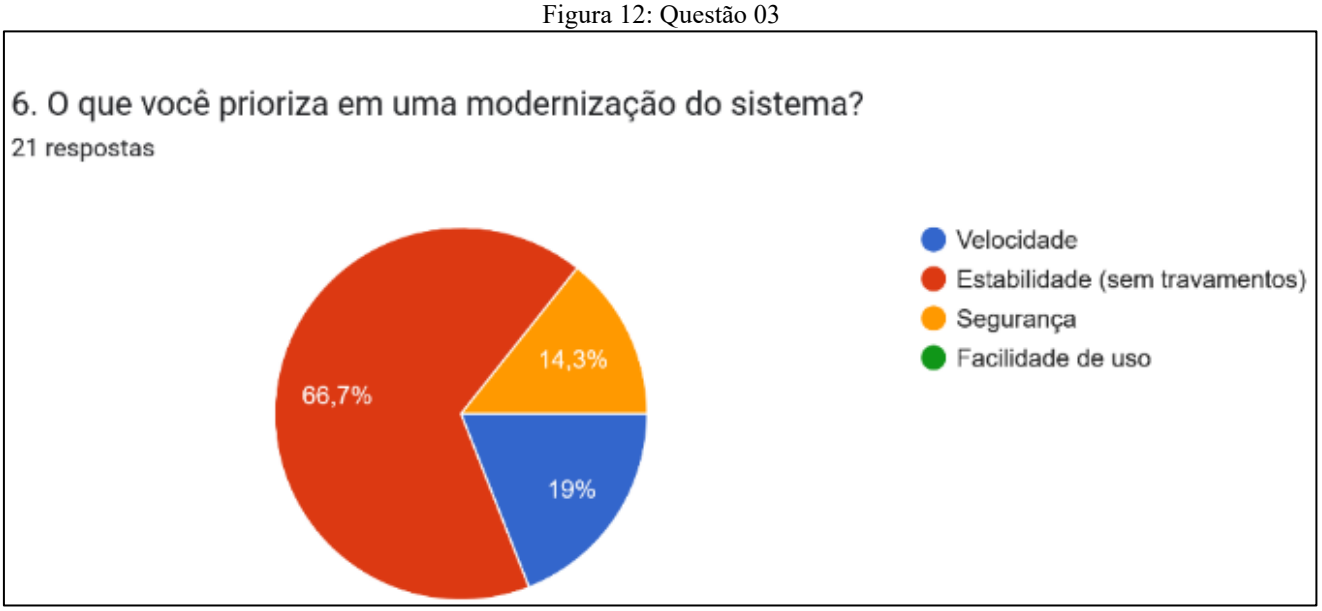
Fonte: Os autores (2025)

Um sistema que exige reinicializações diárias de mais da metade de sua base de usuários falha em seu propósito fundamental de prover um ambiente de trabalho funcional, demonstrando uma eficácia operacional extremamente baixa.

3.2.2 Satisfação (Satisfaction): Frustração e impacto colateral

A satisfação refere-se à percepção subjetiva e à frustração do usuário. Embora não medida diretamente por uma nota, a satisfação é evidenciada pelas prioridades de melhoria e por problemas colaterais.

Figura 12: Questão 03



Fonte: Os autores (2025)

- Prioridades de Modernização: A frustração dos usuários com a ineficiência e a falta de eficácia é clara. Ao serem perguntados sobre o que priorizariam em uma modernização, 85,7% apontaram para "Estabilidade (sem travamentos)" (66,7%) e "Velocidade" (19%). Notavelmente, "Segurança" (14,3%) não é a principal preocupação do usuário final, pois ele sente o impacto da performance, e não o risco da vulnerabilidade.
- Impacto na Rede: A infraestrutura legada também parece gerar problemas de rede mais amplos. 52,4% dos usuários (11 servidores) relataram "Dificuldade para acessar sistemas Web". Isso é consistente com a análise técnica, que identificou a desativação da DNSNameResolutionRequired (Figura 04), sugerindo que o controlador de domínio legado e suas configurações de DNS incorretas estão prejudicando a performance da rede como um todo, não apenas o acesso a arquivos.

Em síntese, os dados do questionário validam quantitativamente as observações técnicas, provando que a infraestrutura legada não é apenas um risco de segurança, mas um gargalo operacional ativo que causa perda de eficiência diária, impede a conclusão de tarefas e gera frustração generalizada entre os servidores.

4 PROPOSTA DE MODERNIZAÇÃO E VALIDAÇÃO (RESULTADOS DA SOLUÇÃO)

A análise diagnóstica revelou uma infraestrutura legada crítica, baseada em um servidor Debian 7 "Wheezy" atuando como um Controlador de Domínio Primário (PDC) NT4. Esta configuração força o rebaixamento de protocolos de segurança (SMBv1) e causa severos gargalos de performance, afetando diretamente a produtividade e expondo o órgão a riscos de segurança.

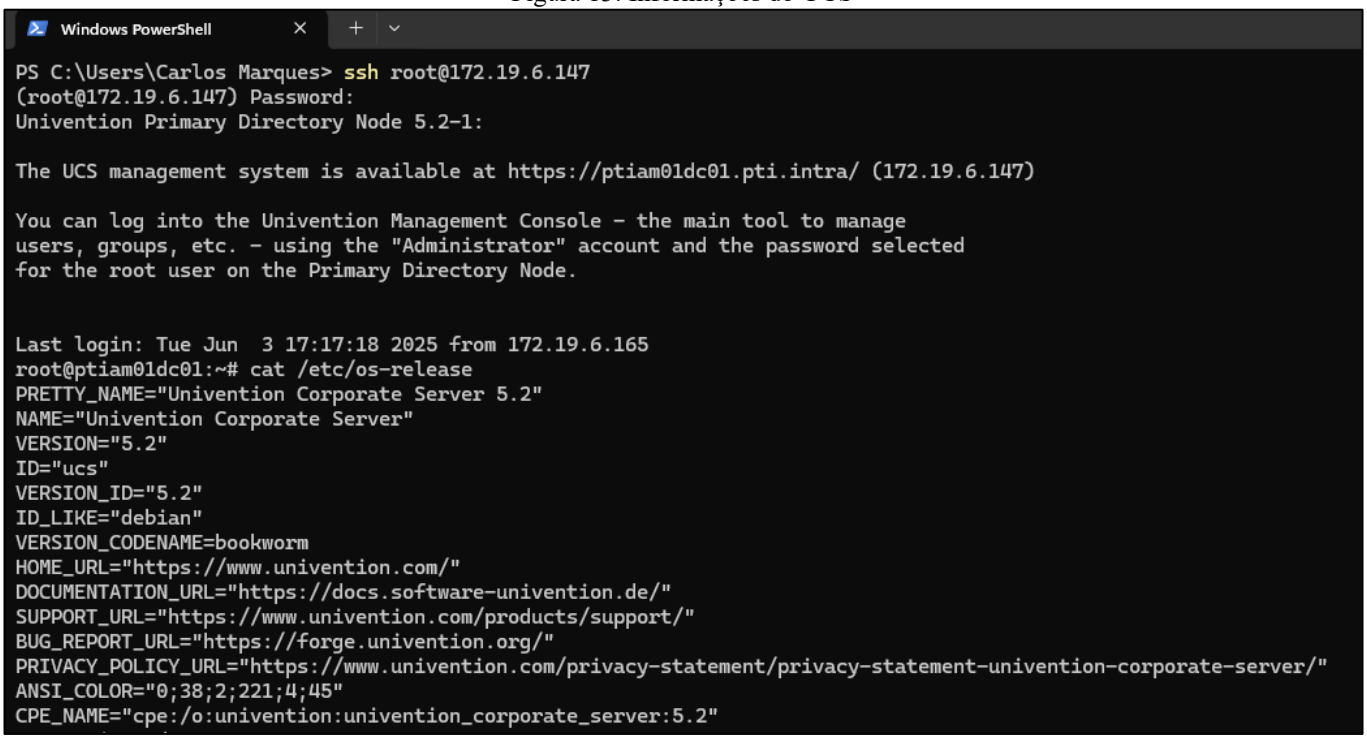
A solução proposta visa endereçar todos os pontos de falha identificados, substituindo a infraestrutura legada por uma plataforma moderna de Gerenciamento de Identidade (IdM), o Univention Corporate Server (UCS). A implementação, conforme demonstrado nas figuras a seguir, resolve os problemas de segurança, desempenho e governança.

4.1 APRESENTAÇÃO DA SOLUÇÃO PROPOSTA

A escolha de uma base sólida baseada em Linux (Debian) para o servidor de diretório segue as melhores práticas de administração de sistemas. Nemeth et al. (2011) destacam que a estabilidade, a auditabilidade do código e a robustez dos sistemas baseados em Unix/Linux são fundamentais para a implementação de serviços de infraestrutura crítica, como autenticação e arquivos.

O primeiro passo da modernização é a substituição do sistema operacional em End-of-Life (EOL). A solução foi implementada utilizando o Univention Corporate Server 5.2, conforme detalhado na Figura 08, que é baseado no Debian 12 "Bookworm". Isso elimina o débito técnico, garantindo um sistema operacional moderno e com atualizações de segurança contínuas.

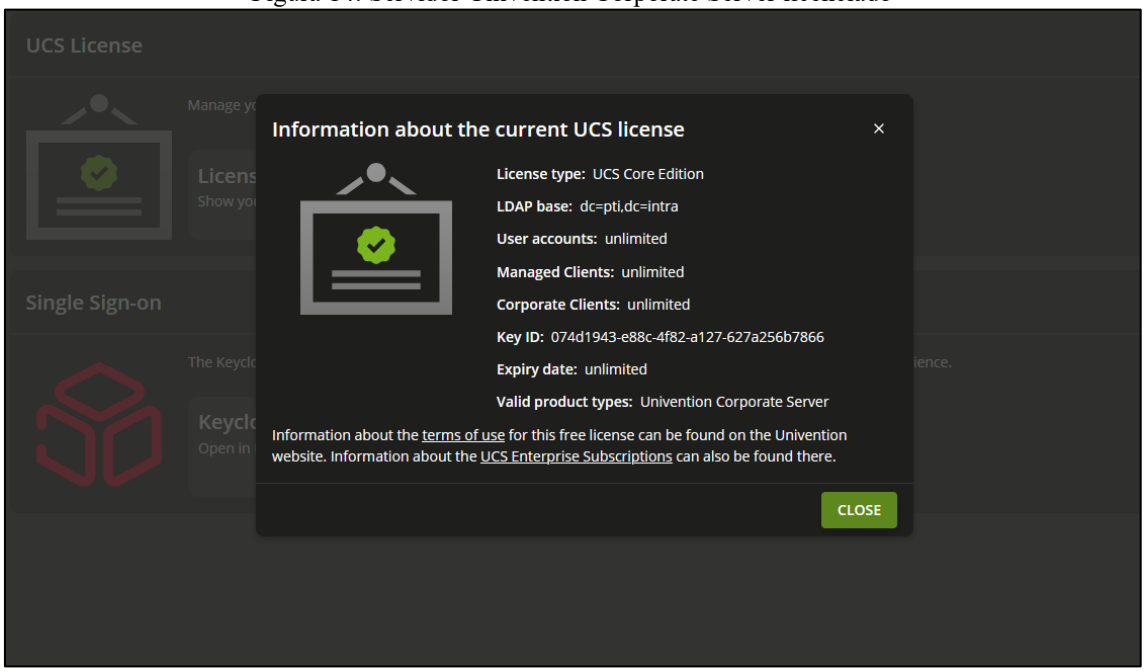
Figura 13: Informações do UCS



Fonte: Os autores (2025)

Respondendo à justificativa de restrições orçamentárias, comuns em órgãos públicos, a solução adota a UCS Core Edition (Figura 14). Esta licença é gratuita, possui data de expiração ilimitada e permite um número ilimitado de contas de usuário e clientes gerenciados, oferecendo uma solução economicamente viável sem custos de licenciamento de software de servidor.

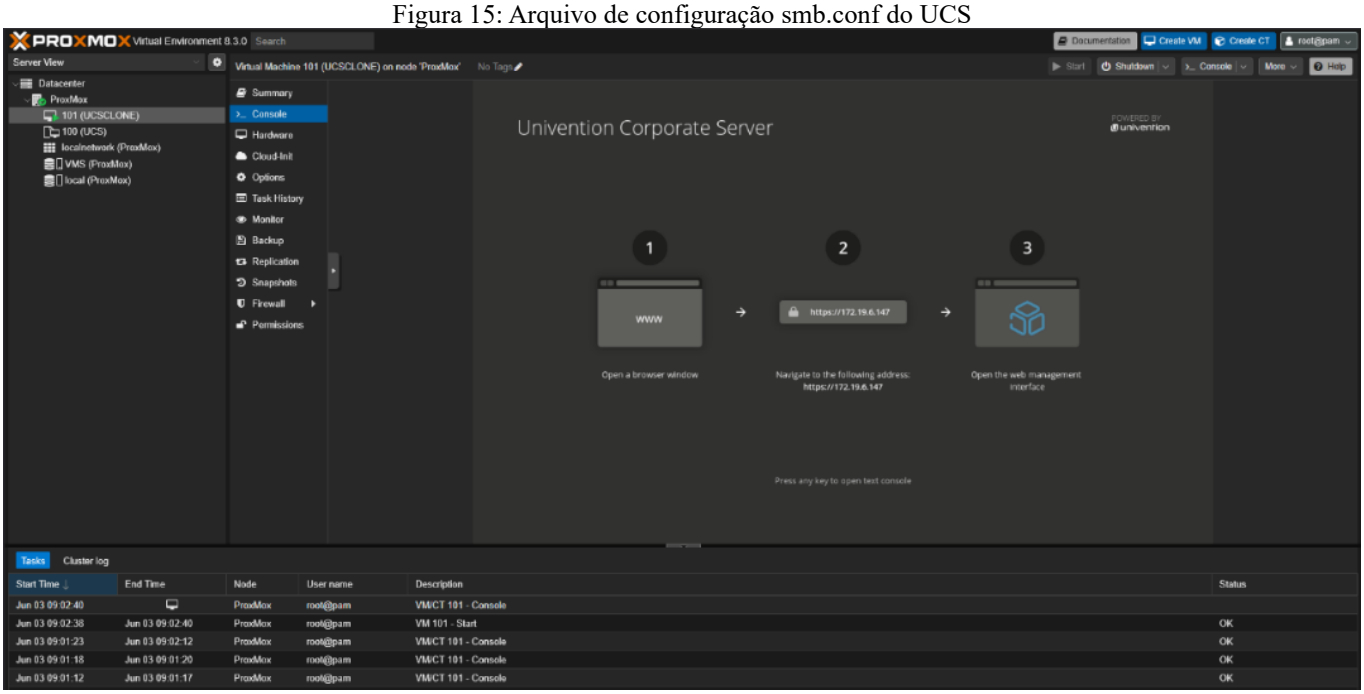
Figura 14: Servidor Univention Corporate Server licenciado



Fonte: Os autores (2025)

A implementação foi realizada em um ambiente de virtualização Proxmox (Figura 15), alinhando-se às práticas modernas de TI que favorecem a flexibilidade, alta disponibilidade e fácil recuperação de desastres.

Figura 15: Arquivo de configuração smb.conf do UCS



Fonte: Os autores (2025)

4.2 RESOLUÇÃO DOS PROBLEMAS DE SEGURANÇA E AUTENTICAÇÃO

O núcleo da proposta é a substituição do obsoleto PDC NT4 por um Controlador de Domínio (DC) moderno. O UCS é configurado como um Controlador de Domínio compatível com Active Directory, conforme visível no arquivo de configuração smb.conf da solução (Figura 16), onde o server role = active directory domain controller.

A proposta central consiste na substituição do controlador de domínio primário obsoleto, baseado no PDC NT4, por um Controlador de Domínio (DC) moderno usando o UCS (Unified Computing System). O UCS é configurado para atuar como um Controlador de Domínio compatível com Active Directory, o que pode ser confirmado no arquivo de configuração smb.conf da solução, onde consta o parâmetro “server role = active directory domain controller”. Essa transição visa trazer uma infraestrutura de autenticação mais atualizada e segura.

Com essa modernização, buscam-se resolver diversas limitações e vulnerabilidades associadas ao antigo PDC NT4. O uso do UCS permite uma melhor integração com os padrões atuais de autenticação e autorização, além de otimizar a gestão centralizada de usuários e políticas de segurança. Isso proporciona um ambiente de TI mais robusto, suportando controle refinado de acessos e facilitando a administração contínua da rede, com maior confiabilidade e escalabilidade. Assim, a solução traz benefícios substanciais

para a segurança e o gerenciamento da infraestrutura digital empresarial, garantindo conformidade com práticas modernas de segurança da informação.

Figura 16: Arquivo de configuração smb.conf do UCS

```
; ----------------------<10global>-------------------------
[global]
        debug level     = 1
        logging         = file
        max log size    = 0

        kdc default domain supported enctypes   = aes256-cts-hmac-sha1-96-sk,aes256-cts-hmac-sha1-96,aes128-cts-hmac-sha1-96,arcfour-hmac-md5

        netbios name    = ptiam01dc01
        server role     = active directory domain controller
        name resolve order      = wins host bcast
        server string   = Univention Corporate Server
        server services = -dns -smb +s3fs -nbt
        server role check:inhibit = yes
        # use nmbd; to disable set samba4/service/nmb to s4
        nmbd_proxy_logon:cldap_server=127.0.0.1
        workgroup       = PTI
        realm           = PTI.INTRA

        tls enabled     = yes
        tls keyfile     = /etc/univention/ssl/ptiam01dc01.pti.intra/private.key
        tls certfile    = /etc/univention/ssl/ptiam01dc01.pti.intra/cert.pem
        tls cafile      = /etc/univention/ssl/ucsCA/CAcert.pem
        tls verify peer = ca_and_name
        ldap server require strong auth = yes
        dsdb:schema update allowed = no
        max open files = 32808
        interfaces      = lo ens18
        bind interfaces only    = yes
        ntlm auth       = ntlmv2-only
        machine password timeout        = 0
        acl allow execute always = True
        kccsrv:samba_kcc = False
```

Fonte: Os autores (2025)

Esta mudança resolve diretamente os dois principais problemas diagnosticados:

1. Segurança de Protocolo (SMBv3): A necessidade de habilitar o inseguro SMBv1 no Windows 11 é eliminada. A Figura 17 (saída do comando smbstatus) comprova que o cliente Windows 11 (neste caso, 172.19.6.210) se conecta ao servidor UCS usando o protocolo SMB3_11.
2. Assinatura e Criptografia: O risco da desativação da assinatura de pacotes (RequireSecuritySignature = 0) é revertido. A Figura 17 demonstra que a conexão SMBv3 utiliza Signing (Assinatura) e Encryption (Criptografia) AES-128-GMAC, esta configuração valida a conformidade com a norma ABNT NBR ISO/IEC 27001, atendendo especificamente ao controle A.8.24 (Uso de criptografia) e A.8.20 (Segurança de redes), que exigem a proteção da confidencialidade e integridade dos dados em trânsito.

Além da substituição tecnológica, a implantação do UCS como Controlador de Domínio traz vantagens significativas em termos de escalabilidade e flexibilidade. Com esta solução, a infraestrutura pode se adaptar facilmente a mudanças no ambiente empresarial, como o crescimento no número de usuários e dispositivos conectados à rede. Essa adaptabilidade é fundamental para garantir que a infraestrutura permaneça eficiente e segura à medida que a organização evolui, possibilitando a

implementação de novas políticas e serviços sem a necessidade de grandes interrupções ou reformulações estruturais.

Outro benefício importante advindo dessa modernização é a possibilidade de integração com outras ferramentas e sistemas de segurança corporativos. O UCS, por ser compatível com o Active Directory, facilita a sincronização e o controle unificado de identidades em múltiplas plataformas, promovendo uma gestão mais eficiente dos acessos e identidades digitais. Isso contribui para mitigar riscos de segurança, melhorar a auditoria e assegurar a conformidade com normas e regulamentos, criando um ambiente corporativo mais seguro e resiliente.

Figura 17: smbstatus do UCS

```
root@ptiam01dc01:~# sudo smbstatus --verbose
using configfile = /etc/samba/smb.conf

Samba version 4.21.1-Univention
PID     Username     Group        Machine                                   Protocol Version  Encryption           Signing
----------------------------------------------------------------------------------------------------------------------------------------
2564    klaiver.araujo Domain Users 172.19.6.210 (ipv4:172.19.6.210:49743)    SMB3_11           -                    partial(AES-128-GMAC)
2564    Administrator Domain Admins 172.19.6.210 (ipv4:172.19.6.210:49743)    SMB3_11           -                    AES-128-GMAC

Service      pid     Machine       Connected at                     Encryption   Signing
---------------------------------------------------------------------------------------------
sysvol       2564    172.19.6.210  ter jun  3 10:42:17 2025 -04     -            AES-128-GMAC
IPC$         2564    172.19.6.210  ter jun  3 10:26:38 2025 -04     -            AES-128-GMAC


Locked files:
Pid          User(ID)   DenyMode   Access      R/W        Oplock           SharePath   Name   Time
---------------------------------------------------------------------------------------------------
2564         2009       DENY_NONE  0x100081    RDONLY     NONE             /var/lib/samba/sysvol   pti.intra   Tue Jun  3 10:42:25 2025
2564         2009       DENY_NONE  0x100081    RDONLY     NONE             /var/lib/samba/sysvol   pti.intra   Tue Jun  3 10:42:25 2025
```

Fonte: Os autores (2025)

4.3 RESOLUÇÃO DOS GARGALOS DE DESEMPENHO

O diagnóstico apontou que a principal causa de lentidão era o processo LSASS nos clientes, forçado a um fallback custoso para autenticação NTLM. A solução UCS resolve essa questão substituindo o domínio NT4 por um Controlador de Domínio compatível com Active Directory.

De acordo com o manual oficial do Univention Corporate Server 5.0, esta implementação integra nativamente o Kerberos como o framework de autenticação padrão do domínio. O manual especifica que em ambientes Samba/AD, o serviço Kerberos é fornecido por uma versão Heimdal integrada ao próprio Samba.

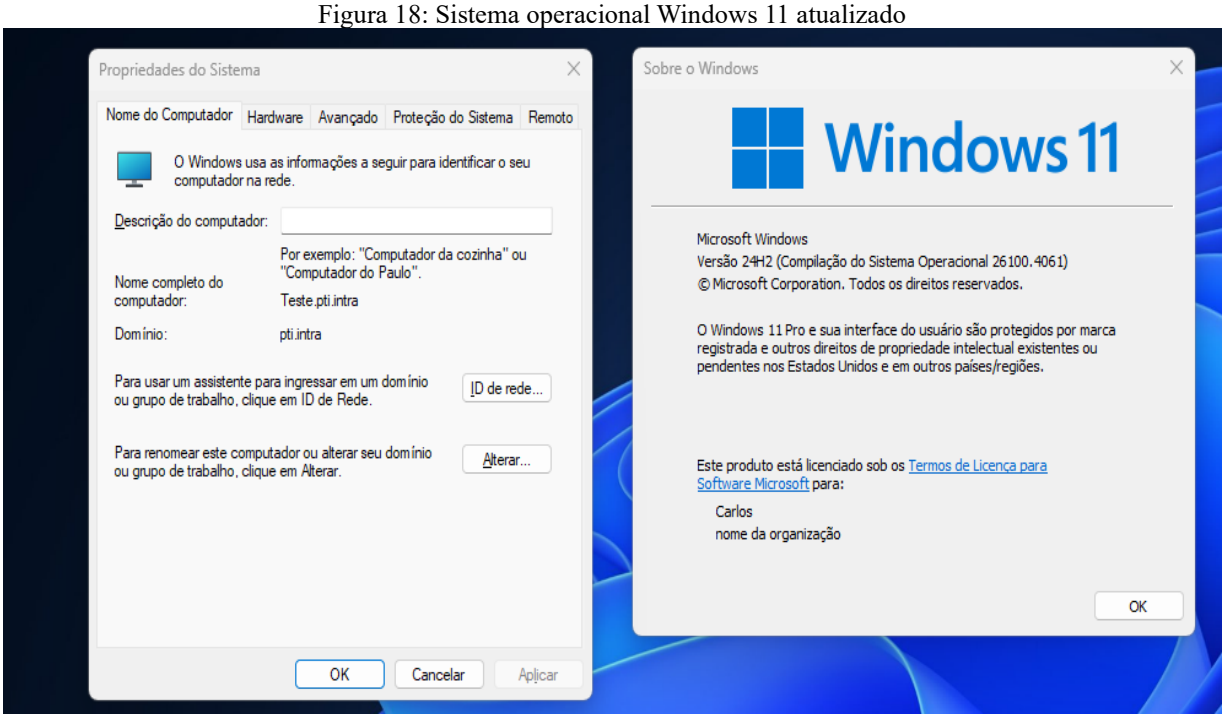
Na prática, clientes Windows 11 ingressados neste novo domínio se autenticam no Key Distribution Center (KDC) do UCS e recebem um ticket Kerberos no momento do login. Esse ticket passa a ser usado para todas as autenticações subsequentes aos recursos do domínio, eliminando o fallback para NTLM e, consequentemente, resolvendo o gargalo de performance no processo LSASS identificado no diagnóstico.

A adoção do Kerberos satisfaz a categoria PR.AA (Gerenciamento de Identidade e Autenticação) da função 'Proteger' do NIST Cybersecurity Framework 2.0, especificamente a subcategoria PR.AA-03, que

determina que usuários e serviços devem ser autenticados de forma robusta antes do acesso, eliminando a vulnerabilidade de interceptação inerente ao NTLM.

Com isso, o cliente Windows 11 (Figura 18) ingressado no novo domínio pti.intra pode utilizar seu método de autenticação nativo e preferencial (Kerberos), eliminando o fallback e resolvendo a causa raiz dos travamentos e da alta utilização de disco relatada por 95,2% dos usuários.

Figura 18: Sistema operacional Windows 11 atualizado



Fonte: Os autores (2025)

4.4 MODERNIZAÇÃO DA GESTÃO

A administração do ambiente legado era caracterizada pela descentralização e pela dependência de intervenções manuais em arquivos de configuração complexos (como o smb.conf), exigindo alto nível de conhecimento técnico específico em comandos de terminal Linux. Este modelo não apenas elevava a curva de aprendizado para novos técnicos, como também aumentava o risco de erros humanos que poderiam comprometer a disponibilidade do serviço.

Com a migração para o Univention Corporate Server, a gestão da infraestrutura foi substituída pela Univention Management Console (UMC). Conforme descrito no manual do sistema, a UMC é uma interface web centralizada que integra a administração de todos os serviços do domínio, incluindo usuários, grupos, computadores, DNS e DHCP, em um único painel intuitivo (UNIVENTION, 2025). A Figura 19 ilustra a interface da UMC implementada, demonstrando a visibilidade clara dos módulos administrativos disponíveis.

A centralização da gestão via UMC facilita o atendimento à função 'Governar' (GV) do NIST CSF 2.0, permitindo que a estratégia de gestão de riscos seja monitorada e aplicada de forma consistente. Sob a ótica da ABNT NBR ISO/IEC 27001, a ferramenta apoia o controle A.5.15 (Controle de acesso), garantindo que as regras de acesso lógico aos ativos de informação sejam gerenciadas de forma auditável e centralizada, em conformidade com as diretrizes da Alta Direção.

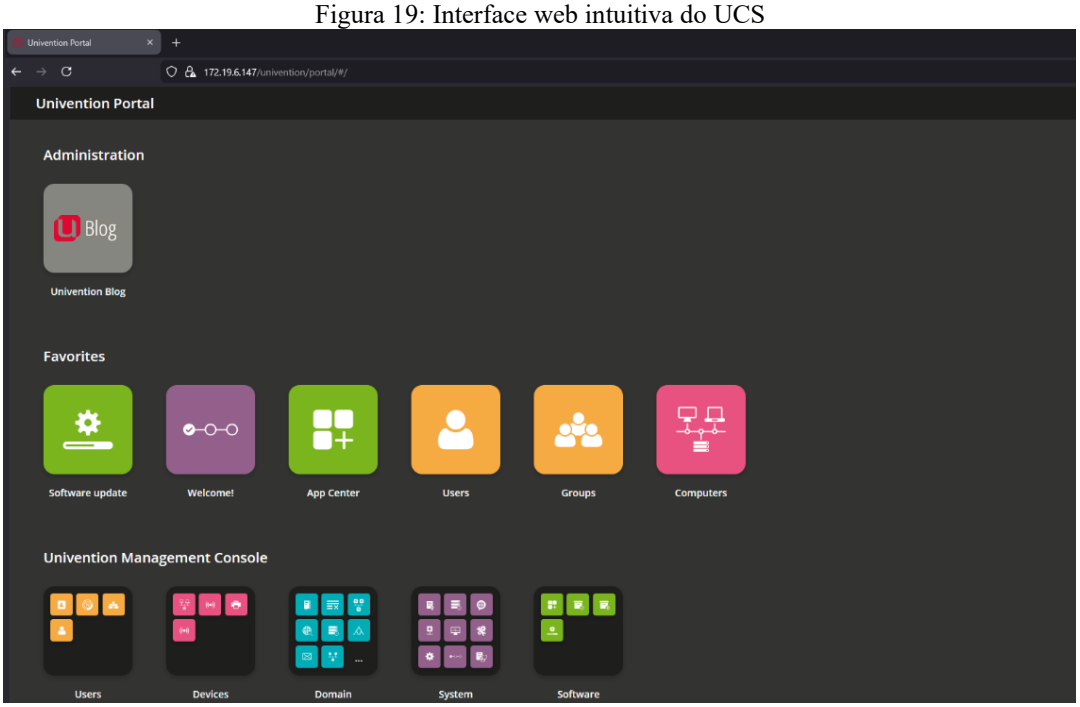
4.4.1 Acesso centralizado via interface web

O acesso à gestão do ambiente modernizado ocorre através de uma interface web centralizada, acessível via navegador (HTTPS) pelo endereço IP ou nome de domínio do servidor. De acordo com o manual do Univention Corporate Server (UNIVENTION, 2025), o ponto de entrada é a página de Portal do UCS, que fornece uma visão unificada de todos os serviços disponíveis no domínio. O processo de autenticação é realizado em uma página de login central, onde os administradores utilizam suas credenciais de domínio (como o usuário Administrator) para acessar os módulos de gestão.

O manual destaca que o sistema suporta Single Sign-On (SSO), permitindo que, após a autenticação inicial no portal, o usuário acesse as diversas aplicações e módulos administrativos (UMC) sem a necessidade de reinserir suas credenciais.

Esta arquitetura não apenas simplifica o acesso para a equipe de TI, eliminando a necessidade de ferramentas de linha de comando dispersas, mas também reforça a segurança ao centralizar o controle de sessões e identidades.

Figura 19: Interface web intuitiva do UCS



Fonte: Os autores (2025)

5 CONCLUSÃO

Este trabalho teve como objetivo geral analisar os impactos de um servidor legado Debian 7 com Samba 3.6.6 em uma repartição pública, e propor uma solução de modernização viável utilizando o Univention Corporate Server (UCS). Os resultados obtidos confirmam integralmente a hipótese de que a manutenção da infraestrutura obsoleta representa não apenas um risco de segurança, mas também um gargalo operacional ativo que prejudica a produtividade diária.

Os objetivos específicos foram alcançados e forneceram um diagnóstico claro. Foi documentado que a interoperabilidade entre o servidor Debian 7 "Wheezy" (EOL) e as estações Windows 11 exigiu a degradação deliberada da segurança, notadamente a ativação do protocolo SMBv1 e a desativação da assinatura de pacotes SMB. Esta configuração demonstrou violar diretamente os princípios da função "Proteger" do NIST CSF 2.0 e múltiplos controles da ABNT NBR ISO 27001, expondo o órgão a riscos de compliance relacionados à LGPD.

A avaliação do impacto nos usuários, baseada na ISO 9241-11, validou os dados técnicos: 95,2% dos servidores classificam o sistema como "Lento" ou "Muito lento" e 61,9% precisam reiniciar seus computadores diariamente devido a falhas. A causa raiz foi identificada nos picos de uso de disco (80%) do processo LSASS, causados pelo fallback forçado de autenticação para o protocolo NTLM, uma vez que o PDC NT4 legado não suporta Kerberos.

A proposta de modernização, detalhada e validada na seção 4, demonstrou ser uma solução eficaz. A migração para o Univention Corporate Server 5.2, atuando como um Controlador de Domínio compatível com Active Directory, resolveu simultaneamente os problemas diagnosticados. A validação técnica comprovou que os clientes passaram a se conectar usando o protocolo moderno SMB3_11 com criptografia e assinatura AES-128-GMAC ativadas. A implementação do Kerberos, nativo no UCS, eliminou o fallback para NTLM, resolvendo a causa raiz da lentidão. Além disso, o uso da UCS Core Edition, que é gratuita e permite usuários ilimitados, confirma a viabilidade econômica da solução para o setor público.

Este estudo contribui ao fornecer subsídios técnicos e quantitativos aos gestores públicos, demonstrando que o custo oculto da perda de produtividade gerado por sistemas legados justifica o investimento em modernização. A pesquisa demonstrou que é possível implementar uma infraestrutura segura, eficiente e gerenciável, promovendo a soberania tecnológica e alinhando o órgão às exigências contemporâneas de segurança da informação.

REFERÊNCIAS

ABNT. NBR ISO 9241-11:2018: Ergonomia da interação humano-sistema - Parte 11: Usabilidade: Definições e conceitos. Rio de Janeiro: ABNT, 2018.

ABNT. NBR ISO/IEC 27001:2022: Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação - Requisitos. Rio de Janeiro: ABNT, 2022.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018].

DESMOND, Brian et al. Active Directory: Designing, Deploying, and Running Active Directory. 5. ed. Sebastopol: O'Reilly Media, 2013.

MICROSOFT. Stop using SMB1. Microsoft Community, 2020. Disponível em: https://techcommunity.microsoft.com/blog/filecab/stop-using-smb1/425858. Acesso em: 20 out. 2025.

MICROSOFT. Melhorias de segurança do SMB. Microsoft Learn, 2025. Disponível em: https://learn.microsoft.com/pt-br/windows-server/storage/file-server/smb-security. Acesso em: 20 out. 2025.

MICROSOFT. Visão geral da assinatura do Bloco de Mensagens do Servidor (SMB). Microsoft Learn, 2025a. Disponível em: https://learn.microsoft.com/pt-br/windows-server/storage/file-server/smb-signing-overview. Acesso em: 20 out. 2025.

MICROSOFT. Não é possível ingressar computadores em um domínio. Microsoft Learn, 2025b. Disponível em: https://learn.microsoft.com/pt-br/previous-versions/troubleshoot/windows-server/cannot-join-computer-to-domain. Acesso em: 20 out. 2025.

MICROSOFT. Visão geral da autenticação Kerberos, 2025c. Disponível em: https://learn.microsoft.com/pt-br/windows-server/security/kerberos/kerberos-authentication-overview. Acesso em: 21 out. 2025.

MICROSOFT. Autenticação de usuário NTLM, 2025d. Disponível em: https://learn.microsoft.com/pt-br/troubleshoot/windows-server/windows-security/ntlm-user-authentication. Acesso em: 21 out. 2025.

NEMETH, Evi et al. UNIX and Linux System Administration Handbook. 4. ed. Upper Saddle River: Prentice Hall, 2011.

NHS ENGLAND. Lessons Learned Review of the WannaCry Ransomware Cyber Attack. Londres: Department of Health and Social Care, 2018. Disponível em: https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf. Acesso em: 20 out. 2025.

NIST. NIST Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology, 2024. Disponível em: https://doi.org/10.6028/NIST.CSWP.29.por. Acesso em: 21 out. 2025.

SAMBA. Hardening Samba as an AD DC, 2025. Disponível em: https://wiki.samba.org/index.php/Hardening_Samba_as_an_AD_DC#ntlm_auth. Acesso em: 21 out. 2025.

SOMMERVILLE, Ian. Engenharia de Software. 9. ed. São Paulo: Pearson Prentice Hall, 2011.

STALLINGS, William; BROWN, Lawrie. Computer Security: Principles and Practice. 3. ed. Upper Saddle River: Pearson, 2014.

TERPSTRA, John H. NT4 PDC Migration to Samba-3. In: sambaXP Conference, 2003, Göttingen. Proceedings... Göttingen: sambaXP, 2003. Disponível em: https://sambaxp.org/archive-data-samba/sxp03/terpstra-XP2003.pdf. Acesso em: 21 out. 2025.

UNIVENTION CORPORATE SERVER. Manual for users and administrators, 2025. Disponível em: https://docs.software-univention.de/manual/latest/en/index.html. Acesso em: 21 out. 2025.