Revista Tecnologia e Sociedade
ISSN: 1984-3526

https://periodicos.utfpr.edu.br/rts

Desafios da segurança cibernética: uma análise da administração pública brasileira

Jady Pâmella Barbacena da Silva
Banco Regional de Brasília (BRB), Brasília, Distrito Federal, Brasil
jadypbs@gmail.com

Lucas Vinicius Andrade Ferreira
Banco do Brasil (BB), Brasília, Distrito Federal, Brasil
lucas.vinicius@live.com

Rafael Rabelo Nunes
Universidade de Brasília (UnB), Brasília, Distrito Federal, Brasil
rafaelrabelo@unb.br

RESUMO

O cenário pós-pandemia intensificou os incidentes cibernéticos, exigindo uma gestão mais eficaz da segurança da informação na administração pública. Este estudo objetivou identificar os principais desafios na Gestão da Segurança Cibernética enfrentados pela administração pública brasileira, segundo a visão de gestores e especialistas no tema. A pesquisa caracteriza-se como aplicada, descritiva e exploratória, com abordagem qualitativa. A coleta de dados utilizou um questionário estruturado em nove construtos e trinta e cinco itens, abrangendo o universo de profissionais das esferas federal, estadual e municipal. O instrumento foi aplicado a 126 indivíduos, resultando em uma amostra final válida de 100 respondentes após o tratamento de dados incompletos ou não-respostas. A análise, realizada por meio de estatística descritiva, apontou desafios críticos como a burocracia nos processos de aquisição, a falta de padronização de processos e a urgência de mudanças culturais e estratégicas. O estudo contribui para o campo ao evidenciar o distanciamento entre as diretrizes normativas estratégicas e a realidade operacional das instituições, destacando o fator humano e a cultura organizacional como elementos fundamentais para a maturidade cibernética no setor público.

PALAVRAS-CHAVE: Governança de TI. Cultura de segurança. Ataques cibernéticos. Proteção de dados. Maturidade cibernética. Administração Pública.

INTRODUÇÃO

A segurança da informação tornou-se um tema essencial no contexto atual, em que os dados representam um ativo estratégico para organizações públicas e privadas (ADMASS; MUNAYE; DIRO, 2024). A proteção eficaz dessas informações é fundamental para garantir a continuidade dos negócios e a tomada de decisões estratégicas, uma vez que os dados permitem a construção de cenários e o entendimento dos ambientes operacionais (CULOT et al., 2021). No entanto, essas informações estão constantemente expostas a riscos, sendo consideradas um patrimônio das organizações que requer gestão e proteção adequadas (BUOGO; FACHINELLI; GIACOMELLO, 2020).

O estudo da segurança da informação é cada vez mais relevante à medida que o volume de dados aumenta e se torna mais acessível para a população (ADMASS; MUNAYE; DIRO, 2024). Nos últimos anos, testemunhou-se um aumento significativo em incidentes cibernéticos, incluindo invasões de sistemas e perdas de dados sensíveis. Esse fenômeno, em parte, decorre da falta de conhecimento por parte dos usuários sobre a importância da segurança da informação e sua aplicação prática na proteção de dados (CULOT et al., 2021). O impacto desses incidentes foi exacerbado pela pandemia de COVID-19, que expôs vulnerabilidades anteriormente não percebidas, principalmente em organizações que não estavam preparadas para a rápida adoção do trabalho remoto (GEORG et al., 2022). O aumento nos crimes cibernéticos durante esse período destacou a necessidade de uma maior conscientização e capacitação dos funcionários para lidar com as novas realidades tecnológicas (BARBOSA et al., 2021).

No setor público, os desafios são particularmente evidentes. A adoção de novas tecnologias trouxe consigo ameaças significativas, capazes de comprometer infraestruturas críticas, causar prejuízos financeiros e minar a confiança da população nas instituições governamentais (GEORG et al., 2022). Ataques cibernéticos recentes, como aqueles direcionados ao Ministério da Saúde (SILVA; OLIVEIRA, 2023) e ao Superior Tribunal de Justiça (VIEIRA, 2022), ilustram os riscos enfrentados pelas instituições públicas brasileiras. Esses incidentes sublinham a urgência de fortalecer a segurança cibernética e de padronizar as práticas de proteção em toda a administração pública federal.

A crescente importância da segurança cibernética, especialmente no setor governamental, tem sido amplamente reconhecida (ALVES et al., 2021). Conforme Hurel (2021) ressalta, cada setor desempenha um papel relevante na formulação e implementação de uma estratégia de segurança cibernética nacional. Não se trata apenas de enfrentar os ataques cibernéticos, mas de entender os principais desafios estruturais e operacionais que cada setor enfrenta para construir uma defesa eficiente (ALVES; GEORG; NUNES, 2023). Com base nessa perspectiva, o objetivo deste estudo é identificar os principais desafios na Gestão da Segurança Cibernética enfrentados pela administração pública brasileira, segundo a visão de gestores e especialistas no tema.

O trabalho foi organizado em quatro seções, iniciando com essa introdução. Em seguida, será apresentada a metodologia aplicada para obtenção e análise das informações. Posteriormente, serão apresentados os resultados obtidos e será realizada a discussão sobre os constructos identificados. Finalmente, na conclusão será apresentado um resumo dos desafios apontados pelos gestores, as contribuições do estudo e sugestão para pesquisas futuras.

A SEGURANÇA CIBERNÉTICA COMO SISTEMA SOCIOTÉCNICO: GOVERNANÇA, CULTURA E DIREITOS

A gestão da segurança cibernética na administração pública contemporânea não pode ser compreendida apenas como um desafio técnico de implementação de hardware e software (ALVES et al., 2024). A segurança da informação constitui um sistema sociotécnico complexo, no qual a eficácia das ferramentas digitais é intrinsecamente condicionada por estruturas organizacionais, valores culturais e decisões políticas (GEORG et al., 2022). A tecnologia, portanto, não é um ente neutro, mas uma construção social moldada pelas escolhas e limitações das instituições que a adotam.

Neste contexto, observa-se frequentemente um distanciamento entre a "norma ideal" (o que a legislação exige) e a "realidade operacional" (a prática quotidiana). A literatura recente demonstra que esse hiato não é exclusivo do setor público. Carvalho, Andrade e Fraga (2025), ao analisarem a adequação à Lei Geral de Proteção de Dados (LGPD) numa startup de tecnologia, identificaram que, mesmo em ambientes inovadores, a conformidade enfrenta barreiras significativas, como a falta de apoio da alta gestão e resistências culturais. Os autores destacam que a regularização não é apenas um trâmite burocrático, mas exige uma mudança de mindset e o mapeamento contínuo de processos para que a proteção de dados seja incorporada à cultura organizacional.

Essa necessidade de alinhamento entre tecnologia e processos humanos torna-se ainda mais crítica na esfera pública, onde a inovação deve respeitar estritamente os direitos fundamentais (HUREL, 2021). A introdução de novas tecnologias, como a Inteligência Artificial (IA) no Poder Judiciário, exemplifica essa tensão. Rossetti e Silva (2024) alertam que a busca pela eficiência processual não pode sobrepor-se a garantias constitucionais, como a privacidade, a isonomia e a segurança jurídica. As autoras argumentam que a governança tecnológica deve ser ética e transparente para mitigar riscos inerentes à opacidade algorítmica e aos vieses discriminatórios, garantindo que a tecnologia atue como promotora da cidadania e não como fator de exclusão.

Portanto, a segurança cibernética na administração pública atua como um mecanismo garantidor desses direitos diante da vulnerabilidade dos sistemas digitais (VIEIRA, 2022). A ineficácia muitas vezes atribuída à "falta de capacitação" dos servidores é, na verdade, sintoma de uma implementação tecnológica desarticulada dos processos sociais (ALVES et al., 2024). A maturidade em segurança cibernética depende, assim, da capacidade de construir arranjos sociotécnicos que integrem diretrizes estratégicas (como a Política Nacional de Segurança da Informação), infraestrutura robusta e o fator humano, promovendo uma governança participativa que assegure tanto a resiliência técnica quanto à conformidade ética e legal (ARAUJO; MENDES, 2025).

METODOLOGIA

Realizou-se uma pesquisa de natureza aplicada com objetivos descritivos e exploratórios. A natureza descritiva permitiu elucidar as características de uma determinada população, fenômeno ou o estabelecimento de relações entre variáveis (GIL, 2025). O viés exploratório visou obter maior familiaridade com o problema estudado e compreender os desafios da segurança cibernética no setor

público brasileiro, possibilitando a construção de hipóteses, que são características de uma pesquisa exploratória (BARDIN, 2016).

A abordagem utilizada foi predominantemente qualitativa, trabalhando com universos de significados, motivos, aspirações, crenças, valores, atitudes, correspondendo a um espaço mais profundo de relações, processos e fenômenos que não podem ser reduzidos à operacionalização de variáveis (GIL, 2025).

O universo da pesquisa compreende profissionais atuantes na gestão de segurança da informação e segurança cibernética que atendem ao setor público. O questionário foi respondido por 126 indivíduos, entretanto, após cortes de não-respostas ou dados incompletos, o número final válido totalizou 100 respondentes. A amostra caracterizou-se como não probabilística por conveniência. Em relação à representatividade institucional, a amostra abrange órgãos das esferas federal, estadual e municipal, com foco analítico predominante na Administração Pública Federal. Os participantes representam segmentos distintos, englobando majoritariamente o Poder Executivo, além do Poder Judiciário, uma participação minoritária do Poder Legislativo e funcionários do setor privado ou terceiro setor que atuam como fornecedores para a Administração Pública. Não é disponibilizada uma lista nominal dos órgãos ou dos cargos específicos dos entrevistados, visto que a metodologia assegurou o anonimato das instituições e dos participantes para garantir a isenção nas respostas.

A coleta de dados ocorreu entre os meses de janeiro e março de 2023, por meio de um questionário construído com base nos construtos e itens sobre os Desafios da Segurança Cibernética no Setor Público propostos por Georg et al. (2022). Optou-se pelo uso do questionário para alcançar um público amplo interessado no tema, o que não seria viável com outras formas de coleta de dados. O instrumento continha questões fechadas, utilizando uma escala do Likert de 5 pontos, com opções que variavam de discordo totalmente a concordo totalmente (FEIJÓ et al., 2020). Também foi incluída a opção não sei/não quero responder para os participantes que indicassem desconhecimento sobre o assunto. Ao final do questionário foi facultada a opção de colocar observações sobre os desafios que não foram abordados no questionário. Elas trazem uma opinião pessoal de alguns respondentes, reforçando desafios citados e trazendo novos, que poderão ser utilizados para trabalhos futuros.

A análise dos dados do questionário foi realizada por meio de estatística descritiva para as questões fechadas. Para fins de interpretação, as respostas foram agrupadas em macrocategorias de "discordância" (agrupando discordo totalmente e discordo) e "concordância" (agrupando concordo e concordo totalmente) , excluindo-se do cálculo percentual as abstenções e respostas neutras. O recorte analítico aprofundou a compreensão do fenômeno ao segmentar os resultados pelo tempo de experiência, comparando profissionais com até 5 anos de atuação versus aqueles com mais de 5 anos.

RESULTADOS E DISCUSSÕES

Os resultados serão apresentados a seguir, seguindo a ordem dos construtos propostos por Georg et al. (2022).

Infraestrutura de TI (Tecnologia da Informação)

Na Tabela 1 apresenta-se os resultados de Infraestrutura de TI. Pode-se perceber a diferença entre as respostas dos respectivos grupos. Para o segundo grupo, por haver mais tempo de atuação na área, parte dos respondentes discordam quanto aos equipamentos estarem defasados, não haver investimentos em softwares adequados e a infraestrutura ser inadequada. Para ambos os grupos, os processos de aquisição são burocráticos e há necessidade de padronização dos processos de trabalho.

Os grupos concordam na necessidade do aumento de relevância das ações de TI. E embora para muitos os equipamentos não estejam defasados, há a prevalência em concordar que os softwares estão desatualizados.

Tabela 1 – Resultados do construto Infraestrutura de TI

	Item do construto Infraestrutura de TI	Até 5 anos		Mais que 5 anos			
		Concordam	Discordam	Concordam	Discordam	Não opinaram	Não concordam / Não discordam
1	Equipamentos defasados	76% (44)	24% (14)	65% (22)	35% (12)	1% (1)	7% (7)
2	Falta de investimentos em *softwares* adequados	75% (41)	25% (14)	74% (25)	26% (9)	2% (2)	9% (9)
3	Burocracia no processo de aquisição	96% (50)	4% (2)	97% (30)	3% (1)	5% (5)	12% (12)
4	Necessidade de padronização de processos de trabalho	95% (55)	5% (3)	97% (31)	3% (1)	1% (1)	9% (9)
5	Aumento de relevância das ações de TI	90% (51)	10% (6)	91% (30)	9% (3)	4% (4)	6% (6)
6	*Softwares* desatualizados	89% (50)	11% (6)	90% (27)	10% (3)	2% (2)	12% (12)
7	Inadequação da infraestrutura de TI	78% (43)	12% (12)	80% (24)	20% (6)	3% (3)	12% (12)

Fonte: os Autores

Falta de investimento em softwares adequados obteve menor concordância, indicando que os principais problemas de infraestrutura de TI estão ligados à burocracia e à falta de padronização dos processos. Segundo Silva; Pinheiro (2013), processos bem definidos em TI garantem operações eficientes, efetivas e em conformidade com as legislações vigentes.

A infraestrutura de TI é fundamental para a eficiência em segurança cibernética, e para a rápida e segura execução dos serviços (LIMA; DA MATA SÁ; PESSOA, 2024). A falta de investimento em melhorias e novos sistemas prejudica o funcionamento e progresso nesse setor, e compromete a segurança dos dados. Além de equipamentos avançados, é essencial ter equipes qualificadas para operá-los adequadamente (VIANNA, 2020).

Estrutura de TI

Na Tabela 2 apresentam-se os resultados de Estrutura de TI. Ambos os grupos concordam que as portarias do Gabinete de Segurança Institucional (GSI) têm abrangência limitada e não são operacionais, especialmente destacando a falta de autonomia para coordenação. Há unanimidade na percepção de falta de padrões para parâmetros de controle e metodologias entre todos os profissionais. Ressalta-se a importância do compartilhamento de boas práticas e a necessidade de orientações práticas para os gestores.

Tabela 2 – Resultados do construto Estrutura de TI

	Item do construto Estrutura de TI	Até 5 anos		Mais que 5 anos			
		Concordam	Discordam	Concordam	Discordam	Não opinaram	Não concordam / Não discordam
1	Portarias não operacionais e com pequena abrangência	79% (38)	21% (10)	73% (19)	21% (5)	4% (4)	24% (24)
2	Não possui autonomia necessária para coordenação	81% (42)	19% (10)	73% (19)	27% (7)	1% (1)	21% (21)
3	Carência de padrão de parâmetros de controle e metodologias	84% (48)	16% (9)	86% (24)	14% (4)	2% (2)	13% (13)
4	Necessidade de compartilhamento de boas práticas	93% (52)	7% (4)	86% (25)	14% (4)	1% (1)	14% (14)
5	Carência por parte dos gestores, de orientações práticas	95% (55)	5% (3)	81% (26)	19% (6)	0% (0)	10% (10)

Fonte: os Autores

Devido à constante evolução dos ataques contra a administração pública, o compartilhamento de boas práticas pode levar à criação de novos modelos de segurança. VIANNA (2020) argumenta que, mesmo com equipamentos de última geração e infraestruturas avançadas, sem a presença de recursos humanos qualificados, é desafiador estabelecer uma capacidade efetiva de segurança cibernética. Isso sublinha a importância da orientação adequada dos gestores e do compartilhamento de boas práticas para o sucesso da área.

Bueno et al. (2021) destaca que, em um contexto próximo ao do Brasil, mais de 75% dos países da América Latina carecem de planos críticos para a proteção de suas infraestruturas contra ciberataques. É necessário que governos invistam mais recursos no fortalecimento dessas estruturas para mitigar os potenciais impactos sociais e econômicos decorrentes de incidentes cibernéticos.

Georg et al. (2022) identificaram que a estrutura atual de segurança cibernética no país é insuficiente, ressaltando a necessidade de um órgão central que coordene de forma eficaz as ações, além da carência de incentivos para a criação de entidades específicas voltadas para essa área. É necessário fortalecer as Equipes de Respostas à Incidentes (ETIRs).

Governança de TI

Na Tabela 3 apresentam-se os resultados do constructo Governança de TI. Ao contrário de outros tópicos, a divergência entre os grupos foi maior. O segundo grupo apresentou porcentagens de divergência em relação ao primeiro grupo. Como a governança é incipiente e inexistente e as áreas estratégicas não consideram a segurança cibernética como um ponto fundamental, o grupo de profissionais mais experientes, devido ao tempo de experiência na área, ficou parcialmente dividido. O mesmo ocorreu quando se tratou do distanciamento dos gestores da alta administração e da falta de uma política específica de segurança cibernética.

Tabela 3 – Resultados do construto Governança

	Item do construto Governança	Até 5 anos		Mais que 5 anos			
		Concordam	Discordam	Concordam	Discordam	Não opinaram	Não concordam / Não discordam
1	Áreas estratégicas não percebem a Segurança Cibernética como ponto elementar	87% (45)	13% (7)	67% (22)	33% (11)	4% (4)	11% (11)
2	Governança é incipiente ou inexistente	74% (34)	26% (12)	57% (16)	43% (12)	3% (3)	15% (15)
3	O controle de processos de TI não é efetivo	78% (43)	22% (12)	77% (20)	23% (6)	7% (7)	3% (3)
4	Distanciamento dos gestores da alta administração	84% (47)	16% (9)	71% (24)	29% (10)	6% (6)	11% (11)
5	Falta de política específica/ modelo de governança da Segurança Cibernética	98% (40)	2% (1)	68% (21)	32% (10)	8% (8)	10% (10)

Fonte: os Autores

A maioria dos respondentes acredita que as áreas estratégicas não veem a Segurança Cibernética como fundamental, o que gera um distanciamento dos gestores de alto nível. Esse afastamento entre o estratégico e o operacional compromete a eficiência da área. A governança envolve mecanismos para alcançar objetivos.

A dificuldade de engajamento da alta administração não é exclusiva do setor público tradicional. Carvalho, Andrade e Fraga (2025) identificaram desafio similar no setor privado, observando que a falta de apoio da liderança e a resistência cultural são entraves críticos para a adequação à LGPD. Isso sugere que a segurança da informação demanda uma mudança de mindset que transcende o tipo de organização, exigindo que a conformidade deixe de ser vista como um entrave burocrático para ser assumida como valor estratégico.

A efetiva gestão ou governança da segurança da informação depende do comprometimento de todos os usuários na aplicação das normas e procedimentos estabelecidos (ADMASS; MUNAYE; DIRO, 2024). A falta de integração entre os níveis operacional e estratégico resulta em estratégias desconectadas da realidade organizacional, o que compromete a governança ao torná-la desatualizada ou desalinhada com as necessidades da entidade.

Paludo; Oliveira (2024) destaca que a perda de governança pode ter um impacto significativamente grave sobre a estratégia organizacional, comprometendo a capacidade da instituição de cumprir sua missão e alcançar seus objetivos. Esse enfraquecimento da governança pode resultar na incapacidade de atender aos requisitos de segurança.

Ataques Cibernéticos

Na Tabela 4 apresentam-se os resultados do constructo Ataques Cibernéticos. Profissionais com menos de cinco anos de experiência, percebem que os ataques mais comuns são focados na obtenção de dados, enquanto aqueles com mais experiência veem os ataques como recorrentes e voltados para prejudicar a imagem do órgão. Ambos os grupos concordam sobre a necessidade de demonstrar capacidade de proteção, mas discordam que os órgãos tenham condições de se defender contra grupos mais avançados.

Tabela 4 – Resultados do construto Ataques Cibernéticos

	Item do construto Ataques Cibernéticos	Até 5 anos		Mais que 5 anos			
		Concordam	Discordam	Concordam	Discordam	Não opinaram	Não concordam / Não discordam
1	Os ataques são comuns, com foco em obter dados	84% (42)	16% (8)	75% (24)	25% (8)	8% (8)	10% (10)
2	Foco na imagem do órgão	79% (34)	21% (9)	88% (22)	12% (3)	10% (10)	22% (22)
3	Necessidade de demonstrar capacidade de proteção	93% (40)	7% (3)	90% (28)	10% (3)	9% (9)	17% (17)
4	Há protocolos para mitigar os riscos	76% (35)	24% (11)	83% (29)	17% (6)	9% (9)	10% (10)
5	Os órgãos tem capacidade de promover a defesa contra grupos mais avançados	44% (20)	56% (25)	67% (18)	33% (9)	12% (12)	16% (16)

Fonte: os Autores

Profissionais experientes reconhecem a existência de protocolos para mitigar riscos cibernéticos, mas destacam a necessidade de atualizá-los devido ao surgimento de novos tipos de ataques. Dados da E-Ciber mostram a vulnerabilidade da segurança cibernética no Brasil, onde apenas 11% dos órgãos da Administração Pública Federal apresentam um bom nível de governança de TI.

Em 2020, o Brasil foi o segundo país com maiores perdas financeiras devido a ataques cibernéticos (BRASIL, 2020).

Cultura

Na Tabela 5, apresentam-se os resultados do construto Cultura. Todos os grupos concordam que é essencial mudar a cultura dos hábitos e estratégias de segurança cibernética, considerando essa mudança mais importante do que as próprias tecnologias. Alguns respondentes destacam que a cultura de TI não é secundária, mas precisa ser mais valorizada por gestores e servidores.

Tabela 5 – Resultados do construto Cultura

	Item do construto Cultura	Até 5 anos		Mais que 5 anos			
		Concordam	Discordam	Concordam	Discordam	Não opinaram	Não concordam / Não discordam
1	Mudança cultural é importante, podendo ser mais relevante que tecnologias e práticas	94% (56)	6% (4)	97% (31)	3% (1)	1% (1)	7% (7)
2	Cultura de TI é considerada secundária	74% (45)	26% (16)	79% (23)	21% (6)	3% (3)	7% (7)
3	Necessidade na mudança de hábitos, assim como de estratégias em tratarem a segurança cibernética como fundamental	98% (61)	2% (1)	94% (30)	6% (2)	3% (3)	3% (3)

Fonte: os Autores

Ferreira (2025) destaca que mudanças na cultura organizacional devem iniciar na alta administração. Essa liderança é fundamental para criar uma cultura de segurança cibernética que combine preocupações operacionais com o desenvolvimento de políticas, garantindo um alinhamento estratégico, conforme aponta Hurel (2021) e Ferreira (2025).

Georg et al. (2022) observam que muitos colaboradores ainda veem a segurança cibernética como um setor isolado com funções específicas, subestimando a importância da cultura de TI, o que prejudica a estrutura de TI da entidade.

Capacitação e Sensibilização

Na Tabela 6, apresentam-se os resultados do construto Capacitação e Sensibilização. Os tópicos desse constructo apresentaram alto índice de concordância entre os grupos, que reconhecem a insuficiência de formação dos gestores de TI e o baixo investimento em cursos avançados. Isso reflete a

percepção de pouca visibilidade da área de segurança cibernética. É enfatizado que investir em programas educacionais sobre segurança cibernética é fundamental para diminuir os riscos para empresas e sociedade (BRASIL, 2020).

Tabela 6 – Resultados do construto Capacitação e Sensibilização

	Item do construto Capacitação e Sensibilização	Até 5 anos		Mais que 5 anos			
		Concordam	Discordam	Concordam	Discordam	Não opinaram	Não concordam / Não discordam
1	Falta de foco na capacitação dos gestores de TI, com poucos investimentos em cursos sofisticados	86% (49)	14% (8)	87% (27)	13% (4)	3% (3)	9% (9)
2	Falta de visibilidade por parte das áreas estratégicas quanto aos investimentos em capacitação de segurança cibernética	84% (47)	16% (9)	80% (24)	20% (6)	4% (4)	10% (10)
3	Necessidade de engajamento em relação à segurança cibernética por parte dos servidores, sendo o lado humano o mais vulnerável	93% (52)	7% (4)	87% (28)	13% (4)	6% (6)	6% (6)
4	Escassez em recursos voltados para à área de segurança cibernética	82% (37)	18% (8)	78% (25)	22% (7)	5% (5)	18% (18)

Fonte: os Autores

Alves et al. (2024) argumentam que a segurança da informação depende tanto de conhecimento quanto de cooperação humana, destacando a importância da conscientização sobre a cooperação adequada e o compromisso com o conhecimento, sem os quais as técnicas de segurança podem falhar.

Investir em cursos e treinamentos para profissionais de segurança não é um custo, mas um investimento essencial para mitigar riscos e ataques futuros. Os investimentos devem visar não apenas uma postura preventiva ou reativa, mas também consultiva, aumentando a confiança nas áreas finalísticas (BRASIL, 2020). Também se recomenda a criação de políticas públicas que promovam a conscientização sobre ameaças cibernéticas e estimulem comportamentos responsáveis e seguros entre os usuários.

Legislação

Na Tabela 7, apresentam-se os resultados do construto Legislação. Há um consenso sobre a preocupação do Estado brasileiro com a legislação na área de

cibernética. Ambos concordam que a maturidade do Brasil em relação ao tema é boa, mas reconhecem que há lacunas significativas em questões específicas.

Tabela 7 – Resultados do construto Legislação

	Item do construto Legislação	Até 5 anos		Mais que 5 anos			
		Concordam	Discordam	Concordam	Discordam	Não opinaram	Não concordam / Não discordam
1	Há preocupação por parte do Estado em relação ao tema	62% (28)	38% (17)	62% (20)	38% (8)	9% (9)	18% (18)
2	A legislação normativa brasileira possui um bom nível de maturidade, mas ainda com grandes lacunas, e muitas vezes com temas muito específicos	76% (37)	24% (12)	74% (17)	26% (6)	10% (10)	18% (18)

Fonte: os Autores

Os resultados mostram que, apesar do reconhecimento de uma legislação brasileira madura em termos de segurança cibernética, as leis frequentemente focam em temas específicos e não cobrem o contexto geral de segurança, trazendo mais burocracia do que soluções práticas. Há uma preocupação estratégica do Estado com as leis, mas são necessárias mais ações operacionais.

Diante dos avanços tecnológicos e das novas necessidades em segurança da informação, é essencial desenvolver marcos legais que regulamentem o uso do espaço cibernético para prevenir conflitos e danos. Políticas públicas eficazes de controle são vitais para combater ataques cibernéticos, conforme sugere Da Silva (2024).

Silva (2021) aborda o aspecto jurídico relacionado aos crimes virtuais, enfatizando a evolução da legislação brasileira para se adaptar às novas demandas do cenário digital contemporâneo. À medida que os crimes informáticos se tornaram mais frequentes e sofisticados, foi necessário que o arcabouço jurídico acompanhasse essa transformação, estabelecendo normas mais rigorosas e específicas para lidar com essas infrações.

Embora a legislação forneça o arcabouço necessário, a aplicação prática exige cautela, especialmente com a introdução de novas tecnologias. Rossetti e Silva (2024) reforçam que a inovação no setor público, como a digitalização e o uso de IA no Judiciário, deve ser acompanhada de uma observância estrita aos direitos fundamentais. A segurança cibernética, portanto, atua como garantidora desses direitos (como a privacidade e o devido processo legal) diante da vulnerabilidade dos sistemas digitais.

E-Ciber (Estratégia Nacional de Cibersegurança)

Na Tabela 8, apresentam-se os resultados do construto E-Ciber. Nota-se que os profissionais do primeiro grupo, comparativamente ao segundo, concordam mais sobre a importância do documento para o desenvolvimento da área, e de que muitos gestores desconhecem o tema, o que resulta na não aplicação das diretrizes práticas.

Tabela 8 – Resultados do construto E-Ciber

	Item do construto E-Ciber	Até 5 anos		Mais que 5 anos			
		Concordam	Discordam	Concordam	Discordam	Não opinaram	Não concordam / Não discordam
1	A E-Ciber foi um importante documento para o desenvolvimento da Segurança Cibernética no Brasil, ajudando a justificar investimentos na área	94% (32)	6% (2)	79% (15)	21% (4)	25% (25)	21% (21)
2	As diretrizes não são operacionais, afastando a estratégia da realidade nas instituições	68% (19)	32% (9)	75% (12)	25% (4)	21% (21)	35% (35)
3	Quanto a sua colocação na prática, há gestores que não tiveram conhecimento	94% (32)	6% (2)	96% (24)	4% (1)	19% (19)	22% (22)
4	Poucos órgãos colocaram suas diretrizes em prática	94% (32)	6% (2)	91% (21)	9% (2)	22% (22)	21% (21)

Fonte: os Autores

De acordo com Brustolin, Nunes e de Assunção (2023), a defesa cibernética pode ser entendida como uma camada acima da segurança cibernética, desempenhando um papel fundamental na garantia da continuidade dos processos e atividades organizacionais, assegurando que estes operem de forma livre de ameaças e interrupções.

O E-Ciber, foi um marco normativo importante para a defesa do país e segurança cibernética na administração pública, que estabeleceu diretrizes essenciais para orientar órgãos e entidades. Essas diretrizes destacam a importância da área e justificam os investimentos feitos. No entanto, apesar da relevância, muitos gestores não estavam cientes dessas diretrizes, resultando em uma implementação limitada nos órgãos. Essa desconexão entre a estratégia e a realidade operacional causa danos significativos, aumentando os riscos e evidenciando que a legislação brasileira ainda está distante da prática efetiva (ALVES et al., 2021).

Cooperação Internacional

Na Tabela 9, apresentam-se os resultados do construto Cooperação Internacional. Ambos os grupos reconhecem a importância da cooperação internacional para o Brasil, um objetivo destacado pela E-Ciber. Embora não haja consenso sobre a independência do Brasil nessa área, é notável que o país tem uma postura proeminente em segurança cibernética na América Latina, atuando como um líder regional (BRASIL, 2020).

Tabela 9 – Resultados do construto Cooperação Internacional

	Item do construto Cooperação Internacional	Até 5 anos		Mais que 5 anos			
		Concordam	Discordam	Concordam	Discordam	Não opinaram	Não concordam / Não discordam
1	A cooperação internacional é fundamental com destaque na OCDE (Organização Para Cooperação E Desenvolvimento Econômico)	100% (37)	0% (0)	90% (20)	10% (2)	18% (18)	23% (23)
2	O Brasil possui uma postura independente, e a cooperação não é percebida como uma prática corriqueira	65% (28)	35% (15)	89% (17)	11% (2)	22% (22)	16% (16)

Fonte: os Autores

Setiabudi e Sumadinata (2023) enfatizam que os desafios relacionados ao tratamento de crimes cibernéticos e ameaças à segurança global não podem ser solucionados de forma isolada por um único país. A colaboração entre nações no domínio da informação e da tecnologia é fundamental para o fortalecimento da segurança cibernética, permitindo a construção de estratégias mais robustas e abrangentes na proteção contra ameaças globais.

A postura conciliatória e pacífica do Brasil resulta em acordos bilaterais com outros países, especialmente vizinhos, facilitando a cooperação e o compartilhamento de boas práticas para combater crimes cibernéticos, ataques a infraestruturas críticas e espionagem cibernética (BRASIL, 2020). Contudo, é vital manter a soberania nacional, especialmente em relação a dados sigilosos e críticos.

O Brasil mantém uma postura independente, sem vínculos exclusivos com países ou blocos econômicos, interagindo com todos. Isso mostra que a cooperação internacional é fundamental para o progresso na área cibernética, mas a sensibilidade do tema exige consideração de vários fatores (ARAUJO; MENDES, 2025).

Principais Desafios

Na Tabela 10, encontram-se os desafios por ordem de prioridade conforme percepção dos respondentes. Os principais problemas enfrentados são a infraestrutura e a estrutura de TI, a cultura organizacional e a E-Ciber. Também se ressalta uma preocupação quanto ao aprofundamento e compreensão em temas como Legislação, E-Ciber e Cooperação Internacional, onde se notou um volume significativo de não respostas, refletindo a falta de conhecimento ou interesse dos participantes nessas áreas.

Tabela 10 – Principais desafios conforme percepção dos respondentes

	Item	Principais desafios	(%)
1	5.3	Necessidade na mudança de hábitos, assim como de estratégias em tratarem a segurança cibernética como fundamental	97%
2	9.1	A cooperação internacional é fundamental com destaque na OCDE	97%
3	1.3	Burocracia no processo de aquisição	96%
4	1.4	Necessidade de padronização de processos de trabalho	96%
5	8.3	Quanto a sua colocação na prática, há gestores que não tiveram conhecimento	95%
6	5.1	Mudança cultural é importante, podendo ser mais relevante que tecnologias e práticas	95%
7	8.4	Poucos órgãos colocaram suas diretrizes em prática	93%
8	4.3	Necessidade de demonstrar capacidade de proteção	92%
9	2.4	Necessidade de compartilhamento de boas práticas	91%
10	6.3	Necessidade de engajamento em relação à segurança cibernética por parte dos servidores, sendo o lado humano o mais vulnerável	91%
11	1.6	*Softwares* desatualizados	90%
12	2.2	Não possui autonomia necessária para coordenação	90%
13	1.5	Aumento de relevância das ações de TI	90%
14	3.4	Distanciamento dos gestores da alta administração	89%
15	8.1	A E-Ciber foi um importante documento para o desenvolvimento da Segurança cibernética no Brasil, ajudando a justificar investimentos na área	89%
16	6.1	Falta de foco na capacitação dos gestores de TI, com poucos investimentos em cursos sofisticados	86%
17	2.3	Carência de padrão de parâmetros de controle e metodologias	85%
18	6.2	Falta de visibilidade por parte das áreas estratégicas quanto aos investimentos em capacitação de segurança cibernética	83%
19	4.2	Foco na imagem do órgão	82%
20	6.4	Escassez em recursos voltados para área de segurança cibernética	81%
21	4.1	Os ataques são comuns, com foco em obter dados	80%
22	1.3	Inadequação da infraestrutura de TI	79%
23	4.4	Há protocolos para mitigar riscos	79%
24	3.1	Áreas estratégicas não percebem a Segurança Cibernética como ponto elementar	79%

	Item	Principais desafios	(%)
25	2.1	Portarias não operacionais e com pequena abrangência	78%
26	3.3	O controle de processos de TI não é efetivo	78%
27	5.2	Cultura de TI é considerada secundária	76%
28	7.2	A legislação normativa brasileira possui um bom nível de maturidade, mas ainda com grandes lacunas, e muitas vezes com temas específicos	75%
29	1.2	Falta de investimentos em *softwares* adequados	74%
30	3.5	Falta de política específica/ modelo de governança da Segurança Cibernética	73%
31	1.1	Equipamentos defasados	72%
32	8.2	As diretrizes não são operacionais, afastando a estratégia da realidade nas instituições	70%
33	3.2	Governança é incipiente ou inexistente	68%
34	7.1	Há a preocupação por parte do Estado em relação ao tema	66%
35	4.5	Os órgãos tem capacidade de promover defesa contra grupos mais avançados	53%

Fonte: os Autores

Desafios Adicionais Apontados nas Observações do Questionário

Além dos desafios previamente identificados, uma análise das respostas abertas dos participantes revelou questões adicionais que merecem destaque na gestão da segurança cibernética. Esses achados complementam os constructos abordados no estudo e trazem novas perspectivas sobre os desafios enfrentados pelas organizações públicas no Brasil. A Figura 1 apresenta uma nuvem de palavras elaborada com base nas respostas abertas dos participantes.

Figura 1 – Nuvem de palavras elaborada com utilizando-se as respostas adicionais dos participantes da pesquisa

Os respondentes destacaram a desvalorização dos profissionais de TI no setor público, com ausência de concursos e alta evasão para o setor privado, comprometendo a qualidade da segurança cibernética. Além da falta de pessoal capacitado, foram citados altos custos de treinamento e poucos programas acessíveis de qualificação. Também foi apontada a necessidade de maior cooperação entre órgãos públicos, criação de repositórios digitais e grupos de estudos para enfrentar as ameaças cibernéticas. O patrocínio da alta

administração é visto como essencial, mas frequentemente falta apoio estratégico e investimentos. A conscientização sobre a importância da segurança cibernética ainda é insuficiente, afetando a percepção dos impactos econômicos e de reputação dos incidentes, sendo necessário fortalecer essa cultura.

CONSIDERAÇÕES FINAIS

A segurança cibernética é essencial para qualquer entidade ou organização. Contudo, ela não deve ser compreendida apenas como uma blindagem técnica, mas como um sistema sociotécnico complexo. Sua implementação efetiva assegura a proteção e integridade dos dados e informações, garantindo a confiança pública e a continuidade dos serviços estatais. No contexto da administração pública federal, sua importância é vital para o funcionamento adequado das instituições e defesa contra ataques cibernéticos.

Este estudo identificou os principais desafios na Gestão da Segurança Cibernética que a administração pública deve superar, segundo a visão de gestores e especialistas no assunto. Os desafios identificados incluem a necessidade de considerar a segurança cibernética como fundamental, integrando-a ao planejamento estratégico.

Muitos respondentes relataram que, apesar das leis, diretrizes e portarias existirem, elas não são efetivamente aplicadas por falta de conhecimento. Além disso, a aplicação é restrita pela ausência de orientações claras. Isso evidencia um hiato entre a "norma ideal" e a "realidade operacional", típico de processos onde a tecnologia é inserida sem a devida articulação com os processos sociais. A falta de comunicação entre gestores e servidores enfatiza a necessidade de maior integração entre estratégias e operações, promovendo não apenas alinhamento, mas também a implementação efetiva das normas e do conhecimento sobre o tema. Nesse sentido, a governança cibernética deve ser ética e transparente, respeitando direitos fundamentais como a privacidade e a segurança jurídica

A pesquisa destacou um alto número de não respostas relacionadas à questão, o que pode indicar um desconhecimento latente sobre o tema. Outro aspecto relevante é a cultura de segurança cibernética. A falta de uma cultura robusta, aliada ao desconhecimento de sua importância fundamental, faz com que muitos servidores negligenciem a segurança, evitando práticas de proteção e sendo descuidados em suas funções. O fator humano é o mais vulnerável, e mudanças culturais nesse sentido podem trazer resultados mais significativos do que simples tecnologias. Portanto, a solução exige uma governança participativa que deixe de ver o servidor apenas como falha de segurança e o integre como parte ativa da defesa institucional.

Os resultados mencionados e apresentados refletiram a análise de uma centena de respostas de profissionais com experiência direta com a segurança cibernética. Dessa forma, é importante ressaltar que os resultados apresentados naturalmente tem limitações quanto a amostra, e de que esse artigo, não buscou esgotar o debate sobre os desafios da segurança cibernética, mas sim explorar a diversidade de opiniões, envolvendo gestores e servidores experientes. Isso permitiu uma visão mais ampla do estado atual da área, identificando oportunidades de melhoria e desenvolvimento da segurança cibernética no Brasil.

Futuramente, novos questionários poderiam avaliar progressos e incluir novos fatores emergentes, como a melhor integração e aplicação de leis e diretrizes nos níveis operacionais, bem como investigar como a cultura de segurança é percebida

pelos servidores na ponta da operação e o impacto de novas tecnologias emergentes na resiliência das instituições públicas.

Cybersecurity Challenges: An Analysis of the Brazilian Public Administration

ABSTRACT

The post-pandemic landscape has intensified cyber incidents, demanding more effective information security management within public administration. This study aimed to identify the main challenges faced in Brazilian cybersecurity management from the perspective of managers and specialists. The research is characterized as applied, descriptive, and exploratory, with a qualitative approach. Data collection employed a questionnaire structured around nine constructs and thirty-five items, covering professionals from federal, state, and municipal levels. The instrument was administered to 126 individuals, resulting in a final valid sample of 100 respondents after processing incomplete data or non-responses. Descriptive statistical analysis identified bureaucracy in acquisition processes, lack of process standardization, and the urgency for cultural and strategic changes as critical challenges. The study contributes to the field by highlighting the gap between strategic normative guidelines and the operational reality of institutions, emphasizing the human factor and organizational culture as fundamental elements for cybersecurity maturity in the public sector.

KEYWORDS: IT Governance. Security culture. Cyberattacks. Data protection. Cyber maturity. Public Administration.

REFERÊNCIAS

ADMASS, W. S.; MUNAYE, Y. Y.; DIRO, A. A. Cyber security: state of the art, challenges and future directions. Cyber Security and Applications, [S. l.], v. 2, p. 100031, jan. 2024. Disponível em: https://doi.org/10.1016/j.csa.2023.100031. Acesso em: 6 dez. 2025.

ALVES, A. A.; ALVES, C. A. de M.; TABOSA, F. G. F.; NUNES, R. R. Riscos da computação em nuvem: estudo na ótica dos gestores de órgãos públicos federais no Brasil. Navus: Revista de Gestão e Tecnologia, Florianópolis, v. 11, p. 01-18, 2021. Disponível em: https://doi.org/10.22279/navus.2021.v11.p01-18.1513. Acesso em: 6 dez. 2025.

ALVES, A. R. N.; ALVES, J. M. H.; VASCONCELOS, I. O.; CRUZ, C. A. B. da. Fator humano na segurança da informação: um mapeamento dos comportamentos de risco no ambiente digital. Texto Livre, Belo Horizonte, v. 17, p. e51184, 2024. Disponível em: https://periodicos.ufmg.br/index.php/textolivre/article/view/51184. Acesso em: 6 dez. 2025.

ALVES, R. S.; GEORG, M. A. C.; NUNES, R. R. Judiciário sob ataque hacker: riscos de negócio para segurança cibernética em tribunais brasileiros. RISTI: Revista Ibérica de Sistemas e Tecnologias de Informação, [S. l.], n. E56, p. 344–357, fev. 2023. Disponível em: https://www.risti.xyz/issues/ristie56.pdf. Acesso em: 6 dez. 2025.

ARAUJO, M.; MENDES, A. Cibersegurança como soberania nacional? Perspectivas do Brasil e da China. Liinc em Revista, Rio de Janeiro, v. 21, n. 1, p. e7548, 2025. Disponível em: https://doi.org/10.18617/liinc.v21i1.7548. Acesso em: 6 dez. 2025.

BARBOSA, J. S. et al. Data protection and information security in the pandemic COVID-19: national context. Research, Society and Development, [S. l.], v. 10, n. 2, p. e40510212557, 2021. Disponível em: https://doi.org/10.33448/rsd-v10i2.12557. Acesso em: 6 dez. 2025.

BARDIN, L. Análise de conteúdo. São Paulo: Edições 70, 2016.

BRASIL. Ministério da Defesa. Livro Branco de Defesa Nacional: Brasil 2024. Brasília, DF: Ministério da Defesa, 2020. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/ajuste-01/estado_e_defesa/livro_branco/Versaodolivroemportugues2020.pdf. Acesso em: 6 dez. 2025.

BRASIL. Presidência da República. Decreto nº 10.222, de 5 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética. Diário Oficial da União: seção 1, Brasília, DF, ed. 26, p. 1, 6 fev. 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm. Acesso em: 6 dez. 2025.

BRUSTOLIN, V.; NUNES, I. A.; DE ASSUNÇÃO, J. Z. Análise estrutural das estratégias de segurança cibernética do Brasil e dos Estados Unidos. Revista Brasileira de Estudos de Defesa, [S. l.], v. 9, n. 2, p. 227–254, 2023. Disponível em: https://doi.org/10.26792/rbed.v9n2.2022.75246. Acesso em: 6 dez. 2025.

BUENO, P. H. M.; MOREIRA, F. R.; LIMA, E. O.; NUNES, R. R. A utilização dos frameworks Nist CSF e da série NBR ABNT ISO 27.000 no contexto da Gestão da Segurança da Informação. In: ENCONTRO NACIONAL DE CURSOS DE GRADUAÇÃO

EM ADMINISTRAÇÃO, 32., 2021, Fortaleza. Anais. Fortaleza: ANGRAD, 2021. Disponível em: https://www.researchgate.net/publication/360082614_A_UTILIZACAO_DOS_FRAMEWORKS_NIST_CSF_E_DA_SERIE_NBR_ABNT_ISO_27000_NO_CONTEXTO_DA_GESTAO_DA_SEGURANCA_DA_INFORMACAO. Acesso em: 6 dez. 2025.

BUOGO, M.; FACHINELLI, A. C.; GIACOMELLO, C. P. Gestão do conhecimento e segurança da informação: uma análise bibliométrica da produção científica. AtoZ: novas práticas em informação e conhecimento, Curitiba, v. 8, n. 2, p. 49-59, 2020. Disponível em: https://doi.org/10.5380/atoz.v8i2.69867. Acesso em: 6 dez. 2025.

CARVALHO, L. A. C.; ANDRADE, E. P.; FRAGA, I. D. Mapeamento do processo de regularização LGPD em uma startup de recrutamento tech. Revista Tecnologia e Sociedade, Curitiba, v. 21, n. 65, p. 154-177, 2025. Disponível em: http://dx.doi.org/10.3895/rts.v21n65.17996. Acesso em: 08 dez. 2025.

CULOT, G.; NASSIMBENI, G.; PODRECCA, M.; SARTOR, M. The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. The TQM Journal, [S. l.], v. 33, n. 7, p. 76-105, 2021. Disponível em: https://doi.org/10.1108/TQM-09-2020-0202. Acesso em: 6 dez. 2025.

DA SILVA, L. G. L. Segurança cibernética no Brasil: uma análise dos fatores institucionais que precedem a política de segurança cibernética entre 2008–2020. 2024. Dissertação (Mestrado em Relações Internacionais) – Universidade Federal da Integração Latino-Americana, Foz do Iguaçu, 2024. Disponível em: https://dspace.unila.edu.br/handle/123456789/8528. Acesso em: 6 dez. 2025.

FEIJÓ, A. M.; VICENTE, E. F. R.; PETRI, S. M. O uso das escalas Likert nas pesquisas de contabilidade. Revista Gestão Organizacional, Chapecó, v. 13, n. 1, p. 27–41, 2020. Disponível em: https://doi.org/10.22277/rgo.v13i1.5112. Acesso em: 6 dez. 2025.

FERREIRA, L. V. A. O papel da auditoria interna na gestão de riscos cibernéticos em instituições financeiras brasileiras: estudo sob a perspectiva das três linhas. 2025. Disponível em: https://repositorio.unb.br/handle/10482/52137. Acesso em: 6 dez. 2025.

GEORG, M. A. C.; RODRIGUES, W. M. S.; ALVES, C. A. M.. SILVEIRA JÚNIOR, A.; NUNES, R. R. Os desafios da Segurança Cibernética no setor público federal do Brasil: estudo sob a ótica de gestores de tecnologia da informação. RISTI: Revista Ibérica de Sistemas e Tecnologias de Informação, [S. l.], n. E54, p. 602-616, nov. 2022. Disponível em: https://www.risti.xyz/issues/ristie54.pdf. Acesso em: 6 dez. 2025.

GIL, A. C. Pesquisa qualitativa básica. Petrópolis: Vozes, 2025.

HUREL, L. M. Cibersegurança no Brasil: uma análise da estratégia nacional de cibersegurança. Rio de Janeiro: Instituto Igarapé, 2021. (Artigo Estratégico, 54). Disponível em: https://igarape.org.br/ciberseguranca-no-brasil-uma-analise-da-estrategia-nacional/. Acesso em: 6 dez. 2025.

LIMA, P.; DA MATA SÁ, S. A.; PESSOA, C. Segurança cibernética, uma análise de infraestrutura segura para um e-commerce. Código 31: Revista de Informação, Comunicação e Interfaces, [S. l.], v. 2, n. 2, p. 9-27, 2024. Disponível em: https://doi.org/10.70493/cod31.v2i2.9617. Acesso em: 6 dez. 2025.

OCDE. ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. Recommendation of the Council on the Protection of Critical Information Infrastructures. Paris: OECD, 2022. OECD/LEGAL/0361. Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0361. Acesso em: 6 dez. 2025.

PALUDO, A. V.; OLIVEIRA, A. G. Governança organizacional pública e planejamento estratégico: para órgãos e entidades públicas. [S. l.]: JM Bosch, 2024.

ROSSETTI, R.; SILVA, C. V. M. Direitos fundamentais no uso de inteligência artificial no Poder Judiciário brasileiro. Revista Tecnologia e Sociedade, Curitiba, v. 20, n. 59, p. 219-235, 2024. Disponível em: http://dx.doi.org/10.3895/rts.v20n59.16406. Acesso em: 08 dez. 2025.

SETIABUDI, W.; SUMADINATA, W. S. Cybercrime and global security threats: a challenge in international law. Russian Law Journal, Moscou, v. 11, n. 3, 2023. Disponível em: https://doi.org/10.52783/rlj.v11i3.1112. Acesso em: 6 dez. 2025.

SILVA, C. F. G.; PINHEIRO, P. R. Eficiência em TI: soluções inteligentes para falhas comuns. Gestão Executiva, [S. l.], v. 2, p. 1–4, 2023. Disponível em: https://doi.org/10.5020/2965-6001.2023.15573. Acesso em: 6 dez. 2025.

SILVA, J. D. S.; OLIVEIRA, R. F. D. Análise das falhas no armazenamento de dados do aplicativo ConecteSUS sob a ótica midiática: desafios da segurança da informação na saúde pública. RIC-CPS: Repositório Institucional do Conhecimento do Centro Paula Souza, São Paulo, 2023. Disponível em: https://ric.cps.sp.gov.br/handle/123456789/19582. Acesso em: 6 dez. 2025.

SILVA, R. D. Segurança Cibernética: o cenário dos crimes virtuais no Brasil. Revista Científica Multidisciplinar Núcleo do Conhecimento, [S. l.], ano 6, v. 3, p. 86-103, mar. 2021. Disponível em: https://www.nucleodoconhecimento.com.br/tecnologia/crimes-virtuais. Acesso em: 6 dez. 2025.

VIANNA, E. W.; CAMELO, J. R. S. Defesa cibernética no Brasil: primícias de uma história de sucesso. Revista da Escola Superior de Guerra, Rio de Janeiro, v. 35, n. 75, p. 127-154, 2020. Disponível em: https://revista.esg.br/index.php/revistadaesg/article/view/1144. Acesso em: 6 dez. 2025.

VIEIRA, J. P. D. C. Cibersegurança e LGPD: a aplicabilidade no caso "Invasão do Superior Tribunal de Justiça". 2022. Trabalho de Conclusão de Curso (Direito) – Faculdade de Inhumas - FacMais, Inhumas, 2022. Disponível em: http://65.108.49.104:80/xmlui/handle/123456789/646. Acesso em: 6 dez. 2025.

Recebido: 19/04/2025
Aprovado: 28/06/2026
DOI: 10.3895/rts.v23n69.20157

Como citar:

SILVA, Jady Pâmella Barbacena da; FERREIRA, Lucas Vinicius Andrade; NUNES, Rafael Rabelo. Desafios da segurança cibernética: uma análise da administração pública brasileira. **Rev. Tecnol. Soc**., Curitiba, v. 23, n. 69, p.157-178, abr./jun, 2026. Disponível em:

https://periodicos.utfpr.edu.br/rts/article/view/20157

Acesso em: XXX.

Correspondência: