Checklist de Segurança Cibernética para Contratações Públicas de TIC: uma proposta baseada em análise normativa e evidências empíricas

Cybersecurity Checklist for Public ICT Procurement: a proposal based on normative analysis and empirical evidence

Telmo Nunes Costa https://orcid.org/0009-0001-0834-4831 Especialização em Privacidade e Segurança da Informação. Universidade de Brasília (UnB) – Brasil. telmo.nunes@gmail.com

Edvan Gomes da Silva https://orcid.org/0009-0005-5271-5328 Mestre em Engenharia Elétrica. Universidade de Brasília (UnB) – Brasil. edvan402@gmail.com

Helton Garcia https://orcid.org/0009-0003-6916-9955 Mestre em Engenharia Elétrica. Universidade de Brasília (UnB) – Brasil. heltongarcia@gmail.com

Lucas Vinicius Andrade Ferreira https://orcid.org/0009-0003-9400-5530 Mestre em Engenharia Elétrica. Universidade de Brasília (UnB) - Brasil. lucas.vinicius@live.com

Rafael Rabelo Nunes https://orcid.org/0000-0002-1538-4276 Doutor em Engenharia Elétrica. Universidade de Brasília (UnB) – Brasil. rafaelrabelo@unb.br

RESUMO

As contratações públicas de Tecnologia da Informação e Comunicação (TIC) são centrais para a modernização administrativa e a implementação de políticas digitais no Estado brasileiro, mas a dependência de serviços tecnológicos complexos e o elevado volume financeiro tornam esse segmento sensível a falhas de planejamento, controle e avaliação de resultados. Apesar da maturidade do arcabouço normativo — como a Lei nº 14.133/2021, a Instrução Normativa nº 94/2022/MGI e frameworks de segurança, persiste uma lacuna operacional na incorporação de controles de segurança cibernética nos processos contratuais de TIC, evidenciada em acórdãos do TCU. Este estudo teve como objetivo desenvolver um checklist de segurança cibernética para apoiar decisões em contratações públicas de TIC. Trata-se de pesquisa aplicada, de abordagem qualitativa, documental, descritiva e exploratória, baseada em análise de 14 acórdãos do Tribunal de Contas da União e em entrevistas semiestruturadas com seis especialistas em governança e fiscalização de TIC da Administração Pública Federal, com análise de conteúdo segundo Bardin (2016). Os resultados evidenciaram lacunas recorrentes no planejamento e na gestão contratual, sobretudo na definição

de métricas, indicadores e mecanismos de aferição de resultados. A convergência entre achados normativos, documentais e empíricos permitiu estruturar um checklist organizado segundo o fluxo da IN nº 94/2022/MGI e fundamentado em três construtos: clareza contratual, desafios de fiscalização e uso de checklist. Conclui-se que o instrumento proposto traduz exigências normativas em controles verificáveis e auditáveis ao longo do ciclo contratual, fortalecendo conformidade, transparência e maturidade da governança no setor público.
Palavras-chave: governança de TIC; contratações públicas; segurança da informação; *checklist*; gestão de riscos.

ABSTRACT

Public procurement of Information and Communication Technology (ICT) is central to administrative modernization and the implementation of digital policies in the Brazilian State, but the dependence on complex technological services and the high financial volume involved make this segment sensitive to failures in planning, control, and performance evaluation. Despite the maturity of the existing regulatory framework—such as Law No. 14,133/2021, Normative Instruction No. 94/2022/MGI, and security frameworks—there remains an operational gap in the incorporation of cybersecurity controls into ICT contractual processes, as evidenced in rulings of the Federal Court of Accounts (TCU). This study aimed to develop a cybersecurity checklist to support decision-making in public ICT procurement. It is an applied research with a qualitative, documentary, descriptive, and exploratory approach, based on analysis of 14 rulings of the Federal Court of Accounts and semi-structured interviews with six specialists in ICT governance and oversight within the Federal Public Administration, using content analysis according to Bardin (2016). The results revealed recurring gaps in contractual planning and management, especially in defining metrics, indicators, and performance measurement mechanisms. The convergence of normative, documentary, and empirical findings enabled the structuring of a checklist organized according to the workflow of Normative Instruction No. 94/2022/MGI and grounded in three constructs: contractual clarity, oversight challenges, and use of checklists. The study concludes that the proposed instrument translates regulatory requirements into verifiable and auditable controls throughout the contractual lifecycle, strengthening compliance, transparency, and governance maturity in the public sector.
Keywords: ICT governance; public procurement; information security; *checklist*; risk management.

Recebido em 05/04/2026. Aprovado em 30/04/2026. Avaliado pelo sistema *double blind peer review*. Publicado conforme normas da ABNT.
https://doi.org/10.22279/navus.v18.2430

1 INTRODUÇÃO

As contratações públicas de Tecnologia da Informação e Comunicação (TIC) são centrais para a modernização administrativa e a sustentação das políticas digitais do Estado brasileiro, e a dependência de serviços tecnológicos complexos e de alto valor torna esse segmento sensível a falhas de planejamento, controle e avaliação de resultados (BRASIL, 2024a; GUARDA; OLIVEIRA; SOUSA JÚNIOR, 2015). O Tribunal de Contas da União (TCU) reforça essa relevância ao registrar volume fiscalizado de cerca de R$ 5 bilhões no ciclo 2023–2024 e R$ 8,08 bilhões em 2024–2025 (BRASIL, 2025c).

Apesar dessa base normativa, auditorias do TCU indicam lacunas na medição e comprovação de resultados: a ausência de indicadores objetivos compromete a eficiência e a economicidade, como mostram os Acórdãos nº 2.513/2019, nº 2.959/2021 e nº 1.508/2020, que apontam a falta de métricas e pagamentos desalinhados ao desempenho em contratações baseadas em Unidades de Serviço Técnico (BRASIL, 2019, 2020a, 2021b, 2025c).

Estudos indicam que, embora o arcabouço normativo seja maduro, faltam diretrizes operacionais para implementar políticas de segurança, e a ausência de práticas consolidadas de gestão de riscos expõe as contratações de TIC a vulnerabilidades que comprometem desempenho e confiabilidade (GEORG et al., 2022; SILVA; OLIVEIRA; CANEDO, 2016). Esse quadro é agravado pelo distanciamento da alta administração das decisões estratégicas de segurança e pela ausência de mecanismos formais de responsabilização, fatores que comprometem a resiliência organizacional frente a incidentes cibernéticos (MARCILIO et al., 2026). Diante desse cenário, o estudo propõe um *checklist* de segurança cibernética como instrumento de apoio à decisão em contratações públicas de TIC.

O artigo organiza-se em: referencial teórico (seção 2), metodologia (seção 3), resultados e discussão (seção 4) e conclusões (seção 5).

2 REFERENCIAL TEÓRICO

2.1 Fundamentos da Segurança da Informação e Cibernética

A segurança da informação é compreendida como a preservação da confidencialidade, integridade e disponibilidade (CID), princípios que estruturam um Sistema de Gestão da Segurança da Informação (SGSI). Chagas e Rodrigues (2025) destacam que um SGSI baseado na ISO 27001 (ISO; IEC, 2022) garante esses pilares por meio de controle e melhoria contínuos. A segurança cibernética amplia esse conceito ao focar a proteção de dados e ativos no ciberespaço contra ameaças (SANTOS; SILVA, 2021).

A literatura recente aponta tendência crescente à integração entre segurança da informação e segurança cibernética, com compartilhamento de processos de gestão de risco e adoção conjunta de *frameworks* como ISO/IEC 27001, NIST, CIS e COBIT (OMOTADE; GHIMIRE; SULTAN, 2025; REDDY, 2024; TANJUNG; NURHAYATI; WIBOWO, 2024).

Neste estudo, segurança cibernética é tratada como extensão da segurança da informação aplicada ao ambiente digital, sendo ambos os termos utilizados de forma complementar, com a gestão de riscos fundamentada na ABNT NBR ISO 31000 (ABNT, 2018; DOS SANTOS, 2021) como elemento transversal que orienta a construção de instrumentos de apoio à decisão, como o checklist proposto.

2.2 Frameworks de Segurança e Governança

O *Center for Internet Security* (CIS) desenvolveu os CIS *Controls* v8 — 18 controles críticos organizados em grupos de implementação (IG1, IG2 e IG3), amplamente reconhecidos por sua objetividade, especialmente em órgãos públicos com recursos limitados (CIS, 2021; BRASIL, 2022b). Contudo, sua implementação exige adaptação aos processos legais e, em contextos específicos como o judiciário brasileiro, pode demandar controles adicionais (RODRIGUES; SILVA; OLIVEIRA, 2023; ALVES et al., 2025).

Instituído pela Portaria SGD/MGI nº 852/2023, o Programa de Privacidade e Segurança da Informação (PPSI) incorporou princípios dos CIS *Controls* v8 adaptados à Administração Pública Federal, configurando um framework nacional com controles em Grupos de Implementação para adoção escalonada (BRASIL, 2023a; BRASIL, 2024b).

O COBIT 2019 é um dos *frameworks* de governança de TIC mais utilizados, alinhando tecnologia, estratégia e controle organizacional (PEREIRA; BORGES, 2023; ISACA, 2019). Contudo, sua adoção no setor público enfrenta resistência cultural, complexidade estrutural e escassez de pessoal especializado, evidenciando a necessidade de instrumentos simplificados como o checklist proposto (PEREIRA; BORGES, 2023). Esse cenário é aprofundado pela baixa presença de lideranças técnicas em segurança: estima-se que 30% dos governos estaduais não dispõem de analistas de cibersegurança e apenas 22% contam com um Chief Information Security Officer (CISO) (MARCILIO et al., 2026).

2.3 Marco Normativo e Instrumentos de Governança em Contratações de TIC

A IN nº 94/2022 é o principal instrumento regulatório das contratações de TIC federais, disciplinando planejamento, seleção e gestão contratual com alinhamento ao Plano Diretor de TIC (PDTIC) (BRASIL, 2022a; BRASIL, 2025b). O Guia de Requisitos e Obrigações quanto à Privacidade e à Segurança da Informação complementa esse marco com orientações para o Termo de Referência (BRASIL, 2024c), articulando-se ao Referencial Básico de Governança Organizacional, focado em resultados e prestação de contas (BRASIL, 2022c).

A literatura reforça que a incorporação de gestão de riscos deve ocorrer desde o planejamento, com cláusulas contratuais que traduzam exigências de governança em obrigações auditáveis e critérios objetivos de desempenho (BRASIL, 1967; BRASIL, 1988; SILVA; OLIVEIRA; CANEDO, 2016; ROSSI, 2023; LUIZ, 2023; BRASIL, 2021a; MELLO; GARBACCIO, 2025).

A articulação entre marco normativo, frameworks de segurança, proteção de dados (D'OLIVEIRA; CUNHA, 2024; BRASIL, 2018) e gestão de riscos contratuais fundamenta instrumentos de apoio à decisão que operacionalizem exigências regulatórias em critérios objetivos de verificação como o *checklist* proposto.

3 METODOLOGIA

Este estudo caracteriza-se como pesquisa aplicada (GIL, 2008), qualitativa, documental e exploratória, combinando análise de acórdãos e normativos com entrevistas semiestruturadas para compreender práticas e percepções relacionadas à incorporação de controles de segurança em contratações de

TIC. O percurso metodológico foi desenvolvido em três etapas interligadas, conforme o fluxograma da Figura 1.

Figura 1 – Processo de Análise

3.1 Revisão normativa e documental

A pesquisa iniciou-se com análise documental sistemática das contratações públicas de TIC, voltada à identificação de falhas recorrentes e de seus impactos na mensuração de resultados e no controle contratual. Os critérios de seleção foram: disponibilidade integral no Portal de Acompanhamento de Aquisições de TIC do TCU, pertinência temática e abrangência temporal (2015–2025). O portal reunia 14 acórdãos, todos analisados integralmente por constituírem o universo completo das decisões disponíveis, dispensando amostragem (BRASIL, 2025c).

Com base na análise documental (BOWEN, 2009), foram examinados os 14 acórdãos para identificar lacunas em indicadores e métodos de aferição de resultados, o Referencial de Governança Organizacional, o Guia de Requisitos e Obrigações quanto à Privacidade e à Segurança da Informação e o *Framework* do PPSI (BRASIL, 2022c; BRASIL, 2024b; BRASIL, 2024c).
Foram também revisados normativos nacionais (Lei nº 14.133/2021, LGPD, IN nº 94/2022/MGI e Portaria SGD/MGI nº 5.950/2023), frameworks internacionais (CIS *Controls* v8, COBIT 2019, ISO/IEC 27001 e ABNT NBR ISO 31000) e estudos sobre gestão de riscos em contratações de TIC (BRASIL, 2018; BRASIL, 2021a; BRASIL, 2022a; BRASIL, 2023b).

3.2 Abordagem exploratória complementar

Foram realizadas entrevistas semiestruturadas com especialistas da Administração Pública, selecionados intencionalmente para representar os principais papéis do ciclo contratual: técnico-administrativo, fiscal, gestor de contrato, pregoeiro, chefe de contratações de TIC e consultor jurídico. Participaram seis profissionais com experiência entre cinco e quinze anos, número considerado suficiente com base no critério de saturação teórica, evidenciado pela convergência temática das respostas a partir da quinta entrevista, verificada pela ausência de novos códigos e categorias na sexta entrevista em relação às cinco anteriores (BARDIN, 2016).

O roteiro foi estruturado em seis blocos temáticos: (1) perfil e experiência do entrevistado; (2) tratamento dos riscos de segurança cibernética no planejamento (ETP e TR); (3) papel dos controles na seleção de fornecedores; (4) mecanismos de fiscalização e evidências utilizadas; (5) utilidade de *checklists* e seus elementos essenciais; e (6) lacunas percebidas na IN nº 94/2022 e sugestões de melhoria. As entrevistas foram realizadas individualmente, de forma *online*, entre setembro e outubro de 2025, com duração média de 20 minutos.

Os dados foram analisados por meio da análise de conteúdo de Bardin (2016) em três fases: (i) pré-análise, com leitura flutuante e organização do corpus; (ii) exploração do material, com codificação em categorias temáticas de clareza contratual, desafios de fiscalização e uso de checklist; e (iii) interpretação dos resultados, com agrupamento em construtos analíticos que identificaram convergências e divergências entre especialistas e achados documentais, garantindo-se anonimato conforme a Resolução CNS nº 510/2016 (BRASIL, 2016).

3.3 Estruturação do checklist

Concebido como ferramenta de governança e apoio à decisão (BRASIL, 2024d; ABNT, 2018), o *checklist* sistematiza a verificação dos requisitos contratuais, reduz a exposição a falhas de controle e fortalece a mensuração objetiva de desempenho e a rastreabilidade das evidências, promovendo transparência na gestão das contratações de TIC.

Os elementos do *checklist* foram selecionados com base em: (i) recorrência nos acórdãos do TCU; (ii) aderência à IN nº 94/2022/MGI; e (iii) validação pelos especialistas, por triangulação entre validade normativa, técnica e empírica. Seguindo o fluxo contratual da IN nº 94/2022/MGI, foram estruturadas oito etapas: Analisar, Identificar, Integrar, Especificar, Evidenciar, Formalizar, Designar e Monitorar.

4 RESULTADOS E DISCUSSÃO

4.1 Revisão normativa documental

O arcabouço regulatório — Lei nº 14.133/2021, Lei nº 13.709/2018 e IN nº 94/2022/MGI (BRASIL, 2021a; BRASIL, 2018; BRASIL, 2022a) — estabelece diretrizes para planejamento e gestão contratual, mas carece de mecanismos operacionais padronizados para comprovação de resultados e aferição de desempenho (GEORG et al., 2022).

As análises dos acórdãos do TCU corroboram essa constatação: o Acórdão nº 2.513/2019 - Plenário evidencia a ausência de indicadores para mensurar eficácia, eficiência e efetividade das entregas, bem como a frágil correlação entre recursos orçamentários e resultados (BRASIL, 2019). O modelo baseado em Unidades de Serviço Técnico (UST), antes visto como alternativa contratual (ARAÚJO, 2017), revelou fragilidades, pois, segundo o Acórdão nº 1.508/2020 - Plenário, a falta de critérios objetivos de aferição resultou em pagamentos dissociados dos resultados alcançados (BRASIL, 2020a).

O Acórdão nº 292/2025 - Plenário apontou deficiência de métricas de monitoramento em contratação de computação em nuvem, classificando essas lacunas como fatores de risco à efetividade contratual (BRASIL, 2025e) —

padrão presente em 11 dos 14 acórdãos analisados (exceção: Acórdãos n° 823/2022, 1432/2024 e 1875/2024).

Quadro 1 — Pesquisa nos acórdãos

Acórdão	Análise / Achados	Fragmento / Acórdão
2362/2015 Plenário	1. Importância da definição de níveis de serviço para aferir resultados. 2. Importância da efetiva fiscalização do contrato. 3. Importância da clareza nas métricas utilizadas para aferir resultados e pagamentos.	...considerarem fatores capazes de maximizar as possibilidades de sucesso das contratações... ...especificação de níveis de serviço... ...efetiva fiscalização do cumprimento das cláusulas contratuais... ...nível de serviço como mecanismo de pagamento por resultados... ...em termos de métricas, restou demonstrado que os serviços, "aparentemente, estão sendo pagos com base em resultados..."
2569/2018 Plenário	1. Importância da definição de níveis de serviço para aferir resultados. 2. Importância da clareza nas métricas utilizadas para aferir resultados e pagamentos. 3. Importância do estabelecimento de penalidades ao descumprimento de níveis de serviço e do alinhamento ao PDTI.	...cláusulas contratuais relacionadas a níveis de serviço que sejam alinhadas aos objetivos de negócio... ...é necessário explicitar, de forma clara, as condições contratuais que definem o período de vigência dos serviços e a responsabilidade do fabricante... ...estabelecimento de penalidades padrão que sejam compatíveis e diretamente relacionadas ao descumprimento desses níveis de serviço, de forma a induzir a aplicação das sanções... ...ausência de alinhamento ao Plano Diretor de Tecnologia da Informação (PDTI)...
2037/2019 Plenário	1. Importância da clareza e rastreabilidade (métricas e evidências). 2. Importância da definição de indicadores de resultados. 3. Importância do alinhamento ao PDTI.	...a utilização de métrica cuja medição não seja passível de verificação afronta o disposto na Súmula TCU 269 (Ac 916/2015-P, item 9.1.6.8)... ...os serviços especificados no Catálogo de Serviços devem estar diretamente vinculados aos resultados esperados da contratação... ...irregularidades no planejamento das contratações: ausência de alinhamento ao PDTI;
915/2020 Plenário	1. Importância da clareza e rastreabilidade (métricas e evidências). 2. Importância da definição de indicadores de resultados.	...ausência de detalhamento dos custos de serviços medidos por UST e métricas semelhantes... ...serviços de TI medidos em UST com o propósito de verificar se a execução contratual está assegurando critérios capazes de aferir pagamentos por resultados a preços razoavelmente condizentes...
1508/2020 Plenário	1. Importância da clareza e	...UST, em termos gerais, implica a elaboração de artefatos que viabilizem

	rastreabilidade (métricas e evidências). 2. Importância da definição de indicadores de resultados. 3. Importância da padronização da unidade de medida (métricas de aferição de resultados).	a adequada e razoável mensuração e definição dos preços das atividades ou serviços, tais como: (i) catálogo de serviços, com a respectiva justificativa; (ii) estudos técnicos que subsidiem a definição de indicadores, como aqueles referentes aos níveis de complexidade das atividades, aos níveis de serviço esperados, aos esforços e aos perfis profissionais; (iii) a correlação entre as atividades e a quantidade de UST; e (iv) planilha de composição de custo e formação de preço unitário da UST. ...UST é o acrônimo de Unidade de Serviços Técnicos ou Unidade de Suporte Técnico, prática que vem sendo utilizada pela Administração Pública, sem restringir-se a um dos poderes, em contratações de TI... ...constata-se que a UST não pode ser entendida como uma unidade de medida e adotada pela Administração como tal, sem a devida padronização...
1756/2021 Plenário	1. Importância da clareza e rastreabilidade (métricas e evidências). 2. Importância da definição de indicadores de resultados. 3. Importância do registro e das justificativas dos requisitos da solução.	...(ii) direcionamento da contratação decorrente de definição excessiva de requisitos e não justificados; (iii) ausência de critério de aceitabilidade e níveis de serviço; e (iv) ausência de catálogo de serviços... ...também foram apresentadas vulnerabilidades, tais como: (i) ausência da planilha de custos e formação de preços; (ii) catálogo de serviços sem critérios de aceitabilidade acerca da qualidade e sem o quantitativo de UST de cada serviço; e (iii) ausência de memória de cálculo do quantitativo total de UST...
823/2022 Plenário	1. Importância da capacitação em planejamento das contratações.	...capacitação em aquisições de TI... ...em função das fragilidades nos planejamentos das contratações identificadas nos dois ciclos do acompanhamento... ...avalie a conveniência e a oportunidade, considerando as prioridades estabelecidas, a estratégia predefinida pela Administração e os recursos disponíveis, de ofertar o curso "Aquisições de TI – Da origem da demanda ao resultado efetivo", de forma autoinstrucional, aberto ao público em geral; ...
2185/2023 Plenário	1. Métricas de aferição e resultados na contratação de	...a equipe de acompanhamento aplicou critérios de maior risco, relevância, materialidade e oportunidade para

	serviços foram considerados de alto risco para a escolha de auditoria, devido à sua recorrência.	selecionar os editais de bens e serviços de TI em que deveria atuar, tais como: valor estimado e objetos com representações recorrentes no TCU (exemplo: contratação de serviços cuja remuneração seria baseada em Unidades de Serviços Técnicos [UST], ou denominações semelhantes)...
980/2023 Plenário	1. Importância do detalhamento dos itens que compõem a solução de TIC. 2. Clareza nas métricas utilizadas para a composição dos serviços contratados. 3. Importância de ferramentas de apoio, tais como *checklists* no rito licitatório.	...o quantitativo de bens e serviços necessários para a composição da solução de TI a contratar deve ser detalhado, motivado e justificado, inclusive quanto à forma de cálculo... ...procedimentos com textos genéricos, sem detalhamento ou listas de verificação, para que os respectivos fiscais verifiquem a autenticidade, a correspondência com o que foi proposto e o quantitativo...
1432/2024 Plenário	1. Importância do detalhamento dos itens que compõem a solução de TIC.	...exija informações detalhadas dos componentes das soluções de TIC que se pretende contratar, a exemplo de: fabricante, modelo, *part number*, descrição oficial do *part number*, descrição técnica, quantidade e preço unitário...
157/2024 Plenário	1. Importância da clareza das responsabilidades do contratante e do contratado. 2. Importância da padronização das formas de medição.	...os mecanismos de gestão contratual são independentes dos controles internos estabelecidos pelo órgão e devem ser especificados em cada contratação, para estabelecer a forma de comunicação entre as partes do contrato e a definir as responsabilidades de cada uma... ...pode-se inferir que a ausência de controle pelos OGSs nesse aspecto resulta em incomparabilidade de preços e heterogeneidade de formas de medição dos serviços contratados...
1875/2024 Plenário	1. Importância da padronização de artefatos do rito licitatório. 2. Reconhecimento de problemas relacionados à carga e ao efetivo da unidade de TIC que elabora as contratações.	...os agentes públicos responsáveis pelo planejamento das contratações devem, sempre que possível, utilizar padrões estabelecidos... ...é possível otimizar o uso dos recursos públicos... ...lembrando que uma unidade de TI típica efetua contratações de diversas soluções, tendo de dominar as especificações técnicas, os mercados e os modelos de comercialização de todas elas, assim como efetuar os respectivos processos de contratação. Esse é um problema apontado nos já citados Acórdãos 2.569/2018 e 2.789/2019, ambos do Plenário do TCU...
292/2025 Plenário	1. Importância da definição e do	..."o órgão ou entidade deve avaliar a utilização de mecanismos e

	detalhamento das evidências para assegurar a devida execução dos serviços. 2. Menção ao Guia de boas práticas em contratação de soluções de TIC do TCU para alinhar definições sobre elementos de contratações.	instrumentos adicionais para assegurar a adequada verificação dos volumes consumidos, ou ainda a exigência, no instrumento convocatório, do fornecimento de evidências rastreáveis que comprovem a execução dos serviços"... ...o Guia de boas práticas em contratação de soluções de tecnologia da informação, elaborado pelo TCU, dispõe, nas páginas 294 e 295, que "o modelo de gestão do contrato descreve como a execução do objeto será fiscalizada pelo órgão, de forma que o objeto do contrato seja fornecido nas condições estabelecidas..."
1299/2025 Plenário	1. Importância do detalhamento de métricas e resultados esperados para evitar sobrepreços e pagamentos por serviços desvinculados do resultado ou da qualidade efetivamente entregue.	...(iv) possíveis sobrepreços na adoção de metodologias de Unidade de Serviço Técnico quando não observadas as recomendações jurisprudenciais e portarias em vigor que demandam planilhas de composição de custos e estudos de viabilidade econômica... ...por fim, foram considerados os riscos inerentes ao uso da metodologia chamada Unidade de Serviço Técnico (UST e similares), os quais já foram tratados com profundidade no Ac 2037/2019-TCU-P, de relatoria do Ministro Substituto Augusto Sherman, e no Ac 1508/2020-TCU-P...

Fonte: Elaborado pelos autores com base em acórdãos do Tribunal de Contas da União (BRASIL, 2025c).

Esses achados convergem com a jurisprudência do TCU e com a literatura (BRASIL, 2022c; 2024d; GUARDA; OLIVEIRA; SOUSA JÚNIOR, 2015; LIMBERGER; TEIXEIRA, 2016), bem como com os normativos e *frameworks* nacionais e internacionais, como o PPSI, CIS *Controls* v8, COBIT 2019, ISO/IEC 27001 e ABNT NBR ISO 31000, que reforçam a centralidade de controles mensuráveis e auditáveis para a efetividade das contratações públicas de TIC (BRASIL, 2024b; 2024c; CIS, 2021; ISACA, 2019; ISO; IEC, 2022; ABNT, 2018; ROSSI, 2023; PEREIRA; BORGES, 2023; CHAGAS; LIMBERGER; TEIXEIRA, 2016; CHAGAS; RODRIGUES, 2025; DOS SANTOS, 2021; RODRIGUES; SILVA; OLIVEIRA, 2023; ALVES et al., 2025).Registre-se que os Acórdãos n° 2.387/2024 e n° 2.430/2024 também evidenciam insuficiências normativas que dificultam a responsabilização direta da alta administração pela gestão de riscos cibernéticos, indicando que as fragilidades identificadas extrapolam a dimensão técnica e alcançam o nível da governança institucional (MARCILIO et al., 2026).

4.2 Abordagem exploratória complementar

A análise de conteúdo identificou três construtos analíticos: clareza contratual, desafios de fiscalização e uso de *checklist*, sintetizados a seguir.

4.2.1 Construto 1 – Clareza contratual

Uma das principais fragilidades identificadas refere-se à forma como os requisitos de segurança cibernética são traduzidos no Estudo Técnico Preliminar (ETP) e no Termo de Referência (TR).

As respostas evidenciaram que, embora a legislação e os guias orientem a necessidade de requisitos claros e mensuráveis, na prática estes são frequentemente descritos de forma genérica, dificultando a fiscalização posterior. Entre os exemplos relatados, destacam-se percepções como a seguinte: "Falta clareza em como os controles devem ser entregues e comprovados." E2

> "Requisitos de segurança entram de forma muito genérica, baseados na LGPD e na IN 94/2022. Há dificuldades pela falta de tempo, pouco conhecimento técnico, excesso de linguagem jurídica e falta de padronização." E4

Essa ausência compromete a exequibilidade das obrigações, dificulta a aplicação de sanções e afeta a segurança jurídica da contratação - daí o construto 'Clareza contratual', que reflete a necessidade de traduzir normas em cláusulas objetivas e mensuráveis.

Quadro 2 — Construto 1: Clareza contratual

#	Descrição
1	Requisitos de segurança pouco detalhados
2	Cláusulas genéricas
3	Ausência de periodicidade
4	Controles difíceis de avaliar
5	Segurança com peso reduzido na escolha
6	Falta de clareza contratual
7	Necessidade de indicadores objetivos

4.2.2 Construto 2 – Desafios de fiscalização

Os entrevistados apontaram que a fiscalização ainda depende da capacidade técnica individual dos fiscais e da subjetividade dos relatórios, sem guias claros ou indicadores objetivos: "A fiscalização depende muito da interpretação do fiscal. Há dificuldade em validar relatórios técnicos sem ferramentas adequadas." E2 e "há falta de padronização e os dados vêm incompletos" E4. Essa fragilidade tem raízes estruturais: é o envolvimento persistente da alta gestão ao longo de todo o ciclo de políticas, formulação, sustentação, monitoramento e aprimoramento, que institucionaliza a segurança da informação como valor organizacional. Sem esse comprometimento, instrumentos técnicos, como o checklist proposto, têm efetividade limitada (MARCILIO et al., 2026).

Quadro 3 — Construto 2: Desafios de fiscalização

#	Descrição
1	Fiscalização subjetiva
2	Falta de capacitação técnica
3	Dependência de relatórios da contratada
4	Fortalecimento da cultura de segurança
5	Importância do apoio jurídico

4.2.3 Construto 3 – Checklist

Os entrevistados convergiram: o checklist só será útil se contemplar critérios objetivos e auditáveis para orientar elaboração e fiscalização das cláusulas. Itens considerados indispensáveis:

> "Na análise de risco deve-se identificar ativos críticos, dados pessoais e sensíveis, usando o PDTIC como apoio. Na avaliação de impacto, deve-se considerar o impacto na continuidade dos serviços. É necessário alinhar o planejamento, incluindo cláusulas no ETP e no TR com justificativas técnicas. Na redação contratual, devem constar cláusulas auditáveis, métricas de aceitação e periodicidade." E2

> "Precisa deixar claro quais evidências o fornecedor deve apresentar, não só citar o controle." E4

Quadro 4 — Construto 3: *Checklist*

#	Descrição
1	Definição de métricas
2	Periodicidade
3	Evidências claras
4	Rastreabilidade
5	Alinhamento entre ETP e TR
6	Utilização de documentos de apoio
7	Mapeamento de riscos e impactos
8	Clareza para o fornecedor

Os construtos convergem para um diagnóstico central: o principal desafio não é a ausência de normativos, mas a dificuldade de traduzi-los em práticas contratuais efetivas — limitação agravada pela sobrecarga das equipes, escassez de tempo e deficiência de apoio jurídico, conforme também evidenciado no Acórdão nº 1875/2024 do TCU.

4.3 Estruturação do *checklist*

Com base na triangulação entre análise normativa, técnica e empírica (Bardin, 2016), e seguindo o fluxo da IN nº 94/2022/MGI (BRASIL, 2022a), os controles e critérios de segurança foram organizados em oito etapas práticas: Analisar, Identificar, Integrar, Especificar, Evidenciar, Formalizar, Designar e Monitorar tendo como eixos estruturantes os três construtos identificados: clareza contratual, desafios de fiscalização e uso de checklist.

As características de cada etapa são sintetizadas no Quadro 5, com apresentação dos elementos essenciais de cada fase. O *checklist* completo, contendo a descrição detalhada de cada item, os controles associados, as evidências requeridas e as referências normativas, encontra-se no Apêndice A deste artigo.

5 CONCLUSÃO

Este estudo desenvolveu um *checklist* de segurança cibernética como instrumento de apoio à decisão em contratações públicas de TIC. A análise

dos acórdãos e as entrevistas convergem para um diagnóstico central: o principal desafio não é a ausência de normativos, mas a dificuldade de operacionalizar métricas e evidências ao longo do ciclo contratual — padrão que persiste mesmo após os avanços da Lei nº 14.133/2021 e da IN nº 94/2022/MGI.

Com base nesse diagnóstico, foi estruturado um *checklist* de segurança cibernética como ferramenta de governança — integrando dimensões normativas, técnicas e operacionais (COBIT 2019, PPSI, ISO/IEC 27001:2022 e ABNT NBR ISO 31000:2018) — para orientar requisitos, evidências e indicadores ao longo do ciclo contratual, fortalecendo a gestão por resultados e a transparência na fiscalização.

Como contribuição prática, oferece aos gestores uma ferramenta aderente à IN nº 94/2022/MGI que traduz exigências normativas em controles auditáveis. Como contribuição teórica, conecta a governança de TIC à operacionalização de controles de segurança, estabelecendo uma ponte entre frameworks internacionais e as demandas concretas do setor público brasileiro.

Reconhecem-se limitações relativas à abordagem qualitativa e ao escopo restrito à Administração Pública Federal, recomendando-se validação em outros contextos e estudos quantitativos sobre desempenho e maturidade em riscos cibernéticos. Como perspectiva complementar de pesquisa, sugere-se o desenvolvimento de frameworks que mensurem o grau de responsabilização formal da alta administração nas decisões de segurança cibernética, incluindo indicadores de participação estratégica e incorporação de metas de cibersegurança nas avaliações de desempenho dos dirigentes (MARCILIO et al., 2026).

Em síntese, a governança de TIC orientada por métricas e evidências configura condição essencial para a segurança cibernética e a integridade das contratações públicas, e o checklist proposto representa um avanço rumo a práticas de gestão mais transparentes, auditáveis e alinhadas à cultura de resultados na Administração Pública.

REFERÊNCIAS

ALVES, Renato S.; SILVA, Jady P. B. da; RIBEIRO JUNIOR, Luiz Antonio; NUNES, Rafael R. Enhancing cybersecurity in the judiciary: Integrating additional controls into the CIS framework. **Computers & Security**, v. 157, p. 104584, out. 2025. DOI: 10.1016/j.cose.2025.104584. Disponível em: https://linkinghub.elsevier.com/retrieve/pii/S0167404825002731. Acesso em: 30 abr. 2026.

ARAÚJO, Pedro A. C. de. **Estudos comparativos de estimativas por Pontos de Função, UST e Homem-Hora**. 2017. Trabalho de Conclusão de Curso (Graduação em Engenharia de Software) — Universidade de Brasília, Brasília, 2017. Disponível em: https://bdm.unb.br/bitstream/10483/30316/1/2017_PedroAugustoCordovaDeA-raujo_tcc.pdf. Acesso em: 23 out. 2025.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO 31000:2018 — Gestão de riscos — Diretrizes**. Rio de Janeiro: ABNT, 2018.

BARDIN, L. **Análise de conteúdo**. 4. ed. Lisboa: Edições 70, 2016.

BOWEN, Glenn A. Document analysis as a qualitative research method. **Qualitative Research Journal**, v. 9, n. 2, p. 27-40, 2009. Disponível em: https://www.researchgate.net/publication/240807798_Document_Analysis_as_a_Qualitative_Research_Method. Acesso em: 25 out. 2025.

BRASIL. ADVOCACIA-GERAL DA UNIÃO - AGU. **Modelos de Verificação TIC – Lei nº 14.133/2021**. Brasília: AGU, set. 2025a. Disponível em: https://www.gov.br/agu/pt-br/composicao/cgu/cgu/modelos/licitacoesecontratos/14133/bens-e-servicos-de-tic. Acesso em: 18 out. 2025.

BRASIL. Conselho Nacional de Saúde. Resolução nº 510, de 7 de abril de 2016. **Dispõe sobre as normas aplicáveis a pesquisas em Ciências Humanas e Sociais**. Diário Oficial da União, Brasília, 24 maio 2016. Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/cns/2016/res0510_07_04_2016.html. Acesso em: 21 out. 2025.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 21 out. 2025.

BRASIL. **Decreto nº 12.069, de 21 de junho de 2024a. Estratégia Nacional de Governo Digital - 2024 a 2027**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2024/decreto/D12069.htm. Acesso em: 11 ago. 2025.

BRASIL. **Decreto-Lei nº 200, de 25 de fevereiro de 1967, que dispõe sobre a organização da Administração Federal, estabelece diretrizes para a Reforma Administrativa e dá outras providências**. Brasília, DF: Presidência da República, 1967. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del0200.htm. Acesso em: 21 out. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 11 ago. 2025.

BRASIL. Lei nº 14.133, de 1º de abril de 2021a. **Lei de Licitações e Contratos Administrativos**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14133.htm. Acesso em: 11 ago. 2025.

BRASIL. MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS. **Guia do Framework de Privacidade e Segurança da Informação, Programa de Privacidade e Segurança da Informação — PPSI**, 2024b. Disponível em: https://www.gov.br/governo-digital/pt-br/privacidade-e-seguranca/ppsi/guia_framework_psi.pdf. Acesso em: 11 ago. 2025.

BRASIL. MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS. **Guia de Requisitos e Obrigações Quanto a Privacidade e à Segurança da Informação — PPSI**, 2024c. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_requisitos_obrigacoes.pdf. Acesso em: 11 ago. 2025.

BRASIL. MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS. **Instrução Normativa nº 94, de 23 de dezembro de 2022a**. Estabelece diretrizes para a contratação de serviços de Tecnologia da Informação e Comunicação – TIC. Disponível em: https://www.gov.br/governodigital/pt-br/contratacoes-de-tic/instrucao-normativa-sgd-me-no-94-de-23-de-dezembro-de-2022. Acesso em: 11 ago. 2025.

BRASIL. MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS. **Sistema Eletrônico de Informações (SEI)**. 2013. Disponível em:

https://www.gov.br/servicoscompartilhados/pt-br/assuntos/gestao-documental/sistema-eletronico-de-informacoes-sei. Acesso em: 11 ago. 2025.

BRASIL. MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS. Secretaria de Governo Digital. Portaria SGD/MGI nº 852, de 28 de dezembro de 2023a. **Institui o Programa de Privacidade e Segurança da Informação (PPSI).** Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-852-de-28-de-marco-de-2023-473750908. Acesso em: 11 ago. 2025.

BRASIL. MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS. Secretaria de Governo Digital. Portaria nº 5.950, de 26 de outubro de 2023b. **Estabelece modelo de contratação de software e de serviços de computação em nuvem, no âmbito dos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal**. Disponível em: https://www.gov.br/governodigital/pt-br/contratacoes-de-tic/legislacao/modelo-de-contratacao-de-software-e-servicos-em-nuvem/vigentes/portaria-sgd-mgi-no-5-950-de-26-de-outubro-de-2023. Acesso em: 27 out. 2025.

BRASIL. SISTEMA DE ADMINISTRAÇÃO DOS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO - SISP. **Assuntos ou temas de TIC, tais como: Plano Diretor de TIC - PDTIC, Contratação de bens e serviços de TIC, Talentos do SISP e Plano de Transformação Digital,** 2025b. Disponível em: https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/sisp/guia-do-gestor. Acesso em: 11 ago. 2025.

BRASIL. TRIBUNAL DE CONTAS DA UNIÃO - TCU. **Portal - Aquisições de Tecnologia da Informação (TI).** Brasília, DF: TCU, 2025c. Disponível em: https://portal.tcu.gov.br/tecnologia-da-informacao/aquisicoes-de-ti-1. Acesso em: 21 out. 2025.

BRASIL. TRIBUNAL DE CONTAS DA UNIÃO. **Acórdão nº 1.299/2025 - Plenário**. Relator: Ministro Jhonatan de Jesus. Brasília, DF, 2025d. Disponível em: https://pesquisa.apps.tcu.gov.br/redireciona/acordao-completo/ACORDAO-COMPLETO-2708978. Acesso em: 21 out. 2025.

BRASIL. TRIBUNAL DE CONTAS DA UNIÃO. **Acórdão nº 1.508/2020 - Plenário**. Relator: Ministro-Substituto André Luís de Carvalho. Brasília, DF, 2020a. Disponível em: https://pesquisa.apps.tcu.gov.br/redireciona/acordao-completo/ACORDAO-COMPLETO-2410535. Acesso em: 21 out. 2025.

BRASIL. TRIBUNAL DE CONTAS DA UNIÃO. **Acórdão nº 2.513/2019 - Plenário**. Relator: Ministro Vital do Rêgo. Brasília, DF, 2019. Disponível em: https://pesquisa.apps.tcu.gov.br/redireciona/acordao-completo/ACORDAO-COMPLETO-2377277. Acesso em: 21 out. 2025.

BRASIL. TRIBUNAL DE CONTAS DA UNIÃO. **Acórdão nº 2.959/2021 - Plenário**. Relator: Ministro Bruno Dantas. Brasília, DF, 2021b. Disponível em: https://pesquisa.apps.tcu.gov.br/redireciona/acordao-completo/ACORDAO-COMPLETO-2515036. Acesso em: 21 out. 2025.

BRASIL. TRIBUNAL DE CONTAS DA UNIÃO. **Acórdão nº 292/2025 - Plenário**. Relator: Ministro Antonio Anastasia. Brasília, DF, 2025e. Disponível em: https://pesquisa.apps.tcu.gov.br/redireciona/acordao-completo/ACORDAO-COMPLETO-2698679. Acesso em: 21 out. 2025.

BRASIL. TRIBUNAL DE CONTAS DA UNIÃO. **Cinco controles de segurança cibernética para ontem**. Brasília: TCU, 2022b. Disponível em: https://portal.tcu.gov.br/publicacoes-institucionais/cartilha-manual-ou-tutorial/5-controles-de-seguranca-cibernetica. Acesso em: 11 ago. 2025.

BRASIL. TRIBUNAL DE CONTAS DA UNIÃO. **Licitações e Contratos: Orientações e Jurisprudência do TCU**. 5. ed. Brasília: TCU, 2024d. Disponível em: https://licitacoesecontratos.tcu.gov.br/wp-content/uploads/sites/11/2024/09/Licitacoes-e-Contratos-Orientacoes-e-Jurisprudencia-do-TCU-5a-Edicao-29-08-2024.pdf.

BRASIL. TRIBUNAL DE CONTAS DA UNIÃO. **Referencial Básico de Governança Organizacional - RBGO. Brasília**: TCU, 2022c. Disponível em: https://portal.tcu.gov.br/governanca/governanca-publica. Acesso em: 11 ago. 2025.

CENTER FOR INTERNET SECURITY – CIS. **Critical Security Controls v8**. 2021. Disponível em: https://www.cisecurity.org/controls/cis-controls-list. Acesso em: 11 ago. 2025.

CHAGAS, C. H.; RODRIGUES, A. H. G. Análise do processo de implementação de um sistema de gestão da segurança da informação com base na ISO/IEC 27001. **Revista FT – Ciências Exatas e da Terra**, v. 29, ed. 142, 2025. Disponível em: https://revistaft.com.br/analise-do-processo-de-implementacao-de-um-sistema-de-gestao-da-seguranca-da-informacao-com-base-na-iso-iec-27001/. Acesso em: 10 out. 2025.

D'OLIVEIRA, Nadine P. C.; CUNHA, Francisco J. A. P. Lei Geral de Proteção de Dados (LGPD): a relação entre as políticas e os regimes de informação. **RDBCI: Revista Digital de Biblioteconomia e Ciência da Informação**, Campinas, SP, v. 22, p. e024015, 2024. Disponível em: https://www.scielo.br/j/rdbci/a/DWntpkXMB9GgCPKycFcxtts. Acesso em: 13 out. 2025.

DOS SANTOS, T. J. **Gestão de riscos e a norma ISO 31000: uma abordagem literária**. Management Journal / Sapientiae, 2021. Disponível em: https://sapientiae.com.br/index.php/managementjournal/article/download/CBPC2674-6417.2021.001.0001/75. Acesso em: 13 out. 2025.

GEORG, Marcus Aurélio C.; RODRIGUES, Walisson M. S.; ALVES, Carlos André de Melo; SILVEIRA JÚNIOR, Aldery; NUNES, Rafael R. Os desafios da segurança cibernética no setor público federal do Brasil: estudo sob a ótica de gestores de tecnologia da informação. **Revista Ibérica de Sistemas e Tecnologias de Informação**, n. E54, p. 602-616, nov. 2022. Disponível em: https://www.researchgate.net/publication/370189315_Os_desafios_da_Seguranca_Cibernetica_no_setor_publico_federal_do_Brasil_estudo_sob_a_otica_de_gestores_de_tecnologia_da_informacao. Acesso em: 13 out. 2025.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas, 2008.

GUARDA, G. F.; OLIVEIRA, E. C.; SOUSA JÚNIOR, R. T. de. **Analysis of IT outsourcing contracts at the TCU (Federal Court of Accounts) and of the legislation that governs these contracts in the Brazilian federal public administration**. JISTEM: Journal of Information Systems and Technology Management, v. 12, n. 1, 2015. DOI: 10.4301/S1807-17752015000100005. Acesso em: 21 out. 2025.

ISO; IEC. **ISO/IEC 27001**: Information security, cybersecurity and privacy protection — Information security management systems — Requirements. 3. ed. Geneva: ISO, 2022.

ISACA. **COBIT 2019 framework: governance and management objectives**. Schaumburg, IL: ISACA, 2019. Disponível em: https://www.isaca.org/resources/cobit. Acesso em: 23 out. 2025.

LIMBERGER, T.; TEIXEIRA, A. V. **Transparency mechanisms and management of public contracts in Brazil: three case studies on the federal public administration**. 2016. DOI: 10.12957/rqi.2016.20184. Acesso em: 21 out. 2025.

LUIZ, E. L. C. A (in)tolerância na aplicação de sanções administrativas nos contratos públicos. **Revista de Administração Contemporânea**, v. 27, p. 1-18, 2023. Disponível em: https://www.scielo.br/j/rac/a/4PSr8LPGw9sBWHfJcqJLrSv/?lang=pt. Acesso em: 13 out. 2025.

MARCILIO, A.; SILVA, E. G. da; TRINKS, V. de M. D.; VINICIUS, L. V. A.; NUNES, R. R. A alta administração na linha de frente da segurança da informação: utopia ou necessidade? Revista Ibérica de Sistemas e Tecnologias de Informação, volume E78, mar. 2026. Disponível em: https://doi.org/10.5281/zenodo.18944685. Acesso em: 02 maio 2026.

MELLO, Allan Del Cistia; GARBACCIO, Grace Ladeira. **O programa de integridade à luz da Lei nº 14.133/2021 e a oportunidade de modernização do Estado por meio do desenvolvimento de uma cultura de compliance efetiva nas contratações públicas**. Revista de Direito Brasileira (RDB), v. 37, n. 14, p. 152-176, 2025. Disponível em: https://indexlaw.org/index.php/rdb/article/view/7483. Acesso em: 13 out. 2025.

OMOTADE, Adedotun L.; GHIMIRE, Ashok; SULTAN, Mahabub. Cybersecurity, data privacy, and information security management. In: INTERNATIONAL CONFERENCE ON ARTIFICIAL INTELLIGENCE AND AUTOMATION CONTROL (AIAC), 3., 2025, Paris. **Anais [...]**. Paris: IEEE, 2025. p. 27-33. DOI: 10.1109/aiac68175.2025.11332518. Disponível em: https://ieeexplore.ieee.org/document/11332518/. Acesso em: 30 abr. 2026.

PEREIRA, Joyce M.; BORGES, Daniel C. **Estruturas de Governança de TI e COBIT – uma revisão da literatura**. Revista FT – Ciências Exatas e da Terra, v. 27, ed. 118, jan. 2023. Disponível em: https://revistaft.com.br/estruturas-de-governanca-de-ti-e-cobit-uma-revisao-da-literatura/. Acesso em: 13 out. 2025.

REDDY, Haritha M. A unified approach to cybersecurity and information security: managing both within one platform. **Zenodo**, 2024. DOI: 10.5281/zenodo.14209348. Disponível em: https://zenodo.org/records/14209348. Acesso em: 30 abr. 2026.

ROSSI, Juliano S. **Tratamento de riscos como técnica de design de contratos**. 2023. 134 f. Dissertação (Mestrado Profissional em Administração Pública) – Escola de Administração de Empresas de São Paulo, Fundação Getúlio Vargas, São Paulo, 2023. Disponível em: https://repositorio.fgv.br/bitstreams/30437840-7c62-4224-b8ec-58ee1635e9fc/download. Acesso em: 13 out. 2025.

SANTOS, Rogério B. dos; SILVA, Tiago Barros Pontes. Gestão da segurança da informação e comunicações: análise ergonômica para avaliação de comportamentos inseguros. **RDBCI: Revista Digital de Biblioteconomia e Ciência da Informação**, Campinas, SP, v. 19, n. 0, p. e021024, 2021. DOI: 10.20396/rdbci.v19i00.8665529. Acesso em: 23 out. 2025.

SILVA, D. A.; OLIVEIRA, E. C.; CANEDO, E. D. Avaliação de riscos do processo de planejamento da contratação de TI: uma proposta para órgãos governamentais brasileiros. **iSys – Revista Brasileira de Sistemas de Informação**, Rio de Janeiro, v. 9, n. 1, p. 168-186, 2016. Disponível em:

https://journals-sol.sbc.org.br/index.php/isys/article/download/305/306/242. Acesso em: 13 out. 2025.

TANJUNG, Dio F.; NURHAYATI, Oky Dwi; WIBOWO, Adi. Design information security in electronic-based government systems using NIST CSF 2.0, ISO/IEC 27001: 2022 and CIS control. **International Journal of Innovative Science and Research Technology**, v. 9, n. IJISRT24JUN1212, p. 523-530, jun. 2024. ISSN 2456-2165. DOI: 10.38124/ijisrt/ijisrt24jun1212. Disponível em: https://www.ijisrt.com/design-information-security-in-electronicbased-government-systems-using-nist-csf-20-isoiec-27001-2022-and-cis-control. Acesso em: 30 abr. 2026.

APÊNDICE A – CHECKLIST DE SEGURANÇA CIBERNÉTICA EM CONTRATAÇÕES DE TIC

Quadro 5 — *Checklist* de Segurança Cibernética em Contratações de TIC

	Descrição	Detalhamento	Decorrência empírica	Entrevistado / acórdão relacionado
1. Analisar	Avaliar os riscos e impactos relacionados aos serviços, sistemas e dados que compõem o objeto da contratação, identificando ativos críticos e potenciais vulnerabilidades de segurança cibernética.	Realizar uma análise prévia de riscos e de impactos sobre a privacidade e a segurança da informação, considerando o tratamento de dados pessoais, dados sensíveis e ativos críticos, conforme as diretrizes da Lei Geral de Proteção de Dados (LGPD). Utilizar o Plano Diretor de TIC (PDTIC) para alinhar a análise aos objetivos institucionais e aos ativos de informação mapeados; o *Framework* PPSI (BRASIL, 2024b) para classificar os riscos e controles mínimos por grupo de implementação (IG1, IG2 e IG3); e o Guia de Requisitos e Obrigações (BRASIL, 2024c) para identificar as obrigações contratuais e técnicas aplicáveis. Nos casos envolvendo computação em nuvem, considerar também a Portaria SGD/MGI nº 5.950 (BRASIL, 2023b). O resultado esperado é um registro de riscos e impactos que sirva de insumo direto para o Estudo Técnico Preliminar (ETP) e o Termo de Referência (TR), orientando a escolha dos controles e cláusulas de mitigação a serem inseridos na contratação.	Corresponde à demanda apontada pelos entrevistados por avaliação prévia de riscos e impactos antes da elaboração do TR.	"Na análise de risco, identificar ativos críticos, dados pessoais e sensíveis, usando o PDTIC como apoio..." E2 Ac 2569/2018-P, Ac 2037/2019-P e Ac 980/2023-P.
2. Identificar	Definir, a partir da análise de riscos, os controles de segurança cibernética aplicáveis ao objeto da contratação, assegurando que cada controle esteja diretamente vinculado a um risco identificado.	Utilizar como base o *Framework* PPSI (BRASIL, 2024b), a Instrução Normativa nº 94/2022/MGI (BRASIL, 2022a) e o Guia de Requisitos e Obrigações quanto à Privacidade e à Segurança da Informação (BRASIL, 2024c) para especificar controles compatíveis com o tipo de serviço, o nível de criticidade e os dados tratados.	Atende à percepção de que os controles são incluídos de forma genérica, sem vinculação direta ao risco identificado.	"Requisitos de segurança entram de forma muito genérica, baseados na LGPD e na IN 94/2022. Há dificuldades pela falta de tempo, pouco conhecimento técnico, excesso de linguagem jurídica e falta de padronização. Equipe reduzida também atrapalha." E4 Ac 1508/2020-P, Ac 823/2022-P e Ac 1875/2024-P.
Int[illegible]	Inserir as exigências de	Prever os controles e medidas de mitigação de riscos no Estudo	Reflete a necessidade,	"Alinhar no planejamento —

	segurança cibernética nos artefatos iniciais da contratação, assegurando que os controles e requisitos estejam previstos desde a etapa de planejamento.	Técnico Preliminar (ETP) e no Termo de Referência (TR), com justificativa técnica que demonstre sua relação com a análise de riscos e a criticidade do serviço. Utilizar como base o *Framework* PPSI (BRASIL, 2024b), a Instrução Normativa nº 94/2022/MGI (BRASIL, 2022a) e o Guia de Requisitos e Obrigações quanto à Privacidade e à Segurança da Informação (BRASIL, 2024c).	apontada pelos fiscais, de previsão antecipada dos requisitos de segurança, evitando exigências apenas na execução contratual.	incluir cláusulas no ETP e no TR com justificativas técnicas.” E2 Ac 2362/2015-P, Ac 2569/2018-P e Ac 157/2024-P.
4. Especificar	Detalhar critérios técnicos de entrega, validação e medição de resultados dos serviços contratados, garantindo objetividade e rastreabilidade e na fiscalização.	Sempre que aplicável, definir de forma explícita, no Termo de Referência (TR), os critérios técnicos de entrega e os indicadores de medição de resultados (IMR). Recomenda-se usar o modelo de TR para serviços de TIC da Advocacia-Geral da União (AGU) (BRASIL, 2025a) como base para IMR e sanções. Os IMR devem conter fórmulas de cálculo, metas, unidades de medida, periodicidade, parâmetros de aceitação e cálculos para glosa, permitindo a avaliação objetiva da execução contratual. Especificar também as ferramentas ou sistemas aceitos para coleta e validação das evidências (como GLPI, SIEM, Zabbix, Bacula e Service Desk, entre outros), bem como os dados obrigatórios que devem constar nas evidências — hostname, IP, data, hora, responsável técnico e descrição da atividade. Nos casos que envolvam monitoramento contínuo, logs ou incidentes, exigir a assinatura digital dos relatórios e a integridade criptográfica dos registros, assegurando autenticidade, integridade e não repúdio. Essas especificações devem seguir as diretrizes da Instrução Normativa nº 94/2022/MGI, do *Framework* PPSI (BRASIL, 2024b) e do Guia de Requisitos e Obrigações (BRASIL, 2024c), para permitir a mensuração objetiva e padronizada dos resultados.	Resultado direto das queixas sobre fiscalização subjetiva e ausência de parâmetros técnicos mensuráveis.	“Normalmente só se fala em boas práticas, sem detalhar. Falta clareza em como os controles devem ser entregues e comprovados.” E2 Ac 1508/2020-P, Ac 157/2024-P e Ac 292/2025-P.
5. Evidenciar	Determinar o tipo, o formato e a qualidade mínima das evidências que	Definir, no Termo de Referência (TR) e/ou no Anexo de Fiscalização, os formatos e critérios de aceitação das evidências que devem ser entregues pela contratada. As evidências podem incluir relatórios	Responde à demanda dos entrevistados por provas documentais claras e	“Os contratos falam em controles, mas sem explicar como cobrar. Precisamos

	comprovam a execução dos controles de segurança e o cumprimento das obrigações contratuais.	técnicos padronizados, registros de logs, capturas de tela, laudos de teste, planilhas de verificação ou documentos assinados digitalmente, devendo conter dados obrigatórios como data, hora, responsável técnico e descrição do evento. Sempre que possível, adotar modelos de relatórios uniformes e exigir assinatura digital com certificado ICP-Brasil, garantindo autenticidade, integridade e não repúdio. Nos casos de controles contínuos (monitoramento, backup, antivírus, firewall, SIEM etc.), estabelecer a periodicidade de envio e retenção das evidências, conforme o disposto na Instrução Normativa nº 94/2022/MGI (BRASIL, 2022a), no *Framework* PPSI (BRASIL, 2024b) e no Guia de Requisitos e Obrigações (BRASIL, 2024c). Essas definições visam padronizar a comprovação técnica e evitar subjetividade na fiscalização, permitindo o cruzamento entre relatórios entregues e IMRs previstos no contrato.	rastreáveis da execução dos controles.	transformar a norma em cláusulas mais específicas.” E2 “Quando fica a cargo da contratada, os relatórios não vêm no padrão...” E5 Ac 2362/2015-P, Ac 2037/2019-P e Ac 157/2024-P.
6. Formalizar	Formalizar a obrigação da contratada em cláusula contratual específica, assegurando que os requisitos de segurança cibernética estejam expressos de forma clara e verificável.	Redigir cláusulas no Termo de Referência e no instrumento contratual que detalhem a periodicidade, o formato e o conteúdo mínimo das entregas e evidências relacionadas aos controles de segurança. As cláusulas devem ser objetivas e padronizadas, evitando termos genéricos como “boas práticas” sem definição operacional. Utilizar como referência a Instrução Normativa nº 94/2022/MGI (BRASIL, 2022a), o *Framework* PPSI (BRASIL, 2024b) e o Guia de Requisitos e Obrigações quanto à Privacidade e à Segurança da Informação (BRASIL, 2024c).	Alinhada ao construto “clareza contratual”, que destacou a falta de padronização e objetividade nas cláusulas de segurança.	“Precisa deixar claro quais evidências o fornecedor deve apresentar, não só citar o controle.” E4 Ac 915/2020-P, Ac 157/2024-P e Ac 292/2025-P.
7. Designar	Designar formalmente o responsável pela verificação técnica e comprovação dos controles de segurança, assegurando clareza quanto às funções e competências	Estabelecer, no Termo de Referência (TR) e no contrato, que o Fiscal Técnico será o responsável pela verificação periódica das entregas e das evidências apresentadas pela contratada, conforme os critérios e indicadores definidos no TR e nos Indicadores de Medição de Resultados (IMR). Recomenda-se que o fiscal disponha de *checklist*s (quando aplicável) e instrumentos de apoio à análise técnica, preferencialmente automatizados,	Proveniente do construto “desafios de fiscalização”, que apontou dependência excessiva da interpretação individual do fiscal.	“A fiscalização depende muito da interpretação do fiscal. Há dificuldade em validar relatórios técnicos sem ferramentas adequadas.” E2 Ac 980/2023-P, Ac 157/2024-P e

	atribuídas.	conforme orientam a Instrução Normativa nº 94/2022/MGI (BRASIL, 2022a), o *Framework* PPSI (BRASIL, 2024b) e o Referencial de Governança Organizacional (BRASIL, 2022c). Esse detalhamento visa reduzir a dependência da interpretação individual e garantir uniformidade e rastreabilidade na fiscalização técnica dos contratos.		Ac 1299/2025-P.
8. Monitorar	Garantir a rastreabilidade, integridade e arquivamento sistemático das evidências de execução contratual, assegurando histórico documental verificável das ações de fiscalização.	Definir, no Termo de Referência (TR) e no Plano de Fiscalização, o local, a periodicidade do registro e arquivamento das evidências, preferencialmente em sistemas oficiais de gestão documental, como o Sistema Eletrônico de Informações (SEI), o sistema de gestão contratual do órgão ou módulos integrados de TIC. O registro deve incluir relatórios mensais, logs, capturas de tela, comprovantes de backup e atas de reuniões de acompanhamento, devidamente assinados. Recomenda-se a criação de pastas ou processos específicos por contrato, contendo as evidências organizadas por período e tipo de controle, para permitir rastreabilidade completa e auditoria futura. Acompanhar os resultados por meio de reuniões periódicas, conforme os critérios definidos no TR.	Vincula-se ao construto "desafios de fiscalização", apontado pelos participantes como essencial para padronização e controle contínuo.	"Costumamos exigir relatórios mensais e reuniões de acompanhamento. Recebemos logs, relatórios assinados, prints e comprovantes de backup. O problema é que a fiscalização é pouca, há falta de padronização..." E4 2569/2018-P, 157/2024-P e 292/2025-P.