# Desenvolvimento de um Modelo de Checklist de Segurança Cibernética Aplicável às Contratações Públicas de TIC

**Telmo Nunes Costa, Rafael Rabelo Nunes**

Programa de Pós-Graduação Profissional em Engenharia Elétrica – PPEE - Universidade de Brasília, Faculdade de Tecnologia, Departamento de Engenharia Elétrica, Brasília, Brasil - CEP 70910-900.

telmo.nunes@gmail.com, rafaelrabelo@unb.br

***Resumo:*** *As contratações públicas de Tecnologia da Informação e Comunicação (TIC) têm papel central na modernização administrativa e na sustentação das políticas digitais do Estado brasileiro. A crescente dependência de serviços tecnológicos complexos e o elevado volume financeiro envolvido tornam esse segmento sensível a falhas de planejamento, controle e avaliação de resultados. O estudo analisou fragilidades recorrentes nas contratações públicas de Tecnologia da Informação e Comunicação (TIC), especialmente na definição de métricas, na mensuração de resultados e na verificação de conformidade técnica e teve como objetivo desenvolver um checklist de segurança da informação como instrumento orientador e de apoio à decisão nas contratações públicas de TIC cujo objeto envolva aspectos de segurança cibernética. Para isso, foram analisados acórdãos do Tribunal de Contas da União e realizadas entrevistas com especialistas das áreas de governança e fiscalização de TIC, comparando-as com a análise das diretrizes na Lei nº 14.133/2021 e da Instrução Normativa nº 94/2022/MGI, de frameworks nacionais e internacionais e do Referencial de Governança das Contratações Públicas do TCU. Com isso, foi possível identificar lacunas nos processos de planejamento e controle contratual, consolidando os achados em um modelo estruturado a partir de critérios técnicos e operacionais de verificação em formato de uma lista de verificação (checklist), oferecendo um instrumento aplicado e sistematizado que auxilia gestores públicos na incorporação efetiva de controles de segurança cibernética em contratações de TIC, fortalecendo a conformidade normativa, a transparência e a maturidade de 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) plays a central role in the administrative modernization and digital policy implementation of the Brazilian State. The growing dependence on complex technological services and the high financial investment involved make this segment particularly sensitive to failures in planning, control, and performance evaluation. This study analyzed recurrent weaknesses in public ICT procurements, especially regarding the definition of metrics, measurement of results,*

*and verification of technical compliance. The objective was to develop an information security checklist as a guiding and decision-support instrument for public ICT procurements involving aspects of cybersecurity. To this end, audit reports from the Federal Court of Accounts (TCU) were examined, and interviews were conducted with governance and ICT oversight specialists, comparing their insights with the guidelines established by Law No. 14.133/2021, Normative Instruction No. 94/2022/MGI, national and international frameworks, and the TCU's Public Procurement Governance Framework. The analysis made it possible to identify gaps in planning and contractual control processes, consolidating the findings into a structured model based on technical and operational verification criteria in the form of a practical checklist. As a contribution, this work provides an applied and systematized instrument that supports public managers in effectively incorporating cybersecurity controls into ICT procurements, strengthening regulatory compliance, transparency, and governance maturity in the public sector.*

*Keywords: ICT governance; public procurement; information security; checklist; risk management.*

## 1. Introdução

As contratações públicas de Tecnologia da Informação e Comunicação - TIC têm assumido papel central na modernização administrativa e na sustentação das políticas digitais do Estado Brasileiro (BRASIL, 2024a). A crescente dependência de serviços tecnológicos complexos, somada ao elevado volume financeiro envolvido, torna esse segmento particularmente sensível a falhas de planejamento, controle e avaliação de seus resultados (GUARDA; OLIVEIRA; SOUSA JÚNIOR, 2015).

Essa relevância é confirmada pelos dados do Tribunal de Contas da União - TCU, que registrou um crescimento expressivo no volume de recursos fiscalizados em contratações de TIC: cerca de R$ 5 bilhões no Ciclo 2023–2024 e R$ 8,08 bilhões no Ciclo 2024–2025 (BRASIL, 2025c).

O art. 6º do Decreto-Lei nº 200/1967 (BRASIL, 1967) estabelece que o princípio do planejamento e do controle pressupõe que a gestão defina metas, as acompanhe e avalie seus resultados. Assim, a ausência de indicadores e parâmetros de monitoramento representa violação direta a esses princípios, comprometendo a capacidade de a Administração de aferir o desempenho contratual (LIMBERGER; TEIXEIRA, 2016).

De igual modo, a definição clara de critérios de medição, periodicidade e evidências de desempenho constitui elemento essencial de governança nas contratações públicas, conforme o princípio do controle e da transparência previsto no art. 70 da Constituição Federal de 1988 (BRASIL, 1988).

A Lei nº 14.133/2021 (BRASIL, 2021) reforça essa exigência ao determinar a necessidade de acompanhamento, registro e comprovação da execução contratual, enquanto a Instrução Normativa nº 94/2022/MGI (BRASIL, 2022a) impõe a inclusão de indicadores de desempenho, critériosde medição e evidênciasde verificação nos artefatos de planejamento e fiscalização de TIC.

Em conjunto, esses dispositivos estruturam uma base normativa que visa não apenas a conformidade formal, mas o controle efetivo por resultados. Auditorias e estudos do Tribunal de Contas da União têm apontado lacunas na adoção de mecanismos de medição e comprovação de resultados nas contratações públicas de TIC (BRASIL, 2025c). O Tribunal reconhece que a ausência de indicadores objetivos viola os princípios da eficiência e da economicidade (BRASIL, 2019; BRASIL, 2021). No Acórdão nº 2.513/2019-Plenário (BRASIL, 2019), destaca-se a necessidade de indicadores para avaliar eficácia, eficiência e efetividade, vinculando desempenho e orçamento.

O Tribunal de Contas da União (TCU), por meio do Acórdão nº 2.959/2021-Plenário (BRASIL, 2021b), destaca que "a ausência de métricas configura fragilidade de gestão, dificultando a aferição do impacto administrativo". Já o Acórdão nº 1.508/2020-Plenário (BRASIL, 2020a), também do TCU, aponta que contratações fundamentadas em Unidades de Serviço Técnico carecem de critérios objetivos de avaliação, o que pode resultar em pagamentos desalinhados ao desempenho efetivo.

Por fim, o Acórdão nº 292/2025-Plenário (BRASIL, 2025e), ao examinar a contratação centralizada de computação em nuvem, enfatiza a importância do planejamento, da mitigação de riscos e da mensuração de resultados para assegurar a conformidade e o alcance dos objetivos pactuados.

Sob a ótica do Referencial de Governança das Contratações Públicas, essas lacunas caracterizam-se como uma falha de governança estratégica, pois interrompe o ciclo integrado de planejamento, execução, monitoramento e avaliação. A falta de métricas e de evidências verificáveis aumenta o risco de subjetividade na atuação dos fiscais, reduz a previsibilidade administrativa e compromete a eficiência e a economicidade da despesa pública (BRASIL, 2020b).

Essa problemática dialoga com o estudo de gestores públicos realizado por (GEORG et al. 2022), o qual aponta que, embora o arcabouço normativo brasileiro apresente bom nível de maturidade, ainda faltam diretrizes mais operacionais que orientem a implementação prática das políticas de segurança na Administração Pública Federal - APF.

Tal afirmação é coerente com o estudo de (SILVA, OLIVEIRA e CANEDO, 2016), que analisaram os riscos associados ao processo de Planejamento da Contratação de Soluções de TI - PCSTI na Administração Pública Federal - APF. Os autores demonstraram que a ausência de práticas consolidadas de gestão de riscos e de instrumentos metodológicos de apoio à decisão expõe as contratações de TIC a vulnerabilidades que comprometem o desempenho e a confiabilidade das entregas.

Diante desse contexto, o estudo propõe um *checklist* de segurança da informação como instrumento orientador e de apoio à decisão nas contratações públicas de TIC cujo objeto envolva aspec-tos de segurança cibernética.

Este artigo está estruturado da seguinte forma: a seção 2 apresenta o referencial teórico e os trabalhos relacionados; a seção 3 descreve os procedimentos metodológicos adotados; a seção 4 traz os resultados e a discussão; seção 5 apresenta as conclusões, limitações e sugestões para pesquisas futuras; e a seção 6 as referências.

## 2. Referencial Teórico

Este referencial organiza os fundamentos conceituais e normativos necessários à compreensão integral do estudo.

### 2.1. Fundamentos da Segurança da Informação e Cibernética

A segurança da informação é tradicionalmente compreendida como a preservação da confidencialidade, integridade e disponibilidade - CID das informações, princípios fundamentais que orientam a estrutura de um Sistema de Gestão da Segurança da Informação. Chagas e Rodrigues (2025) ressaltam que a implementação deum Sistema de Gestão de Segurança da Informação - SGSI baseado na ISO 27001(ISO; IEC,2022) visa precisamente garantir esses três pilares, promovendo um modelo contínuo de controle e melhoria voltado à proteção dos ativos informacionais.

A segurança cibernética amplia o conceito tradicional de segurança da informação ao abordar a proteção de dadose ativos no ciberespaço. Segundo Santos e Silva (2021), trata-se de ações direcionadas para a segurança de operações, com intuito a garantir que os sistemas de informação sejam protegidos contra ameaças no ciberespaço.

Nesse contexto, a gestão de riscos surge como elemento transversal da segurança da informação e da cibernética, Dos Santos (2021) define o risco com base na norma ABNT NBR ISO 31000 (ABNT, 2018) como um fato inerente às atividades empresariais, cuja gestão é fundamental para que as organizações tomem decisões assertivas e criem valor de forma sustentável. Segundo o autor, o risco representa a possibilidade de ocorrência de um evento futuro incerto que pode gerar efeitos positivos ou negativos sobre os objetivos organizacionais.

### 2.2. Frameworks de Segurança e Governança

O *Center for Internet Security* - CIS desenvolveu os *CIS Controls* v8 (CIS, 2021), um conjunto de 18 controles críticos distribuídos em grupos de implementação (IG1, IG2 e IG3), priorizados conforme o nível de maturidade organizacional. Esses controles são amplamente reconhecidos por sua objetividade e aplicabilidade prática, especialmente em órgãos públicos com recursos limitados (BRASIL, 2022b).

Além disso, estudos indicam que frameworks de segurança, como o *CIS Controls*, são amplamente reconhecidos como referenciais de boas práticas, mas evidenciam o desafio prático de operacionalizá-los (RODRIGUES; SILVA; OLIVEIRA, 2023).

Instituído pela Portaria SGD/MGI nº 852/2023 (BRASIL, 2023a), o Programa de Privacidade e Segurança da Informação - PPSI adotou os princípios do *CIS Controls* v8 às particularidades da Administração Pública Federal, oferecendo um framework nacional de segurança cibernética (BRASIL, 2024b).

O PPSI estrutura seus controles em Grupos de Implementação (IGs), que funcionam como etapas graduaisde consolidação da maturidadeem segurança, similar ao framework CIS. Essa organização permite que órgãos públicos com diferentes níveis de capacidade adotem controles de forma escalonada (BRASIL, 2024b).

A governança de TIC constitui uma referência consolidada para o alinhamento entre tecnologia, estratégia e controle organizacional (BRASIL, 2022c). Segundo Pereira e Borges (2023), o COBIT (COBIT, 2019) é um dos frameworks mais utilizados para a estruturação da governança e gestão de TIC, pois oferece um modelo de referência com domínios e processos definidos que permitem alinhar os objetivos estratégicos às práticas tecnológicas.

## 2.3. Marco Normativo e Instrumentos de Governança em Contratações de TIC

A Instrução Normativa nº 94/2022 constitui o principal instrumento regulatório sobre contratações de TIC no âmbito federal, definindo diretrizes para planejamento, seleção e gestão contratual. Ela também estabelece que toda contratação de TIC deve estar alinhada ao Plano Diretor de Tecnologia da Informação e Comunicação - PDTIC, instrumento que direciona investimentos e aquisições conforme as prioridades institucionais (BRASIL,2022a; BRASIL, 2025b).

Em complemento, o Guia de Requisitos e Obrigações quanto à Privacidade e à Segurança da Informação (BRASIL, 2024c) fornece orientações práticas para a elaboração do Termo de Referência, detalhando requisitos técnicos e controles aplicáveis às soluções de TIC.

Tais diretrizes estão em consonância com o Referencial de Governança das Contratações Públicas (BRASIL, 2020b), que define boas práticas para o planejamento, execução e monitoramento de contratos, com foco na prestação de contas e no alcance de resultados

Nesse mesmo contexto normativo, a proteção de dados pessoais e a gestão de riscos contratuais emergem como dimensões complementares da governança pública contemporânea, conforme D´Oliveira e Cunha (2024), a implementação da Lei Geral de Proteção de Dados - LGPD (BRASIL, 2018) requer políticas de transparência e cláusulas contratuais específicas que assegurem o tratamento ético e responsável das informações pessoais nas relações contratuais.

De forma convergente, Luiz (2023) destaca que a nova Lei de Licitações e Contratos Administrativos (BRASIL, 2021a) reforça a centralidade das cláusulas contratuais como instrumentos de responsabilização e controle, ao detalhar obrigações auditáveis e critérios objetivos de desempenho.

Já Mello e Garbaccio (2025) observam que, embora a mesma Lei de Licitações e Contratos represente um marco de probidade e transparência, especialmente ao exigir programas de integridade em contratações de grande vulto, sua efetividade depende da definição de métricas e mecanismos de governança contratual que permitam comprovar resultados e mensurar riscos.

## 3. Metodologia

Este estudo caracteriza-se como pesquisa aplicada, onde propõe um checklist de segurança da informação como instrumento orientador e de apoio à decisão nas contratações públicas de TIC cujo objeto envolva aspectos de segurança cibernética. De acordo com Gil (2008), a pesquisa aplicada tem como propósito a solução de problemas práticos, o que se alinha ao objetivo desta investigação.

A abordagem é de natureza qualitativa, pois busca compreender percepções e interpretações relacionadas à incorporação de controles de segurança em contratos. É também documental, por se apoiar na análise de normativos, guias e relatórios institucionais, e descritiva, por expor e organizar os elementos que orientam a formalização de requisitos de segurança em processos licitatórios (GIL, 2008).

O percurso metodológico foi desenvolvido em três etapas interligadas, conforme o fluxograma da Figura 1, detalhadas a seguir:

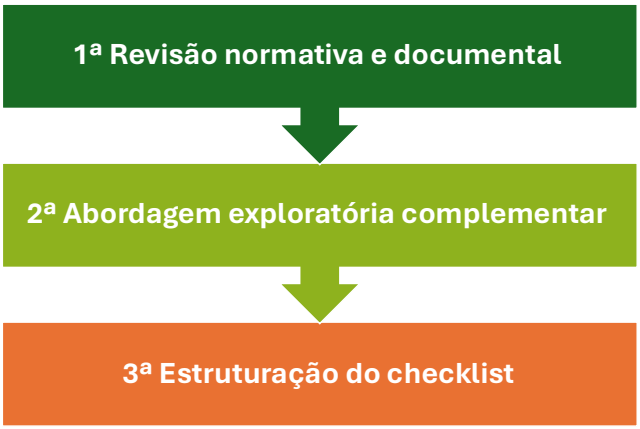


Figura 1 – Processo de Análise

### 3.1. Revisão normativa e documental

A pesquisa teve início com uma análise documental sistemática, orientada à identificação de falhas recorrentes nas contratações públicas de TIC e quais delas impactam diretamente a mensuração de resultados e o controle contratual, a partir do exame integral de todos os acórdãos disponibilizados pelo TCU no Portal de Acompanhamento de Aquisições de TIC, compreendendo os Acórdãos 2362/2015, 2569/2018, 2037/2019, 915/2020, 1508/2020, 1756/2021, 823/2022, 980/2023, 2185/2023, 157/2024, 1875/2024, 1432/2024, 292/2025 e 1299/2025 (BRASIL, 2025c).

Diferentemente do portal tradicional do TCU, voltado ao conjunto geral de processosde controle externo, o portal específico de TICconcentra-se nascontratações públicas da área de tecnologia, cujo acórdãos contém a síntese de dezenas de auditorias, com o objetivo de assegurar eficiência, economicidade e transparência nas aquisições (BRASIL, 2025c). Importa destacar que os acórdãos listados já estão presentes na página inicial do referido portal de TIC.

De acordo com Bowen (2009) a análise documental é um procedimento sistemático para revisar ou avaliar documentos, impressos ou eletrônicos, com o propósito de extrair significados, compreender fenômenos e desenvolver conhecimento empírico. Segundo o autor, "o procedimento analítico envolve encontrar, selecionar, avaliar (atribuir sentido) e sintetizar dados contidos nos documentos" (BOWEN, 2009, p. 28).

Para esta análise, foram examinados todos os acórdãos disponíveis no portal de TIC (totalizando 14 acórdãos à época da investigação), seguindo-se o procedimento de análise documental sistemática descrito por Bowen (2009), com o objetivo de identificar lacunas nos indicadores e métodos de aferição de resultados.

Além das decisões do TCU, foram analisados o Referencial de Governança das Contratações Públicas (BRASIL, 2020b) e os documentos orientadores do Ministério da Gestão e da Inovação em Serviços Públicos - MGI, como o Guia de Requisitos e Obrigações quanto à Privacidade e à Segurança da Informação (BRASIL, 2024c) e o Framework do Programa de Privacidade e Segurança da Informação (BRASIL, 2024b).

Também foram revisados os normativos nacionais aplicáveis à governança e ao processo licitatório, incluindo a Lei nº 14.133/2021 Lei de Licitações e Contratos Administrativos (BRASIL, 2021a, a Lei nº 13.709/2018 Lei Geral de Proteção de Dados – LGPD (BRASIL, 2018), a Instrução Normativa nº 94/2022/MGI (BRASIL, 2022a) e a Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023 (BRASIL, 2023b).

Em paralelo, foram avaliados *frameworks* internacionais de segurança, risco e governança, como o CIS *Controls* v8 (CIS, 2021), o COBIT 2019 (ISACA, 2019) e as normas ISO/IEC 27001 (ISO; IEC, 2022) e ABNT NBR ISO 31000 (ABNT, 2018), além de estudos especializados que evidenciam fragilidades na gestão de riscos e na mensuração de resultados em contratações públicas de TIC.

### 3.2. Abordagem exploratória complementar

Complementarmente, foi adotada uma abordagem exploratória, fundamentada em entrevistas semiestruturadas com especialistas da Administração Pública que atuam em processos de contratação e fiscalização de serviços de TIC . É oportuno mencionar que foram utilizados os dados da etapa anterior para compor o questionário utilizado nas entrevistas.

As entrevistas foram conduzidas individualmente, com duração média de 20 minutos, entre os meses de setembro e outubro de 2025.

Participaram seis servidores públicos com atuação direta em processos de contratação de TIC, abrangendo os perfis de técnico administrativo, fiscal de contrato, gestor de contrato, pregoeiro, chefe do setor de contratações de TIC e consultor jurídico, com tempo de experiência na área variando entre cinco e quinze anos.

Todas as entrevistas foram realizadas de forma on-line, devidamente gravadas e tiveram como propósito identificar percepções, dificuldades práticas e experiências relacionadas ao processo licitatório de soluções de TIC.

As entrevistas foram guiadas pelos seguintes temas orientadores:

Perfil e experiência: Identificação da função do entrevistado, tempo de atuação e experiência na elaboração, gestão e/ou fiscalização de contratações públicas de TIC.

Consideração de riscos e detalhamento no planejamento: Questionamento de como os riscos de segurança cibernética são tratados nas fases iniciais do processo, incluindo o nível de detalhamento dos controles nos artefatos (ETP e TR) e as dificuldades encontradas.

Papel dos controles na seleção do fornecedor: Visão do entrevistado sobre o impacto dos critérios e requisitos de segurança cibernética na fase de seleção.

Fiscalização e evidências utilizadas: Identificação dos mecanismos adotados para fiscalizar contratos de TIC, tipos de evidências considerados válidos e barreiras enfrentadas na monitoração da execução contratual.

Opiniões sobre lista de verificação (*checklist*): Prospecção e conveniência de uma lista de verificação como instrumento de apoio para contratação, gestão e fiscalização contratual, além da identificação de elementos considerados essenciais (ex.: critérios objetivos, indicadores, periodicidade, evidências, rastreabilidade, alinhamento entre documentos e clareza para o fornecedor).

Lacunas da IN nº 94/2022 e melhorias sugeridas: Percepção dos entrevistados sobre dispositivos da normativa que não são plenamente refletidos nos contratos, bem como sugestões de critérios e evidências que podem aprimorar a conformidade e a fiscalização.

Os dados qualitativos coletados foram tratados por meio da análise de conteúdo de Bardin (BARDIN, 2016), seguindo as etapas de pré-análise, exploração do material e tratamento dos resultados. A partir desse processo, foram identificadas unidades de registro que, após categorização, originaram construtos analíticos.

O estudo respeitou os princípios éticos científicos, garantindo anonimato e confidencialidade, em conformidade com a Resolução CNS nº 510/2016 (BRASIL, 2016).

### 3.3. Estruturação do Checklist

Concebido como uma ferramenta metodológica de governança e apoio à decisão (BRASIL, 2020b; ABNT, 2018), o checklist propõe sistematizar a verificação dos requisitoscontratuais, reduzira exposição a falhasde controle,fortalecer amensuração objetiva de desempenho e aperfeiçoar a rastreabilidade das evidências de execução, promovendo transparência e aprendizado institucional na gestão das contratações públicas de TIC.

Dessa forma, confrontaram-se os achados dos acórdãos e normativos (validade normativa) com frameworks técnicos (validade técnica) e com as percepções dos especialistas, buscando pontos de convergência e divergência capazes de sustentar a derivação de critérios objetivos para o instrumento proposto.

## 4. Resultados e Discussões

Esta seção apresenta os principais resultados obtidos e está organizada para evidenciar a convergência entre diretrizes normativas e as percepções práticas dos especialistas, destacando lacunas e oportunidades que subsidiaram a construção do checklist.

### 4.1. Revisão normativa documental

A revisão normativa e documental evidenciou convergências e lacunas entre os dispositivos legais, as orientações administrativas e as boas práticas internacionais de governança e segurança cibernética aplicáveis às contratações de TIC.

De modo geral, observou-se que o arcabouço regulatório abordado neste estudo composto pela Lei nº 14.133/2021, Lei nº 13.709/2018 e Instrução Normativa nº 94/2022/MGI (BRASIL, 2021a; BRASIL, 2018; BRASIL, 2022a) apresentam diretrizes para planejamento e gestão contratual, porém ainda carece de mecanismos operacionais padronizados para a comprovação de resultados e aferição de desempenho (GEORG et al., 2022).

As análises dos acórdãos do Tribunal de Contas da União reforçam essa constatação. O Acórdão nº 2.513/2019-Plenário (BRASIL, 2019) destacou a ausência de indicadores objetivos capazes de mensurar eficácia, eficiência e efetividade das entregas, vinculando essa fragilidadeàfalta de correlação entre recursosorçamentários e resultados obtidos.

O modelo baseado em Unidades de Serviço Técnico - UST, antes considerado uma alternativa moderna e eficaz (ARAÚJO, 2017), acabou revelando fragilidades, conforme apontado pelo Acórdão nº 1.508/2020-Plenário (BRASIL, 2020a) do Tribunal de Contas da União, a ausência de critérios objetivos de aferição levou à realização de pagamentos dissociados dos resultados efetivamente alcançados.

Já o Acórdão nº 292/2025-Plenário (BRASIL, 2025e), ao acompanhar a contratação centralizada de serviços de computação em nuvem, ressaltou a deficiência de métricas de monitoramento e de mecanismos de mensuração de resultados, classificando tais lacunas como fatores de risco à efetividade contratual.

Ademais, a metodologia aplicada possibilitou mapear, de forma comparada e cronológica, as ocorrências relacionadas a falhas recorrentes nas contratações públicas de TIC, notadamente aquelas vinculadas à ausência de métricas, indicadores e métodos de aferição de resultados.

Essas ocorrências evidenciam a repetição do tema em 11 dos 14 acórdãos estudados, apenas 3 acórdãos não tratam de métricas, indicadores e métodos de aferição de resultados (823/2022, 1432/2024, e 1875/2024), evidenciando a deficiência de métricas e indicadores como um risco recorrente observado pelo Tribunal de Contas da União nas contratações públicas de TIC ao longo da última década. A Tabela 1 evidencia os achados frente ao conteúdo dos acórdãos.

| Acórdão | Análise / Achado(s) | Fragmento / Acordão |
|---|---|---|
| **2362/2015 Plenário** | 1- Importância da definição de níveis de serviços para aferir resultados.<br><br>2- Importância da efetiva fiscalização do contrato.<br><br>3- Importância da clareza nas métricas utilizados para aferir resultados e pagamentos. | ...considerarem fatores capazes de maximizar as possibilidades de sucesso das contratações...<br>...especificação de níveis de serviços...<br>...efetiva fiscalização do cumprimento das cláusulas contratuais...<br>...nível de serviço como mecanismo de pagamento por resultados...<br>...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 serviços para aferir resultados.<br><br>2- Importância da clareza nas métricas utilizados para aferir resultados e pagamentos.<br><br>3- Importância do estabelecimento de penalidades ao descumprimento de níveis de serviço e alinhamento ao PDTI. | ...cláusulas contratuais relacionadas a níveis de serviço que sejam alinhadas aos objetivos de negócio...<br>...é necessário explicitar, de forma clara, as condições contratuais que definem o período de vigência dos serviços e a responsabilidade do fabricante...<br>...estabelecimento de penalidades padrões que sejam compatíveis e diretamente relacionadas ao descumprimento desses níveis de serviço, de forma a induzir a aplicação das sanções...<br>...ausência de alinhamento ao Plano Diretor de Tecnologia da Informação (PDTI)... |

| | | |
|---|---|---|
| **2037/2019 Plenário** | 1- Importância da clareza e rastreabilidade (métricas e evidências).<br><br>2-Importância da definição de indicadores de resultados.<br><br>3-Importância do alinhamento com o PDTI. | ...a utilização de métrica cuja medição não seja passível de verificação afronta o disposto na Súmula TCU 269 (Acórdão 916/2015-Plenário, item 9.1.6.8)...<br>...os serviços especificados no Catálogo de Serviços devem estar diretamente vinculados aos resultados esperados da contratação...<br>...irregularidades no planejamento das contratações: ausência de alinhamento ao PDTI; |
| **915/2020 Plenário** | 1- Importância da clareza e rastreabilidade (métricas e evidências).<br><br>2-Importância da definição de indicadores de resultados. | ... ausência de detalhamento dos custos de serviços medidos por UST e métricas semelhantes...<br>...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 rastreabilidade (métricas e evidências).<br><br>2- Importância da definição de indicadores de resultados.<br><br>3- Importância da padronização da unidade de medida (métricas de aferição de resultados). | ...UST, em termos gerais, implica a elaboração de artefatos que viabilizem a adequada e razoável mensuração e definição dos preços das atividades ou serviços, tais como: (i) catálogo de serviços, assim como referido anteriormente, 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, aos perfis de 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.<br>...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...<br>...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).<br><br>2- Importância da definição de indicadores de resultados.<br><br>3- Importância do registro / 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 serviços; e (iv) ausência de catálogo de serviços...<br>...também foram apresentadas as vulnerabilidades encontradas, tais como: (i) ausência da planilha de custos e formação de preços; (ii) catálogo de serviços sem critérios de aceitabilidade acercada 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<br>...Em função das fragilidades nos planejamentos das contratações identificadas nos dois ciclos do acompanhamento...<br>... 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 de contratação de serviços foram considerados como de alto risco para escolha de auditoria, devido a sua recorrência. | ...a equipe de acompanhamento aplicou critérios de maior risco, relevância, materialidade e oportunidade para 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 compões a solução de TIC.<br><br>2- Clareza nas métricas utilizadas para a composição dos serviços contratados.<br><br>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...<br>...procedimentos com textos genéricos, sem detalhamento ou listas de verificação, para que os respectivos fiscais verificassem a autenticidade, a correspondência com o que foi proposto e o quantitativo... |
| **1432/2024 Plenário** | 1- Importância do detalhamento dos itens que compões 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 clareza das responsabilidades do contratante e do contratado.<br><br>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, de modo a estabelecer a forma de comunicação entre as partes do contrato e a definir as responsabilidades de cada uma...<br>...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. | ...os agentes públicos responsáveis pelo planejamento das contratações devem, sempre que possível, utilizar padrões estabelecidos...<br>... é possível otimizar o uso dos recursos públicos... |

| | | |
|---|---|---|
| | 2- Reconhecimento de problemas relacionados a carga e efetivo da unidade de TIC que elabora as contratações. | ...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 detalhamento das evidências para assegura a devida execução dos serviços.<br><br>2- Menção ao Guia de boas práticas em contratação de soluções de TIC do TCU para alinhar definições sobre elementos de contratações. | ..."o órgão ou entidade deve avaliar a utilização de mecanismos e 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"...<br>...o Guia de boas práticas em contratação de soluções de tecnologia da informação, elaborado pelo TCU[endnoteRef:7], 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 ao resultado/qualidade que foi 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...<br>...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 Acórdão 2037/2019-TCU-Plenário, de relatoria do Ministro Substituto Augusto Sherman, e no Acórdão 1508/2020-TCU-Plenário... |

Tabela 1 – Pesquisa_Acórdãos

Esses achados convergem com o Referencial de Governança das Contratações Públicas, que define a mensuração de resultados e a definição de indicadores como elementos estruturantes do ciclo de governança (BRASIL, 2020b). Também corroboram os apontamentos de (GUARDA; OLIVEIRA; SOUSA JÚNIOR, 2015) e (Limberger; Teixeira, 2016), que identificaram deficiências no monitoramento de contratos de TIC e na formalização de evidências de execução.

Em âmbito normativo, o Guia de Requisitos e Obrigações quanto à Privacidade e à Segurança da Informação e o Framework do PPSI reafirmam a importância da coleta de evidências e da verificação de conformidade (BRASIL, 2024b; BRASIL, 2024c).

De forma similar, frameworks e normas internacionais, como o *CIS Controls* v8 (CIS, 2021), o COBIT 2019 (ISACA, 2019) e as normas ISO/IEC 27001 (ISO; IEC, 2022) e ABNT NBR ISO 31000 (ABNT, 2018), amparam a importância de controles mensuráveis, monitoráveis e auditáveis, reforçando que a definição de métricas e mecanismos de verificação contínua é essencial para reduzir riscos e garantir efetividade (ROSSI, 2023; PEREIRA; BORGES, 2023; CHAGAS; RODRIGUES, 2025; DOS SANTOS, 2021).

## 4.2. Abordagem exploratória complementar

A análise de conteúdo das entrevistas permitiu identificar três construtos principais que refletem os fatores críticos observados nas contratações públicas de TIC: clareza contratual, desafios de fiscalização e checklist.

Esses construtos sintetizam as percepções dos especialistas e representam a transposição prática das categorias definidas no roteiro de entrevistas.

### 4.2.1. Construto 1 – Clareza contratual

Segundo os relatos obtidos uma das principais fragilidades percebidas pelos entrevistados refere-se à forma como os requisitos de segurança cibernética são traduzidos nos documentos de contratação, especialmente 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:

*"Falta clareza em como os controles devem ser entregues e comprovados."*

*"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"*

Essa ausência de detalhamento contratual compromete a exequibilidade das obrigações e aumenta a subjetividade na fiscalização. Além disso, parte dos respondentes apontou que, sem indicadores objetivos, torna-se difícil aplicar sanções em caso de descumprimento, o que afeta a própria segurança jurídica da contratação.

Dessa forma, as ideias apresentadas foram agrupadas para formar o construto "Clareza Contratual", que reflete a necessidade de traduzir normas e guias técnicos em cláusulas objetivas, executáveis e passíveis de mensuração.

CONSTRUTO 1: CLAREZA CONTRATUAL

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 da execução dos contratos de TIC ainda é fortemente dependente de relatórios subjetivos e da capacidade técnica individual dos fiscais. A ausência de guias claros e indicadores objetivos aumenta a margem para interpretações divergentes.

*"A fiscalização depende muito da interpretação do fiscal. Há dificuldade em validar relatórios técnicos sem ferramentas adequadas.*

*"O problema é que a fiscalização é pouca, há falta de padronização e os dados vêm incompletos."*

CONSTRUTO 2: DESAFIOS DE FISCALIZAÇÃO

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 na percepção de que uma ferramenta de apoio como um *checklist* só será útil se contemplar critérios objetivos e auditáveis, capazes de orientar tanto a elaboração das cláusulas quanto a sua fiscalização. Nesse sentido, foram destacados itens considerados indispensáveis:

*"Na Análise de risco – identificar ativos críticos, dados pessoais e sensíveis, usando o PDTIC como apoio. Avaliação de impacto – considerar impacto na continuidade dos serviços. Alinhar no planejamento – incluir cláusulas no ETP e TR com justificativas técnicas. Redação contratual – cláusulas auditáveis, métricas de aceitação e periodicidade."*

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

CONSTRUTO 3: *CHECKLIST*

1. Definição de métricas
2. Periodicidade
3. Evidências claras
4. Rastreabilidade
5. Alinhamento ETP/TR
6. Utilizar documentos de apoio
7. Mapear riscos/impactos
8. Clareza para o fornecedor

Deste modo, o conjunto dos construtos corrobora que as fragilidades não são decorrem da ausência de normativos ou guias técnicos, mas da dificuldade em traduzi-los em práticas contratuais (visto nas seções anteriores).

Conforme demonstrado nas entrevistas em muitos casos, essa limitação também está associada a fatores contextuais, como a falta de atenção decorrente da sobrecarga de atividades, a escassez de tempo para detalhar adequadamente os instrumentos de contratação ou ainda a deficiência de apoio jurídico para converter orientações normativas em cláusulas exequíveis. Essa constatação também foi evidenciada no acórdão 1875/2024 (supra).

## 4.3. Estruturação do *checklist*

Com base na análise normativa documental, associada à exploração empírica conduzida por meio da análise de conteúdo de Bardin (BARDIN, 2016), o estudo estruturou um *checklist* de segurança cibernética voltado às contratações públicas de TIC quando objeto de segurança cibernética.

A construção do instrumento fundamentou-se no rito da Instrução Normativa nº 94/2022 (BRASIL, 2022). As falas dos entrevistados evidenciaram três fatores críticos, clareza contratual, desafios de fiscalização e checklist que se tornaram eixos estruturantes do checklist.

À luz dos resultados obtidos e considerando o fluxo lógico estabelecido pela IN 94/2022 (BRASIL, 2022), que se inicia na análise da necessidade e culmina no monitoramento da execução contratual, procedeu-se à seleção, priorização e sistematização dos controles e critérios de segurança, os quais foram organizados em oito etapas práticas: Analisar, Identificar, Integrar, Especificar, Evidenciar, Formalizar, Designar e Monitorar. As características de cada etapa são apresentadas na Tabela 2.

## Checklist de Segurança Cibernética em Contratações de TIC

| Nº | 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 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).<br>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, quando nuvem, Portaria SGD/MGI nº 5.950 (BRASIL, 2023b).<br>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 sensíveis, usando o PDTIC como apoio..."* / *2569/2018-Plenário, 2037/2019-Plenário e 980/2023-Plenário.* |

| Nº | Descrição | Detalhamento | Decorrência Empírica | Entrevistado / Acórdão Relacionado |
|---|---|---|---|---|
| **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."* / 1508/2020-Plenário, 823/2022-Plenário e1875/2024-Plenário. |
| **3. Integrar** | Inserir as exigências de segurança cibernética nos artefatos iniciais da contratação, assegurando que os controles e requisitos estejam previstos desde a etapa de planejamento. | Prever os controles e medidas de mitigação de riscos no Estudo 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) | Reflete a necessidade, apontada pelos fiscais, de previsão antecipada dos requisitos de segurança, evitando exigências apenas na execução contratual. | *"Alinhar no planejamento – incluir cláusulas no ETP e TR com justificativas técnicas."* / 2362/2015-Plenário, 2569/2018-Plenário e 157/2024-Plenário. |

| Nº | Descrição | Detalhamento | Decorrência Empírica | Entrevistado / Acórdão Relacionado |
|---|---|---|---|---|
| **4. Especificar** | Detalhar critérios técnicos de entrega, validação e medição de resultados dos serviços contratados, garantindo objetividade e rastreabilidade 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.<br>Os IMR devem conter fórmulas de cálculo, metas, unidades de medida, periodici-dade, 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, Service Desk, entre outros), bem como os dados obrigatórios que devem constar nas evidências - hostname, IP, data, hora, responsável técnico e descrição da atividade.<br>Nos casos que envolvam monitoramento contínuo, logs ou incidentes, exigir a assinatura digital dos relatórios e 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) de modo a 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."* / 1508/2020-Plenário, 157/2024-Plenário e 292/2025-Plenário. |

| Nº | Descrição | Detalhamento | Decorrência Empírica | Entrevistado / Acórdão Relacionado |
|---|---|---|---|---|
| **5. Evidenciar** | Determinar o tipo, o formato e a qualidade mínima das evidências que comprovam a execução dos controles de segurança e o cumprimento das obrigações contratuais. | 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.<br>As evidências podem incluir relatórios 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.<br>Sempre que possível, adotar modelos de relatórios uniformes e exigir assinatura digital com certificado ICP-Brasil, garantindo autenticidade, integridade e não repúdio.<br>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. | Responde à demanda dos entrevistados por provas documentais claras e rastreáveis da execução dos controles. | *"Os contratos falam em controles, mas sem explicar como cobrar. Precisamos transformar a norma em cláusulas mais específicas." "Quando fica a cargo da contratada, os relatórios não vêm no padrão ..."* / 2362/2015-Plenário, 2037/2019-Plenário e 157/2024-Plenário. |
| **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.<br>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."* / 915/2020-Plenário, 157/2024-Plenário e 292/2025-Plenário. |

| Nº | Descrição | Detalhamento | Decorrência Empírica | Entrevistado / Acórdão Relacionado |
|---|---|---|---|---|
| **7. Designar** | Designar formalmente o responsável pela verificação técnica e comprovação dos controles de segurança, assegurando clareza quanto às funções e competências atribuídas. | 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).<br>Recomenda-se que o fiscal disponha de *checklists* (quando aplicável) e instrumentos de apoio à análise técnica, preferencialmente automatizados, conforme orientam a Instrução Normativa nº 94/2022/MGI (BRASIL, 2022a), o Framework PPSI (BRASIL, 2024b) e o Referencial de Governança das Contratações Públicas (BRASIL, 2020b).<br>Esse detalhamento visa reduzir a dependência da interpretação individual e garantir uniformidade e rastreabilidade na fiscalização técnica dos contratos. | 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."* / *980/2023-Plenário, 157/2024-Plenário e 1299/2025-Plenário.* |
| **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 (definir periodicidade), logs, capturas de tela, comprovantes de backup e atas de reuniões de acompanhamento, devidamente assinados.<br>Recomenda-se a criação de pastas ou processos específicos por contrato, contendo as evidências organizadas por período e tipo de controle, de modo a 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, comprovantes de backup. O problema é que a fiscalização é pouca, há falta de padronização..."* / *2569/2018-Plenário, 157/2024-Plenário e 292/2025-Plenário* |

Tabela 2 – *Checklist*

## 5. Conclusão

Este estudo teve como objetivo desenvolver um *checklist* de segurança da informação como instrumento orientador e de apoio à decisão nas contratações públicas de TIC cujo objeto envolva aspectos de segurança cibernética.

Partindo da análise de acórdãosdo Tribunal de Contasda União (TCU) e de entrevistas com especialistas em governança e fiscalização de TIC, a pesquisa evidenciou que, embora o arcabouço normativo brasileiro tenha avançado de forma significativa, as contratações públicas ainda enfrentam fragilidades recorrentes nos processos de planejamento, controle e mensuração de resultados.

Constatou-se que tais fragilidades decorrem, em grande parte, da ausência de critérios objetivos de desempenho e de mecanismos padronizados de comprovação de resultados, o que compromete a eficiência e a economicidade das contratações.

A pesquisa documental confirmou que essa lacuna é reiteradamente observada pelo TCU em seus acórdãos, revelando um padrão histórico de inconsistências na tradução das exigências legais em práticas de governança efetivas.

Nesse sentido, mesmo com os avanços promovidos pela Lei nº 14.133/2021, que consolidou princípios de planejamento e controle orientados por resultados, e pela Instrução Normativa nº 94/2022/MGI, que instituiu diretrizes técnicas específicas para contratações de TIC, a distância entre a norma e a execução ainda persiste, especialmente no que tange à mensuração de desempenho e à rastreabilidade de evidências contratuais.

Com base nesse diagnóstico, o estudo propôs um *checklist* de segurança da informação concebido como ferramenta metodológica de governança, integrando dimensões normativas, técnicas e operacionais.

O instrumento foi construído a partir da triangulação entre:

(i) análise normativa e jurisprudencial, que fundamentou os critérios mínimos de conformidade e controle;

(ii) entrevistas com especialistas, que permitiram compreender as limitações práticas e as necessidades de padronização percebidas por gestores e fiscais; e

(iii) referenciais nacionais e internacionais, como o COBIT 2019 (ISACA, 2019), o Programa de Privacidade e Segurança da Informação (PPSI), o Guia de Requisitos e Obrigações quanto à Privacidade e à Segurança da Informação (BRASIL, 2024c), o Referencial de Governança das Contratações Públicas (BRASIL, 2020b), a ISO/IEC 27001:2022 (ISO; IEC, 2022) e a ABNT NBR ISO 31000:2018 (ABNT,2018).

Como contribuição, o estudo busca uma abordagem inovadora ao posicionar o *checklist* não apenas como um roteiro de verificação, mas como uma ferramenta que orienta a entrega, a produção de evidências e a definição de indicadores de desempenho, organizada em etapas que abrangem desde a análise de riscos e impactos até o monitoramento e o registro das evidências contratuais. Dessa forma, a proposta tem potencial para fortalecer a gestão por resultados e promover maior transparência na fiscalização técnica.

Em termos de limitações, reconhece-se que a pesquisa se baseou em uma abordagem qualitativa, com número restrito de entrevistas e foco no contexto da Administração Pública Federal, o que pode limitar a generalização dos resultados.

Como perspectivas para pesquisas futuras, recomenda-se a validação empírica do *checklist* em diferentes órgãos e tipos de contrato, de modo a mensurar sua efetividade em contextos variados, bem como sua contribuição para a maturidade em gestão de riscos cibernéticose para o aprimoramento daspráticasde governança dascontratações públicas de TIC.

Além disso, sugere-se a realização de estudos quantitativos de correlação entre o uso de instrumentos de verificação e os indicadores de desempenho contratual, ampliando a compreensão sobre como metodologias estruturadas de controle podem impactar positivamente a eficiência, a conformidade e a segurança institucional no setor público.

Em síntese, o estudo reafirma que a governança de TIC orientada por métricas e evidências é condição essencial para a segurança cibernética e a integridade das contratações públicas, e que o checklist proposto representa um passo rumo à consolidação de práticas de gestão mais transparentes, auditáveis e alinhadas à cultura de resultados no âmbito da Administração Pública brasileira.

## 6. Referências


ARAÚJO, Pedro Augusto Córdova 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_PedroAugustoCordovaDeAraujo_tcc.pdf. Acesso em: 23 out. 2025.

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

BARDIN, L. (BARDIN, 2016). *Análise de conteúdo* (4ª ed.). Edições 70.

BOWEN Glenn A. **2009** "Document Analysis as a Qualitative Research Method", 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, DF, 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**. *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**. https://www.gov.br/governodigital/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**. 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). Disponível em: https://www.gov.br/servicoscompartilhados/pt-br/assuntos/gestao-documental/sistema-eletronico-de-informacoes-sei **2013**. 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 27 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, [s.d.] **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 Bruno Dantas. Brasília, DF, **2025d**. Disponível em: https://pesquisa.apps.tcu.gov.br/. Acesso em: 21 out. 2025.

BRASIL. TRIBUNAL DE CONTAS DA UNIÃO. *Acórdão nº 1.508/2020-Plenário.* Relator: Ministro Augusto Nardes. Brasília, DF, **2020a**. Disponível em: https://pesquisa.apps.tcu.gov.br/documento/acordao-completo/1.508%252F2020/%2520/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/11. Acesso em: 21 out. 2025.

BRASIL. TRIBUNAL DE CONTAS DA UNIÃO. *Acórdão nº 2.513/2019-Plenário.* Relator: Ministro Augusto Nardes. Brasília, DF, **2019**. Disponível em: https://pesquisa.apps.tcu.gov.br/documento/acordao-completo/2.513%252F2019/%2520/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/3. 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/documento/acordao-completo/2.959%252F2021/%2520/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/5. Acesso em: 21 out. 2025.

BRASIL. TRIBUNAL DE CONTAS DA UNIÃO. *Acórdão nº 292/2025-Plenário.* Relator: Ministro Walton Alencar Rodrigues. Brasília, DF, **2025e**. Disponível em: https://pesquisa.apps.tcu.gov.br/documento/acordao-completo/292%252F2025/%2520/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/0. 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/data/files/4D/E3/DF/81/8C0848102DFE0FF7F18818A8/__5%20Controles%20de%20seguranAa%20cibernAtica%20para%20ontem_final_web.pdf. Acesso em: 11 ago. 2025.

BRASIL. TRIBUNAL DE CONTAS DA UNIÃO. Licitações e Contratos: Orientações e Jurisprudência do TCU. 5. ed. Brasília: TCU, **2024d**.

BRASIL. TRIBUNAL DE CONTAS DA UNIÃO. Referencial Básico de Governança de Tecnologia da Informação. 3. ed. Brasília: TCU, **2020b**.

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

*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**. 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 Passos Conceição; CUNHA, Francisco José Aragão Pedroza. Lei Geral de Proteção de Dados (LGPD): a relação entre as políticas e os regimes de informação. **2024** Disponível em: https://www.scielo.br/j/rdbci/a/DWntpkXMB9GgCPKycFcxtts/?lang=pt . Acesso em: 13 out. 2025

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

GEORG, Marcus Aurélio Carvalho; RODRIGUES, Walisson Magno Silva; ALVES, Carlos André de Melo; SILVEIRA JÚNIOR, Aldery; NUNES, Rafael Rabelo. 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 (RISTI), 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, A. C. Métodos e técnicas de pesquisa social (6ª ed.) **2008**. Atlas.

GUARDA, G. F., OLIVEIRA, E. C., & SOUSA JÚNIOR, R. T. de. Analisys 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. Disponível em: https://doi.org/10.4301/S1807-17752015000100005 .**2015**. Acesso em: 21 out. 2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO); INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC). ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements. 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. Disponível em: https://doi.org/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.

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.

PEREIRA, Joyce Mariana; BORGES, Daniel Clarismundo. 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.

ROSSI, Juliano Scherner. 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 Batista dos; SILVA, Tiago Barros Pontes e. *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.Disponível em: https://www.scielo.br/j/rdbci/a/ny4trmDrqqPVshh5yRZwWtp/?lang=pt. 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.