A ETIR além da Resposta a Incidentes: Evidências de sua Atuação como Estrutura de Governança Operacional na Administração Pública Federal

Ailton Soares de Aguiar
Universidade de Brasília (UnB)
Brasília, Distrito Federal, Brasil
ailton.aguiar@esporte.gov.br

Edna Dias Canedo
Universidade de Brasília (UnB)
Brasília, Distrito Federal, Brasil
ednacanedo@unb.br

Abstract

Contexto: A crescente digitalização da Administração Pública Federal ampliou a dependência de serviços digitais e evidenciou a necessidade de mecanismos capazes de integrar segurança da informação, proteção de dados pessoais e gestão de riscos. Embora o Programa de Privacidade e Segurança da Informação (PPSI) estabeleça diretrizes para fortalecer a governança da informação, ainda há poucas evidências empíricas sobre o papel da Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR) como estrutura de governança operacional. Objetivo: Investigar em que medida a ETIR desempenha funções típicas de uma estrutura de governança operacional na Administração Pública Federal, analisando capacidades relacionadas à governança normativa, coordenação institucional, implementação operacional, aprendizado organizacional e consolidação estratégica. Método: Foi conduzido um estudo exploratório baseado em um survey com 23 profissionais de diferentes órgãos da Administração Pública Federal. Os dados quantitativos foram analisados por estatística descritiva e as respostas abertas por meio de análise temática. Resultados: Os resultados indicam que a ETIR já exerce papel relevante na operacionalização da governança da segurança da informação, especialmente na coordenação da resposta a incidentes, implementação de controles operacionais e promoção do aprendizado organizacional. Entretanto, persistem desafios relacionados à integração entre áreas, retenção do conhecimento, disponibilidade de recursos humanos especializados, apoio da alta administração e institucionalização das práticas de governança. A análise permitiu identificar cinco capacidades organizacionais que sustentam a atuação da ETIR como estrutura de governança operacional. Conclusões: Os resultados sugerem que a efetividade da ETIR transcende sua função técnica tradicional de resposta a incidentes, configurando-a como um mecanismo de integração entre governança, gestão de riscos, coordenação institucional e melhoria contínua. Como principal contribuição, o estudo propõe um modelo conceitual que descreve as capacidades organizacionais necessárias para consolidar a ETIR como estrutura de governança operacional na Administração Pública Federal.

Keywords

Governança Operacional; Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR); Governança da Segurança da Informação; Administração Pública Federal; Resiliência Cibernética

1 Introdução

A expansão da transformação digital no setor público tem redefinido profundamente os paradigmas de governança da informação, impondo novos desafios relacionados à segurança, privacidade e resiliência cibernética [15]. Em um ambiente caracterizado pela crescente sofisticação das ameaças digitais e pela ampliação da dependência de serviços públicos digitais, a Administração Pública Federal passa a demandar não apenas frameworks normativos de segurança, mas estruturas organizacionais capazes de operacionalizar respostas rápidas, coordenadas e continuamente aperfeiçoadas, sob pena de comprometimento da continuidade dos serviços públicos e da própria confiança institucional [2].

Nesse contexto, a proteção de dados pessoais deixa de representar apenas uma exigência regulatória e passa a ocupar posição central na governança da informação estatal, sendo compreendida como desdobramento do direito fundamental à privacidade e da autodeterminação informativa[6]. A crescente circulação e processamento de dados pessoais pelo Estado ampliam os riscos associados a incidentes cibernéticos e evidenciam a necessidade de mecanismos institucionais capazes de assegurar não apenas conformidade normativa, mas efetiva proteção dos direitos dos titulares de dados[22]. No contexto brasileiro, esse movimento é consolidado pela Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018)[6], que estabelece obrigações rigorosas quanto à adoção de medidas

técnicas e administrativas aptas a prevenir incidentes de segurança da informação. Em complemento, o Ministério da Gestão e da Inovação em Serviços Públicos (MGI), por meio da Portaria SGD/MGI nº 852/2023, institui o Programa de Privacidade e Segurança da Informação (PPSI), reforçando a tentativa de estruturar uma governança mais integrada, orientada à gestão de riscos e à proteção de dados como política pública [2, 13].

Todavia, estudos sobre governança de tecnologia da informação demonstram que a simples adoção de normas, políticas e frameworks não garante, por si só, maturidade organizacional ou capacidade efetiva de resposta institucional[4]. A efetividade da governança depende da existência de mecanismos decisórios claros, integração entre áreas técnicas e estratégicas, definição de responsabilidades e capacidade organizacional de transformar diretrizes normativas em práticas operacionais contínuas [26].

No campo da segurança da informação, estudos internacionais evidenciam que estruturas de resposta a incidentes, como os Computer Security Incident Response Teams (CSIRT), constituem elementos essenciais para a resiliência institucional, pois permitem não apenas a contenção técnica de incidentes, mas também a coordenação estratégica da resposta organizacional, a mitigação de riscos e o aprendizado contínuo baseado em eventos críticos. Diretrizes internacionais reforçam que a maturidade em segurança da informação depende diretamente da capacidade dessas equipes de atuar de forma estruturada, integrada e alinhada aos processos de governança organizacional [9, 10, 18, 19].

Além disso, frameworks contemporâneos de segurança e privacidade da informação destacam que a governança eficaz depende da articulação entre gestão de riscos, capacidades operacionais e mecanismos contínuos de monitoramento, resposta e melhoria organizacional [8, 18]. Nesse sentido, modelos internacionais como ISO/IEC 27001:2022 [12] e ISO/IEC 27701:2019 [11] estabelecem requisitos robustos para sistemas de gestão de segurança e privacidade da informação, porém ainda são incipientes as discussões acerca de como tais diretrizes são efetivamente traduzidas em estruturas operacionais permanentes no contexto da Administração Pública.

Nesse cenário, a Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR) pode ser compreendida não apenas como uma unidade técnica de resposta, mas como uma estrutura estratégica de governança operacional. Sua relevância decorre justamente da capacidade de integrar, de forma sistêmica, três dimensões fundamentais da maturidade organizacional em segurança da informação: a tomada de decisão em situações críticas, a implementação coordenada de controles e a revisão contínua baseada em aprendizado organizacional e melhoria contínua [10, 18].

Apesar dos avanços normativos e da crescente institucionalização da segurança da informação no setor público, observa-se ainda uma lacuna relevante na literatura quanto à compreensão da ETIR como elemento integrante da governança da informação e da governança operacional no contexto estatal. Grande parte das abordagens existentes concentra-se predominantemente nos aspectos técnicos de resposta a incidentes, sem aprofundar o papel estratégico dessas estruturas na integração entre decisão, execução, coordenação institucional e aprendizado organizacional.

Dessa forma, este estudo parte do problema de pesquisa que busca compreender em que medida a ETIR pode ser considerada uma estrutura de governança operacional capaz de integrar decisão, execução e aprendizado organizacional no contexto da Administração Pública Federal, especialmente diante das exigências contemporâneas de segurança da informação, proteção de dados pessoais e resiliência cibernética.

Assim, este artigo tem como objetivo investigar empiricamente em que medida a ETIR desempenha funções típicas de uma estrutura de governança operacional na Administração Pública Federal, analisando como capacidades relacionadas à autoridade decisória, coordenação institucional, implementação operacional e aprendizado organizacional são percebidas pelos profissionais envolvidos com sua atuação.

Como principal contribuição, este estudo propõe um modelo conceitual fundamentado em evidências empíricas que caracteriza a ETIR como uma estrutura de governança operacional na Administração Pública Federal. O modelo identifica cinco capacidades organizacionais complementares, governança normativa, autoridade e coordenação institucional, capacidade operacional, aprendizado organizacional e consolidação estratégica que descrevem como essas equipes contribuem para integrar segurança da informação, gestão de riscos, proteção de dados pessoais e resiliência cibernética. Além da contribuição teórica para a compreensão da ETIR sob a perspectiva da governança, os resultados oferecem subsídios práticos para gestores públicos envolvidos na implementação do Programa de Privacidade e Segurança da Informação (PPSI) e no fortalecimento da maturidade da governança da segurança da informação no setor público.

2 Governança de Tecnologia da Informação no Setor Público

A governança de tecnologia da informação no setor público insere se em um contexto de profunda transformação digital, no qual a tecnologia deixa de exercer função meramente operacional para assumir papel estratégico na formulação, implementação e sustentação de políticas públicas digitais [14]. Esse movimento amplia a dependência das organizações públicas em relação às infraestruturas tecnológicas e exige novas capacidades institucionais voltadas à coordenação, supervisão e gestão dos recursos informacionais do Estado [3].

Nesse cenário, a governança de TI passa a ser compreendida como um conjunto de mecanismos responsáveis por orientar a

tomada de decisão, definir responsabilidades institucionais e estabelecer formas de controle sobre o uso da tecnologia. Trata-se de um modelo voltado à geração de valor público, buscando assegurar que os investimentos em tecnologia promovam

eficiência administrativa, transparência, accountability e melhoria da prestação dos serviços públicos [24].

Além disso, a literatura destaca que a efetividade da governança de TI depende diretamente da integração entre mecanismos de governança, gestão de riscos e processos decisórios organizacionais, especialmente em ambientes caracterizados por elevada complexidade operacional e crescente dependência tecnológica [3]. Sob essa perspectiva, a governança de TI deixa de representar apenas uma função administrativa de suporte e passa a assumir papel estruturante na coordenação das capacidades institucionais relacionadas à transformação digital.

Diferentemente do setor privado, a governança de TI no setor público está condicionada a princípios constitucionais que limitam e orientam a atuação estatal. A legalidade, a moralidade administrativa, a eficiência e a publicidade impõem que a gestão da tecnologia seja pautada não apenas por critérios técnicos e econômicos, mas também por fundamentos jurídicos voltados à proteção dos direitos fundamentais dos cidadãos. Nesse contexto, a tecnologia da informação deve ser compreendida como instrumento de concretização de direitos fundamentais em uma sociedade marcada pela crescente digitalização dos serviços públicos. A forma como o Estado organiza, controla e governa seus sistemas informacionais impacta diretamente a efetividade de direitos relacionados à privacidade, ao acesso à informação e à proteção de dados pessoais [6].

A governança de TI, portanto, não pode ser compreendida apenas como um conjunto de práticas técnicas ou mecanismos administrativos isolados. Trata-se de um fenômeno sociotécnico e interdisciplinar que envolve estruturas organizacionais, processos decisórios, aspectos regulatórios e capacidades institucionais voltadas à coordenação da tecnologia em ambientes públicos complexos [14]. A efetividade da governança de TI depende da existência de estruturas decisórias claras, nas quais sejam definidos os papéis e responsabilidades dos atores envolvidos. A ausência dessas estruturas tende a gerar fragmentação decisória, sobreposição de competências, dificuldades de coordenação institucional e baixa capacidade organizacional de resposta a demandas críticas relacionadas à tecnologia e

à segurança da informação [14].

Além disso, a integração entre áreas técnicas e administrativas constitui elemento essencial para o sucesso da governança de TI. A separação entre essas esferas compromete a capacidade institucional de responder a demandas complexas e de alinhar a tecnologia às necessidades organizacionais [7]. No contexto da transformação digital do setor público, estruturas organizacionais fragmentadas, processos excessivamente verticalizados e baixa integração entre áreas técnicas e administrativas dificultam a coordenação institucional e comprometem a efetividade das iniciativas digitais [7, 25].

No setor público, essa integração assume relevância ainda maior, uma vez que as decisões tecnológicas impactam diretamente a prestação de serviços à população. A governança de TI, nesse sentido, deve ser orientada à geração de valor público, considerando não apenas eficiência interna, mas também qualidade, acessibilidade, continuidade e confiabilidade dos serviços digitais ofertados à sociedade [7]. A crescente incidência de incidentes cibernéticos evidencia a necessidade de incorporar a gestão de riscos e a resiliência organizacional como elementos centrais da governança de TI. Sob essa perspectiva, a proteção de sistemas, serviços e dados institucionais passa a representar não apenas uma demanda técnica, mas uma condição essencial para a continuidade dos serviços públicos, para a preservação da confiança institucional e para a proteção de

direitos fundamentais [9, 10]

A segurança da informação, sob essa perspectiva, deixa de ser uma preocupação restrita às áreas técnicas, assumindo caráter estratégico dentro das organizações públicas. Dessa forma, as instituições passam a demandar estruturas operacionais capazes de atuar de maneira coordenada na prevenção, detecção, contenção e resposta a incidentes de segurança, promovendo aprendizado organizacional contínuo e redução de vulnerabilidades institucionais [18]. A adoção de padrões internacionais de segurança da informação reforça a necessidade de modelos de governança mais robustos e alinhados às melhores práticas globais. Esses padrões oferecem diretrizes voltadas à estruturação de políticas, controles e processos capazes de fortalecer a proteção de dados, a gestão de riscos e a continuidade operacional das organizações públicas [10, 12].

Nesse sentido, políticas institucionais recentes da Administração Pública Federal evidenciam a crescente preocupação em integrar governança, gestão de riscos, segurança da informação e proteção de dados pessoais. A Política de Segurança da Informação do Ministério da Integração e do Desenvolvimento Regional (MIDR) [17], por exemplo, estabelece diretrizes voltadas à gestão sistemática de riscos, monitoramento contínuo, resposta a incidentes, melhoria contínua e fortalecimento da cultura organizacional de segurança [23]. A referida norma também reconhece explicitamente a necessidade de estruturas especializadas, como a Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR), articuladas aos mecanismos institucionais de governança e gestão da segurança da informação.

De maneira complementar, a Política de Proteção de Dados Pessoais do MIDR reforça a necessidade de adoção de medidas técnicas e administrativas capazes de reduzir riscos e assegurar a efetividade da proteção de dados pessoais, incluindo mecanismos de resposta a incidentes, monitoramento contínuo, planos de mitigação e integração entre estruturas organizacionais responsáveis pela segurança e governança dos dados [17]. A norma evidencia, ainda, a importância da ETIR como estrutura operacional voltada à comunicação, contenção e tratamento de incidentes relacionados à proteção de dados pessoais.

Contudo, a simples adoção de normas, frameworks e diretrizes regulatórias não garante, por si só, a efetividade da governança de TI. A literatura aponta que a maturidade organizacional depende da capacidade institucional de transformar diretrizes normativas em capacidades operacionais concretas, integradas às práticas

cotidianas da organização e sustentadas por processos contínuos de coordenação, monitoramento e aprendizado [3, 14].

A governança de TI no setor público também enfrenta desafios relacionados à limitação de recursos, à burocracia, à fragmentação institucional e à complexidade organizacional. Esses fatores dificultam a implementação de modelos eficientes de governança e exigem soluções adaptadas às especificidades da Administração Pública. Apesar desses desafios, a consolidação de práticas estruturadas de governança de TI representa avanço significativo na modernização do Estado. A adoção de mecanismos formais de coordenação, gestão de riscos, monitoramento e resposta a incidentes contribui para o fortalecimento da transparência, da accountability, da resiliência institucional e da qualidade dos serviços públicos digitais [1, 21].

Nesse cenário, a articulação entre governança da informação, governança de TI, proteção de dados pessoais e segurança da informação torna-se fundamental para assegurar uma abordagem integrada da transformação digital no setor público. Essa integração permite maior capacidade institucional de gerenciamento de riscos, coordenação organizacional e proteção dos ativos informacionais do Estado [4, 7]. Dessa forma, a governança de tecnologia da informação no setor público deve ser compreendida como elemento central para a construção de uma Administração Pública mais eficiente, segura, resiliente e orientada à proteção de direitos fundamentais. Nesse contexto, estruturas organizacionais especializadas, como as Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR), assumem papel estratégico na operacionalização dos mecanismos de governança, gestão de riscos e segurança da informação. Essas estruturas atuam como elementos de coordenação sociotécnica, responsáveis por integrar capacidades técnicas, processos institucionais e mecanismos de resposta organizacional voltados à mitigação de incidentes e à promoção da resiliência institucional.

3 O Modelo de Governança da Informação no MGI e o PPSI

A consolidação de modelos de governança da informação na Administração Pública Federal tem sido impulsionada pela crescente digitalização estatal e pela ampliação da dependência de sistemas informacionais para a execução de políticas públicas e prestação de serviços digitais. Nesse cenário, a informação assume posição estratégica na atuação do Estado, exigindo mecanismos institucionais capazes de assegurar não apenas eficiência administrativa, mas também proteção de dados pessoais, segurança da informação e continuidade operacional [2].

A transformação digital do setor público amplia significativamente a complexidade dos ambientes informacionais governamentais, tornando as organizações públicas mais expostas a riscos relacionados a incidentes cibernéticos, vazamentos de dados e indisponibilidade de serviços críticos [26]. Como consequência, a governança da informação deixa de representar apenas um modelo de coordenação administrativa e passa a incorporar dimensões relacionadas à gestão de riscos, resiliência organizacional e proteção de direitos fundamentais [14].

Nesse contexto, o Ministério da Gestão e da Inovação em Serviços Públicos (MGI) assume papel relevante na formulação de diretrizes voltadas à organização da governança da informação na Administração Pública Federal. A instituição do Programa de Privacidade e Segurança da Informação (PPSI), por meio da Portaria SGD/MGI nº 852/2023, representa um esforço de estruturação de um modelo integrado de governança orientado à articulação entre privacidade, segurança da informação e gestão de riscos [2].

Sob uma perspectiva organizacional, o PPSI pode ser compreendido como um framework de governança destinado à coordenação de políticas, responsabilidades institucionais, mecanismos de controle e estruturas operacionais voltadas à proteção dos ativos informacionais do Estado. Mais do que um instrumento de conformidade normativa, o programa busca consolidar capacidades institucionais capazes de promover prevenção, monitoramento, resposta a incidentes e melhoria contínua da segurança da informação no setor público [2].

A incorporação da proteção de dados pessoais como eixo estruturante da governança da informação evidencia uma mudança paradigmática na atuação estatal. A informação deixa de ser tratada exclusivamente sob a lógica da eficiência administrativa e passa a ser compreendida também como objeto de tutela jurídica, diretamente relacionado à proteção da privacidade, à autodeterminação informativa e à garantia de direitos fundamentais [2].

Nesse sentido, a Lei Geral de Proteção de Dados Pessoais (LGPD) introduz novas exigências relacionadas ao tratamento de dados no setor público, impondo a adoção de medidas técnicas e administrativas capazes de assegurar a proteção dos dados pessoais tratados pelas organizações governamentais [6]. A aplicação da LGPD à Administração Pública demanda, portanto, uma reorganização institucional orientada à integração entre governança da informação, segurança cibernética e gestão de riscos.

O PPSI surge como um mecanismo institucional para operacionalizar essa integração no âmbito da Administração Pública Federal. O framework estabelece diretrizes voltadas à implementação de mecanismos de segurança, definição de responsabilidades organizacionais, monitoramento contínuo, gestão de riscos e resposta a incidentes, buscando promover maior alinhamento entre estruturas técnicas, administrativas e decisórias [2].

Além disso, o PPSI incorpora referenciais internacionais amplamente reconhecidos, como ISO/IEC 27001[12], ISO/IEC 27701[11], NIST Cybersecurity Framework [20] e boas práticas da ENISA [10], evidenciando a tentativa de alinhar a governança da informação do setor público brasileiro a modelos globais de segurança e privacidade.

Entretanto, a literatura aponta que a simples adoção de normas, frameworks e diretrizes regulatórias não garante, por si só, a efetividade da governança da informação. Modelos excessivamente normativos tendem a concentrar esforços na

conformidade formal, sem necessariamente promover mudanças concretas nas rotinas organizacionais e nos processos institucionais [5, 14]. Essa tensão entre normatividade e operacionalização constitui um dos principais desafios da governança da informação no setor público contemporâneo. A existência de políticas, diretrizes e padrões técnicos representa condição necessária, mas insuficiente, para assegurar a efetividade da proteção informacional [22]. A consolidação de uma governança efetiva depende da capacidade institucional de transformar diretrizes abstratas em práticas organizacionais contínuas, integradas e operacionalmente sustentáveis.

Nesse cenário, a gestão de riscos emerge como elemento estruturante da governança da informação. A crescente sofisticação das ameaças cibernéticas exige modelos organizacionais capazes de identificar vulnerabilidades, monitorar ativos críticos, responder rapidamente a incidentes e reduzir impactos associados à indisponibilidade de sistemas e ao comprometimento de dados institucionais [4, 16].

Sob essa perspectiva, o PPSI não se limita à definição de controles técnicos, mas busca estruturar capacidades institucionais voltadas à coordenação organizacional da segurança e da privacidade. O framework estabelece segmentações de maturidade, define papéis institucionais e propõe mecanismos contínuos de monitoramento e governança, evidenciando uma abordagem orientada não apenas à conformidade, mas também à operacionalização da gestão da informação [2]. A dimensão institucional da governança da informação também envolve a definição clara de competências e responsabilidades organizacionais. A literatura de governança de TI destaca que a ausência de estruturas decisórias formalizadas tende a gerar fragmentação institucional, sobreposição de responsabilidades e

dificuldades de coordenação entre áreas técnicas e administrativas [14].

Nesse sentido, o PPSI busca promover uma estrutura organizacional integrada, articulando atores responsáveis pela governança da informação, segurança da informação, gestão de riscos, proteção de dados pessoais e resposta a incidentes. A integração entre essas estruturas revela a tentativa de superar modelos fragmentados de gestão informacional tradicionalmente presentes na Administração Pública Federal. Além disso, o framework reconhece explicitamente a necessidade de mecanismos operacionais capazes de concretizar as diretrizes institucionais de segurança e privacidade. O PPSI estabelece que a efetividade da governança depende da existência de processos contínuos de monitoramento, prevenção, resposta e aprendizado organizacional, reforçando a importância de estruturas organizacionais especializadas para a operacionalização dessas atividades [2].

A integração entre governança da informação e segurança da informação constitui, portanto, um dos elementos centrais do modelo proposto pelo PPSI [2]. Essa articulação permite que políticas de proteção de dados, gestão de riscos e segurança cibernética sejam implementadas de forma coordenada, fortalecendo a capacidade institucional de resposta a incidentes e mitigação de vulnerabilidades [6, 12]. Nesse contexto, a efetividade dessas diretrizes depende diretamente da capacidade das organizações públicas de desenvolver estruturas operacionais aptas a responder a situações críticas de maneira coordenada e contínua. A ausência de mecanismos institucionais capazes de integrar decisão, execução e monitoramento tende a comprometer a efetividade das políticas de segurança e limitar a capacidade estatal de reação diante de incidentes cibernéticos[18]

Nesse contexto, estruturas especializadas de resposta a incidentes passam a assumir papel estratégico dentro da governança da informação. Essas estruturas não apenas executam atividades técnicas de contenção e mitigação de incidentes, mas também promovem coordenação organizacional, comunicação institucional, gestão de vulnerabilidades e aprendizado contínuo baseado em eventos críticos [10, 20]. A atuação dessas equipes evidencia que a governança da informação não pode ser compreendida apenas sob uma dimensão normativa ou regulatória, exigindo mecanismos concretos de operacionalização capazes de integrar capacidades técnicas, processos organizacionais e tomada de decisão institucional. Sob essa perspectiva, a resposta a incidentes deixa de representar atividade meramente operacional e passa a constituir componente central da governança contemporânea da informação.

A análise do modelo de governança da informação no MGI evidencia, portanto, avanços significativos na institucionalização da proteção de dados, da segurança da informação e da gestão de riscos no setor público federal. O PPSI representa um esforço relevante de construção de um modelo integrado de governança orientado à coordenação institucional e à resiliência organizacional. Contudo, os desafios relacionados à operacionalização dessas diretrizes demonstram que a efetividade da governança depende da existência de estruturas capazes de transformar políticas e normas em práticas organizacionais concretas. A consolidação de uma governança da informação efetiva exige não apenas normatividade, mas capacidade operacional, integração organizacional e mecanismos contínuos de monitoramento, resposta e aprendizado institucional.

É nesse cenário que se insere a relevância das Equipes de Tratamento e Resposta a Incidentes Cibernéticos (ETIR), compreendidas não apenas como estruturas técnicas de segurança, mas como mecanismos estratégicos de governança operacional. Ao integrar gestão de riscos, coordenação institucional, resposta a incidentes e aprendizado organizacional, a ETIR se apresenta como elemento essencial para a concretização prática das diretrizes estabelecidas pelo PPSI e pela LGPD no âmbito da Administração Pública Federal.

4 Metodologia

Este estudo adotou uma abordagem exploratória, utilizando a técnica de *survey* como estratégia de coleta de dados. O instrumento combinou questões fechadas e abertas, permitindo a obtenção de informações descritivas sobre o perfil dos

participantes e a exploração qualitativa de suas percepções acerca da ETIR como estrutura de governança operacional.

O instrumento de pesquisa foi elaborado a partir da fundamentação teórica apresentada nas seções anteriores, contemplando conceitos relacionados à governança de Tecnologia da Informação, governança da informação, gestão de riscos, segurança da informação, continuidade de negócios e proteção de dados pessoais. Também foram considerados os principais referenciais normativos aplicáveis à Administração Pública Federal, em especial o Programa de Privacidade e Segurança da Informação (PPSI), instituído pela Portaria SGD/MGI nº 852/2023, a Lei Geral de Proteção de Dados Pessoais (LGPD) e a norma ABNT NBR ISO/IEC 27001:2022.

O instrumento foi estruturado de forma a refletir o modelo conceitual discutido nas seções anteriores, permitindo investigar como mecanismos normativos, estratégicos e operacionais se articulam na consolidação da ETIR como estrutura de governança operacional.

O questionário foi estruturado em seis seções temáticas, organizadas de forma a representar o ciclo de operacionalização da governança institucional. A primeira seção reúne questões de caracterização do perfil profissional dos participantes, incluindo órgão de atuação, área organizacional, tempo de experiência e grau de envolvimento com atividades relacionadas à ETIR, à segurança da informação e ao PPSI. A segunda seção investiga aspectos relacionados à estrutura normativa, ao alinhamento institucional e à implementação do PPSI. A terceira seção aborda o papel da ETIR na tomada de decisão estratégica durante incidentes cibernéticos. A quarta seção concentra-se na implementação de controles operacionais, procedimentos de resposta, preservação de evidências e continuidade dos serviços. A quinta seção investiga mecanismos de aprendizado organizacional, retenção do conhecimento e maturidade institucional após incidentes. Por fim, a sexta seção analisa os principais desafios para a consolidação da ETIR como estrutura de governança, contemplando aspectos culturais, institucionais, orçamentários e de recursos humanos, bem como possíveis melhorias para o fortalecimento da resiliência cibernética na Administração Pública Federal.

As seis seções do instrumento representam capacidades complementares da governança operacional. Em conjunto, elas permitem analisar como aspectos normativos, decisórios, operacionais e organizacionais se articulam para sustentar a atuação da ETIR como estrutura permanente de governança da segurança da informação.

O instrumento contemplou questões fechadas para caracterização dos participantes e questões abertas destinadas a captar as percepções dos respondentes acerca da maturidade institucional, dos processos decisórios, das práticas de governança e dos desafios enfrentados pelas ETIR. Essa combinação permitiu obter evidências descritivas sobre o perfil dos participantes e, simultaneamente, explorar em profundidade suas experiências e percepções acerca da operacionalização da governança da segurança da informação.

A estrutura do instrumento de pesquisa é apresentada na Tabela 1. O questionário foi organizado em seis seções temáticas que representam as principais dimensões investigadas neste estudo, iniciando pela caracterização do perfil dos participantes e avançando para aspectos relacionados à estrutura normativa e ao alinhamento institucional do PPSI, ao papel estratégico da ETIR na tomada de decisão, à implementação de controles operacionais, aos mecanismos de aprendizado organizacional e, por fim, aos desafios para a consolidação da ETIR como estrutura de governança operacional. Essa organização foi concebida para analisar, de forma sequencial, como a ETIR atua na operacionalização da governança da informação, integrando mecanismos de coordenação institucional, gestão de riscos, resposta a incidentes e aprendizado organizacional no contexto da Administração Pública Federal.

Antes da aplicação definitiva, foi realizado um estudo piloto com três integrantes de ETIR pertencentes a duas instituições distintas

Table 1: Estrutura do instrumento de pesquisa

Seção	Questão	Objetivo da questão	Tipo
Perfil Profissional	Q1	Identificar o órgão ou entidade da Administração Pública Federal em que o participante atua.	Aberta
	Q2	Caracterizar a área de atuação do participante (TI, Segurança da Informação, Jurídico, Ouvidoria, Área Finalística etc.).	Aberta
	Q3	Identificar o tempo de experiência do participante na Administração Pública Federal.	Fechada
	Q4	Verificar o grau de envolvimento do participante com a ETIR, Segurança da Informação ou PPSI.	Fechada
	Q5	Identificar experiências prévias relacionadas à resposta a incidentes cibernéticos.	Fechada
Capacidade 1 – Estrutura Normativa e Alinhamento Institucional	Q6	Avaliar a percepção sobre a maturidade da implementação do PPSI no órgão.	Aberta
	Q7	Investigar os impactos da LGPD sobre prioridades institucionais, orçamento e apoio da alta administração.	Aberta
	Q8	Analisar a contribuição dos inventários de dados pessoais e da gestão de riscos para a governança institucional.	Aberta
Capacidade 2 – Autoridade Decisória e Coordenação Estratégica	Q9	Avaliar a autonomia decisória da ETIR durante incidentes críticos.	Aberta
	Q10	Compreender como ocorre a comunicação entre a ETIR e a alta administração durante incidentes.	Aberta
	Q11	Identificar mecanismos de articulação externa da ETIR e os desafios de coordenação institucional.	Aberta
Capacidade 3 – Implementação Operacional	Q12	Verificar a existência e utilização de procedimentos formais de resposta a incidentes.	Aberta
	Q13	Identificar obstáculos técnicos e procedimentais enfrentados pela ETIR.	Aberta
	Q14	Avaliar a maturidade dos planos de continuidade de negócios e da infraestrutura de TIC.	Aberta
Capacidade 4 – Aprendizado Organizacional	Q15	Investigar a adoção de processos de lições aprendidas após incidentes.	Aberta
	Q16	Analisar os impactos da rotatividade e da terceirização sobre a retenção do conhecimento institucional.	Aberta
	Q17	Investigar como os conhecimentos produzidos após incidentes são disseminados na organização.	Aberta
Capacidade 5 – Consolidação da Governança Operacional	Q18	Investigar barreiras culturais e dificuldades de integração entre áreas técnicas e áreas finalísticas.	Aberta
	Q19	Identificar limitações institucionais, orçamentárias, jurídicas e de recursos humanos para consolidação da ETIR.	Aberta
	Q20	Identificar mudanças estruturais necessárias para fortalecer a governança e a resiliência cibernética na Administração Pública Federal.	Aberta

da Administração Pública Federal. O objetivo do piloto foi avaliar a clareza, a compreensão e a adequação das questões propostas. Com base nas contribuições recebidas, foram realizados exclusivamente ajustes de redação destinados a melhorar a clareza e reduzir ambiguidades, sem alteração do conteúdo investigado. As respostas obtidas durante essa etapa não foram incorporadas ao conjunto de dados utilizado na análise dos resultados.

Após a validação do instrumento, o questionário foi disponibilizado eletronicamente e encaminhado aos coordenadores das ETIR de diferentes órgãos e entidades da Administração Pública Federal, que atuaram como pontos focais para disseminação do questionário entre os integrantes de suas respectivas equipes. A participação foi voluntária, mediante aceite do Termo de Consentimento Livre e Esclarecido apresentado no início do formulário, sendo assegurados o anonimato dos participantes e o tratamento confidencial das informações coletadas. Ao término do período de coleta foram obtidas 23 respostas válidas, utilizadas nas análises apresentadas na seção de resultados.

4.1 Procedimentos de análise

As respostas às questões fechadas foram analisadas por meio de estatística descritiva, utilizando frequências absolutas e relativas para caracterizar o perfil dos participantes. As questões abertas foram examinadas por meio de análise qualitativa de conteúdo, buscando identificar padrões recorrentes relacionados à governança operacional, coordenação institucional, gestão de riscos, tomada de decisão e aprendizado organizacional. As categorias analíticas utilizadas foram definidas a partir das dimensões investigadas pelo instrumento de pesquisa.

4.2 Procedimentos de Análise dos Dados

As respostas às questões fechadas foram analisadas por meio de estatística descritiva, utilizando frequências absolutas e relativas para caracterizar o perfil dos participantes. As respostas às questões abertas foram examinadas por meio de análise temática *(Braun; Clarke, 2006)*. Inicialmente, o primeiro autor realizou a leitura integral das respostas, identificou unidades de significado e atribuiu códigos aos trechos relacionados aos objetivos de cada questão. Em seguida, os códigos semanticamente relacionados foram agrupados em categorias e subcategorias temáticas. A segunda autora revisou a codificação, a definição das categorias e sua correspondência com as respostas originais. Eventuais divergências foram discutidas até a obtenção de consenso.

A análise combinou uma orientação dedutiva, baseada nas dimensões contempladas pelo instrumento de pesquisa, com uma orientação indutiva, destinada a identificar padrões e aspectos recorrentes emergentes das respostas. As frequências apresentadas nos resultados correspondem ao número de participantes cujas respostas foram associadas a cada categoria. Respostas sem conteúdo interpretável ou sem informações suficientes para classificação foram registradas separadamente e não foram utilizadas na interpretação qualitativa da respectiva questão.

5 Resultados

5.1 Perfil Profissional dos Participantes

A pesquisa contou com 23 participantes vinculados a diferentes órgãos e entidades públicas. Todos os respondentes registraram concordância com o Termo de Consentimento Livre e Esclarecido.

A Tabela 2 apresenta a distribuição dos participantes quanto ao tempo de atuação na Administração Pública Federal, ao envolvimento com atividades relacionadas à ETIR, à Segurança da Informação ou ao PPSI e à experiência prévia em situações envolvendo incidentes cibernéticos.

Os resultados evidenciam um grupo de participantes com experiência profissional significativa no setor público. A maioria dos respondentes, correspondente a 15 participantes (65,2%), informou possuir mais de dez anos de atuação na Administração Pública Federal. Outros cinco participantes (21,7%) possuíam menos de dois anos de experiência, enquanto dois (8,7%) se encontravam na faixa de dois a cinco anos e apenas um participante (4,3%) declarou Table 2: Perfil profissional dos participantes

Característica	*n*	%
Tempo de atuação na Administração Pública Federal		
Menos de 2 anos	5	21,7
De 2 a 5 anos	2	8,7
De 5 a 10 anos	1	4,3
Mais de 10 anos	15	65,2
Envolvimento com ETIR, Segurança da Informação ou PPSI		
Sim	14	60,9
Parcialmente	5	21,7
Não	4	17,4
Participação em situações envolvendo incidentes cibernéticos		
Sim, diretamente	11	47,8
Sim, indiretamente	8	34,8
Não	3	13,0
Prefiro não responder	1	4,3

experiência entre cinco e dez anos. Essa distribuição indica a predominância de profissionais com trajetória consolidada na Administração Pública, embora o conjunto também contemple percepções de participantes com ingresso mais recente no serviço público.

Quanto à proximidade com o objeto investigado, 14 participantes (60,9%) declararam possuir atuação direta ou participação em processos relacionados à ETIR, à Segurança da Informação ou ao PPSI, enquanto cinco (21,7%) indicaram envolvimento parcial. Assim, 19 dos 23 respondentes (82,6%) apresentavam algum nível de participação nessas atividades. Além disso, 11 participantes (47,8%) relataram ter atuado diretamente em situações envolvendo incidentes cibernéticos, e oito (34,8%) participaram indiretamente. Em conjunto, esses resultados mostram que 19 participantes (82,6%) possuíam experiência direta ou indireta com incidentes, conferindo às respostas uma base empírica relevante para a análise das práticas de governança operacional e resposta institucional.

Os participantes estavam distribuídos por diferentes órgãos e entidades públicas, abrangendo instituições da Administração Pública Federal direta e indireta, universidades públicas, agências reguladoras, instituições financeiras públicas e órgãos do Poder Judiciário. Após a uniformização das diferentes formas de escrita utilizadas nas respostas, foram identificadas aproximadamente 16 organizações. A Universidade de Brasília apresentou o maior número de participantes (n= 4), seguida pelo Ministério do Desenvolvimento e Assistência Social, pelo Tribunal Regional Federal da 1ª Região e pelo Ministério do Esporte, cada um com dois respondentes. As demais organizações foram representadas por um participante.

Em relação à área de lotação, observou-se predominância de profissionais vinculados a funções técnicas. Após o agrupamento semântico das respostas abertas, 12 participantes (52,2%) foram classificados em áreas de Tecnologia da Informação, infraestrutura ou desenvolvimento de sistemas, enquanto sete (30,4%) atuavam especificamente em Segurança da Informação ou Segurança Cibernética. Dois participantes (8,7%) estavam vinculados à proteção de dados pessoais ou à gestão da informação, e um participante (4,3%) atuava em área administrativa. Uma resposta não apresentou informação suficiente para classificação. Essa composição demonstra que a maior parte dos respondentes possuía inserção profissional diretamente relacionada aos processos técnicos e organizacionais examinados no estudo.

Table 3: Áreas de atuação dos participantes

Área de atuação agrupada	*n*	%
Tecnologia da Informação, infraestrutura ou desenvolvimento	12	52,2
Segurança da Informação ou Segurança Cibernética	7	30,4
Proteção de dados ou gestão da informação	2	8,7
Área administrativa	1	4,3
Não identificada	1	4,3

5.2 Estrutura Normativa, Alinhamento Institucional e PPSI

Esta seção analisa as percepções dos participantes sobre três aspectos relacionados à institucionalização da segurança da informação: a transposição das diretrizes formais do PPSI para as práticas organizacionais, os efeitos da LGPD sobre o apoio institucional e as prioridades orçamentárias e a contribuição dos inventários de dados pessoais e das metodologias de avaliação de riscos. Das 23 respostas coletadas, 22 apresentaram conteúdo interpretável nas questões desta seção. Uma resposta foi desconsiderada da análise qualitativa por não conter informações semanticamente válidas.

Em relação à transposição das diretrizes formais do PPSI para as práticas cotidianas de segurança da informação, predominou a percepção de que os órgãos se encontram em um estágio intermediário ou em desenvolvimento. Essa categoria reuniu 15 das 22 respostas válidas (68,2%), conforme apresentado na Tabela 4 (Q6). Os participantes reconheceram a existência de normas, políticas, controles e iniciativas institucionais, mas indicaram que esses mecanismos ainda não estão plenamente consolidados ou aplicados de maneira uniforme entre as diferentes áreas organizacionais.

Quatro participantes (18,2%) avaliaram a maturidade como baixa ou incipiente, destacando processos ainda em definição, lacunas na execução das diretrizes e insuficiência de profissionais qualificados. Apenas três respondentes (13,6%) apresentaram uma avaliação predominantemente positiva ou consideraram seus órgãos maduros, embora uma dessas respostas também tenha reconhecido a existência de oportunidades de melhoria.

As respostas evidenciam, portanto, uma distância entre a formalização normativa e sua incorporação às rotinas organizacionais. Um participante observou que o órgão possuía "normas, políticas e procedimentos alinhados ao PPSI", mas ainda

enfrentava dificuldades para transformar as diretrizes em práticas padronizadas em todas as áreas. Outro respondente destacou que controles como segmentação de rede, autenticação multi-fator e monitoramento já estavam implementados na área técnica, enquanto, fora da TI, o cumprimento das normas ainda dependia predominantemente da atuação individual dos servidores.

Esse resultado indica que a institucionalização do PPSI não depende apenas da existência de documentos e controles técnicos, mas também da capacidade de disseminar práticas, responsabilidades e mecanismos de verificação por toda a organização. A predominância de avaliações intermediárias sugere que a implementação está em curso, mas ainda não alcançou um nível homogêneo de operacionalização.

Quanto aos efeitos da LGPD sobre as prioridades institucionais (Q7), 11 participantes (50,0%) perceberam aumento da priorização da segurança cibernética ou do apoio da alta administração (Tabela 4). As respostas associaram a LGPD à maior visibilidade da proteção de dados pessoais, à criação de grupos de trabalho, ao fortalecimento de comitês institucionais e à integração entre as áreas de segurança da informação, proteção de dados e gestão de riscos.

Seis participantes (27,3%), entretanto, afirmaram que a LGPD não alterou significativamente as prioridades orçamentárias ou não apresentou relação direta com as decisões de segurança cibernética. Outros três respondentes (13,6%) identificaram mudanças ainda parciais ou em estágio inicial, enquanto dois participantes (9,1%) declararam não possuir informações suficientes para avaliar o apoio da alta administração ou as decisões orçamentárias.

Entre os participantes que reconheceram efeitos positivos, foram mencionados maior facilidade para aprovação de ferramentas de monitoramento e capacitação, alterações em políticas e contratos e inclusão da LGPD no planejamento estratégico. Apesar disso, uma resposta destacou que a disponibilização de recursos ainda ocorre de forma predominantemente reativa, quando surge uma exigência formal, e não como parte de um investimento contínuo e previamente planejado.

Os resultados mostram que a LGPD atua como um importante mecanismo de legitimação das iniciativas de segurança e proteção de dados, mas seu impacto não é uniforme entre os órgãos. Em parte das instituições, a legislação ampliou o apoio estratégico e facilitou a mobilização de recursos; em outras, seus efeitos permaneceram restritos ou ainda não foram percebidos pelos participantes.

A contribuição dos inventários de dados pessoais e das metodologias de avaliação de riscos foi avaliada de forma predominantemente positiva (Q8). Treze participantes (59,1%) consideraram que esses instrumentos ampliaram efetivamente a visibilidade sobre os dados tratados, os fluxos de informação e os riscos organizacionais, conforme apresentado na Tabela 4. As respostas destacaram benefícios como o mapeamento dos locais em que os dados são armazenados, a identificação de seus fluxos e o envolvimento de diferentes áreas na gestão de riscos.

Três participantes (13,6%) reconheceram benefícios, mas avaliaram que a implementação ainda se encontra em estágio inicial ou enfrenta dificuldades para se transformar em uma prática organizacional recorrente. Por outro lado, cinco respondentes (22,7%) entenderam que os instrumentos permanecem predominantemente associados ao atendimento formal de exigências normativas, auditorias ou obrigações relacionadas à LGPD. Um participante (4,5%) não possuía informações suficientes para realizar a avaliação.

As respostas revelam uma distinção entre a elaboração do inventário e sua efetiva integração à gestão de riscos. Um participante afirmou que o inventário produziu ganhos reais ao mapear onde os dados estavam localizados e por onde circulavam, mas destacou que a avaliação de riscos ainda era realizada principalmente quando exigida por auditorias. Outro respondente observou que o instrumento permanecia formal no âmbito da LGPD, embora tivesse produzido benefícios para a segurança da informação.

Esses resultados indicam que os inventários de dados pessoais apresentam potencial para superar a função estritamente documental e apoiar a identificação e o tratamento de riscos. Contudo, esse potencial depende de sua atualização contínua, de sua integração aos processos decisórios e da utilização das informações produzidas nas rotinas de governança, em vez de sua elaboração apenas para demonstrar conformidade.

De forma integrada, os resultados desta seção mostram que a estrutura normativa associada ao PPSI e à LGPD já produziu avanços perceptíveis em parte das organizações investigadas, especialmente quanto à visibilidade da segurança da informação, à articulação entre áreas e ao reconhecimento dos riscos relacionados ao tratamento de dados pessoais. Entretanto, a predominância de avaliações intermediárias e a presença de práticas orientadas principalmente à conformidade demonstram que a existência de normas não assegura, por si só, sua incorporação às rotinas institucionais. A operacionalização dessas diretrizes depende da consolidação de processos, da disponibilidade de capacidades técnicas e humanas e da integração contínua entre governança, gestão de riscos e execução operacional.

5.3 A ETIR na Tomada de Decisão Estratégica

Esta dimensão investigou como as Equipes de Tratamento e Resposta a Incidentes Cibernéticos (ETIR) participam dos processos decisórios durante incidentes críticos, como ocorre a comunicação entre a equipe técnica e a alta administração e quais desafios são enfrentados na articulação com órgãos externos. As respostas foram analisadas por meio de análise temática, resultando nas categorias apresentadas na Tabela 5.

Em relação à autonomia decisória da ETIR (Q9), observou-se que a categoria predominante correspondeu à autonomia técnica parcial, identificada em dez respostas (43,5%). Nesses casos, os participantes relataram que a equipe possui autonomia para executar medidas técnicas emergenciais, como isolamento de

ativos ou contenção inicial do incidente, porém decisões com maior impacto institucional, como interrupção de serviços críticos, permanecem condicionadas à autorização da alta administração.

Oito participantes (34,8%) descreveram uma estrutura com autonomia formal consolidada, na qual a ETIR dispõe de autoridade delegada para atuar em situações críticas, respaldada por procedimentos previamente estabelecidos ou pela atuação em salas de crise. Em contraste, cinco participantes (21,7%) relataram baixa autonomia institucional, caracterizada pela ausência de delegação formal, dependência de instâncias superiores ou pelo fato de a equipe ainda estar em processo de estruturação.

As respostas evidenciam que a capacidade técnica da ETIR encontrase, em muitos órgãos, mais desenvolvida do que sua autonomia institucional. Um participante sintetizou essa situação ao afirmar que a equipe possui autonomia para executar ações técnicas previamente estabelecidas, mas que decisões capazes de interromper serviços críticos dependem da autorização da gestão superior.

A análise da comunicação entre a ETIR e a alta administração (Q10) revelou diferentes níveis de institucionalização dos processos de coordenação. Dez participantes (43,5%) relataram a existência de fluxos formais previamente definidos, envolvendo procedimentos documentados, comissões de crise, coordenadores da ETIR e protocolos específicos para escalonamento das decisões (Tabela 5).

Entretanto, sete participantes (30,4%) indicaram que a comunicação ocorre predominantemente por mecanismos informais, utilizando grupos de mensagens instantâneas, chamadas telefônicas e contatos diretos entre gestores e equipes técnicas. Outros seis participantes (26,1%) relataram inexistência de fluxos estruturados ou afirmaram desconhecer os procedimentos adotados durante incidentes.

Uma das respostas ilustra claramente esse cenário ao afirmar que a comunicação "funciona porque o time é pequeno e todo mundo se conhece", embora ainda não exista um fluxo formal plenamente estruturado. Esse resultado evidencia que parte das organizações ainda depende do conhecimento tácito e das relações interpessoais para coordenar a resposta a incidentes, característica típica de níveis intermediários de maturidade em governança operacional.

Quanto à articulação externa durante incidentes (Q11), observouse predominância de canais institucionais de comunicação, mencionados por nove participantes (39,1%), incluindo CTIR Gov, CSIC, CNJ, CJF e outros órgãos responsáveis pela coordenação governamental da segurança cibernética. Outros oito participantes (34,8%) indicaram o correio eletrônico como principal mecanismo utilizado para as comunicações externas.

Apesar da existência desses canais, seis participantes (26,1%) destacaram desafios recorrentes relacionados à burocracia, à demora na tramitação das comunicações oficiais, à necessidade de replicação das mesmas informações para diferentes órgãos e à ausência de mecanismos nacionais de coordenação mais integrados.

Uma das respostas ressaltou que, em determinadas situações, "a comunicação externa demora mais que a própria resolução técnica do incidente", evidenciando que as dificuldades enfrentadas pelas ETIR extrapolam aspectos tecnológicos e envolvem limitações organizacionais e institucionais relacionadas à coordenação entre diferentes atores governamentais.

De forma integrada, os resultados desta dimensão indicam que as ETIR já desempenham papel relevante na coordenação operacional da resposta a incidentes cibernéticos. Entretanto, sua atuação estratégica permanece condicionada à existência de mecanismos formais de delegação de autoridade, processos institucionalizados de comunicação e estruturas organizacionais capazes de integrar equipes técnicas, alta administração e órgãos externos. Esses resultados reforçam que a efetividade da ETIR como estrutura de governança operacional depende não apenas de competências técnicas, mas também da consolidação de mecanismos

Table 4: Categorias temáticas identificadas nas respostas sobre estrutura normativa, alinhamento institucional e PPSI

Questão	Categoria principal	Subcategorias identificadas	*n*	%
Q6 Maturidade na implementação do PPSI	Maturidade intermediária ou em desenvolvimento	Processos em amadurecimento; práticas parcialmente implementadas; necessidade de melhoria contínua; implementação desigual entre áreas.	15	68,2
	Maturidade baixa ou incipiente	Estruturas ainda iniciais; insuficiência de pessoal qualificado; processos em definição; lacunas na execução.	4	18,2
	Maturidade elevada ou avaliação positiva	Diretrizes consolidadas; práticas implementadas; existência de margem para aprimoramento.	3	13,6
Q7 Efeitos institucionais da LGPD	Maior priorização e apoio institucional	Ampliação da visibilidade; apoio da alta administração; priorização da segurança; integração entre segurança, privacidade e riscos.	11	50,0
	Ausência de alteração significativa	Manutenção das prioridades existentes; ausência de relação direta; falta de impacto orçamentário percebido.	6	27,3
	Mudanças ainda parciais ou em estágio inicial	Ações em desenvolvimento; atendimento básico; formação de grupos de trabalho; avanços ainda insuficientes.	3	13,6
	Informação insuficiente para avaliação	Desconhecimento sobre decisões orçamentárias ou apoio da alta administração.	2	9,1
Q8 Inventários e avaliação de riscos	Contribuição efetiva para a gestão de riscos	Maior visibilidade dos dados e ativos; identificação de fluxos de informação; melhoria da gestão de riscos; envolvimento de diferentes áreas.	13	59,1
	Contribuição parcial ou implementação incipiente	Benefícios reconhecidos, mas com implantação lenta; dificuldades de operacionalização; avaliação de riscos ainda não rotineira.	3	13,6
	Predominância do atendimento formal	Produção orientada à conformidade; atendimento a auditorias; baixa incorporação à gestão cotidiana; ausência de contribuição significativa.	5	22,7
	Informação insuficiente para avaliação	Desconhecimento sobre a implementação dos inventários e das metodologias.	1	4,5

Table 5: Categorias temáticas identificadas na dimensão "A ETIR na Tomada de Decisão Estratégica"

Questão	Categoria temática	Subcategorias identificadas	*n*	%
Q9 Autonomia da ETIR	Autonomia técnica parcial	Autonomia para ações técnicas imediatas; decisões críticas dependem da alta administração; compartilhamento de decisões; autonomia relativa.	10	43,5
	Autonomia formal consolidada	Autoridade delegada; sala de crise; procedimentos formalizados; capacidade de decisão emergencial.	8	34,8
	Baixa autonomia institucional	ETIR apenas recomenda ações; inexistência de delegação formal; dependência da chefia; estrutura ainda em implantação.	5	21,7
Q10 Comunicação interna	Fluxos formais institucionalizados	Fluxos documentados; coordenador da ETIR; comissões; salas de crise; procedimentos previamente definidos.	10	43,5
	Comunicação predominantemente informal	WhatsApp; Teams; telefone; contato direto entre gestores e equipe técnica.	7	30,4
	Fluxos pouco estruturados ou desconhecidos	Ausência de processo formal; desconhecimento do fluxo; comunicação desestruturada.	6	26,1
Q11 Articulação externa	Canais institucionais consolidados	CTIR Gov; CSIC; CNJ/CJF; órgãos reguladores; e-mail institucional.	9	39,1
	Comunicação predominantemente por e-mail	E-mail como principal mecanismo de comunicação externa.	8	34,8
	Principais desafios	Burocracia; demora na comunicação; duplicidade de informações; falta de coordenação nacional; limitação de autonomia.	6	26,1

institucionais que sustentem a tomada de decisão, a coordenação organizacional e a articulação interinstitucional durante situações críticas.

5.4 Implementação de Controles Operacionais e Resposta

Esta dimensão investigou a capacidade operacional das ETIR para executar procedimentos formais de resposta a incidentes, preservar evidências digitais e assegurar a continuidade dos serviços essenciais durante situações críticas. As respostas foram analisadas por meio de análise temática, resultando nas categorias apresentadas na Tabela 6. Assim como na seção anterior, uma resposta foi desconsiderada da análise qualitativa por não apresentar conteúdo interpretável.

Em relação aos procedimentos formais de resposta a incidentes (Q12), observou-se que a categoria predominante correspondeu à existência de procedimentos documentados cuja execução ainda depende significativamente da experiência individual dos profissionais, identificada em 11 das 23 respostas (47,8%), conforme apresentado na Tabela 6. Embora os participantes reconheçam a existência de normas, manuais e fluxos formais, a resposta efetiva aos incidentes continua fortemente apoiada no conhecimento acumulado pelas equipes técnicas, especialmente diante de situações não previstas ou incidentes mais complexos.

Sete participantes (30,4%) relataram que seus órgãos possuem procedimentos formalizados e regularmente utilizados durante a resposta a incidentes, indicando maior grau de institucionalização das práticas operacionais. Em contraste, cinco respondentes (21,8%) afirmaram que a resposta permanece predominantemente dependente da experiência individual, evidenciando ausência ou baixa adoção dos procedimentos formais.

As respostas revelam que a formalização documental, embora importante, não garante por si só a padronização das ações durante incidentes cibernéticos. Um dos participantes sintetizou essa percepção ao afirmar que "o procedimento formal serve mais como referência geral; o passo a passo real na hora do incidente costuma vir do conhecimento acumulado da equipe". Esse resultado sugere que parte do conhecimento crítico ainda permanece tácito, tornando a capacidade operacional dependente da permanência e da experiência dos profissionais envolvidos.

Quanto aos obstáculos enfrentados para identificação, coleta e preservação de evidências digitais (Q13), predominou a percepção de que as principais limitações estão relacionadas aos recursos humanos e à capacitação das equipes, categoria identificada em nove respostas (39,1%). Os participantes mencionaram insuficiência de pessoal especializado, acúmulo de funções, necessidade de capacitação contínua e dificuldades para manter equipes dedicadas às atividades periciais.

Em seguida, sete participantes (30,4%) destacaram limitações relacionadas à infraestrutura tecnológica, incluindo insuficiência de ferramentas especializadas, ausência de soluções de monitoramento, dificuldades na padronização de registros e limitações para análise de logs. Outros quatro respondentes (17,4%) apontaram obstáculos de natureza procedimental e organizacional, como demora na comunicação de incidentes pelos usuários, dificuldades relacionadas à cadeia de custódia das evidências e limitações decorrentes da estrutura administrativa das organizações. Três participantes (13,1%) declararam não possuir informações suficientes para avaliar a questão.

Os resultados demonstram que os desafios enfrentados pelas ETIR extrapolam aspectos estritamente tecnológicos e envolvem limitações organizacionais relacionadas à disponibilidade de profissionais qualificados, processos estruturados e mecanismos adequados para preservação de evidências digitais. Essas limitações reduzem a capacidade institucional de investigação, aprendizado e responsabilização após incidentes cibernéticos.

A percepção sobre os planos de continuidade de negócios, prontidão e redundância de infraestrutura (Q14) revelou predominância de avaliações intermediárias. Doze participantes (52,2%) consideraram que seus órgãos apresentam estruturas em desenvolvimento ou em processo de amadurecimento, reconhecendo a existência de iniciativas relacionadas à redundância, continuidade dos serviços e preparação para incidentes, embora ainda existam limitações quanto à validação prática desses mecanismos.

Sete respondentes (30,4%) avaliaram que os planos apresentam baixa maturidade, destacando fragilidades relacionadas à documentação, ausência de testes periódicos, dependência de fornecedores externos e insuficiência de mecanismos efetivos para assegurar a continuidade dos serviços essenciais durante incidentes cibernéticos. Apenas quatro participantes (17,4%) descreveram seus órgãos como bem preparados, mencionando planos consolidados,

Table 6: Categorias temáticas identificadas na dimensão "Implementação de Controles Operacionais e Resposta"

Questão	Categoria temática	Subcategorias identificadas	*n*	%
Q12 Procedimentos de resposta	Procedimentos documentados com dependência da experiência	Normativos existentes; resposta baseada na experiência; adaptação a incidentes não previstos; conhecimento tácito.	11	47,8
	Procedimentos formalizados e utilizados	Fluxos documentados; observância dos procedimentos; institucionalização das práticas.	7	30,4
	Predominância da experiência individual	Ausência de procedimentos consolidados; dependência do conhecimento individual.	5	21,8
Q13 Preservação de evidências	Recursos humanos e capacitação insuficientes	Falta de equipe especializada; capacitação; acúmulo de funções.	9	39,1
	Limitações tecnológicas	Ferramentas insuficientes; SIEM/SOC; monitoramento; padronização de logs.	7	30,4
	Obstáculos procedimentais e organizacionais	Cadeia de custódia; demora na comunicação; dificuldades administrativas.	4	17,4
	Informação insuficiente	Desconhecimento sobre os procedimentos adotados.	3	13,1
Q14 Continuidade dos serviços	Maturidade intermediária ou em desenvolvimento	Redundância parcial; planos em amadurecimento; preparação gradual.	12	52,2
	Baixa maturidade	Planos frágeis; documentação insuficiente; dependência de terceiros; ausência de testes.	7	30,4
	Boa preparação institucional	Redundância consolidada; planos estruturados; mecanismos de continuidade implementados.	4	17,4

redundância de infraestrutura e mecanismos estruturados de continuidade operacional.

Entre as respostas, destacou-se a percepção de que muitos planos permanecem predominantemente teóricos e ainda não foram submetidos a exercícios ou simulações capazes de validar sua efetividade. Um dos participantes afirmou que "não é um plano de continuidade testado de verdade", evidenciando que a existência formal dos procedimentos nem sempre corresponde à capacidade organizacional de executá-los durante situações reais de crise.

De forma integrada, os resultados desta dimensão evidenciam que a capacidade operacional das ETIR encontra-se em processo de consolidação na maior parte das organizações investigadas. Embora procedimentos formais, mecanismos de resposta e iniciativas relacionadas à continuidade dos serviços já estejam presentes em diversos órgãos, sua efetividade permanece fortemente condicionada à experiência individual dos profissionais, à disponibilidade de recursos humanos especializados, à maturidade dos processos e à existência de infraestrutura adequada para apoiar a resposta a incidentes. Esses resultados indicam que a operacionalização da governança da segurança da informação depende não apenas da formalização de controles, mas também da capacidade institucional de transformar procedimentos documentados em práticas organizacionais continuamente executadas, avaliadas e aperfeiçoadas.

5.5 Revisão, Aprendizado Organizacional e Maturidade

Esta dimensão investigou como os órgãos públicos incorporam os conhecimentos obtidos durante incidentes cibernéticos para fortalecer a governança da segurança da informação. Foram analisados aspectos relacionados à realização de processos formais de lições aprendidas, aos impactos da retenção do conhecimento institucional e aos mecanismos utilizados para transformar experiências anteriores em ações permanentes de conscientização, capacitação e aperfeiçoamento organizacional. A análise temática das respostas resultou nas categorias apresentadas na Tabela 7.

Em relação aos processos de revisão após incidentes (Q15), observou se predominância de organizações que afirmaram realizar processos formais de lições aprendidas, identificada em 13 das 23 respostas (56,5%). Os participantes relataram a utilização de bases de conhecimento, registros estruturados, análises pós-incidente (*post mortem*) e revisão de políticas e procedimentos como mecanismos para preservar o conhecimento gerado durante a resposta aos incidentes.

Cinco participantes (21,7%) indicaram que esses processos ainda se encontram em fase de implantação ou amadurecimento institucional. Nesses casos, embora exista reconhecimento da importância das lições aprendidas, os registros ainda ocorrem de forma parcial ou dependem da iniciativa das equipes responsáveis. Outros cinco respondentes (21,7%) relataram ausência ou baixa institucionalização desse processo, indicando que as experiências adquiridas durante os incidentes permanecem predominantemente no conhecimento individual dos profissionais.

As respostas evidenciam que a maioria das organizações já reconhece a importância da aprendizagem decorrente dos incidentes cibernéticos. Entretanto, a institucionalização desse conhecimento ainda apresenta diferentes níveis de maturidade, indicando que a simples realização de registros não garante sua incorporação sistemática aos processos de governança.

Quando questionados sobre os impactos da carência de profissionais especializados, da rotatividade de servidores e da terceirização na retenção do conhecimento institucional (Q16), observou-se forte convergência entre os participantes. Dezesseis respostas (69,6%) indicaram que esses fatores comprometem significativamente a preservação do conhecimento organizacional, afetando diretamente a continuidade das capacidades desenvolvidas após os incidentes.

Os participantes destacaram a perda de servidores especializados, a elevada rotatividade de profissionais terceirizados, dificuldades para reposição de especialistas e limitações decorrentes da baixa atratividade das carreiras públicas em tecnologia da informação. Em diversos relatos, a perda de conhecimento foi associada não apenas à saída dos profissionais, mas também à dificuldade de documentar adequadamente experiências acumuladas ao longo da atuação da ETIR.

Quatro respondentes (17,4%) reconheceram impactos moderados, indicando que mecanismos internos, como bases de conhecimento e documentação técnica, contribuem parcialmente

para reduzir a perda de conhecimento institucional. Apenas três participantes (13,0%) classificaram a situação como específica de seus contextos organizacionais ou declararam não possuir elementos suficientes para avaliá-la.

Table 7: Categorias temáticas identificadas na dimensão "Revisão, Aprendizado Organizacional e Maturidade"

Questão	Categoria temática	Subcategorias identificadas	*n*	%
Q15 Lições aprendidas	Processos formais implementados	Base de conhecimento; registros; pós-mortem; revisão de políticas e procedimentos.	13	56,5
	Processos em implantação	Ações em adaptação; registros parciais; institucionalização em desenvolvimento.	5	21,7
	Baixa institucionalização	Ausência de processo estruturado; conhecimento pouco documentado.	5	21,7
Q16 Retenção do conhecimento	Impacto elevado da rotatividade	Perda de especialistas; terceirização; baixa remuneração; dificuldade de retenção.	16	69,6
	Impacto moderado	Conhecimento parcialmente preservado; mecanismos internos mitigam perdas.	4	17,4
	Situação específica ou não aplicável	Não aplicável; informação insuficiente.	3	13,0
Q17 Disseminação do conhecimento	Transformação em ações institucionais	Treinamentos; campanhas; atualização de procedimentos; simulados; capacitação.	11	47,8
	Compartilhamento parcialmente estruturado	Bases de conhecimento; reuniões; troca informal de experiências.	8	34,8
	Ausência de processo contínuo	Conhecimento permanece individual; inexistência de capacitação sistemática.	4	17,4

Os resultados demonstram que a retenção do conhecimento representa um dos principais desafios para a consolidação da governança operacional, uma vez que a resolução de incidentes nem sempre resulta na preservação das competências adquiridas pelas equipes. Como sintetizou um dos participantes, "muito conhecimento fica concentrado em quem viveu o incidente [...] e esse conhecimento se perde fácil", evidenciando a dependência de conhecimento tácito e a fragilidade dos mecanismos institucionais de retenção.

Em relação à transformação das experiências acumuladas em ações contínuas de conscientização e capacitação (Q17), observouse que onze participantes (47,8%) afirmaram que os conhecimentos obtidos durante incidentes são incorporados aos processos institucionais por meio de treinamentos, campanhas de conscientização, atualização de procedimentos, reuniões de lições aprendidas, simulados e elaboração de orientações técnicas.

Oito respostas (34,8%) indicaram que o compartilhamento do conhecimento ocorre de maneira parcialmente estruturada, principalmente por meio de reuniões internas, bases de conhecimento ou comunicação entre as equipes técnicas, mas sem constituir programas permanentes de capacitação institucional. Nesses casos, a disseminação das experiências permanece concentrada entre os profissionais diretamente envolvidos na resposta aos incidentes.

Por outro lado, quatro participantes (17,4%) relataram inexistência de processos contínuos para disseminação das lições aprendidas, destacando que o conhecimento permanece associado à experiência individual ou é utilizado apenas durante o planejamento de ações futuras, sem documentação sistemática ou treinamento estruturado.

Esses resultados indicam que, embora diversas organizações já utilizem incidentes anteriores como fonte de aprendizagem, a institucionalização desse conhecimento ainda apresenta níveis distintos de maturidade. Em muitos casos, a aprendizagem organizacional permanece dependente da iniciativa das equipes técnicas, dificultando sua incorporação permanente às práticas de governança da segurança da informação.

De forma integrada, os resultados desta dimensão evidenciam que a maturidade da governança operacional não depende exclusivamente da capacidade de responder aos incidentes, mas da habilidade institucional de transformar experiências operacionais em conhecimento organizacional permanente. Embora processos de lições aprendidas estejam presentes em parte significativa das organizações investigadas, sua efetividade ainda é limitada por fatores como rotatividade de profissionais, terceirização, insuficiência de servidores especializados e mecanismos incompletos de disseminação do conhecimento. Dessa forma, observa-se que a consolidação da governança operacional exige não apenas estruturas formais de resposta, mas também mecanismos capazes de preservar, compartilhar e reutilizar continuamente o conhecimento produzido durante a gestão dos incidentes cibernéticos.

5.6 Desafios Gerais e Consolidação da ETIR como Estrutura de Governança

A última dimensão investigou os fatores organizacionais que ainda dificultam a consolidação da ETIR como uma estrutura estratégica de governança na Administração Pública Federal. Foram analisadas as percepções dos participantes sobre aspectos culturais e de integração institucional, limitações estruturais para fortalecimento da ETIR e mudanças necessárias no modelo de governança estabelecido pelo PPSI para ampliar a resiliência cibernética dos órgãos públicos.

As categorias resultantes da análise temática são apresentadas na Tabela 8.

Em relação à integração entre as áreas de Tecnologia da Informação, Segurança da Informação e áreas finalísticas (Q18), observouse predominância da percepção de resistência cultural e dificuldades de integração institucional, identificada em quinze respostas (65,2%). Os participantes destacaram que grande parte das áreas finalísticas ainda percebe a segurança da informação como responsabilidade exclusiva da área técnica ou como um elemento burocrático que dificulta a execução das atividades institucionais.

Diversos relatos indicaram baixo nível de conscientização sobre riscos cibernéticos, reduzido engajamento das unidades administrativas e dificuldades para incorporar práticas de segurança às atividades cotidianas. Em vários casos, os participantes ressaltaram que as demandas operacionais e a escassez de pessoal fazem com que as equipes priorizem respostas imediatas em detrimento de ações preventivas e colaborativas.

Quatro participantes (17,4%) relataram que seus órgãos apresentam integração satisfatória entre as áreas envolvidas, enquanto outros quatro (17,4%) identificaram uma situação

intermediária, caracterizada por avanços na colaboração, embora ainda persistam desafios relacionados à comunicação e à conscientização institucional.

Os resultados indicam que os principais obstáculos para consolidação da governança cibernética não decorrem apenas de limitações técnicas, mas também de fatores organizacionais e culturais que dificultam a integração entre segurança da informação e as áreas responsáveis pela execução das políticas públicas.

Quanto aos fatores que dificultam a consolidação da ETIR como estrutura estratégica de governança (Q19), observou-se que a principal limitação está relacionada aos recursos humanos, identificada em onze respostas (47,8%). Os participantes destacaram insuficiência de profissionais especializados, elevada rotatividade, dificuldades para retenção de especialistas e dependência excessiva de equipes terceirizadas como fatores que comprometem a continuidade das capacidades organizacionais.

Em seguida, oito respondentes (34,8%) apontaram restrições orçamentárias e institucionais como obstáculos relevantes, mencionando limitações para aquisição de ferramentas, capacitação das equipes e financiamento de ações permanentes de segurança cibernética.

Outros quatro participantes (17,4%) enfatizaram aspectos relacionados ao reconhecimento institucional da ETIR, incluindo necessidade de maior autonomia, fortalecimento do apoio da alta administração, definição clara de responsabilidades e inserção da equipe nas estruturas estratégicas de governança.

Esses resultados reforçam que a consolidação da ETIR depende de um conjunto de condições organizacionais que extrapolam aspectos técnicos, envolvendo recursos humanos, financiamento, comprometimento institucional e mecanismos formais de governança.

Em relação às mudanças consideradas necessárias para fortalecer o modelo de governança estabelecido pelo PPSI (Q20), observouse predominância de propostas voltadas ao fortalecimento institucional da segurança da informação. Oito participantes (34,8%) defenderam maior envolvimento da alta administração, fortalecimento da autonomia da ETIR, institucionalização da segurança como função estratégica e definição de responsabilidades organizacionais mais claras.

Sete respondentes (30,4%) enfatizaram a necessidade de ampliar investimentos em capacitação contínua, valorização profissional e melhoria das condições de trabalho, considerando esses fatores essenciais para reduzir a rotatividade e fortalecer as capacidades institucionais.

Cinco participantes (21,7%) sugeriram ampliar mecanismos de integração, padronização e compartilhamento entre órgãos públicos, incluindo criação de bases nacionais de conhecimento, disseminação de boas práticas, compartilhamento de *playbooks*, *runbooks* e realização de exercícios conjuntos de resposta a incidentes.

Por fim, três respondentes (13,1%) defenderam a evolução do próprio modelo estabelecido pelo PPSI, propondo maior flexibilidade para contemplar diferentes níveis de maturidade institucional, digitalização de processos, fortalecimento da gestão de riscos e mecanismos de acompanhamento mais aderentes às características dos diversos órgãos da Administração Pública Federal.

As respostas demonstram que os participantes compreendem a consolidação da ETIR como um desafio predominantemente organizacional, cuja superação exige articulação entre governança institucional, recursos humanos, investimentos permanentes e mecanismos colaborativos de aprendizagem entre os órgãos públicos.

De forma integrada, os resultados desta dimensão evidenciam que a consolidação da ETIR como estrutura de governança operacional depende da convergência entre fatores organizacionais, institucionais e humanos. Embora avanços importantes tenham sido observados na implementação do PPSI e na institucionalização das práticas de segurança da informação, permanecem desafios relacionados à cultura organizacional, integração entre áreas, disponibilidade de recursos especializados, apoio da alta administração e compartilhamento sistemático do conhecimento. Assim, os participantes indicam que o fortalecimento da resiliência cibernética da Administração Pública Federal requer não apenas a implementação de controles técnicos, mas também o desenvolvimento de capacidades organizacionais capazes de integrar governança, coordenação institucional, aprendizado contínuo e gestão estratégica da segurança da informação.

Os resultados obtidos nas seis dimensões investigadas evidenciam que a consolidação da ETIR como uma estrutura de governança operacional ocorre de forma progressiva e depende da integração de diferentes capacidades organizacionais. A análise temática permitiu identificar cinco capacidades complementares que emergiram das respostas dos participantes: (i) governança normativa, responsável por estabelecer políticas, papéis e diretrizes institucionais; (ii) autoridade e coordenação institucional, relacionadas à integração entre áreas e ao suporte da alta administração; (iii) capacidade operacional, voltada à execução dos processos de prevenção, resposta e continuidade; (iv) aprendizado organizacional, associado à retenção do conhecimento, às lições aprendidas e à capacitação contínua; e (v) consolidação estratégica, que representa a institucionalização dessas capacidades para fortalecer a resiliência cibernética da Administração Pública Federal. A Figura 1 sintetiza esse modelo conceitual emergente da pesquisa, evidenciando o caráter cíclico da governança operacional, no qual o aprendizado organizacional retroalimenta continuamente o aprimoramento da governança normativa.

6 Discussão

Os resultados obtidos permitem ampliar a compreensão da ETIR para além de sua função tradicional de resposta técnica a incidentes cibernéticos. Embora a literatura frequentemente descreva essas equipes como estruturas responsáveis pela detecção, contenção e recuperação de incidentes [10, 18], as evidências empíricas deste estudo indicam que, no contexto da Administração Pública Federal, sua atuação envolve um conjunto mais amplo de capacidades relacionadas à governança operacional.

A primeira evidência refere-se ao papel da ETIR como mecanismo de operacionalização das diretrizes estabelecidas pelo Programa de Privacidade e Segurança da Informação (PPSI). Os participantes reconheceram avanços importantes na implementação das políticas institucionais de segurança e proteção de dados pessoais, mas também indicaram que a efetividade dessas diretrizes depende da existência de estruturas capazes de coordenar sua aplicação nas atividades cotidianas. Esse resultado reforça argumentos da literatura segundo os quais frameworks normativos, por si só, não garantem maturidade organizacional, sendo necessária a existência de mecanismos institucionais que convertam políticas em práticas operacionais [3, 14].

Os resultados também evidenciam que a atuação da ETIR depende fortemente de mecanismos de coordenação organizacional. Aspectos como autonomia decisória, integração entre equipes técnicas e alta administração, comunicação interinstitucional e definição clara de responsabilidades apareceram de forma recorrente nas respostas dos participantes. Esses achados convergem com modelos internacionais de governança da segurança da informação, que enfatizam que a capacidade de resposta organizacional resulta da integração entre estruturas técnicas, processos decisórios e gestão de riscos, e não apenas da adoção de controles tecnológicos [10, 12, 20]. Outro aspecto relevante refere-se ao aprendizado organizacional. Embora diversas organizações relatem processos formais de lições aprendidas, a pesquisa mostrou que a retenção do conhecimento permanece fortemente comprometida pela rotatividade de profissionais, terceirização e escassez de especialistas. Essa evidência demonstra que a maturidade da governança operacional depende não apenas da capacidade de responder aos incidentes, mas também da capacidade institucional de preservar, compartilhar e reutilizar continuamente o conhecimento produzido durante esses eventos.

A análise integrada das cinco dimensões investigadas permitiu identificar um conjunto de capacidades organizacionais que sustentam a atuação da ETIR como estrutura de governança operacional. Diferentemente de modelos prescritivos encontrados na literatura, essas capacidades emergiram diretamente das percepções dos profissionais que atuam na Administração Pública Federal, resultando no modelo conceitual proposto neste estudo. Esse modelo descreve uma evolução organizacional que inicia na governança normativa, avança para mecanismos de coordenação institucional, consolida capacidades operacionais, incorpora processos de aprendizado organizacional e culmina na consolidação estratégica da governança operacional.

Sob a perspectiva prática, os resultados sugerem que iniciativas voltadas exclusivamente à aquisição de ferramentas ou à implementação de controles técnicos tendem a produzir ganhos limitados quando não acompanhadas pelo fortalecimento da coordenação institucional, da retenção do conhecimento, da capacitação contínua e do apoio da alta administração. Assim, a consolidação da ETIR como estrutura de governança operacional exige uma abordagem integrada que articule governança, gestão de riscos, segurança da informação e desenvolvimento organizacional.

7 Conclusão

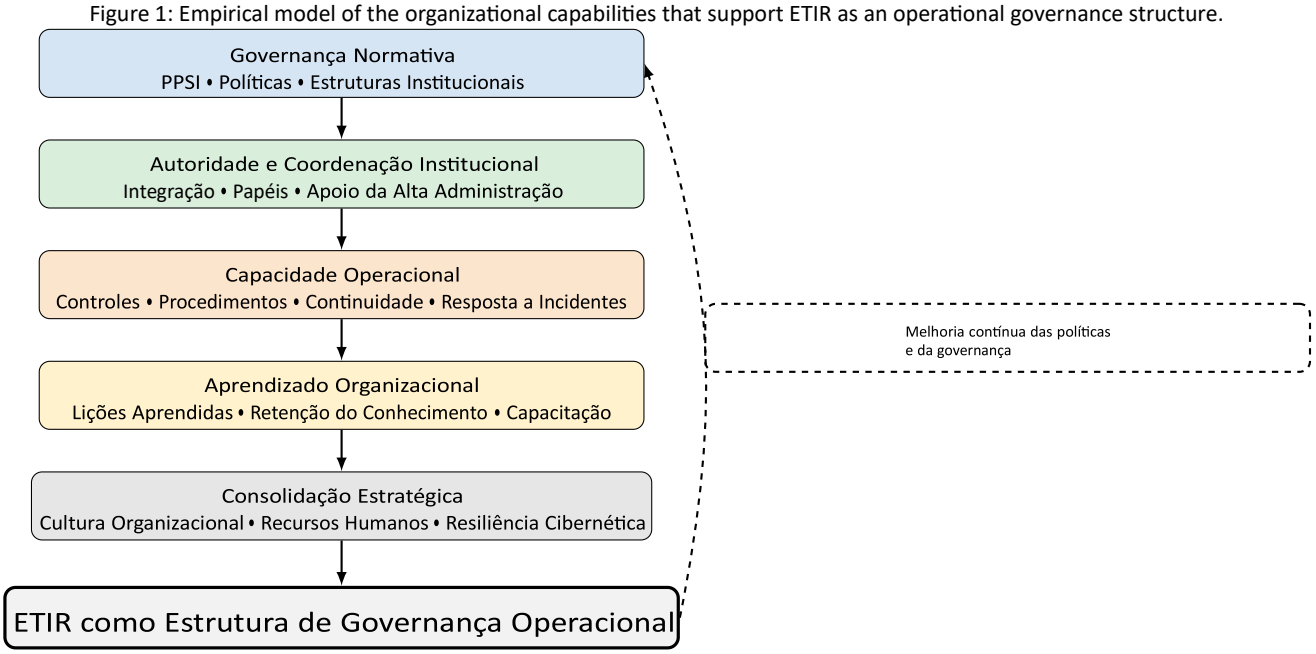
Este estudo investigou em que medida a Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR) pode ser compreendida como uma estrutura de governança operacional no contexto da Administração Pública Federal. Partindo da constatação de que a literatura concentra suas discussões predominantemente nos aspectos técnicos da resposta a incidentes, buscou-se analisar empiricamente como a atuação da ETIR se articula com mecanismos de governança, coordenação institucional, implementação operacional e aprendizado organizacional.

Os resultados evidenciaram que a ETIR exerce funções que extrapolam a contenção técnica de incidentes. As percepções dos participantes demonstram que sua atuação envolve coordenação entre diferentes áreas organizacionais, apoio aos processos decisórios,

Table 8: Categorias temáticas identificadas na dimensão "Desafios Gerais e Consolidação da ETIR como Estrutura de Governança"

Questão	Categoria temática	Subcategorias identificadas	*n*	%
Q18 Integração institucional	Resistência cultural e baixa integração	Baixa conscientização; segurança percebida como responsabilidade exclusiva da TI; dificuldades de colaboração entre áreas técnicas e finalísticas.	15	65,2
	Integração satisfatória	Boa articulação entre TI, Segurança da Informação e áreas de negócio.	4	17,4
	Integração parcial	Avanços na colaboração, porém ainda com limitações de comunicação e engajamento.	4	17,4
Q19 Consolidação da ETIR	Recursos humanos e retenção de especialistas	Carência de profissionais; rotatividade; terceirização; baixa remuneração.	11	47,8
	Restrições orçamentárias e institucionais	Orçamento insuficiente; limitações para aquisição de ferramentas e capacitação.	8	34,8
	Reconhecimento estratégico da ETIR	Necessidade de apoio da alta gestão; autonomia; definição de responsabilidades.	4	17,4
Q20 Fortalecimento do PPSI	Fortalecimento institucional	Maior participação da alta administração; autonomia da ETIR; institucionalização da segurança.	8	34,8
	Capacitação e valorização profissional	Treinamentos; valorização dos servidores; retenção de especialistas.	7	30,4
	Integração e compartilhamento	Base nacional de conhecimento; playbooks; colaboração entre órgãos.	5	21,7
	Evolução do modelo do PPSI	Maior flexibilidade; gestão de riscos; digitalização e acompanhamento da maturidade.	3	13,1

Figure 1: Empirical model of the organizational capabilities that support ETIR as an operational governance structure.



implementação de controles operacionais, disseminação de conhecimento e fortalecimento da gestão de riscos. Esses elementos indicam que a ETIR desempenha papel relevante na operacionalização das diretrizes estabelecidas pelo Programa de Privacidade e Segurança da Informação (PPSI), contribuindo para aproximar os mecanismos normativos das práticas organizacionais cotidianas.

Ao mesmo tempo, o estudo identificou desafios importantes para a consolidação dessa estrutura. A elevada rotatividade de profissionais, a dependência de mão de obra terceirizada, as limitações orçamentárias, a insuficiência de recursos humanos especializados, a baixa integração entre áreas finalísticas e técnicas e a necessidade de maior apoio da alta administração foram apontadas como fatores que dificultam a maturidade da governança operacional e reduzem a capacidade institucional de resposta e aprendizado contínuo.

Como principal contribuição científica, esta pesquisa propõe um modelo conceitual derivado empiricamente das percepções dos participantes, estruturado em cinco capacidades organizacionais complementares: (i) governança normativa, (ii) autoridade e coordenação institucional, (iii) capacidade operacional, (iv) aprendizado organizacional e (v) consolidação estratégica. Em conjunto, essas capacidades descrevem como a ETIR evolui de uma equipe predominantemente técnica para uma estrutura de governança operacional capaz de fortalecer a resiliência cibernética das organizações públicas.

Do ponto de vista prático, os resultados oferecem subsídios para gestores públicos envolvidos na implementação do PPSI, indicando que o fortalecimento da ETIR requer não apenas investimentos em infraestrutura tecnológica, mas também mecanismos permanentes de coordenação institucional, retenção do conhecimento, capacitação contínua e integração entre governança, gestão de riscos e segurança da informação.

Este estudo apresenta algumas limitações. A pesquisa foi conduzida com um número restrito de participantes e baseou-se na percepção de profissionais vinculados à Administração Pública Federal, o que limita a generalização dos resultados para outros contextos organizacionais. Além disso, a natureza exploratória da investigação não permite estabelecer relações causais entre as capacidades identificadas e o nível de maturidade das organizações.

Como trabalhos futuros, recomenda-se ampliar a investigação para outros poderes e esferas da administração pública, realizar estudos comparativos entre diferentes modelos de governança da segurança da informação e desenvolver instrumentos quantitativos capazes de avaliar o grau de maturidade das capacidades organizacionais identificadas neste estudo. Também se mostra promissora a validação empírica do modelo conceitual proposto por meio de estudos de caso ou pesquisas com amostras mais amplas.

Por fim, conclui-se que a consolidação da ETIR como estrutura de governança operacional depende menos da adoção isolada de controles técnicos e mais da capacidade institucional de integrar governança normativa, coordenação organizacional, execução operacional e aprendizado contínuo. Sob essa perspectiva, a ETIR deixa de representar apenas uma equipe especializada em resposta a incidentes para assumir papel estratégico na construção da resiliência cibernética da Administração Pública Federal.

References

[1] Ekrem T Baser and Evrim Tan. 2023. Citizen expectations, agency reputation and public service quality. *Public Management Review* (2023), 1–27. https://doi.org/10.1080/14719037.2023.2245842

[2] Brasil. Secretaria de Governo Digital / Ministério da Gestão e Inovação em Serviços Públicos. 2026. *Guia do Framework de Privacidade e Segurança da Informação — PPSI 2.0.* Technical Report. SGD/MGI, Brasília, DF. https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi2.0/arquivos/guiafwppsi2-0-v1-2-30012026.pdf Versão 1.2, 30 jan. 2026.

[3] Edna Dias Canedo, Ana Paula Morais do Vale, Rogério Machado Gravina, Alessandra de Vasconcelos Sales, Bruno J. G. Praciano, Vinicius Eloy dos Reis, Fábio Lúcio Lopes de Mendonça, and Rafael Timóteo de Sousa Júnior. 2022. ICT Governance and Management Macroprocesses of a Brazilian Federal Government Agency. *Inf.* 13, 5 (2022), 231. doi:10.3390/INFO13050231

[4] Edna Dias Canedo, Ana Paula Morais do Vale, Rogério Machado Gravina, Rafael Leite Patrão, Leomar Camargo de Souza, Vinicius Eloy dos Reis, Fábio Lúcio Lopes de Mendonça, and Rafael T. de Sousa Jr. 2021. An Applied Risk Identification Approach in the ICT Governance and Management Macroprocesses of a Brazilian Federal Government Agency. In *Proceedings of the 23rd International Conference on Enterprise Information Systems, ICEIS 2021, Online Streaming, April 26-28, 2021, Volume 1*, Joaquim Filipe, Michal Smialek, Alexander Brodsky, and Slimane Hammoudi (Eds.). SCITEPRESS, 272–279. doi:10.5220/0010475902720279

[5] Angela Maria Cristina Clara, Edna Dias Canedo, and Rafael Timóteo de Sousa Júnior. 2017. Elements that Orient the Regulatory Compliance Verification Audits on ICT Governance. In *Proceedings of the 18th Annual International Conference on Digital Government Research, DG.O 2017, Staten Island, NY, USA, June 7-9, 2017*, Charles C. Hinnant and Adegboyega Ojo (Eds.). ACM, 177–184. doi:10.1145/3085228.3085286

[6] Nartional Congress da República, Presidência. 2018. Brazilian General Data Protection Law (LGPD). *Nartional Congress, accessed in April 10, 2022* 1, 1 (2018), 1–31. https://www.pnm.adv.br/wp-content/uploads/2018/08/Brazilian-GeneralData-Protection-Law.pdf

[7] Marianne Batista Diniz Da Silva[1], Eduardo Coelho Silva[1], Fernando Alves De Carvalho Filho[1], Thauane Moura Garcia[1], Isabel Nunes, and Rogério Patrício Chagas Do Nascimento[1]. 2017. Public ICT governance: A quasi-systematic review. *In Proceedings of the 19th International Conference on Enterprise Information Systems (ICEIS 2017)* 2 (2017), 351–359. https://www.scitepress.org/PublishedPapers/2017/63146/63146.pdf

[8] Jason Edwards. 2024. *A comprehensive guide to the NIST cybersecurity framework 2.0: Strategies, implementation, and best practice*. John Wiley & Sons.

[9] IMPROVING PRIVACY THROUGH ENTERPRISE. April 14, 2025. NIST PRIVACY FRAMEWORK: A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT, VERSION 1.1. *National Institute of Standards and Technology* (April 14, 2025). doi:10.6028/NIST.CSWP.40.ipd

[10] European Union Agency for Cybersecurity ENISA. 2010. *Good Practice Guide for Incident Management*. Technical Report. ENISA, European Union. https://www.enisa.europa.eu/sites/default/files/publications/Incident_Management_guide.pdf

[11] International Organization for Standardization (ISO). 2019. Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines. https://www.iso.org/standard/71670.html

[12] International Organization for Standardization (ISO). 2022. ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection — Information security management systems — Requirements. https://www.iso.org/standard/27001

[13] Gabinete de Segurança Institucional da Presidência da República (GSI/PR). 2022. *Plano de Gestão de Incidentes Cibernéticos para a Administração Pública Federal (Plangic)*. Technical Report. GSI/PR, Brasília, DF. https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/plano-de-gestao-de-incidentes-ciberneticos-plangic/plangic.pdf

[14] Wim Grembergen and Steven Haes. 2009. Enterprise governance of information technology: achieving strategic alignment and value.

[15] Manar Saleh Husain, Shroog Abdulhadi M. Alqahtani, Saqib Saeed, Hina Gull, Sardar Zafar Iqbal, and Madeeha Saqib. 2026. Cybersecurity Challenges of Digital Transformation in the Entertainment Industry. *Inf.* 17, 3 (2026), 219. doi:10.3390/INFO17030219

[16] Fernando Rocha Moreira, Edna Dias Canedo, Rafael Rabelo Nunes, André Luiz Marques Serrano, Cláudia Jacy Barenco Abbas, Marcelo Lopes Pereira Júnior, and Fábio Lúcio Lopes de Mendonça. 2025. Cybersecurity Risk Assessment Through Analytic Hierarchy Process: Integrating Multicriteria and Sensitivity Analysis. In *Proceedings of the 27th International Conference on Enterprise Information Systems, ICEIS 2025, Porto, Portugal, April 4-6, 2025, Volume 2*, Joaquim Filipe, Michal Smialek, Alexander Brodsky, and Slimane Hammoudi (Eds.). SCITEPRESS, 117–128. doi:10.5220/0013197300003929

[17] VALDER RIBEIRO DE MOURA. 2025. *PORTARIA MIDR Nº 3.228, DE 31 DE OUTUBRO DE 2025 – Política de Proteção de Dados Pessoais do Ministério da Integração e do Desenvolvimento Regional.* Technical Report. MINISTRO DE ESTADO DA INTEGRAÇÃO E DO DESENVOLVIMENTO REGIONAL, Brasilia–DF. https://www.in.gov.br/en/web/dou/-/portaria-midr-n-3.228-de-31-deoutubro-de-2025-666148611 [18] Alex Nelson, Sanjay Rekhi, Murugiah Souppaya, and Karen Scarfone. 2025. *Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile*. Technical Report NIST SP 800-61 Rev. 3. National Institute of Standards and Technology, Gaithersburg, MD, USA. doi:10.6028/NIST.SP.800-61r3

[19] National Institute of Standards and Technology. 2023. Artificial Intelligence Risk Management Framework (AI RMF 1.0). *National Institute of Standards and Technology* 1 (2023), 1–48. doi:10.6028/NIST.AI.100-1

[20] National Institute of Standards and Technology. February 26, 2024. The NIST Cybersecurity Framework (CSF) 2.0. *National Institute of Standards and Technology, NIST CSWP 29* (February 26, 2024). doi:nistpubs/CSWP/NIST.CSWP.29.pdf

[21] Glauco Vitor Pedrosa, Wander Cleber Maria Pereira da Silva, and Rejane Maria da Costa Figueiredo. 2025. EXPLORATORY STUDY OF QUALITY ATTRIBUTES IN BRAZILIAN DIGITAL PUBLIC SERVICES. *Environmental & Social Management Journal/Revista de Gestão Social e Ambiental* 19, 4 (2025).

[22] Lucas Dalle Rocha and Edna Dias Canedo. 2025. Optimizing Compliance: Comparative Study of Data Laws and Privacy Frameworks. *J. Internet Serv. Appl.* 16, 1 (2025), 431–452. doi:10.5753/JISA.2025.5247

[23] ANTONIO WALDEZ GÓES DA SILVA. 2026. *PORTARIA MIDR Nº 386, DE 3 DE FEVEREIRO DE 2026 – Política de Segurança da Informação - PSI do Ministério da Integração e do Desenvolvimento Regional - MIDR.* Technical Report. MINISTRO DE ESTADO DA INTEGRAÇÃO E DO DESENVOLVIMENTO REGIONAL, Brasilia–DF. https://www.in.gov.br/en/web/dou/-/portaria-midr-n-3.228-de-31de-outubro-de-2025-666148611

[24] Amit Anand Tiwari, Samrat Gupta, Efpraxia D Zamani, Neeraj Mittal, and Renu Agarwal. 2024. An overarching conceptual framework for ICT-enabled responsive governance. *Information Systems Frontiers* 26, 3 (2024), 1161–1182.

[25] Álvaro Vaya-Arboledas, Mikel Ferrer-Oliva, and José Amelio Medina-Merodio. 2025. Evolution and Perspectives in IT Governance: A Systematic Literature Review. *Computers* 14, 12 (2025), 520. https://doi.org/10.3390/computers14120520 [26] Elaine Venson, Rejane Maria da

Costa Figueiredo, and Edna Dias Canedo. 2024. Leveraging a startup-based approach for digital transformation in the public sector: A case study of Brazil's startup gov.br program. *Gov. Inf. Q.* 41, 3 (2024), 101943. doi:10.1016/J.GIQ.2024.101943