

Notificação e Coordenação de Incidentes Cibernéticos nos Três Poderes Federais

Juliano Aléssio da Silva
Programa de Pós-Graduação em Engenharia Elétrica
Universidade de Brasília (UnB)
Brasília, DF, Brasil
julianosilva@utfpr.edu.br

João Souza Neto
Programa de Pós-Graduação em Engenharia Elétrica
Universidade de Brasília (UnB)
Brasília, DF, Brasil
neto.joao@unb.br

Resumo—Este artigo analisa como documentos oficiais dos Poderes Executivo, Legislativo e Judiciário Federais disciplinam a notificação e a coordenação de incidentes cibernéticos entre 2020 e 2025. A pesquisa aplica análise documental comparativa, qualitativa e exploratória-descritiva a normas, planos, protocolos e atos institucionais dos três Poderes, examinados segundo categorias que abrangem responsável, destinatário, abrangência institucional e material, critérios de acionamento e coordenação intrapoder e interpoderes. Os resultados mostram mecanismos internos formalizados, porém assimétricos entre os Poderes. Nos atos normativos examinados, nenhum dos cinco mecanismos técnicos explicita o conteúdo mínimo do primeiro reporte; apenas o fluxo regulatório o define. Tampouco foi identificado protocolo público comum aos três Poderes que articule gatilho, conteúdo mínimo, prazo, roteamento, confirmação e retorno. A LGPD e a regulamentação da ANPD formam uma camada regulatória transversal para incidentes com dados pessoais, sem substituir a coordenação técnica. Conclui-se que a arquitetura documentada combina redes internas e conexões seletivas, sem que tenha sido identificada interface pública comum e verificável entre os Poderes. A contribuição do estudo consiste em oferecer uma matriz descritiva, uma matriz comparativa e elementos de referência para uma interface entre estruturas autônomas.

Palavras-chave—Segurança da informação, incidentes cibernéticos, notificação de incidentes, coordenação interinstitucional, setor público federal.

I. INTRODUÇÃO

A transformação digital ampliou a dependência do Estado em relação a sistemas conectados, serviços de nuvem, fornecedores e plataformas compartilhadas. Esse processo favorece a eficiência e o acesso aos serviços públicos, mas também aumenta o impacto potencial de falhas e ataques à confidencialidade, à integridade, à disponibilidade e à autenticidade das informações [1].

Incidentes cibernéticos nem sempre se restringem ao órgão em que foram detectados. Uma vulnerabilidade em um produto amplamente utilizado, o comprometimento de um fornecedor ou a indisponibilidade de um serviço compartilhado podem afetar instituições distintas. Nesses casos, a comunicação tempestiva permite correlacionar

ocorrências, bloquear indicadores maliciosos e adotar medidas preventivas antes da propagação do mesmo vetor.

Em 2024, o Tribunal de Contas da União (TCU) registrou que o Estado brasileiro não dispunha de organização responsável por orientar a atividade cibernética nacional nem de órgão que consolidasse informações de todo o setor público [2], [3]. Ao mesmo tempo, o TCU apontou diferenças de maturidade e dificuldades na implementação de controles [4]. No levantamento associado ao Acórdão nº 2.387/2024, 69% das organizações do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) avaliadas encontravam-se nos estágios iniciais ou básicos [4]. A Lista de Alto Risco informou ainda que, nos órgãos, autarquias e fundações do Executivo Federal, os incidentes de segurança da informação passaram de 3.402 em 2022 para 5.302 em 2024 [2]. Esses dados não medem a coordenação entre os Poderes, mas evidenciam a relevância de mecanismos capazes de transformar detecções locais em alertas úteis para outras instituições.

Entre 2020 e 2025, os três Poderes estabeleceram mecanismos próprios de segurança e de resposta. No Executivo, destacam-se a Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC), o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) e o Plano de Gestão de Incidentes Cibernéticos para a Administração Pública Federal (PlanGIC). Também se destacam o Programa de Privacidade e Segurança da Informação (PPSI) e, no âmbito do programa, o Centro Integrado de Segurança Cibernética do Governo Digital (CISC Gov.br) [5]–[7].

No Judiciário, o Conselho Nacional de Justiça (CNJ) estruturou uma rede própria e protocolos específicos, enquanto o Supremo Tribunal Federal (STF) preservou um processo autônomo [8]–[12].

No Legislativo, o Senado instituiu a Política Corporativa de Gestão de Incidentes de Segurança da Informação (PCGIS) e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) [13], [14]. A Câmara atualizou sua Política de Segurança da Informação e Cibernética (POSIC) e definiu o Grupo de Resposta a Incidentes de Segurança da Informação da Câmara dos Deputados (GRIS-CD) [15].

A existência desses mecanismos não demonstra, por si só, como a informação atravessa os limites de cada Poder. Redes internas podem funcionar adequadamente em suas comunidades e, ainda assim, depender de contatos *ad hoc* quando um incidente envolve um fornecedor comum, uma vulnerabilidade amplamente explorada ou um serviço interconectado. A questão central é saber se os documentos tornam verificável quem comunica, quem recebe, qual conteúdo é necessário, em que prazo ocorre o envio, como a mensagem é roteada e qual retorno chega ao notificante. A literatura brasileira descreve avanços institucionais, mas também a persistência de desafios de articulação na governança nacional de cibersegurança [16].

Diante desse contexto, o estudo pretende responder à seguinte pergunta: como os documentos oficiais dos três Poderes Federais disciplinam a notificação e a coordenação de incidentes cibernéticos? Como questão derivada, o estudo pergunta ainda quais elementos seriam necessários para uma interface de comunicação entre mecanismos institucionalmente autônomos.

O objetivo geral é identificar os principais instrumentos, descrever seus responsáveis, destinatários, abrangências e requisitos de comunicação, comparar as formas de coordenação intrapoder e interpoderes e apresentar elementos de referência compatíveis com as limitações encontradas.

A Lei Geral de Proteção de Dados Pessoais (LGPD) e a regulamentação da Autoridade Nacional de Proteção de Dados (ANPD) integram o recorte como camada regulatória transversal, pois um mesmo incidente pode exigir tratamento técnico e comunicação regulatória [17], [18].

A pesquisa limita-se ao desenho publicamente documentado. Não mede a eficácia das equipes, a quantidade de incidentes compartilhados nem o tempo de resposta em tempo real e não presume a inexistência de práticas reservadas ou não publicadas.

A contribuição consiste em reunir atos dispersos, comparar os mecanismos e indicar elementos que possam facilitar a comunicação entre estruturas autônomas.

II. REFERENCIAL TEÓRICO E INSTITUCIONAL

A. Notificação e gestão de incidentes

A resposta a incidentes envolve preparação, detecção, qualificação, contenção, recuperação e aprendizagem. O NIST SP 800-61 Rev. 3 integra essas atividades ao gerenciamento de riscos de cibersegurança e às funções de governar, identificar, proteger, detectar, responder e recuperar [19]. O *CSIRT Services Framework*, do *Forum of Incident Response and Security Teams* (FIRST), inclui, entre os serviços das equipes, o recebimento de reportes, a análise, a coordenação, o apoio à mitigação e o compartilhamento de informações [20].

Neste artigo, *evento* é uma ocorrência observada em um sistema ou em uma rede. *Incidente* é o evento ou conjunto de eventos que compromete ou ameaça ativos, serviços ou

informações e requer tratamento. *Notificação* ou *reporte* é a comunicação formal do incidente a uma equipe, um centro ou uma autoridade. Sua finalidade varia conforme o destinatário: o reporte a um CSIRT busca apoio técnico, correlação e coordenação; a comunicação à ANPD atende à obrigação regulatória; e a divulgação pública relaciona-se à transparência e à orientação dos usuários.

Regras excessivamente vagas dificultam a decisão de reportar, enquanto critérios amplos podem gerar sobrecarga [21]–[23]. Um fluxo funcional precisa esclarecer, ao menos, o gatilho, o destinatário, o conteúdo mínimo, a temporalidade, o canal e o retorno. O gatilho pode decorrer de impacto relevante, de risco de propagação, de dependência compartilhada ou de necessidade de apoio externo. A função do gatilho é reduzir a hesitação sem transformar todo evento local em reporte à rede.

Para permitir a triagem, o conteúdo inicial inclui, em geral, o órgão notificante, a data e a hora, o serviço afetado, uma descrição breve, a gravidade preliminar, os indicadores disponíveis, as medidas já adotadas e o contato técnico. Exigir um relatório completo antes do primeiro aviso pode atrasar a comunicação. Por isso, as recomendações de harmonização e a Diretiva NIS 2 adotam uma lógica de reporte em etapas, com alerta inicial e complementação posterior [24], [25].

O canal precisa autenticar as partes, registrar o envio e limitar o acesso. Quando a mensagem alcança um destinatário inadequado, o roteamento deve permitir seu encaminhamento ao centro competente, sem exposição desnecessária.

Por fim, o retorno informa se o reporte foi recebido, se há necessidade de complemento e se foram identificadas correlações ou medidas adicionais. Esses elementos orientam a análise documental, mas não constituem uma escala de maturidade.

B. Coordenação entre organizações autônomas

Coordenação não significa comando único. Redes interorganizacionais permitem cooperação entre instituições juridicamente autônomas, desde que existam regras, capacidade conjunta e mecanismos de gestão compatíveis com o grau de interdependência [26], [27]. No domínio da segurança da informação, a ISO/IEC 27035-4:2024 trata especificamente da coordenação da gestão de incidentes entre múltiplas organizações [28].

No caso brasileiro, essa autonomia tem fundamento constitucional. Os arts. 2º, 51, IV, 52, XIII, e 96, I, da Constituição Federal preveem a independência entre os Poderes e as competências privativas da Câmara, do Senado e dos tribunais sobre sua organização e funcionamento [29]. Essas disposições afastam a instituição unilateral, pelo Executivo, de um dever de notificação aplicável aos demais Poderes. A cooperação depende, portanto, de instrumento pactuado, como adesão, acordo de cooperação técnica, ato conjunto ou colegiado interinstitucional. Essa condição não impede a interface; apenas condiciona sua forma jurídica.

A literatura sobre reporte obrigatório acrescenta um elemento de incentivo. O envio de informações sobre incidentes envolve custos assimétricos: o custo reputacional recai sobre quem reporta, enquanto o benefício da correlação se distribui pela comunidade [22]. Na ausência de obrigação simétrica e de retorno útil ao notificante, a tendência é o subreporte. Esse ponto ajuda a explicar por que a interface entre comunidades autônomas depende menos da criação de novas estruturas e mais de regras que tornem o reporte previsível e acompanhado de retorno ao notificante.

A coordenação amplia a consciência situacional. Cada órgão observa seus próprios alertas e impactos, enquanto um centro que recebe informações de diferentes fontes pode reconhecer padrões, correlacionar indicadores e alertar instituições ainda não afetadas [30]. Em incidentes que envolvem a cadeia de suprimentos, a nuvem ou produtos amplamente utilizados, essa visão agregada reduz investigações isoladas e favorece a contenção preventiva.

Três funções são particularmente relevantes. O encaminhamento leva o reporte ao destinatário competente, a correlação reúne ocorrências possivelmente relacionadas e o retorno informa ao notificante se a mensagem foi recebida e se há orientação adicional. Para que essas funções operem, são necessários dados suficientes, envio rápido e proteção adequada da informação. O *Traffic Light Protocol* (TLP), por exemplo, auxilia na marcação de limites de distribuição, sem afastar as regras de sigilo e de proteção de dados aplicáveis ao setor público [31].

Relatórios internacionais sobre harmonização apontam dificuldades recorrentes: conceitos divergentes, prazos incompatíveis, formulários duplicados e ausência de retorno ao notificante [24], [32]. O reporte perde valor quando não produz confirmação, orientação ou aprendizagem institucional [23], [33], [34].

C. Mecanismos federais e elementos de comparação

Esta seção apresenta os mecanismos em caráter contextual. A análise categorial de cada um é desenvolvida na Seção IV. No Executivo, a ReGIC organiza a gestão de incidentes e é coordenada pelo CTIR Gov. O PlanGIC detalha procedimentos e critérios de comunicação, enquanto o PPSI estrutura ações de privacidade e de segurança da informação no SISP. No âmbito do programa, o CISC Gov.br coordena operacionalmente as equipes, sem substituir as atribuições do CTIR Gov [5]–[7].

A Política Nacional de Cibersegurança (PNCiber), a Estratégia Nacional de Cibersegurança de 2025 (E-Ciber 2025) e a Política Nacional de Segurança da Informação (PNSI 2025) reforçam objetivos de cooperação e resiliência, mas não criam, isoladamente, um fluxo uniforme entre os três Poderes [35]–[37].

No Judiciário, a Resolução CNJ nº 396/2021 estruturou a rede de cooperação e determinou o reporte ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ), excetuado

o STF [8]. A Portaria CNJ nº 162/2021 aprovou o Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ), o Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCRC-PJ) e o Protocolo de Investigação de Ilícitos Cibernéticos do Poder Judiciário (PIILC-PJ). O mesmo ato aprovou também manuais e glossário técnico [9]. A Portaria CNJ nº 172/2022 criou o CPTRIC-PJ e previu o canal seguro, a troca de informações, alertas e apoio às equipes [10]. O STF mantém processo próprio [11], [12].

No Legislativo, o Senado instituiu a Política Corporativa de Gestão de Incidentes de Segurança da Informação (PCGIS) e a ETIR, com canais internos de notificação e comunicação ao CTIR Gov [13], [14]. A Câmara atualizou a POSIC em 2025, reorganizou o Comitê Gestor de Segurança da Informação e Cibernética (CGSIC), definiu o GRIS-CD e previu representação institucional junto ao CTIR Gov [15].

A LGPD estabelece a obrigação transversal de comunicação à ANPD e, quando cabível, aos titulares, em caso de incidentes com dados pessoais que possam causar risco ou dano relevante [17]. A Resolução CD/ANPD nº 15/2024 fixa o prazo geral de três dias úteis [18]. Esse fluxo não substitui a coordenação técnica, pois nem todo incidente envolve dados pessoais e um mesmo evento pode acionar ambos os fluxos.

Os elementos discutidos nesta seção fundamentam o esquema categorial empregado na comparação, cuja definição operacional e cujas perguntas de análise são formalizadas na Seção III.B e na Tabela II. Em termos gerais, o esquema distingue dimensões voltadas à estrutura e aos limites dos mecanismos daquelas destinadas ao acionamento, à condução da comunicação e à coordenação.

Para os fins deste estudo, mecanismo documentado é o conjunto de atos que organiza a notificação em uma comunidade institucional. Fluxo é a sequência operacional da comunicação. Interface é a ligação formal entre mecanismos. Arquitetura documentada é o conjunto desses mecanismos e de suas conexões públicas. Essa terminologia permite distinguir a organização interna de cada Poder das regras necessárias à comunicação entre eles.

Considera-se interface comum o instrumento público que, simultaneamente, identifica as comunidades conectadas, define o gatilho de transbordo, especifica o conteúdo mínimo do primeiro aviso, fixa orientação temporal, indica canal e regra de roteamento e prevê confirmação de recebimento e retorno ao notificante. A ausência de um ou mais desses elementos caracteriza interface incompleta segundo o parâmetro analítico adotado, sem implicar inexistência de comunicação operacional. Essa definição delimita o objeto verificado e o critério empregado nas afirmações da Seção V.

III. PROCEDIMENTOS METODOLÓGICOS

A. Desenho, recorte e corpus

A pesquisa é qualitativa, aplicada e exploratória-descritiva. Como a pergunta incide sobre o conteúdo formal dos mecanismos, o procedimento principal é a análise documental comparativa, com tratamento categorial adaptado das etapas de pré-análise, exploração e interpretação propostas por Bardin [38]. De Bardin, adotou-se a sequência de etapas, não o tratamento frequencial: não houve contagem de ocorrências nem inferência sobre o emissor, pois o interesse recai sobre o conteúdo prescritivo dos atos.

As categorias foram definidas *a priori*, a partir do referencial, e não emergiram indutivamente do material. A revisão bibliográfica fundamenta os conceitos e a interpretação dos achados, mas não impõe obrigações aos órgãos brasileiros.

O período analisado vai de 1º de janeiro de 2020 a 31 de dezembro de 2025. A E-Ciber 2020 define o marco inicial. O recorte inclui os atos de 2025, exclui documentos de 2026 da classificação e não constitui uma série temporal anual.

A busca documental destinada à composição do *corpus* foi realizada nos portais oficiais da Presidência da República, do Gabinete de Segurança Institucional da Presidência da República, do CTIR Gov, do Governo Digital, do CNJ, do STF, da Câmara dos Deputados, do Senado Federal, da ANPD e do TCU. A busca foi encerrada em 28 de julho de 2026.

Foram incluídos documentos de origem oficial, vigentes ou com efeitos no período e diretamente relacionados à gestão, à notificação ou à coordenação de incidentes. Foram excluídas notícias sem conteúdo normativo, propostas sem vigência, normas estaduais ou municipais e atos sem relação com as categorias de análise. Atos revogados foram utilizados apenas para contextualizar a evolução. O *corpus* é intencional: reúne atos pertinentes às categorias, sem pretensão de exaustividade.

Os documentos submetidos à análise categorial totalizam treze atos, distribuídos conforme a Tabela I.

Registre-se que a padronização de notificação mantida pelo CTIR Gov em seu sítio eletrônico não foi incorporada ao *corpus*, por não constituir ato normativo publicado no período. Essa exclusão deve ser considerada na leitura da categoria conteúdo no mecanismo do Executivo, cuja classificação decorre da remissão feita pelo PlanGIC.

A Constituição Federal e as páginas institucionais do GSI/CTIR Gov, utilizadas exclusivamente para fundamentação jurídica e contextual, também não integram o *corpus* e não tiveram efeito sobre as classificações.

A Tabela I organiza cinco conjuntos. Os quatro primeiros reúnem os atos submetidos à análise categorial. O último reúne políticas, estratégias e auditorias utilizadas para contextualizar a evolução institucional e interpretar os resultados.

Tabela I
CORPUS ANALÍTICO E FONTES CONTEXTUAIS

Conjunto	Documentos centrais
Executivo	Decreto nº 10.748/2021; Portaria DSI/GSI/PR nº 120/2022; e Portaria SGD/MGI nº 852/2023 (PPSI e CISC Gov.br).
Judiciário	Resolução CNJ nº 396/2021; Portaria CNJ nº 162/2021 (PPINC-PJ, PGCRC-PJ e PIILC-PJ); Portaria CNJ nº 172/2022; e Instruções Normativas STF nº 267/2022 e nº 304/2024.
Legislativo	Ato da Comissão Diretora do Senado nº 15/2024 (PCGIS); Ato da Diretoria-Geral do Senado nº 30/2025 (ETIR); e Ato da Mesa da Câmara nº 231/2025 (POSIC, CGSIC e GRIS-CD).
Privacidade Contexto e controle	LGPD e Resolução CD/ANPD nº 15/2024. E-Ciber 2020; Estratégia Nacional de Cibersegurança de 2025; PNCiber; PNSI 2025; Lista de Alto Risco; e Acórdãos do TCU.

A composição do *corpus* mostra que cada caso institucional é composto por atos complementares, e não por um único documento. Decretos e resoluções estabelecem a estrutura geral, enquanto portarias, planos e instruções normativas detalham as responsabilidades e os procedimentos. As fontes de contexto e controle não foram submetidas à codificação categorial. Sua função foi situar os mecanismos e apoiar a discussão dos achados.

No caso do mecanismo CNJ/CPTRIC-PJ, o fluxo comparado foi reconstruído com base na Resolução CNJ nº 396/2021 e nos atos operacionais subsequentes [8]–[10].

B. Categorias e procedimento de análise

Nos casos institucionais, a unidade de análise é o mecanismo documentado de cada comunidade, ainda que formado por mais de um ato; sua abrangência é atributo do próprio mecanismo. O objeto comparado é o fluxo formal reconstruído a partir do conjunto de atos, e não o tipo documental. O fluxo LGPD/ANPD é mantido separadamente como camada regulatória transversal, pois se destina à comunicação regulatória, e não à coordenação técnica entre equipes.

As unidades comparadas são assimétricas: o Executivo é tratado como mecanismo único; o Judiciário, como dois mecanismos, devido à exclusão do STF da rede do CPTRIC-PJ; e o Legislativo, como dois mecanismos, porque os atos não instituem estrutura comum às Casas. A leitura das matrizes deve considerar essa assimetria institucional.

A unidade de contexto é o documento e sua função no mecanismo institucional. A unidade de registro corresponde ao artigo, item, seção ou trecho operacional que contém evidência de uma ou mais categorias. Como a mesma disposição pode indicar simultaneamente o responsável, o destinatário e a abrangência, os registros puderam ser associados a mais de uma categoria de análise.

Cada registro foi associado ao órgão emissor, documento, data, vigência, dispositivo e síntese da evidência. A Tabela II reúne as seis categorias e as perguntas que orientaram a identificação das evidências.

Tabela II
CATEGORIAS E PERGUNTAS DE ANÁLISE

Categoria	Pergunta de análise
Responsável	Quem comunica ou gerencia o incidente?
Destinatário	Qual equipe, centro ou autoridade recebe a informação?
Abrangência institucional	Quais órgãos ou entidades estão submetidos ao mecanismo?
Abrangência material	Quais incidentes são tratados?
Critérios, conteúdo e prazo	Há gatilho, conteúdo mínimo e orientação temporal?
Coordenação intrapoder e interpoderes	Intrapoder: há uma rede ou um centro que articule órgãos ou instituições distintos pertencentes ao mesmo Poder? Interpoderes: há encaminhamento, cooperação ou retorno com o centro, a equipe ou a autoridade vinculada a outro Poder?

A grade distingue três funções analíticas. Responsável, destinatário e abrangências descrevem a estrutura e os limites do mecanismo. A categoria *critérios, conteúdo e prazo* examina o acionamento e a condução da comunicação. A categoria *coordenação intrapoder e interpoderes*, por suas duas subdimensões, examina a articulação com as estruturas do mesmo Poder e de outros Poderes. Essa separação permite comparar os fluxos sem convertê-los em um índice de maturidade.

Na consolidação das matrizes comparativas, cada elemento foi classificado em uma de quatro situações: previsto (P), parcialmente previsto (PP), não identificado (NI) e não aplicável (NA). “Previsto” exige disposição expressa e suficiente para identificar o elemento. “Parcialmente previsto” indica previsão sem detalhamento suficiente. “Não identificado” indica ausência de evidência no *corpus*, sem afirmar inexistência institucional. “Não aplicável” indica categoria incompatível com a finalidade do mecanismo.

Duas ressalvas orientam a leitura dessas classificações. P, PP e NI registram grau de explicitação documental, não maturidade ou desempenho. A classificação também não avalia a calibragem: um gatilho que determine o relato de qualquer suspeita pode ser explícito e, ainda assim, não estabelecer limiar de transbordo.

Cabe delimitar a correspondência entre o parâmetro da Seção II.A e a grade da Tabela II. Foram codificados, em cada mecanismo, o responsável, o destinatário, as abrangências, o gatilho, o conteúdo, o prazo e a coordenação.

O canal, o roteamento e a confirmação de recebimento não foram codificados como categorias autônomas porque seu detalhamento operacional completo, em regra, depende de instrumentos externos aos atos codificados. Quando o texto se refere a esses três elementos, a afirmação diz respeito à ausência de instrumento comum que os organize entre os Poderes, e não à classificação atribuída a cada mecanismo.

As classificações são independentes: a previsão de relação

com a estrutura de outro Poder em um mecanismo não implica previsão recíproca nos atos do mecanismo correspondente.

A exploração ocorreu em três movimentos: leitura integral e extração dos trechos operacionais; codificação dos registros por categorias e subdimensões; e revisão dos casos duvidosos na fonte antes da consolidação das matrizes.

A mera criação de uma equipe não foi considerada prova do dever de notificar. Da mesma forma, a referência técnica ao CTIR Gov não foi considerada obrigação de encaminhamento, e a menção genérica à cooperação não foi classificada como protocolo completo.

Para reconhecer a coordenação intrapoder, exigiu-se a existência de uma estrutura de rede ou de um centro que articulasse órgãos ou instituições distintos pertencentes ao mesmo Poder.

Para reconhecer a coordenação interpoderes, exigiu-se um destinatário vinculado a outro Poder, vínculo institucional formal ou dever de encaminhamento. Nos casos duvidosos, prevaleceram a leitura integral, a interpretação conservadora e a conferência da fonte. A subdimensão reúne modalidades distintas — dever de comunicação, vínculo formal e retorno —, identificadas na Tabela IV.

Nos mecanismos de uma única instituição, como o STF, o Senado e a Câmara, a coordenação intrapoder foi classificada como NI, pois a articulação com órgãos congêneres é conceitualmente possível e sua ausência nos atos é informativa.

Os atos normativos vigentes receberam prioridade. Planos, protocolos e manuais oficiais foram considerados ao detalhar a operação. Páginas institucionais serviram para localizar documentos ou esclarecer a estrutura, enquanto artigos e referências internacionais fundamentaram conceitos, sem atribuir deveres aos órgãos brasileiros. Quando dois atos abordavam o mesmo ponto, o documento mais recente e específico orientou a classificação.

O tratamento produziu perfis descritivos e matrizes comparativas. A interpretação manteve separadas a coordenação técnica entre equipes e a comunicação regulatória dirigida à ANPD.

Os elementos de referência foram definidos a partir do referencial internacional de reporte [20], [24], [25], [32] e relacionados às lacunas recorrentes observadas no *corpus*; não emergiram indutivamente do material. Funcionam como parâmetro analítico, sem constituir escala de maturidade; a contribuição empírica está no mapeamento de sua explicitação nos mecanismos brasileiros.

C. Limitações

A análise alcança o desenho formal, não a rotina real. A ausência de previsão pública não prova a inexistência de contatos informais, acordos reservados ou procedimentos internos. Também não é possível inferir, apenas pelos atos, a frequência dos reportes, o tempo efetivo de resposta ou a qualidade da cooperação.

Parte do arranjo pode legitimamente não ser pública. O Decreto nº 10.748/2021 restringe o acesso a informações específicas sobre incidentes e características técnicas dos ativos [5]. Por isso, o estudo não mede a coordenação real, mas a verificabilidade pública de seu desenho, dimensão relevante para o controle externo e para a previsibilidade do órgão notificante.

A codificação foi manual e não foi calculada uma medida de concordância. Além disso, não foram registrados, de forma padronizada, todos os termos de busca nem o fluxo numérico de seleção, o que limita a replicação estrita. A documentação preservada permitiu conferir as fontes incluídas, os dispositivos e a lógica das classificações, mas não reproduzir integralmente a recuperação inicial. Essas limitações recomendam que os resultados sejam lidos como descrição comparativa da arquitetura pública documentada.

IV. RESULTADOS

A. Poder Executivo

A E-Ciber 2020 tratou a coordenação como tema estratégico, mas não definiu sozinho o fluxo de notificação [1]. O Decreto nº 10.748/2021 instituiu a ReGIC, atribuiu sua coordenação ao CTIR Gov e definiu os participantes e as hipóteses de comunicação [5]. O desenho alcança o Executivo Federal e permite a participação de instituições externas nas condições previstas no decreto, sem estender automaticamente a rede aos demais Poderes.

O PlanGIC detalha a prevenção, o tratamento, a resposta e a comunicação [6]. Entre os gatilhos expressos estão incidentes com possível perda de vidas, impacto em infraestruturas críticas ou em serviços digitais de governo, vazamento de dados e exploração potencial em larga escala. O plano também prevê colaboração e compartilhamento de informações. As notificações seguem a padronização do CTIR Gov, sem campos mínimos gerais explicitados no próprio PlanGIC. A orientação temporal é qualitativa: maior brevidade possível, sem prazo numérico geral.

No SISP, a Portaria SGD/MGI nº 852/2023 instituiu o Programa de Privacidade e Segurança da Informação (PPSI) e estabeleceu, entre suas iniciativas, o CISC Gov.br como unidade de coordenação operacional das equipes de prevenção, tratamento e resposta [7]. O centro atua como equipe principal para os serviços da Plataforma Gov.br e para outros serviços sob responsabilidade da Secretaria de Governo Digital. Os órgãos e entidades devem notificar os incidentes identificados ao centro e integrar-se aos padrões, tecnologias, procedimentos e processos estabelecidos. A portaria preserva as atribuições do CTIR Gov e das coordenações setoriais da ReGIC, evitando sobreposição formal entre os centros.

A PNCiber e os instrumentos nacionais de 2025 reforçam integração, cooperação e resiliência, mas permanecem programáticos quanto à interface entre os Poderes [35]–[37]. A PNCiber explicita como objetivo ampliar a atuação coordenada e o intercâmbio de informações entre Executivo,

Legislativo e Judiciário, embora o Comitê Nacional de Cibersegurança não reserve assentos ao Judiciário ou ao Legislativo, admitindo sua participação por convite, sem voto [35].

No mecanismo do Executivo, ReGIC, CTIR Gov, PlanGIC, PPSI e CISC Gov.br estruturam a coordenação intrapoder. Para outros Poderes, o Decreto nº 10.748/2021 prevê vinculação mediante convite e adesão formal; após a adesão, a entidade reporta à coordenação setorial ou ao CTIR Gov nas hipóteses previstas [5]. Trata-se de rota individual e facultativa, não de interface entre os mecanismos de coordenação de cada Poder; por isso, a coordenação interpoderes é classificada como PP.

B. Poder Judiciário

A Resolução CNJ nº 396/2021 instituiu a estratégia de segurança da informação e cibernética do Judiciário, criou uma rede de cooperação e determinou que os órgãos abrangidos reportassem incidentes ao CPTRIC-PJ, exceto o STF [8]. A Portaria CNJ nº 162/2021 aprovou o PPINC-PJ, o PGCRC-PJ e o PIILC-PJ, além de manuais e glossário técnico vinculados à estratégia [9]. A Portaria CNJ nº 172/2022 criou o centro, integrou as equipes à rede e previu o canal seguro, a troca de informações, alertas, apoio e a consolidação de dados [10].

No mecanismo CNJ/CPTRIC-PJ, responsável, destinatário e abrangência institucional estão definidos. O CPTRIC-PJ deve estabelecer canal seguro, apoiar as equipes, divulgar alertas e consolidar informações e estatísticas. O PGCRC-PJ determina a comunicação dos incidentes graves ao CPTRIC-PJ, e os protocolos definem critérios de gravidade e conteúdos para situações específicas. A orientação temporal é qualitativa, com comunicação imediata ou tempestiva nas hipóteses aplicáveis, sem prazo numérico geral. A coordenação intrapoder está formalizada pela rede do CPTRIC-PJ. A Resolução nº 396/2021 prevê troca de informações e parcerias com outros Poderes, sem fluxo comum de reporte [8].

O STF mantém processo autônomo. A Instrução Normativa nº 267/2022 instituiu o processo de gestão de incidentes, e a Instrução Normativa nº 304/2024 o atualizou, atribuindo à Coordenadoria de Segurança Cibernética o recebimento, a análise, a classificação, o tratamento e o reporte dos incidentes [11], [12]. A norma de 2024 formalizou o registro do incidente reportado, a triagem e a severidade, além das comunicações relacionadas à proteção de dados.

No fluxo técnico, a norma prevê registro de informações relevantes e procedimentos por tipo de incidente, mas não conteúdo mínimo nem limiar geral de reporte. Nos incidentes com risco ou dano relevante aos titulares, o Comitê Executivo de Proteção de Dados e o encarregado devem ser informados prontamente. Esse gatilho e essa orientação temporal são específicos do subfluxo de proteção de dados, sem equivalentes gerais identificados no fluxo técnico.

A Instrução Normativa nº 304/2024 também adota recomendações do CTIR Gov para uniformizar os tipos de incidentes. Essa referência favorece a compatibilidade técnica, mas não estabelece destinatário externo nem dever geral de envio. Assim, no Judiciário, a cooperação intrapoder está formalizada na rede coordenada pelo CNJ, enquanto o STF mantém processo separado. A interface interpoderes permanece menos detalhada.

C. Poder Legislativo

O Senado instituiu a Política Corporativa de Gestão de Incidentes de Segurança da Informação (PCGIS) em 2024 [13]. O ato distribui responsabilidades, estabelece canais e relaciona a gestão de incidentes à continuidade e à proteção dos ativos. Em 2025, o Ato da Diretoria-Geral nº 30 criou a ETIR, responsável pelo tratamento dos casos e orientada por padrões do CTIR Gov [14].

As notificações podem ser recebidas por formulário na intranet ou pelo endereço eletrônico da equipe, e a comunicação externa cabe ao Diretor do Prodasen. A PCGIS determina que colaboradores internos, externos e unidades administrativas relatem qualquer suspeita de evento ou incidente e admite solicitar informações adicionais, sem explicitar conteúdo mínimo completo ou orientação temporal geral. A ligação com o CTIR Gov é expressa. Não foi identificada articulação formal com a Câmara.

Registre-se que o Senado é o único mecanismo examinado cuja unidade de reporte é o evento, e não o incidente, o que amplia o volume potencial de comunicações internas sem estabelecer limiar de transbordo.

A Câmara atualizou sua Política de Segurança da Informação e Cibernética (POSIC) no fim de 2025 [15]. O ato reorganizou o CGSIC, definiu o GRIS-CD em modelo combinado ou misto, estabeleceu o reporte interno ao grupo e previu representante institucional junto ao CTIR Gov. A POSIC atribui ao GRIS-CD a gestão dos incidentes de segurança cibernética, enquanto critérios, campos e prazos dependem parcialmente de plano posterior. Tampouco foi identificada articulação formal com o Senado. Editada em dezembro de 2025, a norma encerra o período com estrutura renovada, ainda sem todos os instrumentos complementares previstos.

Senado e Câmara convergem na existência de estruturas formais, pontos focais e relação com o CTIR Gov, mas estão em diferentes estágios de detalhamento. O Senado já identifica canais internos; a Câmara, cuja POSIC foi editada ao fim de 2025, depende parcialmente do plano posterior previsto no ato.

D. LGPD e ANPD

A LGPD obriga o controlador a comunicar os incidentes que possam causar risco ou dano relevante à ANPD e, quando cabível, aos titulares [17]. A Resolução CD/ANPD nº 15/2024 define fatores de avaliação, conteúdo e prazo geral de três dias úteis, contados a partir do conhecimento de que o incidente afetou dados pessoais [18].

Esse fluxo regulatório possui responsável, destinatário, gatilho, conteúdo e prazo claramente definidos. A comunicação deve informar, entre outros elementos, a natureza e as categorias dos dados, o número estimado de titulares e de registros, os riscos envolvidos, as medidas de segurança e de mitigação e os dados do encarregado.

A abrangência institucional do fluxo é transversal, mas sua abrangência material é específica. Desse modo, ataques que comprometam apenas a disponibilidade ou a integridade, sem afetar dados pessoais ou sem atingir o limiar regulatório, podem não acionar a ANPD e, ainda assim, demandar coordenação técnica. A ANPD não atua como centro geral de correlação de ataques contra serviços públicos. Por isso, a comunicação regulatória complementa os fluxos técnicos sem substituí-los.

E. Comparação dos mecanismos

A comparação foi organizada em duas matrizes complementares, correspondentes a tarefas analíticas distintas: primeiro, reconhecer a estrutura e o alcance de cada mecanismo ou fluxo; depois, comparar como a comunicação é acionada e conduzida.

A Tabela III apresenta as categorias estruturais e identifica, em cada mecanismo ou fluxo, quem atua, quem recebe o reporte e quais instituições e incidentes estão abrangidos. Nos documentos examinados, esses quatro elementos são identificáveis em todos os mecanismos e no fluxo regulatório. Por não discriminarem entre os casos, não recebem classificação, e a matriz é apresentada em forma descritiva.

Tabela III
CATEGORIAS ESTRUTURAIS: PERFIL DESCRITIVO DOS MECANISMOS E DO FLUXO REGULATÓRIO

Mecanismo/ fluxo	Responsável	Destinatário	Abrangência institucional	Abrangência material
Executivo	equipes da ReGIC e órgãos do SISP	CTIR Gov ou CISC Gov.br, no âmbito do PPSI	Executivo, SISP e participantes externos previstos na ReGIC	incidentes e vulnerabilidades previstos nos atos
CNJ/ CPTRIC-PJ	órgãos e equipes abrangidos	CPTRIC-PJ	Poder Judiciário, exceto STF	incidentes abrangidos pela estratégia e pelos protocolos
STF	Coordenadoria de Segurança Cibernética	Coordenadoria de Segurança Cibernética	Supremo Tribunal Federal	ativos, serviços e informações do STF
Senado	ETIR do Senado e Diretor do Prodasen	ETIR do Senado e CTIR Gov	Senado Federal	incidentes abrangidos pelos atos internos
Câmara	usuários e GRIS-CD	GRIS-CD	Câmara dos Deputados	incidentes de segurança cibernética
LGPD/ ANPD	controlador	ANPD e, quando cabível, titulares	três Poderes quando sujeitos à LGPD	dados pessoais com risco ou dano relevante

Definidos os atores e os limites de aplicação, a análise passa à forma como o reporte é acionado e conduzido. A Tabela IV reúne gatilho, conteúdo, prazo e, em colunas distintas, coordenação intrapoder e coordenação interpoderes, mantendo separada a comunicação regulatória à ANPD.

Na leitura da matriz, P, PP e NI expressam apenas o grau de explicitação documental de cada elemento, enquanto NA indica que a categoria não se aplica à finalidade do

mecanismo ou fluxo. As classificações devem ser lidas de forma independente, conforme os critérios da Seção III.B. Nas colunas de gatilho, conteúdo e prazo, elas avaliam a explicitação de cada elemento no fluxo correspondente, sem pressupor equivalência funcional. A padronização comum entre os Poderes é tratada separadamente na interpretação comparativa.

Tabela IV
CATEGORIAS OPERACIONAIS E COORDENAÇÃO INTRAPODER E INTERPODERES

Mecanismo/ fluxo	Gatilho	Conteúdo	Prazo	Coordenação intrapoder	Coordenação interpoderes
Executivo	P impactos definidos e incidentes identificados no SISP	PP padronização remetida ao CTIR Gov; sem campos mínimos no PlanGIC	PP comunicação imediata no decreto da ReGIC e maior brevidade possível no PlanGIC; sem prazo numérico geral	P ReGIC e CISC Gov.br, no âmbito do PPSI, articulam o SISP	PP adesão facultativa aberta a órgãos de outros Poderes, com reporte ao CTIR Gov após a adesão; sem interface entre mecanismos
CNJ/ CPTRIC-PJ	P incidentes graves devem ser comunicados ao CPTRIC-PJ	PP conteúdo detalhado apenas para situações específicas	PP imediato/tempestivo nas hipóteses aplicáveis; sem prazo numérico	P rede de cooperação do Judiciário, exceto STF	PP cooperação prevista: troca de informações e parcerias com outros Poderes; sem fluxo comum de reporte
STF	PP risco/dano a titulares aciona comunicação específica; sem limiar geral técnico	PP informações relevantes por tipo; sem conteúdo mínimo geral	PP prontamente no subfluxo de proteção de dados; sem prazo geral técnico	NI processo autônomo, sem participação identificada na rede do CPTRIC-PJ	NI referência técnica: adoção de recomendações do CTIR Gov sem dever geral de envio
Senado	P qualquer suspeita de evento ou incidente deve ser relatada; sem limiar de transbordo	PP formulário e complementação; sem conteúdo mínimo completo	NI sem orientação temporal geral identificada	NI sem articulação formal identificada com a Câmara	P dever de comunicação: comunicação expressa ao CTIR Gov
Câmara	PP depende de plano posterior	PP depende de plano posterior	PP depende de plano posterior	NI sem articulação formal identificada com o Senado	P vínculo institucional: representação expressa junto ao CTIR Gov
LGPD/ ANPD	P risco ou dano relevante	P conteúdo regulamentado	P três dias úteis	NA fluxo regulatório, não coordenação técnica	NA fluxo regulatório, não coordenação técnica

Nas categorias estruturais, responsáveis, destinatários e limites institucionais e materiais são identificáveis em todos os casos; por isso, a Tabela III é descritiva. A assimetria decorre do alcance de cada arranjo: os mecanismos técnicos cobrem ativos, serviços e informações de suas comunidades, enquanto o fluxo da ANPD se restringe a dados pessoais com risco ou dano relevante. Na Câmara, o plano posterior afeta dimensões operacionais, não a abrangência material geral.

Nas categorias operacionais, concentram-se as diferenças. Executivo e CNJ/CPTRIC-PJ apresentam gatilhos

expressos, com conteúdo e prazo parciais. No STF, os três elementos são parciais. No Senado, o gatilho é expresso, o conteúdo é parcial e não há orientação temporal geral identificada. Na Câmara, os três dependem parcialmente de plano posterior. A ANPD define gatilho, conteúdo e prazo para a finalidade regulatória.

Senado e Câmara formalizam ligação com o CTIR Gov; o STF adota referência técnica sem dever geral de envio; o Executivo prevê adesão de órgãos de outros Poderes; e o CNJ/CPTRIC-PJ prevê troca de informações e parcerias.

Nenhum dos cinco mecanismos técnicos explicita o

conteúdo mínimo do primeiro reporte nos atos normativos examinados, ao contrário do fluxo regulatório. As cinco classificações PP na coluna Conteúdo registram previsão de conteúdo sem especificação de campos mínimos, e não ausência de qualquer previsão. Essa ausência de especificação, portanto, não pode ser atribuída, com base neste estudo, a impedimento jurídico.

As matrizes indicam que a lacuna não está na ausência de centros ou destinatários. O que não foi identificado, no *corpus*, é uma interface compartilhada que reúna gatilho, conteúdo mínimo e prazo e que os articule ao roteamento, à confirmação e ao retorno nos incidentes que ultrapassem a comunidade de origem. As classificações registram apenas explicitação documental, não *ranking*.

V. DISCUSSÃO

A. Padrões da arquitetura documentada

A comparação revela três padrões. O primeiro é a *coordenação intrapoder*. A ReGIC e, no âmbito do PPSI, o CISC Gov.br organizam participantes do Executivo, enquanto o CPTRIC-PJ conecta as equipes do Judiciário abrangido. No Executivo, os atos do mecanismo preveem rota de adesão aberta a órgãos de outros Poderes, mas não interface entre as estruturas de coordenação de cada Poder. No CNJ/CPTRIC-PJ, os atos preveem troca de informações e parcerias com outros Poderes, sem fluxo comum de reporte.

O segundo padrão é a *interface interpoderes com o CTIR Gov*. Ela aparece, de modo expresso, nos atos do Senado e da Câmara. No STF, a relação limita-se à adoção de referências técnicas. Essas conexões possuem alcances distintos e não são equivalentes quanto ao gatilho, ao destinatário e ao dever de envio.

O terceiro padrão é a *camada regulatória transversal*. A ANPD recebe comunicações dos controladores sujeitos à LGPD quando o incidente envolve dados pessoais e risco ou dano relevante. O mesmo evento pode exigir tratamento pela equipe técnica, comunicação ao centro de coordenação e notificação à ANPD. Os fluxos devem permanecer distinguíveis. A equipe técnica procura conter, erradicar e correlacionar a ameaça. O controlador avalia o risco aos titulares e cumpre a obrigação regulatória. A integração é necessária para evitar atrasos e duplicidades, mas não transforma a ANPD em um centro operacional de resposta.

O resultado central não é a ausência de coordenação. Existem redes internas e conexões formais. A limitação está no fato de não ter sido identificado, no *corpus*, um protocolo público comum que organize incidentes de interesse simultâneo dos três Poderes. Essa conclusão é compatível com a literatura sobre governança em rede: instituições autônomas podem cooperar sem uma hierarquia única, mas dependem de regras de interface e de capacidades compartilhadas [26]–[28].

À luz de Provan e Kenis, os arranjos da ReGIC e da rede coordenada pelo CPTRIC-PJ aproximam-se do

modelo de organização líder, com um centro coordenando participantes formalmente autônomos [26]. Senado e Câmara permanecem sem rede comum. No plano interpoderes, observam-se conexões bilaterais com um nó do Executivo, não uma rede dotada de regras próprias. Como a literatura associa esse modelo a consenso de objetivos e legitimidade do nó coordenador [26], [27], tais condições entre Poderes autônomos dependeriam de pactuação.

Uma evidência contextual externa ao *corpus* normativo reforça essa leitura. Na relação TLP:CLEAR publicada pelo GSI, o CNJ, o Senado Federal, o STF e o TCU constam entre os órgãos aderidos à ReGIC. O CNJ figura também entre os órgãos setoriais, enquanto o STF e o TCU reaparecem na relação de órgãos convidados [39]. A sobreposição das categorias na própria página recomenda cautela na interpretação do *status* institucional de cada participante e evidencia participação formal de instituições de diferentes Poderes, sem demonstrar uso operacional do fluxo em incidentes concretos.

Esse dado é compatível com a classificação PP do Executivo: há rotas individuais de vinculação à ReGIC, mas não protocolo comum entre os mecanismos de coordenação dos Poderes. Por não ser ato normativo, a lista não integrou a codificação.

Também como evidência contextual, as orientações do CTIR Gov especificam conteúdo da notificação, uso de TLP, notificação inicial tempestiva seguida de complementação, canal de envio, confirmação de recebimento e número de identificação do caso [40]. Esses elementos demonstram viabilidade técnica e presença de práticas documentadas no fluxo do Executivo. O que não foi identificado no *corpus* é previsão normativa que lhes confira alcance comum às demais comunidades de Poder; sua aplicação externa depende da vinculação ao fluxo da ReGIC.

Responsável e destinatário são identificados em todos os fluxos; a dificuldade surge quando a informação interessa a mais de uma comunidade, pois não há, no *corpus*, regra comum para envio direto, remessa pelo centro de origem ou comunicação simultânea.

A abrangência institucional permanece fragmentada, de forma coerente com a autonomia dos Poderes. A abrangência material também varia: os mecanismos técnicos cobrem ativos, redes, serviços e informações, enquanto o fluxo da ANPD exige dados pessoais afetados e risco ou dano relevante. O mesmo evento pode acionar ambos os campos.

Nas categorias operacionais, a maior diversidade está nos critérios, no conteúdo, no prazo e na coordenação interpoderes. Não foram identificados formulário ou prazo comuns para a comunicação entre Poderes, e as modalidades variam entre dever de comunicação, representação institucional, referência técnica e cooperação. Contato formal, porém, não garante roteamento, confirmação ou retorno. Esse quadro é semelhante aos problemas de harmonização descritos pelo *Department of*

Homeland Security e pelo *Financial Stability Board* [24], [32].

Também é preciso distinguir explicitação de calibragem: o Senado, por exemplo, possui gatilho expresso para qualquer suspeita, mas sem limiar de transbordo. No *corpus*, gatilhos calibrados por impacto não se dirigem necessariamente a outro Poder, enquanto vínculos interpoderes dependem de adesão prévia ou não definem o gatilho. Essa fragmentação reforça o interesse em soluções pactuadas de interface.

A assimetria também reflete momentos distintos de formalização: a ReGIC e o mecanismo coordenado pelo CNJ acumulam instrumentos desde 2021, enquanto os atos do Legislativo são de 2024 e 2025. O menor detalhamento da Câmara, cuja POSIC foi editada ao fim do período, não deve ser lido isoladamente como deficiência consolidada.

No contexto de fornecedores, serviços e produtos compartilhados, a coordenação amplia a correlação e o alerta a órgãos ainda não afetados [30]. O valor do reporte, contudo, depende de confirmação, orientação e aprendizagem [23], [33], [34], elementos não identificados de forma uniforme entre os Poderes.

As auditorias do TCU reforçam a relevância do problema de articulação, embora não mensurem diretamente a coordenação entre os Poderes. A Lista de Alto Risco apontou o alcance restrito das políticas do Executivo e a ausência de organização oficial voltada ao nível de maturidade do país como um todo [2]. Os Acórdãos nº 2.430/2024 e nº 2.387/2024 registraram, respectivamente, a ausência de órgão que reunisse informações do restante do setor público e a baixa maturidade em parcela relevante do SISP [3], [4]. Goldoni, Rodrigues e Medeiros também descrevem avanços e desafios na articulação da governança nacional de cibersegurança [16].

Esses achados não demonstram falha operacional. O que a análise permite afirmar é que, nas regras públicas examinadas, não foi identificada uma interface comum completa e verificável para incidentes que atravessem os três Poderes.

B. Elementos de referência para uma interface comum

Uma interface comum não exige centralizar a defesa cibernética; basta definir quando e como um mecanismo informa outro, preservando as competências de cada Poder. A independência dos Poderes e as competências privativas de suas estruturas administrativas, nos termos dos arts. 2º, 51, IV, 52, XIII, e 96, I, da Constituição Federal [29], afastam a imposição unilateral desse dever. Assim, os elementos propostos devem integrar instrumento pactuado entre os mecanismos existentes, e não norma de um Poder sobre os demais.

Os mecanismos existentes já oferecem pontos de apoio. No Executivo, o CTIR Gov coordena a ReGIC, enquanto o PPSI organiza iniciativas no SISP, entre elas a atuação do CISC Gov.br. No Judiciário, o CPTRIC-PJ mantém rede e canal seguros, e o STF utiliza referências técnicas

compatíveis. Senado e Câmara, por sua vez, mantêm relações formais com o CTIR Gov. A interface seria especialmente útil em incidentes envolvendo fornecedor comum, serviço interconectado, vulnerabilidade crítica amplamente explorada ou indicadores de campanha distribuída.

A Tabela V sintetiza os elementos de referência utilizados na análise das lacunas documentais. Eles constituem uma referência inicial, não um modelo de implementação validado.

Tabela V
ELEMENTOS DE REFERÊNCIA DERIVADOS DA ANÁLISE

Elemento	Finalidade
Gatilho comum	Definir quando um incidente deve ultrapassar a comunidade de origem, com base na propagação, na dependência compartilhada ou na necessidade de apoio.
Conteúdo mínimo	Permitir triagem rápida sem exigir um relatório completo no primeiro envio.
Prazo em etapas	Separar o alerta inicial, a atualização e o encerramento.
Canal e roteamento	Autenticar as partes, registrar o envio e encaminhar o caso ao centro competente.
Confirmação e retorno	Informar recebimento, solicitar complemento e devolver orientações ou correlações.
Proteção da informação	Compatibilizar o compartilhamento técnico, o sigilo, a minimização de dados pessoais e os limites de distribuição.

Os elementos formam um ciclo: o gatilho aciona o fluxo; conteúdo, prazo e canal tornam o reporte utilizável; roteamento, confirmação e retorno mantêm a circulação; e a proteção da informação limita sua distribuição. A falta de qualquer desses componentes reduz a verificabilidade da interface.

Um instrumento interinstitucional poderia conectar os centros existentes sem criar nova estrutura administrativa. O primeiro aviso conteria campos essenciais. As atualizações agregariam evidências e medidas adotadas. O receptor confirmaria o recebimento, correlacionaria o caso e o encaminharia quando necessário.

Sigilo, necessidade de conhecimento, minimização de dados pessoais e marcação de distribuição devem limitar o compartilhamento. A validação desse desenho dependeria de exercícios conjuntos, entrevistas e casos reais, evidências que esta pesquisa documental não produz.

VI. CONCLUSÃO

O estudo analisou como documentos oficiais dos Poderes Executivo, Legislativo e Judiciário Federais disciplinaram, entre 2020 e 2025, a notificação e a coordenação de incidentes cibernéticos.

Os resultados mostram mecanismos internos formalizados, porém assimétricos. O Executivo dispõe da ReGIC, do CTIR Gov, do PlanGIC e do PPSI, no âmbito do qual atua o CISC Gov.br. No Judiciário, o CNJ organiza a rede, os protocolos PPINC-PJ, PGCRC-PJ e PIILC-PJ, e o CPTRIC-PJ, enquanto o STF mantém um

processo autônomo, atualizado em 2024. No Legislativo, o Senado encerra o período com a PCGIS e a ETIR, e a Câmara com a POSIC, o CGSIC e o GRIS-CD. Ambas as Casas apresentam interfaces formais com o CTIR Gov, em níveis distintos de detalhamento.

A LGPD e a regulamentação da ANPD estabelecem uma obrigação transversal para determinados incidentes envolvendo dados pessoais, mas não substituem a coordenação técnica.

Entre os elementos operacionais, o conteúdo mínimo do primeiro reporte é o menos explicitado nos atos normativos: nenhum dos mecanismos técnicos o define, e apenas o fluxo regulatório o estabelece.

A comparação identificou coordenação intrapoder formalizada no Executivo e na rede do Judiciário, coordenada pelo CNJ; conexões interpoderes seletivas no CNJ; conexões do Legislativo com o CTIR Gov; e comunicação regulatória à ANPD. No Executivo, a relação com outros Poderes ocorre por rota individual de vinculação, dependente de convite e formalização. No *corpus* examinado, não foi identificado protocolo público comum aos três Poderes que reúna gatilho, conteúdo mínimo e prazo comuns e que os articule ao roteamento, à confirmação e ao retorno.

A contribuição do artigo consiste em organizar os mecanismos, comparar seus elementos e indicar elementos de referência para uma interface entre estruturas autônomas. Esses elementos não pressupõem um centro único nem a transferência de competências e destinam-se a facilitar a comunicação em incidentes de interesse compartilhado.

A pesquisa limita-se aos documentos públicos e não avalia práticas reservadas, desempenho ou efetividade. Estudos futuros podem combinar entrevistas, registros de protocolo e exercícios conjuntos, além de atualizar o diagnóstico após os planos decorrentes dos atos de 2025. Consulta formal aos centros sobre protocolos interpoderes não publicados permitiria distinguir a ausência de previsão da ausência de publicidade.

REFERÊNCIAS

- [1] Brasil, Decreto nº 10.222, de 5 de fevereiro de 2020, “Aprova a Estratégia Nacional de Segurança Cibernética.” [Online]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm. Acesso em: 28 jul. 2026.
- [2] Tribunal de Contas da União, *Lista de Alto Risco na Administração Pública Federal*, 2ª edição, dez. 2024, tema “Segurança da Informação e Segurança Cibernética”. [Online]. Disponível em: https://sites.tcu.gov.br/listadealtorisco/seguranca_da_informacao_e_seguranca_cibernetica.html. Acesso em: 28 jul. 2026.
- [3] Tribunal de Contas da União, Acórdão nº 2.430/2024–Plenário, TC 010.387/2024-2, Rel. Min. Benjamin Zymler, sessão de 13 de novembro de 2024. [Online]. Disponível em: <https://pesquisa.apps.tcu.gov.br/redireciona/acordao-completo/ACORDAO-COMPLETO-2682822>. Acesso em: 28 jul. 2026.
- [4] Tribunal de Contas da União, Acórdão nº 2.387/2024–Plenário, TC 010.390/2024-3, Relator Min. Augusto Nardes, 2024. [Online]. Disponível em: <https://pesquisa.apps.tcu.gov.br/redireciona/a>
- cordao-completo/ACORDAO-COMPLETO-2686174. Acesso em: 28 jul. 2026.
- [5] Brasil, Decreto nº 10.748, de 16 de julho de 2021, “Institui a Rede Federal de Gestão de Incidentes Cibernéticos.” [Online]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/d10748.htm. Acesso em: 28 jul. 2026.
- [6] Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República, Portaria DSI/GSI/PR nº 120, de 21 de dezembro de 2022, *Plano de Gestão de Incidentes Cibernéticos para a Administração Pública Federal*. [Online]. Disponível em: <https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/plano-de-gestao-de-incidentes-ciberneticos-plangic/plangic.pdf>. Acesso em: 28 jul. 2026.
- [7] Ministério da Gestão e da Inovação em Serviços Públicos, Portaria SGD/MGI nº 852, de 28 de março de 2023, “Dispõe sobre o Programa de Privacidade e Segurança da Informação.” [Online]. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-852-de-28-de-marco-de-2023-473750908>. Acesso em: 28 jul. 2026.
- [8] Conselho Nacional de Justiça, Resolução nº 396, de 7 de junho de 2021, “Institui a Estratégia Nacional de Segurança da Informação e Cibernética do Poder Judiciário.” [Online]. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/3975>. Acesso em: 28 jul. 2026.
- [9] Conselho Nacional de Justiça, Portaria nº 162, de 10 de junho de 2021, “Aprova protocolos e manuais criados pela Resolução CNJ nº 396/2021.” [Online]. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/3982>. Acesso em: 28 jul. 2026.
- [10] Conselho Nacional de Justiça, Portaria nº 172, de 25 de maio de 2022, “Institui o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ).” [Online]. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/4559>. Acesso em: 28 jul. 2026.
- [11] Supremo Tribunal Federal, Instrução Normativa nº 267, de 12 de maio de 2022, “Institui o Processo de Gestão de Incidentes de Segurança da Informação do STF.” [Online]. Disponível em: <https://www.stf.jus.br/arquivo/norma/instrucao/norma267-2022.pdf>. Acesso em: 28 jul. 2026.
- [12] Supremo Tribunal Federal, Instrução Normativa nº 304, de 9 de julho de 2024, “Altera a Instrução Normativa nº 267/2022.” [Online]. Disponível em: https://noticias-stf-wp-prd.s3.sa-east-1.amazonaws.com/wp-content/uploads/wpallimport/uploads/2024/08/13095800/IN_304_2024.pdf. Acesso em: 28 jul. 2026.
- [13] Senado Federal, Ato da Comissão Diretora nº 15, de 2024, “Institui a Política Corporativa de Gestão de Incidentes de Segurança da Informação.” [Online]. Disponível em: <https://adm.senado.leg.br/normas/ui/pub/normaConsultada?idNorma=14383477>. Acesso em: 28 jul. 2026.
- [14] Senado Federal, Ato da Diretoria-Geral nº 30, de 2025, “Institui a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) do Senado Federal.” [Online]. Disponível em: <https://adm.senado.leg.br/normas/ui/pub/normaConsultada?idNorma=14384314>. Acesso em: 28 jul. 2026.
- [15] Câmara dos Deputados, Ato da Mesa nº 231, de 22 de dezembro de 2025, “Atualiza a Política de Segurança da Informação e Cibernética da Câmara dos Deputados.” [Online]. Disponível em: <https://www2.camara.leg.br/login/int/atomes/2025/atodame-sa-231-22-dezembro-2025-798555-norma-cd-mesa.html>. Acesso em: 28 jul. 2026.
- [16] L. R. F. Goldoni, K. F. Rodrigues e B. P. Medeiros, “Qual é o futuro da governança de cibersegurança no Brasil?,” *Cadernos Gestão Pública e Cidadania*, vol. 29, art. e90972, 2024, doi: 10.12660/cgpc.v29.90972.
- [17] Brasil, Lei nº 13.709, de 14 de agosto de 2018, “Lei Geral de Proteção de Dados Pessoais.” [Online]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 28 jul. 2026.
- [18] Autoridade Nacional de Proteção de Dados, Resolução CD/ANPD nº 15, de 24 de abril de 2024, “Aprova o Regulamento de Comunicação de Incidente de Segurança.” [Online]. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis. Acesso em: 28 jul. 2026.

- [19] A. Nelson, S. Rekhi, M. Souppaya e K. Scarfone, *Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile*, NIST SP 800-61 Rev. 3, abr. 2025, doi: 10.6028/NIST.SP.800-61r3.
- [20] Forum of Incident Response and Security Teams, *CSIRT Services Framework, Version 2.1*, 2020. [Online]. Disponível em: https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1. Acesso em: 28 jul. 2026.
- [21] S. Schmitz-Berndt, “Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive,” *Journal of Cybersecurity*, vol. 9, no. 1, art. tyad009, 2023, doi: 10.1093/cybsec/tyad009.
- [22] S. Laube e R. Böhme, “The economics of mandatory security breach reporting to authorities,” *Journal of Cybersecurity*, vol. 2, no. 1, pp. 29–41, 2016, doi: 10.1093/cybsec/tyw002.
- [23] N. Ebert *et al.*, “Learning from safety science: Designing incident reporting systems in cybersecurity,” *Journal of Cybersecurity*, vol. 11, no. 1, art. tyaf019, 2025, doi: 10.1093/cybsec/tyaf019.
- [24] Financial Stability Board, *Recommendations to Achieve Greater Convergence in Cyber Incident Reporting*, 2023. [Online]. Disponível em: <https://www.fsb.org/2023/04/recommendations-to-achieve-greater-convergence-in-cyber-incident-reporting-final-report/>. Acesso em: 28 jul. 2026.
- [25] Parlamento Europeu e Conselho, Diretiva (UE) 2022/2555 (NIS 2), *Jornal Oficial da União Europeia*, L 333, pp. 80–152, 2022. [Online]. Disponível em: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>. Acesso em: 28 jul. 2026.
- [26] K. G. Provan e P. Kenis, “Modes of network governance: Structure, management, and effectiveness,” *Journal of Public Administration Research and Theory*, vol. 18, no. 2, pp. 229–252, 2008, doi: 10.1093/jopart/mum015.
- [27] K. Emerson, T. Nabatchi e S. Balogh, “An integrative framework for collaborative governance,” *Journal of Public Administration Research and Theory*, vol. 22, no. 1, pp. 1–29, 2012, doi: 10.1093/jopart/mur011.
- [28] International Organization for Standardization e International Electrotechnical Commission, *ISO/IEC 27035-4:2024, Information Technology—Information Security Incident Management—Part 4: Coordination*, 1ª ed., dez. 2024. [Online]. Disponível em: <https://www.iso.org/standard/80973.html>. Acesso em: 28 jul. 2026.
- [29] Brasil, *Constituição da República Federativa do Brasil de 1988*. [Online]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 28 jul. 2026.
- [30] M. Leitner, F. Skopik e T. Pahi, “Operational cyber incident coordination revisited: providing cyber situational awareness across organizations and countries,” *Information Security Journal: A Global Perspective*, vol. 33, no. 5, pp. 486–507, 2024, doi: 10.1080/19393555.2024.2334787.
- [31] Forum of Incident Response and Security Teams, *Traffic Light Protocol (TLP): FIRST Standards Definitions and Usage Guidance, Version 2.0*, 2022. [Online]. Disponível em: <https://www.first.org/tlp/>. Acesso em: 28 jul. 2026.
- [32] U.S. Department of Homeland Security, *Harmonization of Cyber Incident Reporting to the Federal Government*, Report to Congress, 2023. [Online]. Disponível em: <https://www.dhs.gov/sites/default/files/2023-09/Harmonization%20of%20Cyber%20Incident%20Reporting%20to%20the%20Federal%20Government.pdf>. Acesso em: 28 jul. 2026.
- [33] C. M. Patterson, J. R. C. Nurse e V. N. L. Franqueira, “Learning from cyber security incidents: A systematic review and future research agenda,” *Computers & Security*, vol. 132, art. 103309, 2023, doi: 10.1016/j.cose.2023.103309.
- [34] S. Buseti e F. M. Scanni, “Evaluating incident reporting in cybersecurity: From threat detection to policy learning,” *Government Information Quarterly*, vol. 42, no. 1, art. 102000, 2025, doi: 10.1016/j.giq.2024.102000.
- [35] Brasil, Decreto nº 11.856, de 26 de dezembro de 2023, “Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança.” [Online]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11856.htm. Acesso em: 28 jul. 2026.
- [36] Brasil, Decreto nº 12.573, de 4 de agosto de 2025, “Institui a Estratégia Nacional de Cibersegurança.” [Online]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/d12573.htm. Acesso em: 28 jul. 2026.
- [37] Brasil, Decreto nº 12.572, de 4 de agosto de 2025, “Institui a Política Nacional de Segurança da Informação.” [Online]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/d12572.htm. Acesso em: 28 jul. 2026.
- [38] L. Bardin, *Análise de Conteúdo*, L. A. Reto e A. Pinheiro, trans., 1ª ed. São Paulo, Brasil: Edições 70, 2016.
- [39] Gabinete de Segurança Institucional da Presidência da República, “Órgãos integrantes da ReGIC.” [Online]. Disponível em: <https://www.gov.br/gsi/pt-br/assuntos/ctir/operacoes-e-servicos/re-gic/orgaos-integrantes-da-regic>. Acesso em: 28 jul. 2026.
- [40] Gabinete de Segurança Institucional da Presidência da República, Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, “Orientações para notificações de incidentes cibernéticos.” [Online]. Disponível em: <https://www.gov.br/gsi/pt-br/assuntos/ctir/operacoes-e-servicos/notificacao-de-incidentes/orientacoes-para-notificacoes-de-incidentes-ciberneticos>. Acesso em: 28 jul. 2026.