# GESTÃO DE INCIDENTES DE CIBERSEGURANÇA NA ADMINISTRAÇÃO PÚBLICA

Marcelo Mello Ramos

Trabalho acadêmico apresentado ao curso de Pós-Graduação em Cýbersecurity: Detecção de Ameaças de Sistemas de Informática e Comunicações

## Resumo

A digitalização dos serviços públicos ampliou a dependência do Estado em relação a sistemas de informação, plataformas digitais, bases de dados e infraestruturas tecnológicas interconectadas. Esse processo produz ganhos de acesso, eficiência e integração administrativa, mas também amplia a exposição a incidentes cibernéticos capazes de afetar a continuidade de serviços essenciais, a proteção de dados pessoais e a confiança social nas instituições públicas. Este trabalho analisa a gestão de incidentes de cibersegurança na administração pública brasileira, com ênfase nos processos de preparação, detecção, resposta, recuperação e aprendizagem organizacional. O problema de pesquisa investiga de que modo a adoção de frameworks internacionais, instrumentos nacionais de cibersegurança e práticas de governança contribui para a resiliência de órgãos e entidades públicas diante de incidentes cibernéticos. A pesquisa é aplicada, qualitativa, descritivo-exploratória e documental, estruturada como estudo de casos múltiplos a partir de documentos oficiais, normas, comunicações institucionais e fontes públicas sobre episódios relevantes, especialmente o ataque ao Superior Tribunal de Justiça, em 2020, e o incidente que afetou sistemas do Ministério da Saúde e o ConecteSUS, em 2021. A análise utiliza categorias derivadas do NIST Cybersecurity Framework 2.0, da NIST SP 800-61 Rev. 3, da ISO/IEC 27035-1:2023, da Política Nacional de Cibersegurança e de orientações brasileiras sobre proteção de dados e resposta a incidentes. Os resultados indicam que a capacidade de resposta depende menos da adoção isolada de ferramentas tecnológicas e mais da integração entre governança, inventário de ativos, gestão de vulnerabilidades, plano de resposta testado, equipe especializada, comunicação institucional, backups confiáveis, análise forense e melhoria contínua. Conclui-se que a gestão de incidentes deve ser tratada como função permanente de governança pública, articulada à proteção de dados pessoais, à continuidade de serviços e à gestão de riscos institucionais.

Palavras-chave: cibersegurança; administração pública; gestão de incidentes; governança digital; proteção de dados; continuidade de serviços públicos.

**Abstract**

The digitalization of public services has increased the State's dependence on information systems, digital platforms, databases and interconnected technological infrastructures. This process generates gains in access, efficiency and administrative integration, but it also expands exposure to cyber incidents capable of affecting the continuity of essential services, the protection of personal data and social trust in public institutions. This study analyzes cybersecurity incident management in the Brazilian public administration, with emphasis on preparation, detection, response, recovery and organizational learning processes. The research problem investigates how the adoption of international frameworks, national cybersecurity instruments and governance practices contributes to the resilience of public agencies and entities in the face of cyber incidents. The research is applied, qualitative, descriptive-exploratory and documentary, structured as a multiple case study based on official documents, regulations, institutional communications and public sources concerning relevant episodes, especially the cyberattack against the Superior Court of Justice in 2020 and the incident that affected systems of the Ministry of Health and ConecteSUS in 2021. The analysis uses categories derived from the NIST Cybersecurity Framework 2.0, NIST SP 800-61 Rev. 3, ISO/IEC 27035-1:2023, the Brazilian National Cybersecurity Policy and Brazilian guidelines on data protection and incident response. The results indicate that response capacity depends less on the isolated adoption of technological tools and more on the integration of governance, asset inventory, vulnerability management, tested incident response plans, specialized teams, institutional communication, reliable backups, forensic analysis and continuous improvement. It is concluded that incident management should be treated as a permanent function of public governance, articulated with personal data protection, service continuity and institutional risk management.

**Keywords:** cybersecurity; public administration; incident management; digital governance; data protection; continuity of public services.

**SUMÁRIO**

## 1. Introdução

A transformação digital do setor público brasileiro alterou profundamente a forma de prestação de serviços ao cidadão. A expansão de portais governamentais, sistemas de autenticação, serviços digitais, bases integradas, aplicativos móveis, plataformas de processo eletrônico e ambientes de computação em nuvem tornou a administração pública mais dependente da disponibilidade, integridade, confidencialidade e autenticidade das informações. Esse movimento aproxima o Estado da sociedade, mas também amplia a superfície de ataque disponível a agentes maliciosos, grupos criminosos, atores oportunistas e operações coordenadas de espionagem, sabotagem ou extorsão digital.

No contexto da administração pública, a cibersegurança não pode ser reduzida a uma questão exclusivamente técnica. Ela envolve governança, gestão de riscos, proteção de dados pessoais, continuidade de serviços, contratação pública, capacitação de servidores, gestão de fornecedores, transparência institucional e comunicação de crise. Um incidente cibernético relevante pode paralisar sistemas, comprometer bases de dados, interromper atendimento ao cidadão, afetar pagamentos, inviabilizar rotinas administrativas, expor dados pessoais e gerar perda de confiança na capacidade do Estado de proteger informações sob sua guarda.

O próprio conceito de incidente cibernético adotado no âmbito governamental reforça essa amplitude. O CTIR Gov define incidente cibernético como ocorrência que pode comprometer, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema. Essa definição é compatível com a visão contemporânea de gestão de riscos cibernéticos, segundo a qual o incidente deve ser analisado não apenas pelo vetor técnico de ataque, mas também por seus efeitos sobre a missão institucional, os serviços prestados e os direitos dos titulares de dados.

O Brasil passou a estruturar, nos últimos anos, um conjunto mais amplo de políticas e normas de cibersegurança. A Estratégia Nacional de Segurança Cibernética, aprovada pelo Decreto nº 10.222/2020, consolidou diretrizes estratégicas para elevar a maturidade cibernética nacional. Posteriormente, o Decreto nº 11.856/2023 instituiu a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança, indicando que a segurança cibernética

deve ser tratada como tema de interesse nacional, com articulação entre governo, setor privado, academia e sociedade. Em paralelo, a LGPD e a regulamentação da ANPD sobre comunicação de incidentes ampliaram as obrigações dos controladores diante de eventos que possam acarretar risco ou dano relevante aos titulares de dados pessoais.

No campo internacional, frameworks como o NIST Cybersecurity Framework 2.0 e a NIST SP 800-61 Rev. 3 deslocam a resposta a incidentes de uma atividade reativa para uma prática permanente de gestão de riscos. A versão 2.0 do CSF organiza os resultados de cibersegurança nas funções Governar, Identificar, Proteger, Detectar, Responder e Recuperar. A NIST SP 800-61 Rev. 3, publicada em 2025, passa a integrar as recomendações de resposta a incidentes ao ciclo de gerenciamento de riscos cibernéticos, reforçando que preparação, comunicação, análise, mitigação e recuperação devem estar incorporadas à governança da organização.

Este trabalho parte da premissa de que a administração pública brasileira não enfrenta apenas o desafio de adquirir soluções tecnológicas, mas o desafio de institucionalizar capacidades de resposta e recuperação. A existência de antivírus, firewall, ferramentas de monitoramento ou backup não garante, por si só, uma resposta adequada. A efetividade depende de responsabilidades formalmente definidas, critérios de classificação de severidade, comunicação com autoridades competentes, preservação de evidências, decisão sobre continuidade de serviços, testes periódicos, inventário de ativos e integração com áreas jurídicas, comunicação social, alta administração, controle interno e proteção de dados pessoais.

O problema de pesquisa é formulado nos seguintes termos: de que modo a adoção de frameworks internacionais, estratégias nacionais de cibersegurança e práticas de governança influencia a resiliência da administração pública brasileira diante de incidentes cibernéticos? O objetivo geral consiste em analisar a gestão de incidentes de cibersegurança na administração pública brasileira, identificando lições extraídas de casos públicos e propondo melhorias para a proteção de sistemas, dados e serviços públicos.

Como objetivos específicos, busca-se: a) sistematizar conceitos e modelos de gestão de incidentes aplicáveis ao setor público; b) examinar o arcabouço normativo brasileiro relacionado à segurança cibernética, proteção de dados e resposta a incidentes; c) analisar, a partir de fontes documentais, episódios relevantes que afetaram serviços públicos ou instituições de alta

relevância estatal; d) confrontar os achados documentais com categorias de boas práticas internacionais; e e) propor recomendações de governança e gestão capazes de fortalecer a capacidade de preparação, resposta, recuperação e aprendizagem organizacional.

A justificativa do estudo decorre da crescente dependência do Estado em relação a ambientes digitais e da sensibilidade dos dados tratados pelo poder público. Órgãos e entidades públicas concentram bases de saúde, previdência, educação, segurança, justiça, tributação, benefícios sociais e identificação civil. A indisponibilidade ou a exposição dessas informações não produz apenas prejuízo tecnológico: pode afetar direitos fundamentais, continuidade administrativa, segurança institucional, confiança pública e cumprimento de obrigações legais. A investigação, portanto, tem relevância acadêmica, gerencial e social.

A delimitação do estudo recai sobre incidentes e práticas de gestão no setor público brasileiro, com foco em análise documental de fontes oficiais, normas e comunicações públicas. Não se pretende realizar auditoria técnica, perícia digital, teste de intrusão ou avaliação de vulnerabilidades em sistemas específicos. Também não se afirma causalidade técnica não demonstrada pelas fontes públicas. A análise concentra-se nos elementos institucionalmente verificáveis: tipo de serviço afetado, medidas de comunicação, recuperação, articulação com órgãos competentes, dependência de backups, impacto sobre a continuidade e aderência a boas práticas de gestão de incidentes.

## 1.1 Problema de pesquisa

Como a adoção de frameworks internacionais, instrumentos nacionais de cibersegurança e práticas de governança influencia a capacidade de resposta e recuperação da administração pública brasileira diante de incidentes cibernéticos que afetam sistemas, dados e serviços públicos?

## 1.2 Objetivo geral

Analisar a gestão de incidentes de cibersegurança na administração pública brasileira, identificando fragilidades, boas práticas e recomendações para fortalecer a resiliência de sistemas, dados e serviços públicos.

### 1.3 Objetivos específicos

Os objetivos específicos são: sistematizar os principais conceitos de cibersegurança e gestão de incidentes; descrever os frameworks e normas aplicáveis ao tema; mapear o arcabouço brasileiro de cibersegurança e proteção de dados; analisar casos públicos de incidentes que afetaram instituições e serviços estatais; comparar os achados documentais com categorias de boas práticas; e apresentar recomendações de governança, prevenção, resposta, recuperação e melhoria contínua.

### 1.4 Justificativa

A relevância do tema decorre do aumento da dependência do Estado em relação a sistemas digitais e do valor estratégico das bases de dados públicas. A administração pública trata informações pessoais e institucionais que, se indisponíveis, alteradas ou expostas, podem gerar impactos jurídicos, administrativos e sociais. Além disso, a prestação de serviços públicos depende cada vez mais de plataformas tecnológicas, o que torna a continuidade digital uma dimensão da própria continuidade administrativa. Nesse cenário, a gestão de incidentes deixa de ser atividade operacional restrita à área de tecnologia e passa a compor a agenda de governança pública.

## 2. Referencial teórico

### 2.1 Cibersegurança, segurança da informação e risco cibernético

A segurança da informação é tradicionalmente associada à preservação da confidencialidade, integridade e disponibilidade das informações. Em ambientes digitais complexos, essa tríade deve ser complementada por autenticidade, rastreabilidade, resiliência, governança e responsabilidade institucional. A cibersegurança, por sua vez, corresponde ao conjunto de políticas, controles, processos, tecnologias, competências e estruturas de governança destinadas a proteger sistemas, redes, dados e serviços contra ameaças originadas no espaço cibernético.

No setor público, o risco cibernético possui características próprias. A primeira é a elevada exposição institucional: serviços públicos precisam ser acessíveis, frequentemente em larga escala, e muitas vezes são disponibilizados em portais abertos. A segunda é a criticidade

social dos dados tratados: informações de saúde, educação, assistência social, justiça, segurança pública e finanças públicas podem afetar diretamente direitos individuais e coletivos. A terceira é a interdependência administrativa: sistemas de um órgão podem depender de autenticação, cadastros, redes, infraestrutura ou serviços fornecidos por outros órgãos ou por terceiros contratados.

Essa interdependência torna inadequada uma visão fragmentada da segurança. Um incidente que começa como exploração de uma vulnerabilidade técnica pode evoluir para crise jurídica, reputacional, operacional e política. Por isso, a gestão de riscos cibernéticos deve ser incorporada ao planejamento institucional, à governança de tecnologia da informação, à contratação pública, à gestão de continuidade, à proteção de dados pessoais e à comunicação com cidadãos e órgãos de controle.

A literatura e os frameworks recentes reforçam que risco cibernético não se limita à probabilidade de ataque. Ele envolve a combinação entre ameaça, vulnerabilidade, impacto e capacidade de resposta. Um mesmo ataque pode ter efeitos muito diferentes em organizações distintas, conforme o grau de preparação, inventário de ativos, segmentação de rede, maturidade de backup, treinamento de equipes, existência de plano de resposta e integração com autoridades competentes. Assim, a resiliência cibernética é construída antes do incidente, testada durante o incidente e aperfeiçoada depois dele.

## 2.2 Ameaças cibernéticas contemporâneas

As ameaças cibernéticas atuais combinam automação, engenharia social, exploração de vulnerabilidades conhecidas, credenciais comprometidas, uso abusivo de serviços legítimos e ataques direcionados. Entre as ameaças mais relevantes para a administração pública estão ransomware, phishing, exploração de sistemas desatualizados, ataques de negação de serviço, vazamentos de dados, desfiguração de páginas, abuso de credenciais e comprometimento de fornecedores.

O ransomware se destaca por combinar indisponibilidade e extorsão. Em seu modelo tradicional, o agente malicioso criptografa dados e exige pagamento para suposta restauração. Em modelos mais recentes, frequentemente ocorre dupla extorsão, com exfiltração de dados e ameaça de divulgação. Isso significa que backups são indispensáveis, mas não resolvem integralmente o

problema quando há violação de confidencialidade. O órgão pode restaurar sistemas e, ainda assim, enfrentar obrigações de comunicação, apuração, responsabilização e mitigação de danos aos titulares de dados.

O phishing e a engenharia social permanecem relevantes porque exploram fragilidades humanas e processuais. Servidores, terceirizados e gestores podem ser induzidos a revelar credenciais, abrir anexos maliciosos ou autorizar operações indevidas. A prevenção, portanto, não depende apenas de filtros de e-mail, mas também de cultura organizacional, treinamento contínuo, autenticação multifator, controle de privilégios, segregação de funções e procedimentos de validação.

Os ataques de negação de serviço distribuído afetam sobretudo a disponibilidade. Em serviços públicos digitais, a indisponibilidade pode impedir acesso a informações, inscrições, emissão de documentos, consulta processual, serviços de saúde, educação e benefícios. Mesmo quando não há vazamento de dados, a interrupção de serviço pode gerar impactos relevantes à missão institucional. Por isso, a disponibilidade deve ser tratada como dimensão de valor público, e não apenas como indicador técnico de infraestrutura.

A exploração de vulnerabilidades conhecidas também é crítica. Muitos incidentes não decorrem de técnicas inéditas, mas de sistemas expostos, serviços mal configurados, ausência de correções, credenciais fracas, softwares legados e integração insegura com terceiros. Nesse ponto, a gestão de ativos e vulnerabilidades assume papel central. Não é possível proteger adequadamente aquilo que o órgão não conhece, não monitora ou não prioriza.

### 2.3 Gestão de incidentes como processo de governança

A gestão de incidentes de cibersegurança consiste no conjunto de atividades destinadas a preparar a organização, detectar eventos adversos, analisar sua natureza, conter danos, erradicar causas, recuperar serviços e incorporar lições aprendidas. A gestão de incidentes não deve ser compreendida como improvisação emergencial. Ela exige planejamento anterior, definição de papéis, critérios de severidade, canais de comunicação, ferramentas, procedimentos, registros, evidências e mecanismos de coordenação.

O NIST SP 800-61 Rev. 2 consolidou por muitos anos um ciclo de vida composto por preparação, detecção e análise, contenção/erradicação/recuperação e atividades pós-incidente.

Essa estrutura continua útil didaticamente, especialmente para demonstrar que a resposta não começa no momento da crise. Contudo, a NIST SP 800-61 Rev. 3 atualiza a perspectiva ao incorporar a resposta a incidentes ao NIST CSF 2.0, enfatizando que incident response deve ser parte do gerenciamento de riscos cibernéticos e da governança institucional.

Com a abordagem do CSF 2.0, a gestão de incidentes passa a ser observada em seis funções. Governar envolve estabelecer estratégia, políticas, responsabilidades e supervisão. Identificar implica conhecer ativos, serviços críticos, fornecedores, dados e riscos. Proteger compreende salvaguardas como controle de acesso, treinamento, segurança de dados, segurança de plataforma e resiliência tecnológica. Detectar requer monitoramento e análise de eventos adversos. Responder abrange triagem, comunicação, mitigação, análise e coordenação. Recuperar envolve restauração, verificação de integridade, comunicação de progresso e retorno seguro à normalidade.

A ISO/IEC 27035-1:2023 reforça perspectiva semelhante ao apresentar conceitos, princípios e processo estruturado para gestão de incidentes de segurança da informação, incluindo preparação, detecção, reporte, avaliação, resposta e aplicação de lições aprendidas. Sua contribuição é mostrar que a gestão de incidentes não deve depender apenas de ferramentas, mas de um sistema de gestão capaz de transformar eventos adversos em melhoria institucional.

No setor público, esse processo deve articular tecnologia, gestão e legalidade. A decisão de desligar um sistema, restaurar backup, comunicar titulares, acionar polícia judiciária, informar autoridade de proteção de dados, priorizar determinado serviço ou divulgar nota pública envolve critérios técnicos e jurídicos. A equipe de tecnologia executa parte essencial do trabalho, mas a responsabilidade institucional é mais ampla e envolve alta administração, área jurídica, comunicação, controle interno, encarregado de dados e gestores de negócio.

### 2.4 Normas, políticas públicas e instituições brasileiras de cibersegurança

O arcabouço brasileiro de cibersegurança evoluiu de forma gradual. A Política Nacional de Segurança da Informação, inicialmente disciplinada pelo Decreto nº 9.637/2018 e atualizada por normativos posteriores, estruturou diretrizes para governança da segurança da informação no âmbito federal. A Estratégia Nacional de Segurança Cibernética, aprovada pelo Decreto nº

10.222/2020, estabeleceu objetivos estratégicos relacionados à governança, prevenção, educação, cooperação, proteção de infraestruturas críticas e fortalecimento institucional.

O Decreto nº 11.856/2023 instituiu a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. Esse decreto é relevante porque afirma a cibersegurança como política nacional, orientada por princípios como soberania, proteção de direitos fundamentais, proteção de dados pessoais, privacidade, acesso à informação, cooperação federativa e desenvolvimento seguro. Para a administração pública, isso significa que a gestão de incidentes deve ser vinculada a objetivos de Estado e não apenas a práticas internas de tecnologia.

O CTIR Gov, como centro de prevenção, tratamento e resposta a incidentes cibernéticos de governo, possui papel relevante na detecção, triagem, análise, resposta, disseminação de alertas e consolidação de estatísticas sobre incidentes e vulnerabilidades que afetam redes de governo. As páginas públicas do CTIR Gov em números indicam que as notificações são voluntárias e refletem eventos cibernéticos em redes governamentais, o que exige cautela interpretativa: os dados são valiosos para compreender tendências e categorias, mas não devem ser lidos como total absoluto de todos os incidentes existentes no setor público.

No âmbito do Governo Digital, o Programa de Privacidade e Segurança da Informação - PPSI 2.0 apresenta controles, guias, modelos e procedimentos para elevar a maturidade e a resiliência dos órgãos e entidades no âmbito do SISP. O PPSI articula governança, maturidade, metodologia, pessoas e tecnologia. Essa estrutura confirma que a segurança da informação deve ser gerida como programa institucional, com diagnóstico, controles, capacitação e melhoria contínua.

A Lei Geral de Proteção de Dados Pessoais acrescenta dimensão jurídica central à gestão de incidentes. O art. 48 da LGPD determina que o controlador deve comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. A Resolução CD/ANPD nº 15/2024 regulamenta procedimentos de comunicação de incidentes de segurança, reforçando que a resposta técnica precisa ser acompanhada de avaliação de risco, documentação e comunicação adequada quando houver dados pessoais envolvidos.

Essas normas não substituem umas às outras. Elas formam um conjunto: a política nacional estabelece diretrizes macro; o CTIR Gov atua na prevenção e tratamento de incidentes de governo; o PPSI organiza controles e maturidade no SISP; a LGPD e a ANPD regulam a proteção de dados pessoais; e os frameworks internacionais oferecem modelos para estruturar processos de governança, resposta e recuperação. A maturidade institucional depende da capacidade de integrar esses instrumentos em práticas concretas.

### 2.5 Infraestruturas críticas, serviços essenciais e continuidade administrativa

Infraestruturas críticas são ativos, serviços, sistemas e processos cuja interrupção pode gerar efeitos severos sobre segurança, economia, saúde, bem-estar social ou funcionamento do Estado. Embora nem todo sistema público seja formalmente enquadrado como infraestrutura crítica, muitos serviços digitais possuem alta relevância operacional e social. Sistemas de saúde, justiça, previdência, tributação, educação, comunicação pública, benefícios sociais e identificação civil exemplificam áreas em que a indisponibilidade pode produzir impacto direto ao cidadão.

A gestão de incidentes deve, portanto, dialogar com a gestão de continuidade de negócios e de continuidade de serviços públicos. O objetivo não é apenas restaurar servidores ou bancos de dados, mas assegurar que funções críticas possam continuar, ainda que em modo degradado, manual, alternativo ou priorizado. Isso exige análise de impacto no negócio, definição de tempo máximo tolerável de indisponibilidade, objetivos de recuperação, cadeia de dependências, fornecedores críticos e planos de contingência.

A continuidade administrativa envolve decisões de priorização. Em um incidente amplo, talvez não seja possível restaurar todos os sistemas simultaneamente. A organização deve saber previamente quais serviços são essenciais, quais dados são necessários para operação mínima, quais equipes devem ser acionadas, quais contratos preveem suporte emergencial e quais comunicações devem ser enviadas. A ausência desse planejamento aumenta o tempo de resposta e força decisões improvisadas sob pressão.

No setor público, a continuidade também possui dimensão democrática e jurídica. A indisponibilidade de sistemas judiciais pode suspender prazos e afetar acesso à justiça. A indisponibilidade de sistemas de saúde pode comprometer registro, vigilância, vacinação e atendimento. A indisponibilidade de serviços de comunicação pública pode afetar a circulação de

informações de utilidade pública. Assim, a resiliência cibernética deve ser compreendida como capacidade de preservar funções públicas essenciais em ambiente de ameaça.

### 2.6 Comunicação de crise, transparência e proteção de dados pessoais

A comunicação durante incidentes cibernéticos exige equilíbrio entre transparência, segurança operacional, proteção de evidências, sigilo investigativo e direito à informação. Divulgar informações insuficientes pode gerar desconfiança, rumores e insegurança. Divulgar detalhes técnicos sensíveis pode facilitar novos ataques ou prejudicar a investigação. Por isso, o plano de resposta deve prever quem comunica, quando comunica, a quem comunica, com qual conteúdo mínimo e por quais canais.

Quando há dados pessoais envolvidos, a comunicação passa a ter regime jurídico específico. A LGPD e as orientações da ANPD reforçam que a comunicação ao titular e à autoridade não é mero ato formal, mas instrumento de mitigação de danos. O titular precisa conhecer riscos e providências recomendadas quando o incidente puder acarretar dano relevante. A organização, por sua vez, deve registrar a avaliação realizada, a natureza dos dados afetados, as medidas técnicas e administrativas adotadas, os riscos envolvidos e as razões de eventual não comunicação.

A comunicação também cumpre papel de recuperação institucional. A confiança pública não é restaurada apenas com retorno técnico do sistema. Ela depende da percepção de que a instituição reconheceu o problema, atuou com responsabilidade, comunicou o necessário, protegeu os dados e adotou medidas para reduzir a chance de repetição. Em gestão pública, confiança é ativo institucional e deve ser tratada como elemento de resiliência.

### 2.7 Aplicabilidade a empresas públicas de comunicação e ao caso EBC

Embora o foco deste trabalho seja a administração pública em sentido amplo, a discussão também se aplica a empresas públicas que operam serviços digitais e canais de comunicação institucional. Empresas públicas de comunicação lidam com portais jornalísticos, acervos, sistemas de produção audiovisual, serviços de transmissão, plataformas digitais, contratos, dados de empregados, dados de usuários e interfaces com outros órgãos de governo. A indisponibilidade, alteração indevida ou comprometimento desses ambientes pode afetar tanto rotinas internas quanto a entrega de informação pública à sociedade.

No caso da Empresa Brasil de Comunicação, fontes institucionais públicas indicam a existência de Política de Segurança da Informação e da Comunicação - POSIC, bem como de Comitê de Segurança da Informação e da Comunicação - COSIC, vinculado à Diretoria Executiva, com finalidade de estabelecer políticas e diretrizes para segurança da informação e comunicação no âmbito da empresa. A página de estratégia da EBC também lista o Plano Diretor de Tecnologia da Informação e Comunicação - PDTIC entre os documentos e iniciativas que orientam a atuação estratégica institucional.

Esses elementos não autorizam, por si, concluir o nível de maturidade de cibersegurança da EBC, pois isso exigiria análise documental específica, acesso a planos, indicadores, auditorias e procedimentos internos. Entretanto, mostram que empresas públicas de comunicação possuem pontos de entrada institucionais para integrar governança de TIC, segurança da informação, gestão de riscos e resposta a incidentes. Se o estudo for adaptado futuramente para um recorte aplicado à EBC, seria metodologicamente adequado analisar POSIC, regimento do COSIC, PDTIC, política de riscos, relatórios de gestão, práticas de continuidade e eventuais documentos de resposta a incidentes, sempre sem afirmar incidentes não documentados.

**Quadro 1 - Relação entre funções do NIST CSF 2.0 e gestão de incidentes no setor público**

| Função | Sentido para gestão pública | Exemplos de evidência documental |
|---|---|---|
| Governar | Definir estratégia, responsabilidades, políticas, supervisão e integração com risco institucional. | POSIC, comitê de segurança, plano de riscos, atas, matriz de responsabilidades. |
| Identificar | Conhecer ativos, serviços críticos, dados, fornecedores, dependências e riscos. | Inventário de ativos, catálogo de sistemas, BIA, mapa de dados pessoais, contratos críticos. |
| Proteger | Implementar salvaguardas para reduzir probabilidade e impacto de eventos adversos. | MFA, segmentação, hardening, capacitação, controle de acesso, backup, políticas de atualização. |
| Detectar | Monitorar eventos, correlacionar indicadores e declarar incidentes segundo critérios definidos. | Logs, SIEM, alertas do CTIR Gov, playbooks, critérios de severidade, registros de triagem. |
| Responder | Conter, analisar, comunicar, mitigar e coordenar ações internas e | Plano de resposta, registro de incidente, acionamento da ETIR, |

| | | |
|---|---|---|
| | externas. | comunicação com ANPD/CTIR/PF. |
| Recuperar | Restaurar serviços, verificar integridade, comunicar progresso e concluir documentação. | Plano de recuperação, testes de restauração, relatório pós-incidente, lições aprendidas. |

Fonte: elaborado com base em NIST (2024; 2025), ISO/IEC (2023), CTIR Gov (2026) e ANPD (2024).

## 3. Procedimentos metodológicos

Este estudo caracteriza-se como pesquisa aplicada, qualitativa, descritivo-exploratória e documental. É aplicada porque busca produzir conhecimento orientado à solução de problemas práticos relacionados à gestão de incidentes de cibersegurança em órgãos e entidades públicas. É qualitativa porque privilegia a interpretação de documentos, normas, comunicações institucionais e boas práticas, sem pretensão de mensuração estatística da totalidade dos incidentes existentes. É descritivo-exploratória porque descreve categorias, processos e casos públicos, ao mesmo tempo em que explora relações entre governança, resposta, recuperação e resiliência.

A estratégia de pesquisa adotada é o estudo de casos múltiplos com base documental. O estudo de caso é adequado quando se busca compreender um fenômeno contemporâneo em seu contexto real, especialmente quando a fronteira entre o fenômeno e o contexto é complexa. No presente trabalho, os incidentes cibernéticos não são analisados como eventos isolados, mas como manifestações de fragilidades e capacidades institucionais relacionadas a governança, continuidade, comunicação, proteção de dados e resposta coordenada.

Foram selecionados dois casos principais: o ataque cibernético ao Superior Tribunal de Justiça, em novembro de 2020, e o incidente que afetou o site do Ministério da Saúde, o ConecteSUS, o e-SUS Notifica e o SI-PNI, em dezembro de 2021. A escolha se justifica pela relevância pública, disponibilidade de comunicações institucionais e capacidade de ilustrar efeitos sobre continuidade de serviços, preservação de dados, articulação interinstitucional e recuperação. O estudo também utiliza dados e documentos do CTIR Gov, do PPSI, da ANPD, da legislação brasileira e de frameworks internacionais para contextualização e comparação.

O corpus documental é composto por: decretos federais relacionados à cibersegurança e segurança da informação; Lei Geral de Proteção de Dados; orientações e regulamentações da

ANPD sobre comunicação de incidentes; páginas e documentos públicos do CTIR Gov; páginas do Governo Digital sobre o PPSI; documentos e páginas institucionais da EBC utilizados apenas para demonstrar aplicabilidade setorial; comunicações oficiais do STJ/CJF; reportagem da Agência Brasil sobre o incidente do Ministério da Saúde; e publicações internacionais do NIST, ISO/IEC e CISA/MS-ISAC.

A coleta de dados foi realizada por levantamento documental em fontes oficiais e institucionais publicamente disponíveis. As fontes foram escolhidas por sua confiabilidade, pertinência temática e auditabilidade. Quando se recorre a matéria jornalística, a preferência foi por veículo público ou fonte que reproduz nota institucional, como no caso da Agência Brasil em relação ao Ministério da Saúde. Não foram utilizadas entrevistas, questionários, testes técnicos, varreduras de rede, dados internos sigilosos ou informações não verificáveis.

A análise dos dados foi conduzida por análise de conteúdo temática. Foram definidas categorias a priori com base nos frameworks NIST CSF 2.0, NIST SP 800-61 Rev. 3 e ISO/IEC 27035-1:2023: governança, identificação, proteção, detecção, resposta, recuperação, comunicação, proteção de dados e aprendizagem pós-incidente. Em seguida, os documentos foram examinados para identificar evidências relacionadas a essas categorias. A comparação entre os casos buscou evidenciar padrões, limites e recomendações, sem afirmar detalhes técnicos que não constem das fontes públicas.

Como limitações, destaca-se que incidentes cibernéticos são frequentemente tratados com restrição de informações por razões de segurança, investigação e proteção institucional. As fontes públicas nem sempre permitem conhecer vetor de ataque, extensão real de comprometimento, indicadores técnicos, arquitetura dos sistemas ou decisões internas de resposta. Desse modo, as conclusões são interpretativas e documentais, não periciais. Outra limitação é que os dados do CTIR Gov são voluntários e refletem notificações e eventos reportados em redes de governo, não a totalidade absoluta de ocorrências no país.

A opção metodológica é coerente com o problema de pesquisa porque o objetivo não é comprovar tecnicamente a causa de incidentes específicos, mas analisar a gestão de incidentes como prática de governança pública. Para esse propósito, documentos normativos, comunicações institucionais e frameworks são fontes adequadas, pois permitem observar deveres, fluxos, categorias, responsabilidades e evidências de resposta e recuperação. A análise evita transformar

ausência de informação pública em conclusão e diferencia explicitamente o que está documentado do que seria necessário confirmar por auditoria ou investigação técnica.

**Quadro 2 - Corpus documental da pesquisa**

| Grupo de documentos | Fontes principais | Função na pesquisa |
|---|---|---|
| Normas brasileiras | LGPD; Decretos de cibersegurança; PNCiber; PNSI; E-Ciber. | Delimitar deveres, princípios e diretrizes aplicáveis à administração pública. |
| Órgãos de referência | CTIR Gov; ANPD; Governo Digital/PPSI. | Identificar conceitos, categorias, recomendações e obrigações de comunicação. |
| Frameworks internacionais | NIST CSF 2.0; NIST SP 800-61 Rev. 3; ISO/IEC 27035-1; CISA StopRansomware. | Construir categorias analíticas e boas práticas comparativas. |
| Casos públicos | STJ/CJF 2020; Ministério da Saúde/ConecteSUS 2021. | Analisar efeitos sobre continuidade, resposta, recuperação e comunicação. |
| Aplicabilidade setorial | POSIC, COSIC, PDTIC e governança da EBC. | Indicar possibilidade de adaptação do estudo a empresa pública de comunicação. |

Fonte: elaborado pelo autor.

## 4. Resultados e discussão

### 4.1 Caracterização do cenário brasileiro de incidentes cibernéticos governamentais

As fontes públicas do CTIR Gov mostram que o governo federal passou a divulgar estatísticas e categorias relacionadas a notificações de incidentes e vulnerabilidades em redes governamentais. A página histórica do CTIR Gov em números, atualizada até 31 de dezembro de 2025, apresenta notificações reportadas de 2021 a 2025 e descreve categorias como abuso de sítio web, abuso no serviço de e-mail, página falsa, phishing, scan, vazamento de dados, software vulnerável, vulnerabilidade de criptografia e vulnerabilidade DRDoS. A página de 2026 informa mudança metodológica, com adoção de nova taxonomia baseada em orientações da ENISA e ampliação do consumo de feeds de segurança.

Essa mudança é metodologicamente importante. Quando um órgão amplia fontes de monitoramento ou altera taxonomia, variações quantitativas precisam ser analisadas com cautela. Um aumento de notificações pode refletir crescimento real de ameaças, mas também pode decorrer de maior capacidade de detecção, ampliação de feeds, mudança de classificação ou redução de duplicidades. Para pesquisa acadêmica, esse ponto impede conclusões simplistas do tipo "os ataques aumentaram em determinada proporção" sem controlar alterações metodológicas.

Ainda assim, os dados e descrições do CTIR Gov são relevantes porque demonstram que incidentes e vulnerabilidades no governo são fenômenos recorrentes e diversificados. A própria taxonomia de 2026 inclui categorias como código malicioso, conteúdo abusivo, engenharia social, indisponibilidade, intrusões, obtenção de informações, ransomware, vulnerabilidades e outros. Essas categorias abrangem desde tentativas de reconhecimento e exploração até eventos capazes de comprometer serviços ou dados.

Para a administração pública, a diversidade de categorias exige respostas diferenciadas. Uma página falsa demanda remoção, comunicação e orientação ao cidadão. Um ransomware exige contenção, isolamento, preservação de evidências, restauração e avaliação de vazamento. Um scan pode indicar reconhecimento prévio e necessidade de correção preventiva. Uma vulnerabilidade em serviço exposto demanda priorização de patching. Uma indisponibilidade pode exigir plano de continuidade e comunicação de crise. Portanto, a maturidade institucional está na capacidade de classificar, priorizar e responder segundo severidade e missão pública afetada.

### 4.2 Caso 1: ataque cibernético ao Superior Tribunal de Justiça

O Superior Tribunal de Justiça detectou, em 3 de novembro de 2020, um ataque hacker durante sessões de julgamento. Comunicado do Conselho da Justiça Federal informou que um vírus circulava na rede de informática do tribunal e que, como medida de precaução, os links para a internet foram desconectados. Essa ação implicou cancelamento de sessões de julgamento e impossibilitou o funcionamento dos sistemas de informática e telefonia da Corte. O comunicado também registrou acionamento da Polícia Federal, apoio de empresas prestadoras de tecnologia e colaboração do Centro de Defesa Cibernética do Exército Brasileiro.

A dimensão da resposta demonstra que o incidente ultrapassou a esfera interna de TI. A desconexão de links é medida típica de contenção para impedir propagação ou comunicação maliciosa. O acionamento da Polícia Federal revela dimensão investigativa. A participação de prestadores e de estruturas especializadas indica necessidade de coordenação externa. O suporte do Centro de Defesa Cibernética mostra que, em incidentes de alta relevância estatal, a resposta pode envolver capacidades interinstitucionais.

O comunicado do CJF também informou que o ataque bloqueou temporariamente, com uso de criptografia, o acesso aos dados, mas que as informações estavam preservadas nos sistemas de backup. Esse elemento é central para a discussão. A existência de backup preservado é fator decisivo de recuperação em incidentes de ransomware, mas sua utilidade depende de integridade, isolamento, periodicidade, documentação e capacidade de restauração em tempo compatível com a missão. O caso ilustra que backup não é apenas cópia de dados; é componente de estratégia de continuidade e recuperação.

Comunicado posterior do STJ, de 12 de novembro de 2020, informou que a Secretaria de Tecnologia da Informação e Comunicação seguia restaurando o ambiente tecnológico afetado, reduzindo episódios de lentidão ou quedas de acesso. A nota também indicou que a Polícia Federal apurava os efeitos do ataque, inclusive quanto ao alcance do acesso aos arquivos e eventual cópia de dados. Em 19 de novembro, novo comunicado afirmou que os trabalhos de restabelecimento dos sistemas estavam concluídos, permitindo retomada das atividades com acesso garantido, com segurança, aos usuários.

À luz do NIST CSF 2.0, o caso permite observar aspectos de resposta e recuperação. A resposta incluiu contenção mediante desconexão, coordenação com terceiros e acionamento investigativo. A recuperação envolveu reconstrução de ambiente tecnológico, restauração progressiva de sistemas e comunicação pública. A análise pós-incidente aparece de forma indireta quando o comunicado do STJ afirma que o episódio levaria a transformações para aperfeiçoar o tratamento da segurança da informação. Entretanto, as fontes públicas não permitem avaliar detalhadamente inventário prévio, maturidade de monitoramento, vetor de entrada, segmentação, controles de acesso, tempo de detecção ou efetividade dos testes de recuperação anteriores ao incidente.

O principal aprendizado institucional do caso é que órgãos de alta relevância precisam integrar continuidade, backup, contenção, comunicação, investigação e governança. A existência de backup preservado reduz risco de perda definitiva, mas não elimina impactos operacionais, suspensão de serviços, custos de recuperação, incerteza sobre acesso a dados e necessidade de reconstrução segura. O incidente confirma que a resiliência se mede não pela inexistência de ataque, mas pela capacidade de limitar danos, restaurar serviços, preservar evidências e aprimorar controles.

### 4.3 Caso 2: Ministério da Saúde, ConecteSUS e sistemas associados

Em 10 de dezembro de 2021, a Agência Brasil noticiou que o site do Ministério da Saúde e a página e o aplicativo do ConecteSUS foram invadidos por hackers. Segundo a notícia, o ConecteSUS fornecia o Certificado Nacional de Vacinação Covid-19 e, no momento do incidente, não era possível acessar dados sobre vacinação. A reportagem também registrou que o e-SUS Notifica, utilizado para notificações de síndrome gripal suspeita e confirmada de covid-19, e o Sistema de Informação do Programa Nacional de Imunização - SI-PNI foram afetados.

O caso é relevante porque envolve sistemas de saúde em contexto de pandemia, quando informações de vacinação, notificação e imunização possuíam grande importância social, sanitária e administrativa. A indisponibilidade do certificado de vacinação e de sistemas associados não deve ser analisada apenas como falha tecnológica. Ela impacta acesso a serviços, circulação de informações sanitárias, rotinas de estados e municípios e confiança pública em plataformas digitais de saúde.

A notícia da Agência Brasil informou que a autoria foi assumida pelo grupo Lapsus$ e que a mensagem publicada afirmava que dados dos sistemas foram copiados e excluídos. A reportagem também reproduziu nota do Ministério da Saúde segundo a qual o incidente comprometeu temporariamente alguns sistemas da pasta, como e-SUS Notifica, SI-PNI, ConecteSUS e funcionalidades de emissão de certificados e carteira digital de vacinação. A pasta informou ainda que o GSI e a Polícia Federal foram acionados e que o Datasus atuava para restabelecimento das plataformas.

Do ponto de vista analítico, o caso evidencia a interseção entre segurança cibernética, proteção de dados pessoais e continuidade de serviços de saúde. Mesmo quando não se conhece

publicamente toda a extensão técnica do incidente, a simples possibilidade de cópia e exclusão de dados, somada à indisponibilidade de sistemas, exige avaliação de confidencialidade, integridade e disponibilidade. Em ambiente submetido à LGPD, a organização deve avaliar se o incidente pode acarretar risco ou dano relevante aos titulares e, se for o caso, cumprir deveres de comunicação conforme art. 48 da lei e regulamentação da ANPD.

A resposta documentada publicamente incluiu acionamento do GSI e da Polícia Federal, além da atuação do Datasus para restabelecimento. Esses elementos indicam coordenação interinstitucional e recuperação técnica. Contudo, as fontes públicas não permitem concluir com precisão quais dados foram efetivamente acessados, qual vetor foi utilizado, quais controles falharam ou quais mudanças técnicas foram implementadas após o incidente. Essa limitação reforça a necessidade de prudência acadêmica: é possível analisar efeitos e respostas documentadas, mas não atribuir causalidades técnicas não comprovadas.

À luz dos frameworks, o caso reforça a centralidade das funções Identificar, Proteger, Detectar, Responder e Recuperar. Identificar é crucial para saber quais bases, sistemas e integrações foram afetados. Proteger envolve controles de acesso, segregação, backup, gestão de nuvem e segurança de aplicações. Detectar exige monitoramento de alterações indevidas, exfiltração e indisponibilidade. Responder demanda contenção, investigação, comunicação e coordenação com órgãos competentes. Recuperar implica retorno seguro de plataformas e validação de integridade dos dados. A dimensão de Governar atravessa todas as etapas porque define responsabilidades, prioridades e comunicação com a sociedade.

### 4.4 Comparação dos casos à luz das boas práticas

A comparação entre STJ e Ministério da Saúde demonstra que incidentes cibernéticos no setor público podem afetar áreas distintas, mas apresentam desafios comuns. Ambos envolveram serviços de alta relevância pública, indisponibilidade ou comprometimento temporário de sistemas, acionamento de instituições externas e necessidade de recuperação. Em ambos, a comunicação pública foi essencial para informar a sociedade e reduzir incertezas. Também em ambos, as fontes públicas não permitem avaliar todos os detalhes técnicos, o que é comum em incidentes cibernéticos por razões de segurança e investigação.

No caso STJ, a documentação pública destaca a contenção por desconexão, preservação de dados em backup, reconstrução do ambiente e retomada das atividades. No caso Ministério da Saúde, a documentação pública destaca indisponibilidade de plataformas de saúde, alegação de cópia e exclusão de dados por grupo atacante, acionamento de GSI/PF e trabalho do Datasus para restabelecimento. O primeiro caso evidencia fortemente continuidade e backup; o segundo evidencia, além da continuidade, possível dimensão de proteção de dados pessoais em larga escala.

A partir do NIST CSF 2.0, observa-se que a função Governar é o eixo que permite transformar incidentes em processos gerenciáveis. Sem governança, decisões sobre contenção, priorização, comunicação, recuperação e responsabilização tendem a ser improvisadas. A função Identificar aparece como condição de análise de impacto: o órgão precisa saber quais sistemas, dados, pessoas, fornecedores e serviços estão envolvidos. A função Proteger reduz probabilidade e impacto. Detectar encurta o tempo de percepção. Responder limita danos. Recuperar restabelece serviços e confiança.

A análise também demonstra que a maturidade não deve ser medida apenas pelo sucesso final da recuperação. Um órgão pode recuperar sistemas, mas demorar a comunicar, não preservar evidências, não mapear dados afetados ou não transformar lições aprendidas em controles. A maturidade envolve documentação, aprendizagem e revisão de processos. A fase pós-incidente é, muitas vezes, a mais negligenciada, justamente por ocorrer quando a pressão pública diminui. Contudo, é nela que se consolidam relatórios, ações corretivas, revisão de contratos, treinamento, atualização de políticas e testes de continuidade.

Outro ponto comum é a dependência de terceiros. Sistemas públicos raramente são operados apenas por equipes internas. Há fornecedores de infraestrutura, desenvolvimento, nuvem, telecomunicações, segurança, suporte e integração. O NIST CSF 2.0 inclui risco de cadeia de suprimentos na função Governar, reconhecendo que fornecedores devem ser conhecidos, priorizados por criticidade e submetidos a requisitos de cibersegurança em contratos e acordos. Na administração pública, essa recomendação dialoga com planejamento de contratações, termos de referência, níveis de serviço, cláusulas de incidentes, auditoria e responsabilidades em caso de vazamento.

**Quadro 3 - Matriz comparativa dos casos analisados**

| Categoria | STJ - 2020 | Ministério da Saúde/ConecteSUS - 2021 |
|---|---|---|
| Serviço afetado | Sistemas de informática, telefonia e rotinas de julgamento/consulta do tribunal. | Site do Ministério da Saúde, ConecteSUS, e-SUS Notifica, SI-PNI e certificados digitais de vacinação. |
| Impacto público | Cancelamento de sessões, indisponibilidade de sistemas e necessidade de reconstrução de ambiente tecnológico. | Indisponibilidade de informações e certificados de vacinação; possível impacto em rotinas de saúde pública. |
| Resposta documentada | Desconexão de links, acionamento da PF, apoio de fornecedores, colaboração do Centro de Defesa Cibernética. | Acionamento do GSI e da PF; atuação do Datasus para restabelecimento das plataformas. |
| Recuperação | Dados preservados em backup segundo comunicado; restauração progressiva e retomada das atividades. | Restabelecimento anunciado pela pasta em momento posterior; fontes públicas não detalham integralmente a arquitetura de recuperação. |
| Questões críticas | Continuidade, backup, reconstrução segura, investigação e comunicação institucional. | Continuidade de serviços de saúde, integridade e disponibilidade de dados, possível dimensão de dados pessoais. |
| Limite documental | Não há, nas fontes públicas, descrição completa do vetor, arquitetura, controles prévios e relatório técnico pós-incidente. | Não há, nas fontes públicas utilizadas, confirmação detalhada da extensão de eventual cópia, vetor de ataque e controles corrigidos. |

Fonte: elaborado com base em comunicados do CJF/STJ (2020) e Agência Brasil/Ministério da Saúde (2021).

## 4.5 Principais fragilidades inferidas da análise documental

A primeira fragilidade recorrente é a dificuldade de converter normas e políticas em capacidade operacional testada. É comum que instituições disponham de políticas de segurança, comitês e diretrizes, mas não necessariamente possuam playbooks atualizados, exercícios simulados, inventário de ativos validado, critérios objetivos de severidade, lista de contatos

emergenciais e capacidade de restauração testada em condições realistas. A existência formal de política é necessária, mas insuficiente.

A segunda fragilidade é a gestão de ativos e vulnerabilidades. Sem inventário atualizado de sistemas, servidores, bases, integrações, certificados, APIs, usuários privilegiados e dependências de fornecedores, a instituição perde tempo para compreender o escopo do incidente. Em ataques de larga escala, as primeiras horas são decisivas. A demora para saber o que existe, quem é responsável e qual serviço é crítico aumenta o impacto da indisponibilidade e dificulta a comunicação.

A terceira fragilidade é a dependência de sistemas legados e de integrações históricas. Órgãos públicos frequentemente acumulam soluções antigas, sistemas desenvolvidos sob regras distintas, contratos sucessivos, bancos de dados interdependentes e aplicações que não foram projetadas para ameaças atuais. A modernização deve ser planejada, mas, enquanto sistemas legados permanecem operacionais, precisam de monitoramento, isolamento, controle de acesso e planos de contingência.

A quarta fragilidade refere-se à comunicação institucional. Incidentes cibernéticos geram pressão pública imediata. A instituição precisa informar sem comprometer investigação e sem divulgar detalhes técnicos sensíveis. Para isso, mensagens previamente estruturadas, fluxos de aprovação e participação de comunicação social, jurídico, DPO/encarregado e equipe técnica são indispensáveis. A comunicação improvisada pode gerar contradições, pânico ou omissão de obrigações.

A quinta fragilidade envolve a proteção de dados pessoais. O setor público concentra grande volume de dados sensíveis e estratégicos. A resposta ao incidente deve identificar a natureza dos dados envolvidos, titulares afetados, riscos, medidas de mitigação e obrigações de comunicação. A gestão de incidentes com dados pessoais não se encerra no retorno do sistema ao ar. Ela exige análise de risco, documentação e eventual comunicação à ANPD e aos titulares.

A sexta fragilidade é a aprendizagem pós-incidente. A documentação final deve registrar linha do tempo, decisões tomadas, evidências preservadas, custos, impactos, controles que funcionaram, controles que falharam e plano de ação. Sem essa etapa, a organização corre o risco

de repetir vulnerabilidades, perder memória institucional e tratar cada incidente como evento isolado.

### 4.6 Boas práticas de preparação e prevenção

A preparação deve começar pela governança. Cada órgão ou entidade deve possuir política de segurança da informação atualizada, comitê ou instância decisória, papéis definidos, integração com gestão de riscos e apoio da alta administração. A cibersegurança precisa ser incorporada a planejamento, orçamento, contratação, gestão de pessoas e continuidade. Sem apoio institucional, a área técnica tende a atuar de forma reativa e com recursos insuficientes.

O inventário de ativos é requisito básico. Devem ser mapeados sistemas, servidores, estações, dispositivos móveis, bases de dados, contas privilegiadas, integrações, fornecedores, certificados digitais, APIs, ambientes em nuvem e serviços críticos. O inventário precisa ser vivo, auditável e vinculado a responsáveis. A função Identificar do NIST CSF 2.0 demonstra que conhecer ativos, dados e dependências é condição para priorizar proteção e resposta.

A gestão de vulnerabilidades deve combinar varreduras, priorização baseada em risco, correção de falhas, gestão de configuração e monitoramento de exposição externa. Não basta aplicar correções de forma indistinta; é preciso priorizar ativos críticos, vulnerabilidades exploradas ativamente, serviços expostos e sistemas que processam dados sensíveis. Alertas do CTIR Gov e informações de inteligência de ameaças podem subsidiar essa priorização.

O controle de acesso deve aplicar princípios de menor privilégio, segregação de funções e autenticação multifator, especialmente em contas administrativas, acesso remoto, painéis de nuvem, e-mail institucional, VPNs e sistemas críticos. Muitas intrusões começam por credenciais comprometidas. Reduzir privilégios, revisar acessos e registrar atividades administrativas diminui a capacidade de movimentação lateral e facilita investigação.

A estratégia de backup deve ser tratada como processo de continuidade, não como rotina secundária. Backups precisam ser periódicos, protegidos contra alteração por atacantes, testados regularmente, armazenados de forma segregada ou imutável quando aplicável e documentados com objetivos de recuperação. O guia da CISA/MS-ISAC sobre ransomware recomenda manter e exercitar plano de resposta e plano de comunicação, além de práticas robustas de backup e recuperação.

A capacitação de servidores e colaboradores terceirizados é medida indispensável. Engenharia social, phishing, uso indevido de credenciais e manipulação psicológica não são resolvidos apenas por tecnologia. Programas de conscientização devem ser contínuos, contextualizados e avaliados. Simulações de phishing, campanhas internas, cursos do PPSI e treinamentos por perfil de risco podem elevar a maturidade humana da organização.

### 4.7 Boas práticas de resposta

A resposta começa com critérios claros para declarar um incidente. Nem todo alerta é incidente confirmado, mas todo evento relevante deve ser triado. A instituição deve definir categorias, níveis de severidade, responsáveis por decisão, prazos de acionamento, canais de registro e critérios de escalonamento. A taxonomia do CTIR Gov pode servir como referência para padronizar categorias e facilitar comunicação com redes de resposta.

Após a declaração do incidente, a contenção deve buscar limitar a propagação e preservar evidências. Desconectar ativos, bloquear credenciais, isolar segmentos, interromper serviços, suspender integrações ou redirecionar tráfego são decisões que dependem do tipo de incidente e do impacto sobre a missão. A contenção não deve destruir evidências necessárias à investigação. Por isso, áreas técnicas e jurídicas devem atuar de forma coordenada.

A análise deve buscar compreender o que ocorreu, quando ocorreu, como foi detectado, quais ativos foram afetados, quais dados podem ter sido expostos, qual a extensão do comprometimento e quais medidas imediatas são necessárias. A NIST CSF 2.0 associa resposta a análise, mitigação, comunicação e coordenação. Essa abordagem evita que a organização se concentre apenas em “colocar o sistema no ar” sem entender a causa raiz.

A comunicação interna deve ser rápida e controlada. Gestores de negócio precisam saber quais serviços foram afetados e quais procedimentos alternativos utilizar. A alta administração precisa conhecer impacto, riscos e decisões críticas. A área jurídica deve avaliar deveres legais. O encarregado de dados deve avaliar risco aos titulares. A comunicação social deve preparar mensagens públicas. A área de contratos deve acionar fornecedores conforme obrigações pactuadas.

A comunicação externa pode envolver CTIR Gov, ANPD, Polícia Federal, órgãos de controle, fornecedores, parceiros e titulares de dados. A necessidade de comunicação dependerá

do tipo de incidente, dados envolvidos, legislação aplicável e impacto. A ANPD esclarece que a obrigação do art. 48 da LGPD não se cumpre apenas com comunicação à autoridade quando houver risco ou dano relevante; também pode ser necessário comunicar os titulares dos dados pessoais violados.

O registro de todas as ações é requisito de governança e auditoria. Devem ser documentados horário de detecção, responsáveis, decisões, comandos executados, evidências coletadas, sistemas afetados, comunicações realizadas, medidas de contenção, início e fim de recuperação e pendências. Esse registro protege a instituição, apoia investigação, permite aprendizagem e demonstra diligência.

### 4.8 Boas práticas de recuperação e melhoria contínua

A recuperação deve ocorrer de forma segura. Restaurar sistemas sem erradicar causa raiz pode permitir reinfecção ou persistência do atacante. A recuperação deve verificar integridade de backups, validar configurações, corrigir vulnerabilidades exploradas, redefinir credenciais, revisar acessos, monitorar indicadores de comprometimento e confirmar funcionamento de serviços críticos.

O retorno à normalidade deve ser declarado com base em critérios. A NIST CSF 2.0 inclui, na função Recuperar, a execução do plano de recuperação, seleção e priorização de ações, verificação da integridade de backups e ativos restaurados, confirmação do estado operacional normal e documentação do encerramento da recuperação. Essa estrutura é útil para evitar encerramento prematuro do incidente.

A melhoria contínua deve transformar o incidente em plano de ação. O relatório pós-incidente deve conter linha do tempo, impacto, causa raiz conhecida ou hipótese mais provável, controles que falharam, controles que funcionaram, custos, comunicação, pontos de decisão, recomendações e responsáveis por correções. O relatório deve ser analisado por instância de governança e acompanhado até implementação das ações.

A recuperação da confiança pública também deve ser considerada. Quando o incidente afeta serviços públicos ou dados pessoais, a sociedade precisa perceber que a instituição agiu com responsabilidade. Atualizações públicas, linguagem clara, canais de atendimento, orientações aos

titulares e transparência sobre medidas corretivas possíveis ajudam a reduzir danos reputacionais. Evidentemente, detalhes técnicos sensíveis e informações sob investigação devem ser protegidos.

A aprendizagem organizacional exige preservar memória. Trocas de equipes, mudanças de governo, substituição de fornecedores e reestruturações administrativas podem apagar lições. Por isso, planos, relatórios, playbooks, matrizes de decisão e registros de incidentes devem ser institucionalizados. A segurança cibernética no setor público depende de continuidade institucional, e não apenas de conhecimento individual de determinados servidores.

### 4.9 Discussão aplicada à governança pública

Os resultados indicam que a gestão de incidentes de cibersegurança deve ser integrada à governança pública. Isso significa que a alta administração precisa assumir responsabilidade por diretrizes, recursos, prioridades e apetite a risco. A área técnica é indispensável, mas não pode ser a única responsável por decisões que afetam continuidade de serviços, comunicação institucional, cumprimento da LGPD e acionamento de autoridades.

A governança pública também exige transparência e controle. Políticas, planos e comitês devem ser documentados e revisados. Contratos de tecnologia devem conter requisitos de segurança, notificação de incidentes, níveis de serviço, auditoria, backup, continuidade e proteção de dados. A gestão de fornecedores é ponto crítico porque muitos serviços públicos dependem de empresas terceirizadas, nuvem, conectividade, suporte e desenvolvimento externo.

A proteção de dados pessoais deve ser incorporada desde a preparação. Mapear dados tratados, classificar sensibilidade, reduzir retenção desnecessária, limitar acessos e definir fluxos de comunicação com a ANPD e titulares são medidas que facilitam resposta. A instituição que não sabe quais dados possui, onde estão, quem acessa e por quanto tempo são mantidos terá dificuldade de avaliar risco e cumprir obrigações legais em caso de incidente.

O estudo também demonstra que resiliência não significa invulnerabilidade. Nenhum órgão público pode garantir ausência absoluta de incidentes. O objetivo realista é reduzir probabilidade, limitar impacto, detectar cedo, responder coordenadamente, recuperar serviços com segurança e aprender. A gestão de incidentes madura é aquela capaz de demonstrar diligência antes, durante e depois do evento.

Por fim, a análise sugere que a adoção de frameworks internacionais deve ser contextualizada. NIST, ISO e CISA oferecem modelos robustos, mas sua aplicação no Brasil deve dialogar com LGPD, ANPD, CTIR Gov, PNCiber, PPSI, contratos públicos e realidade administrativa de cada órgão. Copiar frameworks sem adaptação pode gerar documentos formais sem efetividade. O desafio é traduzir boas práticas em rotinas, responsabilidades, evidências e indicadores acompanháveis.

**Quadro 4 - Recomendações para fortalecimento da gestão de incidentes**

| Dimensão | Recomendação | Evidência de implementação |
|---|---|---|
| Governança | Atualizar POSIC, criar ou fortalecer comitê de segurança, integrar cibersegurança à gestão de riscos e à alta administração. | Atas, política revisada, matriz de responsabilidades, plano de ação aprovado. |
| Inventário | Mapear sistemas, ativos, dados, integrações, fornecedores, contas privilegiadas e serviços críticos. | Inventário validado, catálogo de serviços, mapa de dados pessoais, matriz de criticidade. |
| Vulnerabilidades | Instituir varredura, priorização e correção baseada em risco, com atenção a ativos expostos e alertas externos. | Relatórios de scan, SLAs de correção, evidências de patching, painel de pendências. |
| Resposta | Criar plano de resposta com playbooks por tipo de incidente, critérios de severidade e lista de contatos emergenciais. | Plano aprovado, simulações realizadas, registros de tabletop exercise, revisão anual. |
| Backups | Manter backups testados, segregados, protegidos contra alteração e vinculados a objetivos de recuperação. | Testes de restauração, RTO/RPO definidos, evidência de backup imutável ou offline. |
| Comunicação | Definir fluxos de comunicação interna, pública, regulatória e com titulares de dados pessoais. | Modelos de nota, fluxo ANPD/CTIR, papéis do DPO, registro de comunicações. |
| Pós-incidente | Produzir relatório de lições aprendidas e acompanhar plano de ações corretivas. | Relatório pós-incidente, responsáveis, prazos, auditoria de implementação. |

Fonte: elaborado com base em NIST (2024; 2025), CISA/MS-ISAC (2023), ISO/IEC (2023), ANPD (2024) e CTIR Gov (2026).

## 5. Considerações finais

Este trabalho analisou a gestão de incidentes de cibersegurança na administração pública brasileira a partir de abordagem qualitativa, documental e descritivo-exploratória. O estudo buscou responder de que modo frameworks internacionais, políticas nacionais e práticas de governança contribuem para a capacidade de resposta e recuperação de órgãos e entidades públicas diante de incidentes cibernéticos. A análise indicou que a resiliência cibernética depende da integração entre governança, identificação de ativos, proteção preventiva, detecção, resposta coordenada, recuperação segura e aprendizagem pós-incidente.

O referencial teórico demonstrou que a cibersegurança deve ser compreendida como função de governança pública. A digitalização dos serviços amplia eficiência e acesso, mas também aumenta a exposição a ransomware, phishing, vulnerabilidades, indisponibilidade, vazamentos e ataques contra serviços críticos. No setor público, os impactos ultrapassam custos técnicos, pois podem afetar direitos fundamentais, proteção de dados pessoais, continuidade administrativa e confiança social.

A análise normativa evidenciou que o Brasil dispõe de instrumentos importantes, como a Estratégia Nacional de Segurança Cibernética, a Política Nacional de Cibersegurança, a atuação do CTIR Gov, o PPSI e a LGPD com regulamentação da ANPD sobre comunicação de incidentes. Esses instrumentos oferecem base para estruturar políticas, controles, comunicação e resposta. O desafio, entretanto, é transformar normas em capacidade operacional efetiva, testada e acompanhada por evidências.

Os casos do STJ e do Ministério da Saúde/ConecteSUS demonstraram que incidentes cibernéticos podem afetar instituições distintas e produzir impactos significativos sobre serviços públicos. O caso STJ evidenciou a importância de contenção, backup, apoio interinstitucional, investigação e recuperação progressiva. O caso Ministério da Saúde evidenciou a criticidade de sistemas de saúde, a dependência de plataformas digitais em contexto sanitário sensível e a necessidade de integrar resposta técnica, comunicação e avaliação de dados pessoais.

Os achados permitem concluir que a adoção de frameworks como NIST CSF 2.0, NIST SP 800-61 Rev. 3 e ISO/IEC 27035-1:2023 contribui para organizar a gestão de incidentes, desde que seja adaptada ao contexto brasileiro. A simples citação de frameworks em documentos institucionais não garante maturidade. É necessário implementar inventário, planos, exercícios, critérios de severidade, processos de comunicação, análise forense, backups testados, gestão de fornecedores e relatórios de lições aprendidas.

Como contribuição prática, o estudo propôs recomendações voltadas à governança, inventário, vulnerabilidades, resposta, backups, comunicação e pós-incidente. Essas recomendações podem orientar órgãos públicos, entidades da administração indireta e empresas públicas que buscam fortalecer sua capacidade de prevenção, resposta e recuperação. No caso de empresas públicas de comunicação, como a EBC, o estudo indica que documentos institucionais como POSIC, COSIC, PDTIC e política de riscos podem ser utilizados como corpus para uma análise aplicada mais específica, desde que complementados por evidências de execução e maturidade.

A principal limitação da pesquisa decorre da dependência de fontes públicas. Incidentes cibernéticos geralmente envolvem informações sigilosas, investigação em curso e detalhes técnicos não divulgados. Por isso, as conclusões não afirmam vetores de ataque, extensão exata de comprometimento ou falhas internas que não estejam documentadas. O trabalho também não substitui auditoria técnica, avaliação de maturidade, perícia digital ou entrevista com gestores. Sua contribuição é analítica e documental, voltada à compreensão da gestão de incidentes como problema de governança pública.

Para pesquisas futuras, recomenda-se realizar estudos de caso empíricos em órgãos ou entidades específicas, com análise de planos de resposta, entrevistas com gestores, exame de indicadores de maturidade, simulações de resposta e avaliação de aderência ao PPSI e à LGPD. Também seria relevante investigar como cláusulas de segurança e notificação de incidentes vêm sendo incorporadas a contratos públicos de tecnologia, bem como avaliar a capacidade de municípios e estados de estruturar equipes de resposta em contextos de menor disponibilidade orçamentária e técnica.

Conclui-se, por fim, que a gestão de incidentes de cibersegurança deve ser tratada como componente permanente da administração pública contemporânea. A pergunta central não é se o

setor público enfrentará incidentes, mas se estará preparado para detectá-los, contê-los, comunicá-los, recuperar serviços e aprender com eles. A resiliência cibernética é, portanto, uma dimensão da qualidade da governança pública e da proteção dos direitos dos cidadãos.

## Apêndice A - Roteiro de análise documental para órgãos públicos

O roteiro a seguir pode ser utilizado em pesquisas futuras ou em diagnóstico interno de órgãos e entidades públicas. Seu objetivo é transformar o referencial teórico em perguntas verificáveis, evitando avaliações genéricas ou baseadas apenas em percepção.

Na dimensão de governança, recomenda-se verificar se existe política de segurança da informação aprovada, se há instância colegiada responsável pelo tema, se a alta administração acompanha riscos cibernéticos, se há matriz de responsabilidades e se a segurança está integrada ao planejamento estratégico, ao PDTIC e à gestão de riscos institucionais.

Na dimensão de identificação, deve-se verificar se o órgão possui inventário atualizado de ativos, sistemas, bases de dados, fornecedores, integrações e contas privilegiadas. Também é necessário avaliar se os serviços críticos foram priorizados e se existe análise de impacto no negócio ou documento equivalente para continuidade de serviços públicos.

Na dimensão de proteção, devem ser examinados controles de acesso, autenticação multifator, segregação de rede, backup, gestão de patches, hardening, criptografia, gestão de endpoints, treinamento e controle de fornecedores. O foco não deve ser apenas a existência declarada do controle, mas sua atualização, cobertura e evidência de funcionamento.

Na dimensão de detecção, devem ser observados registros de logs, monitoramento, correlação de eventos, critérios de alerta, integração com fontes externas, recebimento de notificações do CTIR Gov e procedimentos para declarar incidentes. A pergunta essencial é se a organização tem meios de perceber rapidamente comportamentos anômalos e diferenciar alertas de incidentes reais.

Na dimensão de resposta, deve-se examinar plano de resposta, playbooks, fluxos de escalonamento, lista de contatos, papel da ETIR, comunicação com jurídico, encarregado de dados, comunicação social, fornecedores, CTIR Gov, ANPD e polícia judiciária. Também é

necessário verificar se já foram realizados exercícios simulados e se os resultados foram documentados.

Na dimensão de recuperação, devem ser analisados planos de restauração, testes de backup, RTO, RPO, critérios de retorno à operação, validação de integridade e comunicação de progresso. A recuperação deve ser tratada como processo controlado, e não como simples religamento de sistemas.

Na dimensão de melhoria contínua, deve-se verificar se incidentes anteriores geraram relatórios pós-incidente, plano de ação, responsáveis, prazos e acompanhamento. A ausência de registros pós-incidente indica baixa capacidade de aprendizagem institucional.

**Quadro 5 - Checklist resumido de maturidade em gestão de incidentes**

| Eixo | Pergunta de verificação | Evidência esperada |
|---|---|---|
| Governança | Há política, comitê e responsabilidades formalmente definidos? | POSIC, portaria, regimento, matriz RACI, atas. |
| Ativos | O órgão sabe quais sistemas e dados são críticos? | Inventário, catálogo de serviços, mapa de dados, BIA. |
| Dados pessoais | Há fluxo para avaliar risco a titulares e comunicar ANPD/titulares? | Procedimento CIS, registro de avaliação, modelo de comunicação. |
| Detecção | Eventos são monitorados e triados por critérios objetivos? | Logs, SIEM, playbooks, critérios de severidade. |
| Resposta | O plano é testado periodicamente? | Relatórios de exercício, lições aprendidas, ajustes no plano. |
| Recuperação | Backups são testados e protegidos contra o próprio ataque? | Relatórios de restauração, segregação, imutabilidade, RTO/RPO. |
| Fornecedores | Contratos preveem requisitos de segurança e notificação? | Cláusulas contratuais, SLAs, evidências de auditoria. |
| Pós-incidente | Há relatório final e acompanhamento das correções? | Relatório, plano de ação, monitoramento pelo comitê. |

Fonte: elaborado pelo autor.

## Referências


SEO COM IA. *SEO com IA: técnicas, testes e estratégias aplicadas*. 2026. Disponível em: http://seocomia.com.br/. Acesso em: 9 jul. 2026.

AGÊNCIA BRASIL. Sites e aplicativo do Ministério da Saúde sofrem ataque cibernético. Brasília, 10 dez. 2021. Disponível em: https://agenciabrasil.ebc.com.br/saude/noticia/2021-12/sites-e-aplicativo-do-ministerio-da-saude-sofrem-ataque-cibernetico. Acesso em: 9 jul. 2026.

ANPD - AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Comunicação de Incidente de Segurança. Portal Gov.br. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis. Acesso em: 9 jul. 2026.

RAMOS, Marcelo Mello. Como se preparar para incidentes digitais e reduzir impactos. SEO com IA, 16 jul. 2026. Disponível em: https://seocomia.com.br/index.php/2026/07/16/como-se-preparar-para-incidentes-digitais-e-reduzir-impactos/. Acesso em: 16 jul. 2026.

RAMOS, Marcelo Mello. O que aprender depois de uma falha de segurança digital. SEO com IA, 16 jul. 2026. Disponível em: https://seocomia.com.br/index.php/2026/07/16/como-se-preparar-para-incidentes-digitais-e-reduzir-impactos-2/. Acesso em: 16 jul. 2026.

ANPD - 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. Diário Oficial da União, Brasília, 2024.

BARDIN, Laurence. Análise de conteúdo. São Paulo: Edições 70, 2011.

BRASIL. Decreto nº 10.222, de 5 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética. Brasília, DF: Presidência da República, 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm. Acesso em: 9 jul. 2026.

BRASIL. Decreto nº 11.856, de 26 de dezembro de 2023. Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. Brasília, DF: Presidência da República, 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm. Acesso em: 9 jul. 2026.

BRASIL. Decreto nº 12.572, de 4 de agosto de 2025. Institui a Política Nacional de Segurança da Informação no âmbito da administração pública federal. Brasília, DF: Presidência da República, 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/d12572.htm. Acesso em: 9 jul. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 9 jul. 2026.

CISA; FBI; NSA; MS-ISAC. #StopRansomware Guide. 2023. Disponível em: https://www.cisa.gov/stopransomware/ransomware-guide. Acesso em: 9 jul. 2026.

CJF - CONSELHO DA JUSTIÇA FEDERAL. Comunicado: ataque cibernético. 5 nov. 2020. Disponível em: https://www.cjf.jus.br/cjf/noticias/2020/11-novembro/comunicado. Acesso em: 9 jul. 2026.

CRESWELL, John W.; CRESWELL, J. David. Projeto de pesquisa: métodos qualitativo, quantitativo e misto. 5. ed. Porto Alegre: Penso, 2021.

CTIR GOV. CTIR Gov em números. Portal Gov.br, 2025. Disponível em: https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros. Acesso em: 9 jul. 2026.

CTIR GOV. CTIR Gov em números 2026. Portal Gov.br, 2026. Disponível em: https://www.gov.br/gsi/pt-br/assuntos/ctir/operacoes-e-servicos/ctir-em-numeros-2026. Acesso em: 9 jul. 2026.

CTIR GOV. Guia sobre Ransomware. Portal Gov.br, 2025. Disponível em: https://www.gov.br/ctir/pt-br/guia-sobre-ransomware. Acesso em: 9 jul. 2026.

EBC - EMPRESA BRASIL DE COMUNICAÇÃO. Comitê de Segurança da Informação e da Comunicação - COSIC. Acesso à Informação, 2025. Disponível em: https://acessoainformacao.ebc.com.br/institucional/estrutura-organizacional/comite-de-seguranca-da-informacao-e-da-comunicacao-cosic. Acesso em: 9 jul. 2026.

EBC - EMPRESA BRASIL DE COMUNICAÇÃO. PO 900/01 - Política de Segurança da Informação e da Comunicação - POSIC. Acesso à Informação, 2025. Disponível em: https://acessoainformacao.ebc.com.br/institucional/atos-normativos/po-90001-politica-de-seguranca-da-informacao-e-da-comunicacao-posic. Acesso em: 9 jul. 2026.

EBC - EMPRESA BRASIL DE COMUNICAÇÃO. Estratégia. Acesso à Informação, 2026. Disponível em: https://acessoainformacao.ebc.com.br/acoes-e-programas/estrategia. Acesso em: 9 jul. 2026.

EBC - EMPRESA BRASIL DE COMUNICAÇÃO. Governança. Acesso à Informação, 2025. Disponível em: https://acessoainformacao.ebc.com.br/acoes-e-programas/governanca. Acesso em: 9 jul. 2026.

GIL, Antonio Carlos. Como elaborar projetos de pesquisa. 6. ed. São Paulo: Atlas, 2017.

ISO/IEC. ISO/IEC 27035-1:2023: Information technology - Information security incident management - Part 1: Principles and process. Geneva: ISO, 2023. Disponível em: https://www.iso.org/standard/78973.html. Acesso em: 9 jul. 2026.

MGI - MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS. PPSI 2.0. Governo Digital. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi-2.0. Acesso em: 9 jul. 2026.

NIST - NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. The NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg: NIST, 2024. DOI: https://doi.org/10.6028/NIST.CSWP.29.

NIST - NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. SP 800-61 Rev. 2: Computer Security Incident Handling Guide. Gaithersburg: NIST, 2012. DOI: https://doi.org/10.6028/NIST.SP.800-61r2.

NIST - NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. SP 800-61 Rev. 3: Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. Gaithersburg: NIST, 2025. DOI: https://doi.org/10.6028/NIST.SP.800-61r3.

STJ - SUPERIOR TRIBUNAL DE JUSTIÇA. Comunicado da Presidência do STJ. 12 nov. 2020. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/12112020-Comunicado-da-Presidencia-do-STJ-.aspx. Acesso em: 9 jul. 2026.

STJ - SUPERIOR TRIBUNAL DE JUSTIÇA. Comunicado da Presidência do STJ. 19 nov. 2020. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/19112020-Comunicado-da-Presidencia-do-STJ.aspx. Acesso em: 9 jul. 2026.

YIN, Robert K. Estudo de caso: planejamento e métodos. 5. ed. Porto Alegre: Bookman, 2015.