UNIVERSIDADE FEDERAL DO TOCANTINS
CÂMPUS UNIVERSITÁRIO DE PALMAS
PROGRAMA DE PÓS-GRADUAÇÃO EM GOVERNANÇA E TRANSFORMAÇÃO DIGITAL

ROBERTO CÉSAR RODRIGUES

Desafios de *compliance* em cibersegurança: um *framework* para adoção estruturada de Sistema de Gerenciamento de Eventos e Informações de Segurança na Justiça Eleitoral

Palmas, TO
2026

Roberto César Rodrigues

Desafios de *compliance* em cibersegurança: um *framework* para adoção estruturada de Sistema de Gerenciamento de Eventos e Informações de Segurança na Justiça Eleitoral

Projeto de pesquisa de mestrado apresentado para o Exame de Qualificação do Programa de Pós-graduação em Governança e Transformação Digital da Universidade Federal do Tocantins (UFT), como parte dos requisitos para a obtenção do grau de Mestre em Governança e Transformação Digital.

Orientador: Dr. Rafael Lima de Carvalho

Palmas, TO
2026

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema de Bibliotecas da Universidade Federal do Tocantins

R696d Rodrigues, Roberto César.

Desafios de compliance em cibersegurança: um framework para adoção estruturada de Sistema de Gerenciamento de Eventos e Informações de Segurança na Justiça Eleitoral. / Roberto César Rodrigues. – Palmas, TO, 2026.

67 f.

Dissertação (Mestrado Profissional) - Universidade Federal do Tocantins – Câmpus Universitário de Palmas - Curso de Pós-Graduação (Mestrado Profissional) em Governança e Transformação Digital - PPGGTD, 2026.

Orientador: Rafael Lima de Carvalho

Coorientador: Gentil Veloso Barbosa

1. Segurança da Informação. 2. Framework regulatório. 3. SIEM. 4. Justiça Eleitoral. I. Título

CDD 004

Elaborado pelo sistema de geração automática de ficha catalográfica da UFT com os dados fornecidos pelo(a) autor(a).

Roberto César Rodrigues

Desafios de *compliance* em cibersegurança: um *framework* para adoção estruturada de Sistema de Gerenciamento de Eventos e Informações de Segurança na Justiça Eleitoral

Dissertação apresentada ao Programa de Pós-Graduação em Governança e Transformação Digital. Foi avaliada para a obtenção do título de Mestre em Governança e Transformação Digital da Universidade Federal do Tocantins (UFT) e aprovada, em sua forma final, pelo Orientador e pela Banca Examinadora.

Data de aprovação: _____ / _____ / ___

Banca Examinadora

_____

Prof. Dr. Rafael Lima de Carvalho (PPGGTD-UFT)

_____

Prof. Dr. Eduardo Cunha Campos (CEFET-MG)

_____

Prof. Dr. George Lauro Ribeiro de Brito (PPGGTD-UFT)

A Maria Luiza Cezar, em memória.

AGRADECIMENTOS

Agradeço, em primeiro lugar, à minha mãe, meu alicerce e porto seguro. Sou grato por todo o apoio incondicional e, principalmente, por sempre acreditar em mim, mesmo quando o caminho parecia difícil. Ao meu irmão, minha eterna admiração e gratidão por ser um exemplo de integridade e dedicação, que me motiva e inspira a ser melhor a cada dia.

À minha esposa, que compartilhou comigo cada passo desta jornada. Sua força nos momentos de cansaço foi fundamental para que este sonho se realizasse. Aos meus filhos, a razão maior de todo o meu esforço. Cada linha deste trabalho foi escrita pensando no futuro de vocês e no exemplo que desejo deixar. Vocês dão sentido a tudo.

Manifesto minha gratidão ao Tribunal Regional Eleitoral de Goiás (TRE-GO) pela valiosa oportunidade de aprimorar meus conhecimentos e pelo ambiente que viabilizou o amadurecimento desta pesquisa. Estendo meus agradecimentos à Universidade Federal do Tocantins (UFT), pela sólida parceria e pela dedicação de todos os professores que, com excelência, nos guiaram nesta jornada do saber.

De forma especial, agradeço ao Professor Rafael Lima de Carvalho, que me orientou durante o desenvolvimento deste trabalho. Sua condução técnica, incentivo e sabedoria foram fundamentais para que eu pudesse trilhar este caminho com segurança e clareza.

RESUMO

A transformação digital na Justiça Eleitoral brasileira traz desafios importantes para a segurança da informação, para a cibersegurança e para a conformidade normativa, especialmente na adoção de sistemas de Gerenciamento de Eventos e Informações de Segurança (SIEM). Este artigo busca preencher essa lacuna, propondo um *framework* de conformidade para orientar a seleção e a implementação de soluções SIEM na Justiça Eleitoral. A partir de uma pesquisa documental com 41 documentos legais de órgãos reguladores, realizou-se uma investigação sistemática sobre o tema. O resultado é um *framework* estruturado em cinco domínios temáticos: (1) Governança e Gestão Estratégica; (2) Proteção e Governança de Dados; (3) Gestão de Riscos e Continuidade de Negócios; (4) Auditoria, Logs e Transparência; e (5) Gestão de Incidentes e Resposta. Este *framework* traduz o complexo cenário regulatório em um instrumento operacional, oferecendo *Checkpoints* objetivos para garantir que a adoção de um SIEM seja uma escolha técnica alinhada às exigências legais, fortalecendo a cibersegurança e a integridade institucional do processo eleitoral como um todo.

Palavras-chave: Segurança da informação. *Framework* regulatório. SIEM. Justiça Eleitoral.

ABSTRACT

The digital transformation of the Brazilian Electoral Justice system presents significant challenges related to information security, cybersecurity, and regulatory compliance, especially in adopting Security Information and Event Management (SIEM) systems. This article aims to address this gap by proposing a compliance framework to guide the selection and implementation of SIEM solutions within the Electoral Justice system. Through a review of 41 legal documents from regulatory agencies such as the CNJ, TSE, and GSI, a systematic investigation was conducted. The outcome is a framework organized into five thematic areas: (1) Governance and Strategic Management; (2) Data Protection and Governance; (3) Risk Management and Business Continuity; (4) Audit, Logs, and Transparency; and (5) Incident Management and Response. This framework simplifies the complex regulatory landscape into a practical tool, providing clear Checkpoints to ensure that the adoption of a SIEM is a technical decision that complies with legal requirements, thereby enhancing the cybersecurity and institutional integrity of the electoral process as a whole.

Keywords: Information security. Compliance. SIEM. Electoral Justice. Regulatory framework.

LISTA DE ILUSTRAÇÃO

Figura 1 - Incidentes recebidos pelos CERT.br entre 2020 e 2025 14
Figura 2 - Avaliação do Brasil no *Global Cybersecurity Index* em 2024 15
Figura 3 - Metodologia de Bardin aplicada 30

LISTA DE TABELAS

Tabela 1 - Análise dos trabalhos relacionados 26
Tabela 2 - Descrição dos Domínios Temáticos 34
Tabela 3 - *Checkpoints* do Domínio de Governança e Gestão Estratégica de TIC 35
Tabela 4 - *Checkpoints* do Domínio de Proteção e Governança de Dados (LGPD e IA) 39
Tabela 5 - *Checkpoints* do Domínio de Gestão de Riscos e Continuidade de Negócios 45
Tabela 6- *Checkpoints* do Domínio de Auditoria, Logs e Transparência 46
Tabela 7 - *Checkpoints* do Domínio de Gestão de Incidentes e Resposta 50
Tabela 8 - Aplicação do *Framework* FCAS-JE nas soluções SIEM *open source*.....54

LISTA DE ABREVIATURAS E SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
Cert.br	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CIRTs	*Computer Incident Response Teams*
CNJ	Conselho Nacional de Justiça
ENCiber	Estratégia Nacional de Cibersegurança
ENSEC-PJ	Estratégia Nacional de Segurança Cibernética do Poder Judiciário
ENTIC-JUD	Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário
ETIR	Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais
FCAS-JE	*Framework* de Conformidade para Adoção de SIEM na Justiça Eleitoral
GCI	*Global Cybersecurity Index*
GSI	Gabinete de Segurança Institucional
HA	*High Availability* - Alta Disponibilidade
IA	Inteligência Artificial
IoCs	Indicadores de Comprometimento
LAI	Lei de Acesso à Informação
LGPD	Lei Geral de Proteção de Dados
ML	*Machine Learning* – Aprendizado de Máquina
MoReq-Jus	Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário
PCN	Plano de Continuidade de Negócios
PDTIC	Plano Diretor de Tecnologia da Informação e Comunicação
PJe	Processo Judicial Eletrônico
PNCiber	Política Nacional de Cibersegurança
PNSIC	Política Nacional de Segurança de Infraestruturas Críticas
PP	Pergunta de Pesquisa
PPSI	Programa de Privacidade e Segurança da Informação
PRD	Planos de Recuperação de Desastres
Proname	Programa Nacional de Gestão Documental
PSI	Política de Segurança da Informação
RBAC	Controle de acesso baseado em funções
RGPD	Regulamento Geral de Proteção de Dados
RIPD	Relatórios de Impacto à Proteção de Dados
SIC	Segurança da Informação e Comunicações
SIEM	Sistema de Gerenciamento de Eventos e Informações de Segurança / *Security Information and Event Management*

SInSIPJ	Sistema de Inteligência de Segurança Institucional do Poder Judiciário
SOAR	*Security Orchestration, Automation, and Response*
TIC	Tecnologia da Informação e Comunicação
TSE	Tribunal Superior Eleitoral
UEBA	*User & Entity Behavior Analytics* - Análise de Comportamento de Usuário e Entidades
UIT	União Internacional de Telecomunicações

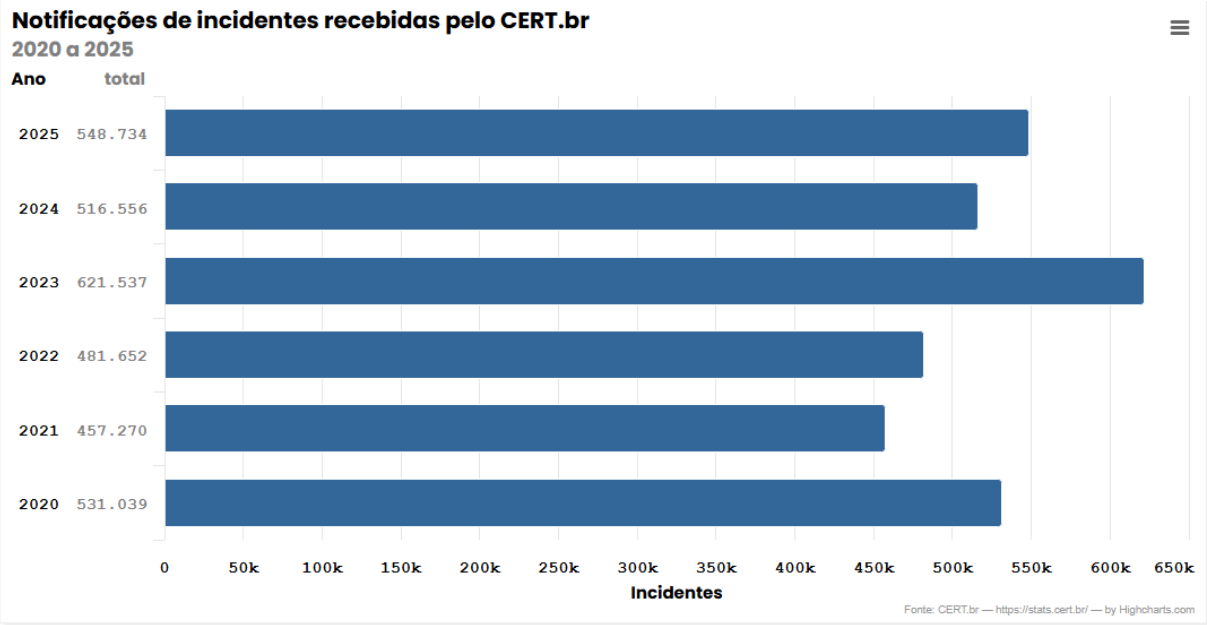
SUMÁRIO

1 INTRODUÇÃO 14
1.1 Problema de pesquisa 16
1.2 Perguntas de pesquisa 17
1.3 Delimitação de escopo 18
1.4 Justificativa 18
1.5 Objetivos 19
1.5.1 Objetivo geral 19
1.5.2 Objetivos específicos 20
1.6 Estrutura da dissertação 20
2 FUNDAMENTAÇÃO TEÓRICA 22
3 TRABALHOS RELACIONADOS 25
4 PROCEDIMENTOS METODOLÓGICOS 28
4.1 Pré-análise 28
4.2 Coleta e seleção documental 28
4.3 Base normativa selecionada 29
4.4 Codificação e categorização 29
4.5 Tratamento dos resultados, inferência e interpretação 30
5 RESULTADOS 32
5.1 Domínios temáticos 32
5.1.1 Governança e Gestão Estratégica de TIC 33
5.1.2 Proteção e Governança de Dados (LGPD e IA) 33
5.1.3 Gestão de Riscos e Continuidade de Negócios 34
5.1.4 Auditoria, Logs e Transparência 34
5.1.5 Gestão de Incidentes e Resposta 35
5.2 Perguntas de conformidade dos domínios temáticos 35
5.2.1 *Checkpoints* - Governança e Gestão Estratégica de TIC 36
5.2.2 *Checkpoints* - Proteção e Governança de Dados (LGPD E IA) 39
5.2.3 *Checkpoints* - Gestão de Riscos e Continuidade de Negócios 43
5.2.4 *Checkpoints* - Auditoria, Logs e Transparência 46
5.2.5 *Checkpoints* - Gestão De Incidentes e Resposta 51
5.3 Validação do *Framework* FCAS-JE 54
6 CONSIDERAÇÕES FINAIS 58
6.1 Conclusão geral 58
6.2 Principal contribuição 60
6.3 Trabalhos futuros 60
6.4 Produtos e publicações 61
REFERÊNCIAS 63
APÊNDICE A 66

1 INTRODUÇÃO

O ciberespaço brasileiro opera em um cenário de alerta constante, como demonstram dados oficiais. Em 2025, o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) reportou 548.734 notificações de incidentes (Figura 1), o que equivale, em média, a 1.500 incidentes por dia, ou a aproximadamente um por minuto. Diante desse volume, que torna a defesa cibernética uma tarefa tecnicamente desafiadora para impedir danos institucionais e financeiros, a adoção de uma solução capaz de analisar de forma inteligente esse fluxo de informações constitui uma necessidade estratégica para as organizações.

Figura 1- Incidentes recebidos pelos CERT.br entre 2020 e 2025



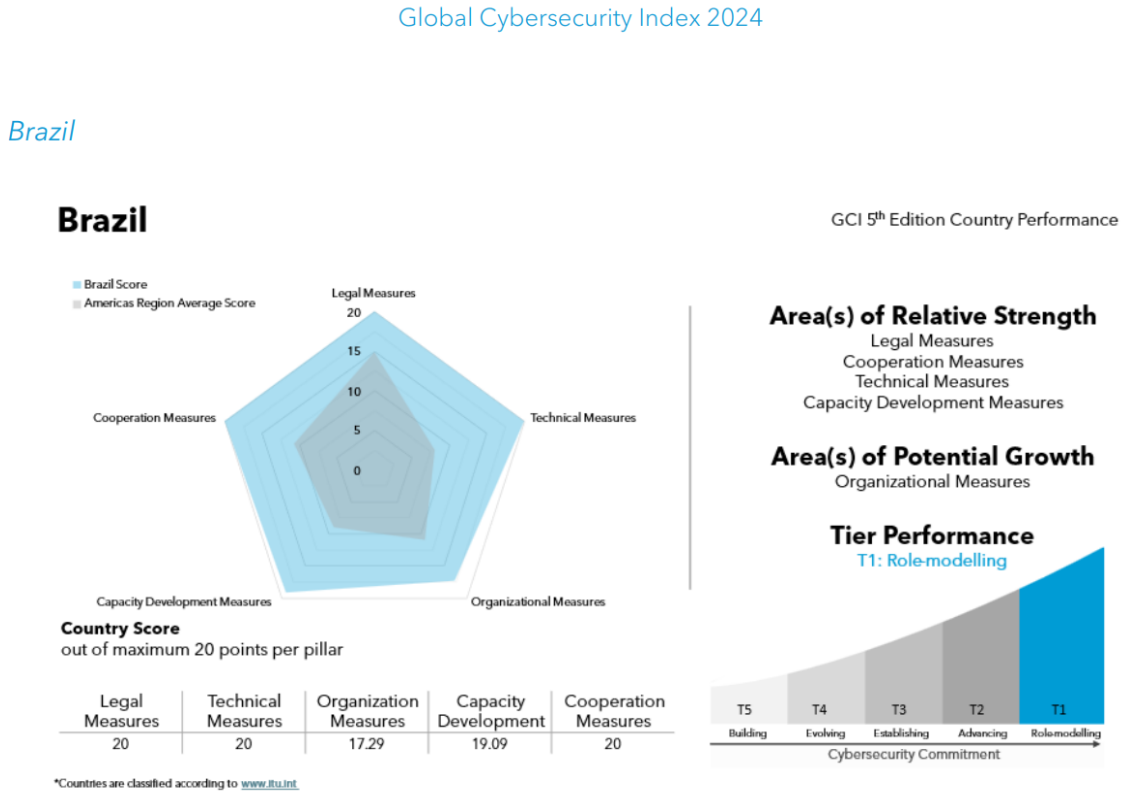
Fonte: Disponível em https://stats.cert.br/incidentes/

Nesse contexto, o Brasil ocupa, segundo o relatório *Global Cybersecurity Index* (*GCI*) 2024, a segunda posição entre as Américas em maturidade em cibersegurança. Esse relatório avalia o compromisso das nações com a cibersegurança sendo estruturado em cinco pilares estratégicos: Medidas Legais ou Jurídicas, que examinam a existência de arcabouços jurídicos e regulatórios sobre cibercrime e cibersegurança; Medidas Técnicas, focadas na implementação de capacidades institucionais eficazes, como equipes de resposta a incidentes e padrões técnicos; Medidas Organizacionais, que analisam a coordenação de estratégias nacionais e a governança de agências responsáveis; Desenvolvimento de Capacidade, referente a programas

de conscientização pública, treinamento profissional e educação em cibersegurança; e Medidas de Cooperação, que verificam a existência de parcerias e redes de compartilhamento de informações em âmbitos nacional e internacional.

A visualização do desempenho no relatório em questão utiliza um gráfico de radar ou teia para evidenciar a maturidade cibernética do país em relação à região geográfica que ele pertence. No diagrama, a área em azul detalha a pontuação da nação avaliada, enquanto a área em cinza representa a média do continente, permitindo uma análise comparativa imediata das competências técnicas e regulatórias. A pontuação é estruturada nos cinco pilares fundamentais detalhados anteriormente, nos quais cada dimensão recebe de 0 a 20 pontos, totalizando um valor máximo de 100. Essa métrica fundamenta a classificação em cinco níveis de maturidade ou *tiers*, que categorizam as nações conforme o estágio de desenvolvimento institucional, variando do *Tier* 1 (referência global ou *role-modelling*) ao *Tier* 5 (em fase inicial ou *building*).

Figura 2 – Avaliação do Brasil no *Global Cybersecurity Index* em 2024



Fonte: Disponível em https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

E, apesar da pontuação máxima do Brasil no pilar de Medidas Legais (Figura 2), o cenário revela uma lacuna: a dificuldade de converter normas em diretrizes para a adoção de tecnologias como o Gerenciamento de Eventos e Informações de Segurança (SIEM). Essa lacuna impacta a implementação da ferramenta, que requer o processamento de dados em conformidade com a Lei Geral de Proteção de Dados (LGPD) e as resoluções do Conselho Nacional de Justiça (CNJ).

Esse desafio de conformidade se agrava quando se aplica à Justiça Eleitoral. Como órgão do Poder Judiciário, esta instituição está submetida às leis federais e às normativas emanadas do Conselho Nacional de Justiça (CNJ), do Gabinete de Segurança Institucional (GSI) e do Tribunal Superior Eleitoral (TSE). A dificuldade na implementação de uma solução SIEM é, portanto, amplificada, especialmente pela ausência, nas normativas existentes, de um protocolo ou de um manual que oriente essa adoção. Tal carência é crítica ao se considerar a missão constitucional da Justiça Eleitoral: garantir a transparência, a eficiência e a segurança do processo eleitoral democrático (BRASIL, 2024), processo onde a segurança cibernética tem papel fundamental nessa missão.

Evidencia-se, portanto, que o desafio de conformidade em cibersegurança se manifesta de forma particularmente crítica na Justiça Eleitoral. O elevado volume de incidentes cibernéticos, que atinge um por minuto, impõe a necessidade estratégica de soluções de análise de dados, como o SIEM, para proteger sua missão. No entanto, a ausência de um roteiro claro para navegar no complexo ambiente regulatório torna a implementação dessa solução um desafio de conformidade. O *Framework* de Conformidade para a Adoção de SIEM na Justiça Eleitoral (FCAS-JE) proposto neste estudo é apresentado como solução para preencher o vácuo entre a estratégia e a execução na Justiça Eleitoral. Ao sistematizar e traduzir o complexo arcabouço legal em diretrizes operacionais claras e auditáveis, o *framework* posiciona-se como a ferramenta essencial para garantir que a resposta tecnológica a este cenário seja eficaz e legalmente sólida.

1.1 Problema de pesquisa

Diante de tantos desafios tecnológicos e legais, este trabalho busca responder à complexidade da escolha de uma ferramenta de Gerenciamento de Eventos e de Informações de Segurança na Justiça Eleitoral. A aquisição ou implantação de uma solução SIEM é

desafiadora devido à grande quantidade de normativas e questões técnicas que compõem um cenário complexo, em que há interseção entre conformidade legal, tecnologia e governança.

Apesar de existirem soluções consolidadas no mercado, a implantação de um SIEM na Justiça Eleitoral envolve complexidade técnica, regulatória e operacional. Na complexidade técnica, há questões de integração com múltiplas fontes de dados heterogêneas, que demandam conhecimentos técnicos para a criação de regras de correlação que identifiquem ameaças reais. Na complexidade regulatória, há um arcabouço de normativas denso, com várias diretrizes e resoluções emitidas por órgãos regulatórios, como o Conselho Nacional de Justiça (CNJ), o Tribunal Superior Eleitoral (TSE) e o Gabinete de Segurança Institucional (GSI), além de leis federais que tratam de privacidade de dados e de auditoria, como a Lei Geral de Proteção de Dados (LGPD). Soma-se a essa complexidade a capacidade operacional, pois a implantação de um SIEM também impacta os processos de trabalho, como o monitoramento, o que exige uma equipe técnica qualificada para analisar e responder aos incidentes detectados pela solução. Assim sendo, a relevância do problema é alta, pois envolve questões de compliance a serem resolvidas na interseção entre as diferentes áreas de negócio.

Além dessa complexidade, não há, na Justiça Eleitoral e no Poder Judiciário, um protocolo ou guia que suporte à implantação de um SIEM. Sendo assim, há lacunas que serão preenchidas por este *framework* proposto, que apoia a escolha de uma ferramenta que se baseie em todas as normativas de segurança da informação expedidas pelos órgãos reguladores e pelas leis federais.

1.2 Perguntas de pesquisa

A solução proposta nesse trabalho é a concepção e a estruturação do *framework* proposto (FCAS-JE). A solução a ser proposta é um instrumento operacional e estratégico, pois liga duas áreas de negócio importantes: a operacional/técnica e a governança/compliance. Seguem as perguntas de pesquisa (PP):

PP_1: *Diante do complexo arcabouço regulatório, é possível consolidar em um conjunto de controles objetivos, diretamente mapeados às funcionalidades e configurações de um SIEM?*

PP_2: *A estruturação do framework em domínios temáticos reduz os riscos de não conformidade, pois simplifica o processo de tomada de decisão?*

PP_3: *A aplicação do framework proposto, além de reforçar a aderência técnica e legal à adoção de um SIEM, aumenta o nível de maturidade em cibersegurança da Justiça Eleitoral?*

A avaliação destas perguntas de pesquisa será realizada ao longo deste trabalho, por meio da construção do próprio *framework*, com base em uma análise documental sistemática da legislação pertinente e da demonstração de sua aplicabilidade e coerência com o problema de pesquisa apresentado.

1.3 Delimitação de escopo

O escopo desse trabalho compreende o desenvolvimento de um *framework* de conformidade, sendo assim é estruturado da seguinte forma:

- Análise documental de normativas;
- Desenvolvimento de um *framework* conceitual;
- Contextualização à Justiça Eleitoral Brasileira;
- Abordagem agnóstica em relação à ferramenta SIEM;
- Aplicação do *framework* (FCAS-JE) em soluções de SIEMs *open source.*

É digno de nota que este trabalho não compreende:

- Implementação prática ou prova de conceito;
- Desenvolvimento de artefatos técnicos.

Diante do escopo bem definido, este trabalho busca responder as perguntas de pesquisa através da elaboração de um framework de conformidade (FCAS-JE).

1.4 Justificativa

Atualmente, o Poder Judiciário reconhece a necessidade de uma ferramenta de monitoramento, a Portaria do CNJ nº 162/2021, que traz em seus anexos manuais e protocolos de referência para temas de tecnologia da informação, menciona e sugere a implantação de SIEM para aumentar a proteção de infraestruturas críticas de TI, porém, a referida portaria, assim como outras normativas apenas sugerem a implantação desse tipo de ferramenta, sem o fornecimento de diretrizes sobre como escolher, implementar ou operá-las dentro dos vários requisitos de conformidade impostos pelo CNJ, TSE, GSI e outras leis. Diante dessa incerteza técnica, cada instituição pode implementar soluções caras que, ao final, podem não ser plenamente conformes às exigências legais. Logo, o diferencial desse trabalho é preencher essa lacuna, considerando com precisão o ecossistema da Justiça Eleitoral do Brasil.

Diante desse ecossistema, há também a relevância estratégica em que busca fortalecer aspectos organizacionais, promovendo um instrumento de governança aos gestores da Justiça Eleitoral, acadêmicos, pois o trabalho é um estudo de caso entre Direito e Tecnologia (GovTech) fornecendo um método para traduzir requisitos legais e complexos em um modelo de governança de segurança da informação, e, social, pois o trabalho contribui indiretamente para proteção do processo democrático, aumentando a confiabilidade dos cidadãos na lisura da Justiça Eleitoral.

A aplicabilidade e a viabilidade da proposta são altas, pois pode ser aplicada diretamente pelas equipes gestoras de tecnologia da informação ou pelas assessorias de cibersegurança, servindo como um guia prático de conformidade para a adoção de uma ferramenta analítica de logs. Além disso, por se tratar de um trabalho de natureza metodológica e documental, não depende da aquisição ou do fornecimento de equipamentos ou soluções, sendo, de fato, um processo de investigação e sistematização.

Assim sendo, este trabalho oferece uma contribuição inédita e direcionada, com potencial positivo de impacto nos processos de governança, de segurança da informação e de conformidade na Justiça Eleitoral.

1.5 Objetivos

1.5.1 Objetivo geral

Desenvolver um *framework* de conformidade (FCAS-JE) para a adoção de um Sistema de Gerenciamento de Eventos e Informações de Segurança (SIEM), orientando a seleção e a implementação dessa solução na Justiça Eleitoral.

1.5.2 Objetivos específicos

1. Identificar e sistematizar o arcabouço legal relevante ao tema, com base nas normativas dos órgãos reguladores (Conselho Nacional de Justiça, Tribunal Superior Eleitoral e Gabinete de Segurança Institucional).
2. Estruturar as normativas, organizando-as em Domínios Temáticos que representam as macroáreas de obrigações de conformidade.
3. Formular perguntas de verificação (*Checkpoints*) em consonância com o embasamento normativo.
4. Elaborar um *framework* de conformidade para adoção de *SIEM* na Justiça Eleitoral.
5. Validar o *framework* proposto em soluções SIEM *open source.*

1.6 Estrutura da dissertação

O trabalho está organizado em seis capítulos correlacionados. O Capítulo 1, Introdução, apresentou, por meio de sua contextualização, o tema deste trabalho. Da mesma forma, foram estabelecidos os resultados esperados por meio da definição de seus objetivos e foram apresentadas as limitações do trabalho, o que permitiu uma visão clara do escopo proposto.

O Capítulo 2, Fundamentação Teórica, aprofunda os conceitos essenciais que sustentam a pesquisa. São abordados temas como o panorama da cibersegurança no Brasil, os princípios da segurança da informação, a arquitetura e o funcionamento de sistemas SIEM, bem como os fundamentos de governança e de conformidade regulatória, estabelecendo a base conceitual para o entendimento do trabalho.

O Capítulo 3, Trabalhos Relacionados, apresenta uma revisão da literatura sobre *framework*s de segurança, metodologias de adoção de SIEM e estudos sobre conformidade no cenário global. A análise crítica desses trabalhos permite posicionar a pesquisa, identificar a lacuna na literatura no que tange a um guia específico para a Justiça Eleitoral e justificar a originalidade da contribuição proposta.

O Capítulo 4, Procedimentos Metodológicos, detalha o percurso da pesquisa. É descrita a metodologia de Análise de Conteúdo de Bardin (2011), detalhando as três fases executadas: a Pré-análise, com a definição do corpus documental a partir das normativas do CNJ, TSE e GSI; a Exploração do Material, com a codificação e categorização dos requisitos; e o Tratamento dos Resultados, que levou à interpretação dos dados e à estruturação da solução.

O Capítulo 5, Resultados, apresenta a principal contribuição deste trabalho: o *framework* de conformidade para a adoção de soluções SIEM na Justiça Eleitoral (FCAS-JE). O capítulo descreve detalhadamente a estrutura do *framework*, seus domínios temáticos e os *Checkpoints* de conformidade desenvolvidos a partir da análise metodológica, oferecendo o instrumento prático gerado pela pesquisa, que, por fim, é validado ao ser aplicado às principais soluções SIEM *open source* de mercado.

No Capítulo 6, Considerações Finais, são apresentadas as conclusões do trabalho, relacionando os objetivos inicialmente identificados aos resultados alcançados. São ainda propostas possibilidades de continuidade da pesquisa, a partir das experiências adquiridas na execução do trabalho.

2 FUNDAMENTAÇÃO TEÓRICA

No atual contexto tecnológico, a transformação digital e a interconexão global dos sistemas computacionais impõem desafios complexos e prementes à segurança da informação. A proteção de dados e a garantia da integridade operacional tornaram-se imperativos para organizações de todos os portes e, particularmente, para aquelas que gerenciam infraestruturas críticas e essenciais para a sociedade (González-Granadillo et al., 2021).

Historicamente, o método de implantação de sistemas SIEM era o modelo tradicional local (*on-premises).* No entanto, a evolução da tecnologia e a expansão da computação em nuvem (*cloud computing)* levaram ao surgimento e à consolidação de modelos baseados em nuvem (Tuyishime *et al*., 2023). A escolha entre esses modelos implica considerações técnicas, operacionais e, no contexto da Administração Pública Federal e da Justiça Eleitoral, de conformidade legal e de governança.

A implantação local é priorizada por organizações que lidam com informações altamente sensíveis ou classificadas, como instituições financeiras, de saúde e entidades governamentais, pois permite atender a requisitos regulatórios rigorosos, garantindo que os dados de segurança permaneçam no ambiente físico da organização. No contexto da Justiça Eleitoral, esse controle é fundamental para a tutela da informação governamental e da soberania dos dados, alinhando-se às exigências de que os logs sejam mantidos em localização física, sujeitos a controles de segurança.

Contudo, a evolução da computação em nuvem levou ao surgimento de soluções de SIEM, como o Serviço (*SIEM-as-a-Service*) e, mais recentemente, o SIEM Nativo de Nuvem, ou *Cloud-Native SIEM* (Jhaveri; Parmar, 2023). As infraestruturas de nuvem são dinâmicas, escaláveis e distribuídas, características que soluções de SIEM tradicionalmente projetadas para ambientes de TI locais podem não ser capazes de acomodar de forma eficiente. Apesar das vantagens de flexibilidade, as organizações governamentais devem considerar as preocupações com a segurança dos dados inerentes ao armazenamento remoto e os desafios de conformidade decorrentes da localização geográfica dos dados.

Diante deste cenário, a Justiça Eleitoral cumpre a missão basilar na condução das eleições e das atividades eleitorais. Precisamente, o Tribunal Regional Eleitoral de Goiás (TRE-GO) trata diariamente de um grande volume de dados e informações, denominados logs. Esses registros são provenientes de ativos de rede, dispositivos e computadores conectados, bem como de acessos a sítios eletrônicos e redes. Tais dados podem conter informações para a

detecção de ciberataques, bem como para a emissão de relatórios de segurança da informação que auxiliam a tomada de decisões estratégicas no âmbito do órgão.

Em resposta à complexidade e ao grande volume de dados gerados por diversas fontes, os sistemas de Gerenciamento de Eventos e Informações de Segurança surgem como ferramentas essenciais nas operações de cibersegurança modernas (Ramakrishnan e Chittibala, 2024). Esses sistemas são responsáveis por funções de agregação, normalização e agrupamento de logs provenientes de diversas fontes para análise em tempo real. Essa funcionalidade, conforme destacam Bhatt et al. (2014), torna possível a correlação de dados, superando a incapacidade de conectar eventos entre sistemas de segurança distintos. Desta forma, o SIEM permite detectar ameaças e responder a incidentes com maior precisão, aprimorando a segurança cibernética da organização.

Um estudo recente sobre cibersegurança, utilizando técnicas de inteligência artificial, demonstrou como a padronização de procedimentos pode ser útil para avaliar sistemas de aprendizado de máquina ou *Machine Learning* (ML), como os SIEMs, e também discutiu como o compartilhamento de dados entre as entidades pode ser importante (Apruzzese et al., 2023). A integração de inteligência artificial (IA) e, em particular, de algoritmos de ML, representa uma transformação no futuro dos SIEMs, permitindo que as organizações detectem, investiguem e respondam a incidentes com maior eficiência e precisão (Ramakrishnan e Chittibala, 2024).

Entre as capacidades aprimoradas pelo uso dessas tecnologias estão o cruzamento de dados e a análise de comportamento. SIEMs aprimorados por IA/ML utilizam algoritmos complexos para correlacionar eventos e informações provenientes de diversas fontes, identificando padrões de ataque intrincados e anomalias que soluções de segurança convencionais, baseadas em regras, poderiam negligenciar. A IA tem a capacidade de "conectar os pontos" entre os diversos eventos de segurança que, isolados, podem parecer inofensivos, mas, coletivamente, indicam um ataque coordenado (Perez, 2023).

Essas técnicas também podem ser utilizadas para a detecção de anomalias e para a redução de falsos positivos. O aprendizado de máquina é fundamental para a Análise de Comportamento de Usuários e Entidades (*UEBA - User and Entity Behavior Analytics*). Ao ser treinado com dados históricos, o sistema aprende os padrões de comportamento normal na rede (usuários, sistemas e aplicações) e é capaz de sinalizar desvios desses padrões (Pulyala, 2023). Soma-se a isso a capacidade de aprendizado contínuo, que permite que o SIEM otimize os parâmetros de detecção, distinguindo com maior eficácia entre atividades normais e ações genuinamente suspeitas. Isso mitiga a sobrecarga de alertas (*alert fatigue*) que afeta os analistas

de segurança, permitindo que as equipes se concentrem em ameaças reais e melhorem a eficiência da resposta (Perez, 2023).

Outras funcionalidades otimizadas com o uso dessas técnicas incluem a detecção de vulnerabilidades e a automação de respostas. Ao analisar tendências e padrões em dados históricos e correlacioná-los com feeds de inteligência de ameaças externas (*Threat Intelligence*), os algoritmos de ML podem prever potenciais vetores de ataque e vulnerabilidades antes que se materializem. A IA potencializa a automação e orquestração de plataformas de *Security Orchestration, Automation, and Response* (SOAR). Após a detecção de um incidente, algoritmos de IA podem triar automaticamente os alertas, avaliar a severidade da ameaça e orquestrar ações de resposta predefinidas (como isolar um dispositivo ou bloquear um IP malicioso) (Ramakrishnan; Chittibala, 2024).

Adicionalmente aos desafios técnicos e orçamentários, há, no Brasil, um panorama regulatório denso e complexo. O compromisso com a cibersegurança no Brasil se reflete em sua posição no Global Cybersecurity Index (CGI), relatório da União Internacional de Telecomunicações (UIT), no qual se posicionou em segundo lugar nas Américas. Essa classificação foi alcançada, entre outras avaliações, pela robustez do seu Pilar Legal, o que evidencia a grande quantidade de normativas existentes no país. Esse denso arcabouço abrange desde a Lei Geral de Proteção de Dados (LGPD) até decretos, resoluções do Conselho Nacional de Justiça (CNJ) e do Tribunal Superior Eleitoral (TSE), e normativas do Gabinete de Segurança Institucional (GSI), que, juntos, estabelecem um conjunto de obrigações para as entidades do setor público. Deve-se levar em consideração as eventuais restrições orçamentárias, especialmente na esfera governamental, onde os sistemas de código aberto (*open source*) constituem uma alternativa (Manzoor et al., 2024).

Contudo, esse crescimento de regulamentações, embora positivo na perspectiva estratégica e de governança, cria uma lacuna prática: a ausência de um guia consolidado que traduza as exigências legais em um roteiro coeso para a implementação de tecnologias de segurança. Essa dificuldade é significativa, especialmente na adoção de uma ferramenta SIEM, que envolve a coleta e a análise de dados sensíveis.

Diante desses desafios normativos e tecnológicos, este trabalho apresenta uma proposta de um *framework* de conformidade para a adoção de soluções de SIEM na Justiça Eleitoral. O *framework* é desenvolvido com base em normativas vigentes e nas diretrizes de avaliação e nos requisitos quantitativos e qualitativos definidos por Mokalled et al. (2020), o que valida tanto aspectos técnicos quanto legais na escolha da solução.

3 TRABALHOS RELACIONADOS

A seção aborda trabalhos correlatos que fundamentam a pesquisa, com foco em metodologias para a seleção de sistemas de SIEM e nos desafios de conformidade impostos pelas regulamentações de proteção de dados, como o Regulamento Geral de Proteção de Dados (RGPD) da União Europeia, cujas premissas se assemelham às da legislação brasileira. A análise desses estudos permite contextualizar a lacuna existente e a originalidade da contribuição deste trabalho.

O trabalho de Mokalled et al. (2020) propõe um método estruturado para a seleção de soluções de SIEM, que serviu de inspiração conceitual para esta dissertação. Os autores defendem uma abordagem orientada às necessidades do cliente (*customer-driven*), em oposição a modelos focados no produto. A metodologia apresentada baseia-se em um processo avaliativo em duas fases, sendo a primeira uma medição quantitativa de conformidade (*compliance*). Nesta fase, os requisitos técnicos e organizacionais da instituição são detalhados e atribuídos um peso (W) de acordo com sua importância. As soluções candidatas são avaliadas, recebendo um valor (V) de acordo com o grau de atendimento a cada requisito. O resultado, uma pontuação objetiva (S = V * W), permite uma classificação técnica e fundamentada. A ideia de utilizar um instrumento sistemático para avaliar a aderência de uma solução a um conjunto predefinido de requisitos de conformidade constitui o ponto de partida do *framework* desenvolvido neste estudo, aplicado ao contexto da Justiça Eleitoral.

Vazão et al. (2019) realizaram um estudo comparativo de soluções de SIEM de código aberto, motivado pela entrada em vigor do RGPD. O objetivo foi selecionar uma ferramenta que atendesse a requisitos legais específicos de proteção de dados, como a pseudonimização, o tempo de retenção e a encriptação de logs. A metodologia envolveu a análise de quatro soluções (*OSSIM, Elastic Stack, Splunk Free e Graylog*) com base em funcionalidades essenciais e, notadamente, em sua capacidade de atender às novas exigências de privacidade. O estudo evidencia a crescente preocupação em alinhar as capacidades técnicas das ferramentas de cibersegurança às obrigações impostas pela legislação de proteção de dados.

Em um estudo subsequente, Vazão et al. (2023) aprofundaram a pesquisa ao apresentar a implementação e avaliação de uma solução SIEM baseada no *Elastic Stack*, projetada para ser compatível com o RGPD. O trabalho detalha uma arquitetura que complementa os componentes padrão do stack com ferramentas externas de código aberto para reforçar a segurança, a auditoria e a capacidade de alerta. A contribuição deste trabalho reside na

demonstração de uma arquitetura técnica viável e específica para endereçar os desafios de conformidade do RGPD em um ambiente de SIEM, deslocando o foco da seleção de ferramentas para sua efetiva implementação e adequação.

Menges et al. (2021) abordam o conflito fundamental entre a funcionalidade dos sistemas SIEM, que dependem da análise em massa de dados para a detecção de ameaças, e os princípios de proteção de dados do RGPD. Para harmonizar essas demandas antagônicas, os autores propõem e avaliam uma arquitetura de SIEM que equilibra segurança e privacidade. A avaliação técnica demonstrou que a pseudonimização de dados pessoais nos logs afeta apenas ligeiramente a qualidade da detecção de incidentes. A avaliação legal conclui que a arquitetura é compatível com o RGPD, fundamentando o tratamento de dados com base no "legítimo interesse". O trabalho é relevante por validar, tecnicamente e juridicamente, uma abordagem para resolver a tensão inerente entre a operação de um SIEM e o direito à privacidade.

Trazendo a discussão para o cenário brasileiro, destaca-se o trabalho de Teixeira (2024), que investiga a resposta aos incidentes cibernéticos no Setor Elétrico Brasileiro (SEB). A relevância deste estudo para a presente pesquisa reside na análise de um setor que, assim como o eleitoral, desempenha atividades críticas para a soberania nacional. A pesquisa de Teixeira (2024) aprofunda-se no arcabouço normativo brasileiro aplicável, analisando desde a Estratégia Nacional de Segurança Cibernética até regulamentações setoriais específicas. Um dos achados centrais do estudo é a constatação de uma "dispersão normativa", na qual a multiplicidade de fontes regulatórias é percebida pelos agentes do setor como um fator que dificulta a implementação e o acompanhamento das diretrizes, o que caracteriza o ambiente como desafiador. Essa dificuldade de traduzir um conjunto de normas dispersas em práticas operacionais coesas, identificada no setor elétrico, é análoga ao desafio que motiva a criação do *framework* proposto neste trabalho para a Justiça Eleitoral.

Já o trabalho de Machado (2024) aborda a automação de tarefas de segurança como um mecanismo para aprimorar a resposta a incidentes cibernéticos, argumentando que a conformidade normativa é um dos pilares que justificam sua implementação. O autor demonstra que a adoção de ferramentas como SIEM e SOAR constitui uma resposta estratégica às exigências de um arcabouço legal denso. O estudo identifica múltiplos instrumentos como impulsionadores da automação, incluindo a Lei Geral de Proteção de Dados (LGPD), a Política Nacional de Segurança da Informação (PNSI), diversas normativas do GSI e o Acórdão 1768/2022 do Tribunal de Contas da União (TCU). A relevância deste ensaio reside em

estabelecer que o próprio ambiente regulatório brasileiro cria uma demanda explícita pela adoção de tecnologias de segurança avançadas, reforçando a necessidade de um guia metodológico que oriente a implementação dessas ferramentas de forma estruturada e em plena conformidade.

Em conjunto, os estudos analisados demonstram que a preocupação com o compliance regulatório na implementação de sistemas SIEM é um tema de crescente relevância na pesquisa nacional e internacional. Evidencia-se um esforço contínuo para a evolução das ferramentas e arquiteturas, visando adequá-las às rigorosas normas de proteção de dados, com especial destaque para o RGPD, análogo à LGPD brasileira. No entanto, a literatura aponta para soluções majoritariamente focadas no contexto europeu e na dimensão técnica da adequação. Para a realidade brasileira, é necessário um olhar mais aprofundado que considere não apenas a LGPD, mas também todo o complexo arcabouço legal que rege a Administração Pública. As informações que podem apoiar a tomada de decisão na adoção de uma ferramenta SIEM encontram-se difusas em múltiplas fontes normativas, criando uma lacuna que faz necessária a construção de um instrumento consolidado, que traduza essa complexidade em um guia de conformidade prático e direcionado. A Tabela 1 resume os trabalhos relacionados e o framework proposto.

Tabela 1 – Análise dos trabalhos relacionados

Referência	Análise Quantitativa	Foco em Privacidade (GDPR/LGPD)	Arquitetura e Aplicação	Contexto de Setor Crítico/Público	Consolidação da Dispersão Normativa
Mokalled et al. (2020)	✔	-	✔	✔	-
Vazão et al. (2019/2023)	✔	✔	✔	-	-
Menges et al. (2021)	*	✔	✔	*	-
Teixeira (2024)	*	-	✔	✔	*
Machado (2024)	-	✔	*	✔	*
Rodrigues e Carvalho (2026)	✔	✔	✔	✔	✔

Legenda: (✔) contempla; (*) contempla parcialmente; (-) não contempla.

4 PROCEDIMENTOS METODOLÓGICOS

A metodologia adotada para a construção do *framework* foi a Análise de Conteúdo, conforme preconiza Bardin (2011). Este método permite a análise sistemática de um conjunto de documentos para inferir conhecimentos e identificar estruturas de sentido. O processo foi organizado em três fases propostas pela autora, iniciando-se pela pré-análise, detalhada a seguir.

4.1 Pré-análise

A fase de pré-análise consistiu na organização e sistematização do plano de trabalho, o que foi fundamental para estruturar o desenvolvimento da pesquisa. Nesta etapa, foram realizadas as atividades de leitura flutuante, a constituição do corpus documental, a reafirmação dos objetivos da pesquisa e a elaboração dos indicadores que guiariam a análise subsequente. O ponto de partida foi a exploração das bases legais e normativas dos órgãos-chave para a regulação da Justiça Eleitoral e da Administração Pública Federal.

Para tanto, realizou-se uma leitura flutuante nas bases de dados digitais do Conselho Nacional de Justiça (CNJ), do Gabinete de Segurança Institucional (GSI) e do Tribunal Superior Eleitoral (TSE), utilizando seus respectivos portais de legislação. Nos campos de busca, foram empregados termos e temas alinhados ao escopo do trabalho, tais como "segurança da informação", "cibersegurança", "gestão de logs", "resposta a incidentes", "proteção de dados" e "normas de TIC". Essa primeira imersão permitiu um contato inicial com um vasto volume de resoluções, portarias, instruções normativas e recomendações, possibilitando a formação de uma visão panorâmica sobre o cenário regulatório e a identificação intuitiva dos documentos potencialmente mais relevantes.

4.2 Coleta e seleção documental

A partir dessa exploração inicial, procedeu-se à escolha dos documentos e à constituição do corpus de análise. Esta seleção foi guiada por critérios de pertinência e representatividade, conforme as premissas estabelecidas nesta pesquisa. Cada documento pré-selecionado na leitura flutuante foi avaliado quanto à sua aderência aos seguintes critérios:

(i) Relevância direta aos temas de segurança da informação, gestão de logs e resposta a incidentes;

(ii) Aplicabilidade à Administração Pública Federal e, por extensão, à Justiça Eleitoral; e

(iii) Significância estratégica para a definição dos requisitos de conformidade de uma solução SIEM.

Este filtro metodológico foi crucial para garantir a homogeneidade do material e delimitar um corpus documental focado e exaustivo para os fins do estudo, resultando na seleção final dos documentos a serem analisados em profundidade.

4.3 Base normativa selecionada

Para garantir a consistência terminológica e o alinhamento conceitual do estudo, a seleção e a interpretação do material levantado foram embasadas nos glossários oficiais que normatizam os termos técnicos no âmbito da segurança da informação e da Tecnologia da Informação no setor público brasileiro. No contexto da Administração Pública Federal, adotou-se como referência a Portaria GSI/PR nº 93/2021, que aprova o Glossário de Segurança da Informação. Foram considerados, de forma complementar e específica ao objeto de estudo, o Glossário de TI da Justiça Eleitoral, disponibilizado pelo Tribunal Superior Eleitoral (TSE), e o Anexo VIII da Portaria CNJ nº 162/2021, que aprova o glossário de termos técnicos aplicáveis aos documentos de Segurança Cibernética. A utilização dessas fontes assegura que os conceitos e requisitos discutidos nesta dissertação estejam em plena conformidade com a linguagem padronizada pelos órgãos reguladores.

Como resultado do processo de coleta e seleção documental, consolidou-se um conjunto de 41 (quarenta e uma) normativas consideradas essenciais ao escopo deste estudo. Extraídas das bases de consulta do Conselho Nacional de Justiça (CNJ), do Tribunal Superior Eleitoral (TSE), do Gabinete de Segurança Institucional (GSI) e da legislação federal aplicável, estas normas constituem o pilar regulatório da pesquisa. O Apêndice A apresenta a relação das bases normativas selecionadas e dos resumos.

4.4 Codificação e categorização

Superada a fase de pré-análise e com o corpus documental devidamente constituído, iniciou-se a etapa de exploração do material. Esta fase, de acordo com Bardin (2011), consiste na aplicação sistemática das decisões tomadas na etapa anterior, envolvendo a gestão das

operações de codificação e categorização do conteúdo, para, ao final, alcançar uma representação simplificada dos dados brutos.

O primeiro procedimento realizado foi a codificação do corpus. Cada documento selecionado foi lido com o objetivo de identificar e extrair as unidades de registro – trechos específicos (artigos, incisos, parágrafos ou sentenças) que continham uma diretriz, um requisito ou uma obrigação de conformidade. A cada unidade de registro extraída, foi atribuído um código que sintetizava seu conteúdo essencial, como, por exemplo, [EVIDENCIAS_DIGITAIS], [GESTÃO_DE_RISCOS], [GOVERNANÇA_DE_TIC], [AUDITORIA], entre outros. Este processo permitiu desconstruir a linguagem jurídica complexa das normativas em um conjunto granular e gerenciável de requisitos objetivos, que serviram de matéria-prima para a construção do *framework*.

A etapa subsequente foi a categorização, cujo objetivo era agrupar os diversos requisitos codificados em conjuntos maiores e coerentes, com base em critérios de similaridade semântica. Foi neste ponto que a metodologia tradicional foi auxiliada por uma ferramenta de Inteligência Artificial, o NotebookLM, para a validação dos temas mais relacionados dentro do conjunto de normas. Os documentos do corpus foram carregados na ferramenta, que foi utilizada não para criar as categorias de forma autônoma, mas como um instrumento de verificação e refinamento das afinidades temáticas identificadas pelo pesquisador. Por meio de questionamentos e solicitações de síntese, a IA auxiliou na confirmação de que diferentes requisitos, extraídos de múltiplas fontes normativas, de fato convergiam para um mesmo conceito central, como "governança de dados" ou "gestão de riscos".

Este processo híbrido, unindo a análise qualitativa do pesquisador com a capacidade da IA de processar e correlacionar semanticamente grandes volumes de texto, permitiu a construção de categorias bem definidas. O resultado direto desta fase foi a consolidação dos domínios temáticos que estruturam o *framework* de conformidade, garantindo que o agrupamento dos requisitos fosse validado por uma análise sistemática das relações de conteúdo presentes no arcabouço legal.

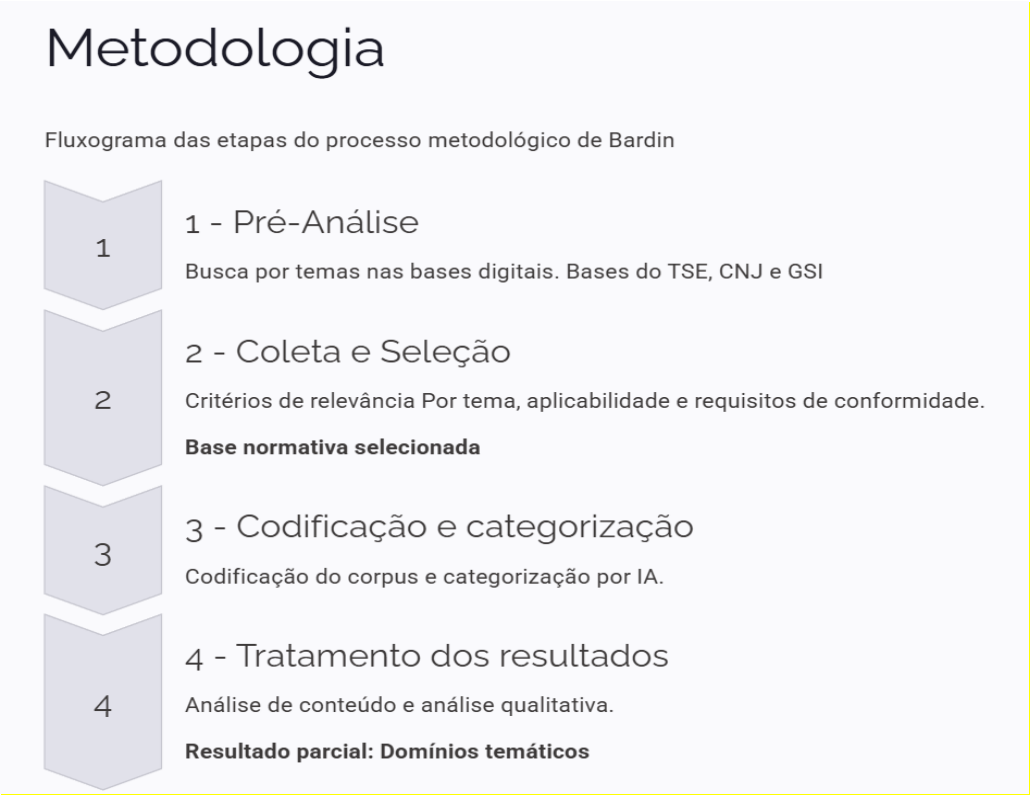
4.5 Tratamento dos resultados, inferência e interpretação

Finalizadas a coleta documental, a codificação e a categorização, foi realizada a análise de conteúdo baseada nos resultados para resultar em uma perspectiva sistemática de todo o material proposto e na interpretação. Os resultados híbridos, obtidos a partir da categorização e

da validação semântica realizadas com o auxílio da ferramenta de IA NotebookLM, forneceram uma base sólida e confiável para a consolidação dos achados. O tratamento dos resultados, portanto, materializou-se na solidificação das categorias previamente identificadas, que foram formalmente estabelecidas como os domínios temáticos do *framework* de conformidade.

Dessa forma, a aplicação da Análise de Conteúdo, apoiada pela validação com a ferramenta de IA, culminou na etapa final de interpretação, na qual os requisitos legais foram traduzidos em um instrumento prático. Este processo resultou na estruturação do *framework* em domínios temáticos, os quais foram preenchidos por *Checkpoints* de conformidade em formato de perguntas objetivas e verificáveis. A apresentação detalhada deste *framework*, principal resultado desta pesquisa, constitui o foco do próximo capítulo, dedicado aos Resultados Parciais. A Figura 3, apresentada a seguir, detalha as etapas aplicadas na metodologia.

Figura 3 – Metodologia de Bardin aplicada



Fonte: Autoria própria

5 RESULTADOS

Este capítulo apresenta o resultado central da pesquisa: a estrutura do *framework* de conformidade para a adoção de sistemas SIEM na Justiça Eleitoral. O desenvolvimento deste artefato é o produto direto da aplicação da metodologia de Análise de Conteúdo de Bardin (2011), conforme detalhado no capítulo anterior. A partir da análise sistemática do corpus documental, composto por um denso arcabouço legal, foi possível sintetizar os requisitos e diretrizes em uma estrutura organizada, que visa traduzir a complexidade normativa em um guia de conformidade operacional.

5.1 Domínios temáticos

O primeiro resultado alcançado, fruto da fase de exploração do material, foi a consolidação das categorias temáticas. A partir da codificação das unidades de registro extraídas das normativas, iniciou-se um processo de categorização para agrupar os requisitos com base em suas afinidades semânticas. A nomeação dessas categorias, que se tornaram os domínios temáticos do *framework*, buscou um equilíbrio entre duas premissas fundamentais: englobar a diversidade de exigências do arcabouço legal brasileiro e, simultaneamente, refletir os requisitos práticos de implementação de um SIEM, baseados nos estudos de Mokalled et al. (2020). Desta forma, os domínios foram concebidos como repositórios de exigências legais e também como áreas funcionais e estratégicas para a adoção da ferramenta.

Os domínios emergentes refletiram aspectos importantes, desde da gestão dos acessos e tratamento de dados da ferramenta, até auditoria e aspectos de inteligência artificial, formando assim o esqueleto do *framework* a ser proposto, atendendo as preocupações dos principais órgãos de controle e as legislações vigentes. A tabela 2 descreve os domínios.

Tabela 2 - Descrição dos Domínios Temáticos

Domínio	Descrição
Governança e Gestão Estratégica de TIC	Compreende as diretrizes para o alinhamento estratégico entre a Tecnologia da Informação e Comunicação (TIC), governança e gestão da segurança da informação e os objetivos estratégicos, o que inclui a definição de políticas, responsabilidades e processos.
Proteção e Governança de Dados (LGPD e IA)	Descreve requisitos essenciais do tratamento de dados pessoais apontados na Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e na Lei nº 12.527/2011 (LAI), além de estabelecer critérios de conformidade em sistemas que fazem uso de Inteligência Artificial (IA).
Gestão de Riscos e	Abarca o ciclo de tratamento de riscos (identificação, análise, avaliação

Continuidade de Negócios	e tratamento) e o planejamento estratégico para garantir a continuidade (alta disponibilidade) dos serviços.
Auditoria, *Logs* e Transparência	Trata-se da capacidade de registrar, armazenar e proteger *logs* de eventos de sistemas. Assegura a rastreabilidade das ações, assim como a capacidade de gerar documentos comprobatórios de auditoria que promovem a transparência e fortalecem a conformidade.
Gestão de Incidentes e Resposta	Define os aspectos técnicos para as capacidades de um SIEM frente a incidentes de segurança cibernética. Aborda funcionalidades integradas de análises e respostas aos incidentes baseadas em detecção de tempo real e análise de comportamento.

5.1.1 Governança e Gestão Estratégica de TIC

Este domínio abrange as diretrizes de alto nível que orientam a gestão da tecnologia da informação e comunicação, incluindo a segurança. Foca no alinhamento da SIEM com os objetivos estratégicos da instituição e na supervisão por parte da alta administração.

Codificações consolidadas:

- Estratégia de Segurança (ENSEC-PJ)
- Estratégia Nacional de Cibersegurança (ENCiber)
- Estrutura e Competências do GSI/PR
- Gestão de Projetos de TIC
- Gestão de TIC
- Governança
- Governança de TIC
- Governança e Gestão de Riscos Cibernéticos
- Plano de Segurança da Informação (PSI)
- Política Nacional de Cibersegurança (PNCiber)
- Segurança da Informação
- Prestação de Contas

5.1.2 Proteção e Governança de Dados (LGPD e IA)

Este domínio concentra-se na proteção de dados pessoais e sensíveis, incluindo as exigências da LGPD e as diretrizes para o uso ético e seguro da Inteligência Artificial. Um SIEM é vital para monitorar o acesso e tratamento de dados.

Codificações consolidadas:

- Auditoria
- Conformidade LGPD
- Ética
- Governança de Dados
- Governança de IA

- Inteligência Artificial (IA) no Serviço Público
- Interoperabilidade
- Proteção de Dados Pessoais
- Proteção de Dados Sensíveis e Classificados

5.1.3 Gestão de Riscos e Continuidade de Negócios

O terceiro domínio foca nas capacidades proativas e reativas da segurança da informação, avaliando como a ferramenta SIEM se insere nos processos de gestão de riscos e nos planos de continuidade de negócios (PCN) e de recuperação de desastres (PRD). Auxilia na identificação de ameaças e na gestão de vulnerabilidades, mas também fornece a observabilidade necessária para acionar planos de contingência e assegurar a resiliência operacional, incluindo a alta disponibilidade da própria plataforma de monitoramento.

Codificações consolidadas:

- Avaliação de Riscos
- Configuração Segura
- Gestão de Continuidade de Negócios
- Gestão de Riscos
- Gestão de Riscos de Segurança da Informação
- Gestão de Vulnerabilidades
- Inteligência de Segurança
- Monitoramento
- Normas de Segurança da Informação e Comunicações (SIC)
- Plano de Continuidade de Negócios (PCN)
- Políticas de Segurança
- Recuperação de Desastres (PRD)
- Segurança Cibernética
- Testes de Segurança

5.1.4 Auditoria, Logs e Transparência

Focado na capacidade de registrar, armazenar e analisar eventos e logs para fins de auditoria, conformidade e prestação de contas. O SIEM é a espinha dorsal deste domínio.

Codificações consolidadas:

- Acesso à Informação
- Auditoria
- Auditoria de Segurança
- Auditoria de Sistemas
- Auditoria Interna

- Certificação Digital
- Controle
- Controle de Acesso
- Criptografia
- Evidências Digitais
- Gerenciamento de Identidades
- Gestão de Acessos e Privilégios
- Gestão de Logs
- Gestão de Processos
- Segurança da Informação
- Transparência

5.1.5 Gestão de Incidentes e Resposta

O quinto e último domínio do *framework* aborda a dimensão operacional da cibersegurança, focando nas capacidades da ferramenta SIEM para gerenciar o ciclo de vida completo de um incidente, desde a detecção em tempo real até a resposta e a investigação pós-incidente. Os *Checkpoints* avaliam funcionalidades avançadas, como a automação da resposta (SOAR), a análise comportamental (UEBA), a integração com inteligência de ameaças e a garantia de soberania dos dados por meio da implantação em infraestrutura local.

Codificações consolidadas:

- Análise Forense
- Auditoria de Sistemas
- Evidências Digitais
- Gestão de Incidentes de Segurança
- Gestão de Logs
- Incidentes de Segurança
- Inteligência de Segurança
- Investigação
- Monitoramento
- Protocolos de Segurança Cibernética
- Resposta a Incidentes
- Requisitos de Segurança
- Segurança Cibernética

5.2 Perguntas de conformidade dos domínios temáticos

Com os domínios temáticos estabelecidos como a estrutura macro do *framework*, a etapa seguinte, correspondente à interpretação dos resultados, consistiu na formulação de perguntas de verificação, também denominadas *Checkpoints* de conformidade. Cada *Checkpoint* foi elaborado para traduzir e abranger as codificações identificadas durante a análise dos

documentos. Essas perguntas transformam a linguagem, por vezes abstrata, da legislação em questionamentos objetivos e auditáveis, permitindo que a instituição avalie, de forma prática, o nível de aderência de uma solução SIEM a cada requisito normativo identificado.

Em suma, a estrutura final do *framework*, que será detalhada a seguir, é o resultado direto da aplicação do método. A análise híbrida, que uniu a interpretação do pesquisador à validação semântica com o auxílio da ferramenta de IA NotebookLM, culminou na criação de um conjunto de domínios temáticos preenchidos por *Checkpoints* de conformidade específicos. Este instrumento, portanto, materializa a passagem da análise teórica dos textos legais para uma ferramenta de aplicação prática, cujo detalhamento constitui o cerne deste capítulo.

5.2.1 *Checkpoints* - Governança e Gestão Estratégica de TIC

O primeiro domínio abarca uma visão integral da Governança e Segurança da Informação em que os requisitos do SIEM estão alinhados com as normas reguladoras dos planos diretores e das estratégias nacionais no Poder Judiciário. Os *Checkpoints* mencionados (Tabela 2) avaliam desde a contribuição para os objetivos da Estratégia Nacional de TIC e da Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ) até o suporte à gestão de ativos e riscos estratégicos, assegurando que a tecnologia escolhida sirva como um pilar para o aprimoramento da governança do órgão. A Tabela 3 apresenta os *Checkpoints* e as normativas de base.

Tabela 3 - *Checkpoints* do Domínio de Governança e Gestão Estratégica de TIC

Item	*Checkpoint* de Conformidade	Normativas de Referência
1.1	Alinhamento Estratégico e de Planejamento: O SIEM proposto contribui para os objetivos da Estratégia Nacional do Poder Judiciário (ENTIC-JUD), planos diretores (PDTIC) e estratégias de segurança (ENSEC-PJ, PSI), oferecendo capacidades de monitoramento, detecção e análise que reforcem a segurança, a eficiência e a modernização dos sistemas da Justiça Eleitoral?	CNJ Resolução nº 325/2020 CNJ Resolução nº 370/2021 CNJ Resolução nº 396/2021 TSE Resolução nº 23.644/2021 GSI Decreto nº 11.856/2023 CNJ Portaria nº 1/2025 TSE Portaria nº 388/2024
1.2	Governança e Prestação de Contas: O SIEM oferece recursos (painéis, relatórios, métricas) que podem suportar decisões da alta administração, contribuindo para a transparência e a prestação de contas (*accountability*) dos controles de segurança implementados?	GSI Instrução Normativa nº 1/2020 GSI Instrução Normativa nº 3/2021 CNJ Resolução nº 396/2021 GSI Decreto nº 11.856/2023 TSE Portaria nº 459/2021
1.3	Gestão de Riscos Estratégicos: O SIEM apoia a gestão estratégica de riscos de segurança da informação, conforme as diretrizes de governança de TIC do CNJ, identificando e mitigando proativamente ameaças à resiliência dos sistemas eleitorais?	CNJ Resolução nº 370/2021 GSI Instrução Normativa nº 3/2021 CNJ Portaria nº 162/2021 (Anexo V) TSE Portaria nº 388/2024

1.4	*Roadmap* de Produto e Suporte: O SIEM disponibiliza publicamente um *roadmap* detalhado com a evolução da solução, novas funcionalidades, ciclos de vida e prazos de suporte, assegurando o planejamento de longo prazo e a sustentabilidade do investimento?	CNJ Resolução nº 325/2020 CNJ Resolução nº 370/2021 CNJ Resolução nº 396/2021 GSI Instrução Normativa nº 3/2021 GSI Decreto nº 10.569/2020 TSE Portaria nº 387/2024 TSE Portaria nº 497/2021
1.5	Gestão de Ativos de TIC: O SIEM oferece recursos que auxiliam na gestão de ativos de TIC, fornecendo monitoramento de segurança desses ativos ao longo do seu ciclo de vida?	CNJ Resolução nº 370/2021 CNJ Resolução nº 396/2021 GSI Instrução Normativa nº 3/2021 CNJ Portaria nº 162/2021 (Anexos I e V) TSE Portaria nº 458/2021

- *Checkpoint* de Conformidade 1.1 e justificativas das normativas norteadoras:

Alinhamento Estratégico e de Planejamento: O SIEM proposto contribui para os objetivos da Estratégia Nacional do Poder Judiciário (ENTIC-JUD), planos diretores (PDTIC) e estratégias de segurança (ENSEC-PJ, PSI), oferecendo capacidades de monitoramento, detecção e análise que reforcem a segurança, a eficiência e a modernização dos sistemas da Justiça Eleitoral?

O embasamento normativo para o alinhamento estratégico de um SIEM é definido por um conjunto de diretrizes do Conselho Nacional de Justiça, como as Resoluções nº 325/2020, nº 370/2021 (ENTIC-JUD) e nº 396/2021 (ENSEC-PJ), que estabelecem os macrodesafios e os objetivos de aprimoramento da segurança, governança e resiliência cibernética do Poder Judiciário. Tais estratégias estão em consonância com a Política Nacional de Cibersegurança (Decreto GSI nº 11.856/2023) e se materializam em Planos Diretores de TIC (Portaria CNJ nº 1/2025) e na Política de Segurança da Informação da Justiça Eleitoral (Resolução TSE nº 23.644/2021). A capacidade de um SIEM de fornecer dados e inteligência de segurança por meio de monitoramento e análise é o que permite às estruturas de governança, como a estabelecida pela Portaria TSE nº 388/2024, executar e verificar o cumprimento dessas diretrizes.

- *Checkpoint* de Conformidade 1.2 e justificativas das normativas norteadoras:

Governança e Prestação de Contas: O SIEM oferece recursos (painéis, relatórios, métricas) que podem subsidiar decisões da alta administração, contribuindo para a transparência e a prestação de contas (accountability) dos controles de segurança implementados?

O embasamento normativo para o suporte à governança e à prestação de contas é definido por um conjunto de diretrizes federais e judiciárias. O Decreto nº 11.856/2023

(PNCiber) e as Instruções Normativas GSI nº 1/2020 e nº 3/2021 estabelecem a necessidade de uma governança baseada em métricas e em um processo formal de Avaliação de Conformidade, cujos relatórios devem ser submetidos à alta administração. No Poder Judiciário, a Resolução CNJ nº 396/2021 (ENSEC-PJ) institui Comitês de Governança com a atribuição de assessorar a liderança. A geração de relatórios para estes processos depende da gestão íntegra de logs, conforme detalhado na Portaria TSE nº 459/2021. A capacidade de um SIEM de centralizar a visibilidade e gerar relatórios analíticos é, portanto, o instrumento técnico que fornece os subsídios para a tomada de decisão e a prestação de contas sobre a eficácia dos controles de segurança.

- *Checkpoint* de Conformidade 1.3 e justificativas das normativas norteadoras:

Gestão de Riscos Estratégicos: O SIEM apoia a gestão estratégica de riscos de segurança da informação, conforme as diretrizes de governança de TIC do CNJ, identificando e mitigando proativamente ameaças à resiliência dos sistemas eleitorais?

O embasamento normativo para o apoio do SIEM à gestão estratégica de riscos é definido por diretrizes de governança e processos mandatórios. A Estratégia Nacional de TIC do Poder Judiciário (Resolução CNJ Nº 370/2021) estabelece a gestão de riscos como um tema central da governança, atribuindo aos comitês gestores a responsabilidade por sua execução. Este processo é metodologicamente orientado pela Instrução Normativa GSI/PR nº 3, que exige a identificação, análise e tratamento contínuo dos riscos, sendo sua operacionalização detalhada no manual da Portaria CNJ nº 162/2021 (Anexo V) por meio de "diagnóstico contínuo". A capacidade de um SIEM de fornecer os insumos para a análise de riscos e o mapeamento de vulnerabilidades permite à Comissão de Segurança da Informação do TSE cumprir suas atribuições, conforme a Portaria TSE Nº 388/2024, e apoiar a gestão estratégica de riscos.

- *Checkpoint* de Conformidade 1.4 e justificativas das normativas norteadoras:

Roadmap de Produto e Suporte: O SIEM disponibiliza publicamente um roadmap detalhado com a evolução da solução, novas funcionalidades, ciclos de vida e prazos de suporte, assegurando o planejamento de longo prazo e a sustentabilidade do investimento?

O embasamento normativo para a necessidade de um *roadmap* de produto e de um ciclo de vida claro é definido por diretrizes estratégicas do Poder Judiciário e do Governo Federal. As Estratégias Nacionais do Poder Judiciário (Resoluções CNJ nº 325/2020, nº 370/2021 e nº

396/2021) e a Estratégia Nacional de Segurança de Infraestruturas Críticas (Decreto GSI nº 10.569/2020) estabelecem a necessidade de planejamento de longo prazo, gestão de riscos de obsolescência e contínuo aprimoramento da segurança. Este planejamento é um requisito do processo de gestão de segurança da informação, que exige alinhamento com a evolução tecnológica, conforme a Instrução Normativa GSI/PR Nº 3/2021. No âmbito do TSE, a previsibilidade sobre a evolução da solução é um requisito para o cumprimento de seu Plano Estratégico Institucional (Portaria TSE Nº 497/2021) e para a manutenção da eficácia operacional da Equipe de Tratamento e Resposta a Incidentes Cibernéticos (Portaria TSE Nº 387/2024).

- *Checkpoint* de Conformidade 1.5 e justificativas das normativas norteadoras:

Gestão de Ativos de TIC: O SIEM oferece recursos que auxiliam na gestão de ativos de TIC, fornecendo monitoramento de segurança desses ativos ao longo do seu ciclo de vida?

O embasamento normativo para o monitoramento de ativos de TIC é definido por diretrizes estratégicas e normas processuais. As Resoluções CNJ nº 370/2021 (ENTIC-JUD) e nº 396/2021 (ENSEC-PJ) estabelecem a obrigatoriedade da gestão e do monitoramento de ativos no Poder Judiciário, alinhando-se ao processo de gestão de riscos da Instrução Normativa GSI/PR nº 3, que exige a identificação de riscos associados a cada ativo. No âmbito do TSE, a Portaria nº 458/2021 institui a norma específica para a Gestão de Ativos, demandando o monitoramento de sua segurança ao longo do ciclo de vida. A capacidade de um SIEM de analisar logs detalhados, cuja coleta é exigida pelos manuais da Portaria CNJ nº 162/2021 (Anexos I e V), é o que permite a identificação e o monitoramento contínuo dos ativos críticos em conformidade com estas diretrizes.

5.2.2 *Checkpoints* - Proteção e Governança de Dados (LGPD e IA)

O segundo domínio do *framework* concentra-se na proteção de dados e na governança da informação, com ênfase na aderência à Lei Geral de Proteção de Dados (Lei nº 13.709/2018 - LGPD) e à Lei de Acesso à Informação (Lei nº 12.527/2011 - LAI). Os *Checkpoints* são desenhados para verificar se a solução SIEM possui as capacidades técnicas necessárias para auditar acessos a dados pessoais, detectar vazamentos, suportar processos de anonimização e garantir a conformidade no uso emergente de sistemas de Inteligência Artificial (IA), assegurando a privacidade dos titulares e a transparência institucional. A tabela 4 apresenta os *Checkpoints* e as normativas de base.

Tabela 4 - *Checkpoints* do Domínio de Proteção e Governança de Dados (LGPD e IA)

Item	*Checkpoint* de Conformidade	Normativos de Referência
2.1	Conformidade com a LGPD e Transparência de Acessos: O *SIEM* audita e monitora acessos a dados pessoais e sensíveis e gera registros que comprovem conformidade com a LGPD e a LAI, fornecendo evidências para fiscalização e conformidade?	Lei nº 13.709/2018 (LGPD) Lei nº 12.527/2011 (LAI) CNJ Resolução nº 363/2021 TSE Resolução nº 23.650/2021 TSE Portaria nº 459/2021
2.2	Suporte à Anonimização/Pseudonimização de Dados em Logs: O *SIEM* dispõe de recursos nativos ou integráveis para anonimizar ou pseudonimizar dados pessoais contidos em logs, conforme as melhores práticas da LGPD e as normas do Judiciário?	Lei nº 13.709/2018 (LGPD) Lei nº 13.853/2019 CNJ Resolução nº 363/2021 TSE Resolução nº 23.650/2021
2.3	Monitoramento e Auditoria do Uso de Inteligência Artificial: Se a solução utilizar IA em suas funcionalidades, ela assegura a transparência, a auditabilidade, a explicabilidade dos resultados e a privacidade dos dados processados, em conformidade com as diretrizes do CNJ?	CNJ Resolução nº 332/2020 CNJ Resolução nº 615/2025
2.4	Suporte à Elaboração do RIPD e Detecção de Vazamentos: O *SIEM* possui mecanismos para identificar potenciais vazamentos de dados e gera relatórios e evidências que possam embasar a elaboração de Relatórios de Impacto à Proteção de Dados (RIPD) e a notificação à Autoridade Nacional de Proteção de Dados (ANPD)?	Lei nº 13.709/2018 (LGPD) Lei nº 13.853/2019 CNJ Resolução nº 363/2021 TSE Resolução nº 23.650/2021 SGD/MGI Portaria nº 852/2023
2.5	Criptografia e Proteção de Sistemas Críticos: O *SIEM* apoia a proteção de sistemas críticos com o uso de criptografia (como TLS) e certificação digital nos canais de comunicação e gera alertas sobre acessos indevidos que podem comprometer a integridade e a confidencialidade dos dados?	CNJ Resolução nº 396/2021 TSE Resolução nº 23.644/2021 TSE Resolução nº 23.650/2021 TSE Portaria nº 444/2021 TSE Portaria nº 263/2024
2.6	Gestão de Acessos e Informações Classificadas: O *SIEM* monitora acessos a informações classificadas em graus de sigilo, alerta sobre tentativas de acesso não autorizadas e se integra a políticas de controle de acesso baseado em funções (RBAC), conforme a LAI?	Lei nº 12.527/2011 (LAI) Lei nº 13.709/2018 (LGPD) TSE Resolução nº 23.650/2021 TSE Portaria nº 262/2024

- *Checkpoint* de Conformidade 2.1 e justificativas das normativas norteadoras:

Conformidade com a LGPD e Transparência de Acessos: O SIEM audita e monitora acessos a dados pessoais e sensíveis e gera registros que comprovem conformidade com a LGPD e a LAI, fornecendo evidências para fiscalização e conformidade?

O embasamento normativo para a auditoria de acessos a dados pessoais e sensíveis é estabelecido pela Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que exige a adoção de medidas de segurança (Art. 46) e a manutenção de registros das operações de tratamento (Art. 37), e pela Lei de Acesso à Informação (Lei nº 12.527/2011), que determina a proteção de informações sigilosas. No Poder Judiciário, a Resolução CNJ nº 363/2021 internaliza essas obrigações, exigindo a implementação de medidas técnicas para o monitoramento e registro de acessos. Para a Justiça Eleitoral, a Resolução TSE nº 23.650/2021 e a Portaria TSE nº 459/2021 detalham esses requisitos, demandando a geração de trilhas de auditoria com rastreabilidade e

a centralização de logs detalhados. A capacidade de um SIEM de coletar, monitorar e gerar registros constitui o meio técnico para fornecer as evidências e a "prova eletrônica" necessárias à demonstração de conformidade com este conjunto normativo.

- *Checkpoint* de Conformidade 2.2 e justificativas das normativas norteadoras:

Suporte à Anonimização/Pseudonimização de Dados em Logs: O SIEM dispõe de recursos nativos ou integráveis para anonimizar ou pseudonimizar dados pessoais contidos em logs, conforme as melhores práticas da LGPD e as normas do Judiciário?

O embasamento normativo para a necessidade de recursos de anonimização e pseudonimização em sistemas SIEM parte da Lei Geral de Proteção de Dados (Lei nº 13.709/2018), alterada pela Lei nº 13.853/2019, que define estes conceitos e estabelece os princípios de segurança e prevenção no tratamento de dados pessoais. Em cumprimento a esta legislação, a Resolução CNJ nº 363/2021 exige que os tribunais implementem medidas técnicas e administrativas para proteger os dados pessoais, sendo a pseudonimização uma medida técnica essencial para logs. No âmbito da Justiça Eleitoral, a Resolução TSE nº 23.650/2021 torna essa exigência explícita, ao determinar a "adoção de anonimização ou pseudonimização, sempre que necessário", e ao requerer que as soluções contratadas garantam a disponibilidade de tais recursos de segurança da informação.

- *Checkpoint* de Conformidade 2.3 e justificativas das normativas norteadoras:

Monitoramento e Auditoria do Uso de Inteligência Artificial: Se a solução utilizar IA em suas funcionalidades, ela assegura a transparência, a auditabilidade, a explicabilidade dos resultados e a privacidade dos dados processados, em conformidade com as diretrizes do CNJ?

O embasamento para o monitoramento e a auditoria de Inteligência Artificial (IA) em um SIEM é definido por normas específicas do Poder Judiciário. A Resolução CNJ nº 332/2020 estabelece a base para o uso de IA exigindo que as soluções atendam a princípios de transparência, previsibilidade e, fundamentalmente, a possibilidade de auditoria, além de garantir a conformidade com a LGPD e o segredo de justiça. Esta diretriz é aprofundada e detalhada pela Resolução CNJ Nº 615/2025, que estabelece requisitos explícitos para a governança, auditoria e monitoramento de soluções de IA. A norma torna mandatório o registro automático da utilização de IA nos logs do sistema para fins de auditoria e exige a anonimização de dados sigilosos utilizados no treinamento de modelos, criando um dever de transparência e controle sobre o funcionamento dos algoritmos.

- *Checkpoint* de Conformidade 2.4 e justificativas das normativas norteadoras:

Suporte à Elaboração do RIPD e Detecção de Vazamentos: O SIEM possui mecanismos para identificar potenciais vazamentos de dados e gera relatórios e evidências que possam embasar a elaboração de Relatórios de Impacto à Proteção de Dados (RIPD) e a notificação à Autoridade Nacional de Proteção de Dados (ANPD)?

O embasamento normativo para a utilização de um SIEM no suporte à elaboração do Relatório de Impacto à Proteção de Dados (RIPD) e à detecção de vazamentos origina-se na Lei Geral de Proteção de Dados (Lei nº 13.709/2018), consolidada pela Lei nº 13.853/2019, que exige a comunicação de incidentes de segurança e a elaboração do RIPD para tratamentos de alto risco. Esta diretriz é ecoada pelo *Framework* de Privacidade e Segurança da Informação da administração pública federal (Portaria SGD/MGI Nº 852/2023). No Poder Judiciário, a Resolução CNJ nº 363/2021 torna mandatórios os planos de resposta a incidentes e a realização de RIPD, processos para os quais um SIEM fornece evidências técnicas. Especificamente na Justiça Eleitoral, a Resolução TSE nº 23.650/2021 detalha essa obrigação, tornando indispensável a capacidade de detecção de um SIEM para cumprir os prazos de notificação e gerar os registros que subsidiam a elaboração e a revisão contínua do RIPD.

- *Checkpoint* de Conformidade 2.5 e justificativas das normativas norteadoras:

Criptografia e Proteção de Sistemas Críticos: O SIEM apoia a proteção de sistemas críticos por meio de criptografia (como TLS) e certificação digital nos canais de comunicação, e gera alertas sobre acessos indevidos que podem comprometer a integridade e a confidencialidade dos dados?

A base normativa para a proteção de sistemas críticos por meio de criptografia e monitoramento de acessos é estabelecida por um conjunto de diretrizes estratégicas e técnicas. A Resolução CNJ Nº 396/2021 e a Política de Segurança da Informação da Justiça Eleitoral (Resolução TSE Nº 23.644/2021) estabelecem como objetivo a proteção da confidencialidade e da integridade da informação, exigindo o uso de recursos criptográficos para dados classificados. Esta diretriz é detalhada tecnicamente pela Norma de Desenvolvimento Seguro (Portaria TSE nº 263/2024), que estabelece o uso de criptografia na transmissão de credenciais e o monitoramento de controles, como a certificação digital. A proteção de dados pessoais por meio desses mecanismos também é um requisito da Política de Privacidade da Justiça Eleitoral (Resolução TSE Nº 23.650/2021), cujos termos são definidos pela Portaria TSE Nº 444/2021. A capacidade de um SIEM de gerar alertas sobre acessos indevidos a estes canais seguros é o

instrumento técnico para verificar a eficácia dos controles e garantir a proteção exigida por estas normas.

- *Checkpoint* de Conformidade 2.6 e justificativas das normativas norteadoras:

Gestão de Acessos e Informações Classificadas: O SIEM monitora acessos a informações classificadas em graus de sigilo, alerta sobre tentativas de acesso não autorizados e integra-se a políticas de controle de acesso baseado em funções (RBAC), conforme a LAI?

O embasamento normativo para o monitoramento de acessos a dados sigilosos e para a aplicação de controles baseados em funções é estabelecido por leis federais e detalhado por normas específicas. A Lei de Acesso à Informação (Lei nº 12.527/2011) e a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) instituem o dever de proteger informações sigilosas e dados pessoais contra acessos não autorizados. No âmbito da Justiça Eleitoral, este mandato é instrumentalizado pela Portaria TSE Nº 262/2024, que exige a implementação de controles de acesso lógico baseados em perfis e funções. Adicionalmente, a Resolução TSE nº 23.650/2021 reforça a necessidade de procedimentos que garantam a segurança dos dados pessoais ao longo de todo o seu ciclo de vida. A capacidade de um SIEM de auditar, monitorar e gerar alertas sobre violações a essas políticas de acesso é, portanto, o mecanismo técnico que possibilita a verificação da conformidade com tais diretrizes.

5.2.3 *Checkpoints* - Gestão de Riscos e Continuidade de Negócios

O terceiro domínio foca nas capacidades proativas e reativas da segurança da informação, avaliando como a ferramenta SIEM se insere nos processos de gestão de riscos e nos Planos de Continuidade de Negócios (PCN) e de Recuperação de Desastres (PRD). Os *Checkpoints* verificam se a solução não apenas auxilia na identificação de ameaças e na gestão de vulnerabilidades, mas também fornece a observabilidade necessária para acionar planos de contingência e assegurar a resiliência operacional dos serviços críticos da Justiça Eleitoral, incluindo a alta disponibilidade da própria plataforma de monitoramento. A Tabela 5 apresenta os *Checkpoints* e as normativas de base.

Tabela 5 - *Checkpoints* do Domínio de Gestão de Riscos e Continuidade de Negócios

Item	*Checkpoint* de Conformidade	Normativos de Referência
3.1	Suporte à Gestão de Riscos de Segurança da Informação: O *SIEM* permite a identificação, avaliação e tratamento contínuos de riscos de segurança da informação, apoiando a detecção de ameaças e a tomada de decisões estratégicas	GSI Instrução Normativa nº 3/2021 CNJ Portaria nº 162/2021 (Anexo I) TSE Portaria nº

	para mitigá-los, em conformidade com as diretrizes normativas?	444/2021 TSE Portaria nº 459/2021
3.2	Gestão de Vulnerabilidades e Requisitos de Segurança: O *SIEM* apoia o cumprimento dos requisitos mínimos de segurança, com capacidade de detectar desvios de configuração, vulnerabilidades e violações de políticas, além de integrar-se a soluções de gestão de vulnerabilidades?	CNJ Resolução nº 396/2021 GSI Instrução Normativa nº 3/2021 TSE Resolução nº 23.644/2021 CNJ Portaria nº 162/2021 (Anexo V)
3.3	Suporte à Ativação de Planos de Continuidade e de Recuperação de Desastres: O *SIEM* contribui para o PCN e o PRD da Justiça Eleitoral, fornecendo dados e alertas que otimizam a resposta a incidentes, reduzem o tempo de inatividade e subsidiam a revisão da resiliência institucional?	CNJ Resolução nº 370/2021 GSI Instrução Normativa nº 3/2021 TSE Portaria nº 459/2021
3.4	Observabilidade sobre Impactos na Resiliência Operacional: O *SIEM* oferece observabilidade (*observability*) sobre o impacto de incidentes, permitindo à gestão avaliar a resiliência operacional, identificar riscos à disponibilidade de sistemas críticos e acionar os planos de contingência?	CNJ Resolução nº 396/2021 GSI Instrução Normativa nº 1/2020 CNJ Portaria nº 162/2021 (Anexos I e V) TSE Portaria nº 387/2024 TSE Portaria nº 459/2021
3.5	Alta Disponibilidade e Resiliência do Próprio *SIEM*: A arquitetura do *SIEM* dispõe de mecanismos de alta disponibilidade (HA) e resiliência para manter a continuidade do monitoramento, mesmo em caso de falhas ou desastres, atendendo às exigências de sistemas críticos do Poder Judiciário?	CNJ Resolução nº 325/2020 CNJ Resolução nº 396/2021 GSI Instrução Normativa nº 3/2021 TSE Portaria nº 459/2021

- *Checkpoint* de Conformidade 3.1 e justificativas das normativas norteadoras:

Suporte à Gestão de Riscos de Segurança da Informação: O SIEM permite a identificação, avaliação e tratamento de riscos de segurança da informação de forma contínua, apoiando a detecção de ameaças e a tomada de decisões estratégicas para mitigar riscos, conforme as diretrizes normativas?

O embasamento normativo para o suporte do SIEM à gestão de riscos de segurança da informação é estabelecido pela Instrução Normativa GSI/PR Nº 3/2021, que institui o processo obrigatório e contínuo de identificação, avaliação e tratamento de riscos na administração pública. A operacionalização deste processo é detalhada no protocolo da Portaria CNJ nº 162/2021, que descreve as funções de "identificar" e "detectar" como essenciais para o diagnóstico contínuo dos ativos. A execução dessas funções depende diretamente da capacidade de um SIEM de realizar o gerenciamento e monitoramento centralizado de logs, um requisito técnico especificado pela Portaria TSE nº 459/2021. A aplicação consistente deste processo é amparada pela padronização de termos como "Risco" e "Ameaça", definidos na Portaria TSE nº 444/2021, garantindo uma abordagem uniforme na tomada de decisões para mitigar riscos.

- *Checkpoint* de Conformidade 3.2 e justificativas das normativas norteadoras:

Gestão de Vulnerabilidades e Requisitos de Segurança: O SIEM apoia o cumprimento dos requisitos mínimos de segurança, com capacidade de detectar desvios de configuração,

vulnerabilidades e violações de políticas, além de integrar-se a soluções de gestão de vulnerabilidades?

O embasamento normativo para a gestão de vulnerabilidades e o cumprimento de requisitos de segurança é estabelecido pela Instrução Normativa GSI/PR Nº 3/2021, que exige um processo contínuo de Avaliação de Conformidade para a administração pública. No Poder Judiciário, a Resolução CNJ Nº 396/2021 (ENSEC-PJ) reforça esta diretriz ao determinar a realização de testes periódicos para aferir a eficácia dos controles. A Política de Segurança da Informação da Justiça Eleitoral (Resolução TSE nº 23.644/2021), por sua vez, institui formalmente o processo de Gestão de Vulnerabilidades. A execução dessas atividades é apoiada por manuais técnicos como o da Portaria CNJ nº 162/2021 (Anexo V), que recomenda o "diagnóstico contínuo" através da análise de logs. A capacidade de um SIEM de centralizar e analisar estes logs para detectar desvios de configuração e vulnerabilidades é, portanto, o mecanismo técnico que operacionaliza o cumprimento dessas normas.

- *Checkpoint* de Conformidade 3.3 e justificativas das normativas norteadoras:

Suporte à Ativação de Planos de Continuidade e Recuperação de Desastres: O SIEM contribui para o PCN e o PRD da Justiça Eleitoral, fornecendo dados e alertas que otimizam a resposta a incidentes, reduzem o tempo de inatividade e subsidiam a revisão da resiliência institucional?

O embasamento normativo para o suporte do SIEM aos Planos de Continuidade de Negócios (PCN) e de Recuperação de Desastres (PRD) é estabelecido pela Instrução Normativa GSI/PR nº 3/2021, que torna a Gestão de Continuidade de Negócios um processo obrigatório, visando minimizar os impactos de desastres e indisponibilidades. A otimização da resposta a incidentes e a redução do tempo de inatividade, objetivos diretos de um SIEM, contribuem para a eficiência e efetividade operacional preconizadas pela Estratégia Nacional de TIC do Poder Judiciário (Resolução CNJ Nº 370/2021). A capacidade do SIEM de fornecer alertas em tempo real e subsídios para a análise pós-incidente depende fundamentalmente da gestão e monitoramento de logs, conforme detalhado na Portaria TSE Nº 459/2021. A análise dos dados providos pelo SIEM é, portanto, o insumo técnico que permite não apenas a ativação da resposta a incidentes, mas também a revisão e o aprimoramento contínuo da resiliência institucional.

- *Checkpoint* de Conformidade 3.4 e justificativas das normativas norteadoras:

Observabilidade sobre Impactos na Resiliência Operacional: O SIEM oferece observabilidade (observability) sobre o impacto de incidentes, permitindo à gestão avaliar a resiliência operacional, identificar riscos à disponibilidade de sistemas críticos e acionar os planos de contingência?

O embasamento normativo para a necessidade de observabilidade sobre a resiliência operacional é estabelecido por diretrizes estratégicas e processuais. A Estratégia Nacional de Segurança Cibernética do Poder Judiciário (Resolução CNJ nº 396/2021) e a Instrução Normativa GSI/PR nº 1/2020 exigem a garantia da continuidade operacional e a gestão dos impactos de incidentes, demandando uma visão clara do ambiente. Esta necessidade é detalhada nos protocolos da Portaria CNJ Nº 162/2021 (Anexos I e V), que definem as funções de "detectar" anomalias e realizar o "diagnóstico contínuo" de infraestruturas críticas. No nível operacional, a Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR), reestruturada pela Portaria TSE Nº 387/2024, utiliza essa visibilidade para avaliar o impacto de eventos e acionar medidas de recuperação. A capacidade de um SIEM de transformar os logs, cuja gestão é normatizada pela Portaria TSE nº 459/2021, em inteligência acionável é o que fornece a observabilidade para a gestão avaliar a resiliência em conformidade com estas normas.

- *Checkpoint* de Conformidade 3.5 e justificativas das normativas norteadoras:

Alta Disponibilidade e Resiliência do Próprio SIEM: A arquitetura do SIEM dispõe de mecanismos de alta disponibilidade (HA) e resiliência para manter a continuidade do monitoramento, mesmo em caso de falhas ou desastres, atendendo às exigências de sistemas críticos do Poder Judiciário?

O embasamento normativo para a alta disponibilidade e resiliência do próprio SIEM derivam das diretrizes estratégicas do Poder Judiciário. As Resoluções CNJ nº 325/2020 e nº 396/2021 estabelecem como objetivos a garantia da "disponibilidade das informações" e a "continuidade operacional" dos serviços essenciais da Justiça, tornando a resiliência das ferramentas de segurança um requisito para o cumprimento dessas estratégias. Esta necessidade alinha-se ao processo obrigatório de Gestão de Continuidade de Negócios, instituído pela Instrução Normativa GSI nº 3/2021, que exige planos para a recuperação de operações em caso de falhas. Adicionalmente, a resiliência do SIEM é um requisito implícito para atender a normas técnicas como a Portaria TSE nº 459/2021, que demanda a disponibilidade e integridade contínuas dos logs para fins de auditoria e investigação.

5.2.4 *Checkpoints* - Auditoria, Logs e Transparência

Este domínio constitui o núcleo técnico da gestão de eventos de segurança, com foco na capacidade da ferramenta SIEM de fornecer trilhas de auditoria robustas, garantir a rastreabilidade das ações e respaldar os princípios de transparência. Os *Checkpoints* avaliam

desde a coleta e a gestão centralizadas de logs até a sua retenção segura e a integridade, assegurando que os registros possam ser utilizados como evidências digitais válidas para auditorias internas e externas, processos legais e para a prestação de contas à sociedade, em linha com a LAI e as normas de gestão documental. A Tabela 6 apresenta os *Checkpoints* e as normativas de base.

Tabela 6 - *Checkpoints* do Domínio de Auditoria, Logs e Transparência

Item	*Checkpoint* de Conformidade	Normativos de Referência
4.1	Coleta e Gestão Centralizada de Logs: O *SIEM* centraliza a coleta, normalização, correlação e o armazenamento seguro de logs de sistemas e infraestrutura da Justiça Eleitoral, em conformidade com as diretrizes de registros do GSI e do Judiciário?	GSI Norma Complementar nº 21/2014 CNJ Portaria nº 162/2021 TSE Portaria nº 263/2024 TSE Portaria nº 459/2021
4.2	Auditoria de Sistemas de Gestão de Processos e Documentos: O SIEM possui capacidade de se integrar a sistemas de terceiros, como os de gestão processual e documental (p. ex., PJe, MoReq-Jus), assegurando a rastreabilidade das ações e a integridade dos registros eletrônicos, conforme as normativas do CNJ e a legislação de arquivos?	CNJ Resolução nº 324/2020 CNJ Resolução nº 522/2023 CNJ Manual de Gestão Documental do Poder Judiciário TSE Portaria nº 263/2024
4.3	Relatórios de Conformidade e Prestação de Contas: O *SIEM* gera relatórios analíticos de conformidade que evidenciam o cumprimento das políticas de segurança, de acesso à informação e de proteção de dados, apoiando a alta gestão na avaliação da postura de segurança e na prestação de contas?	Lei nº 12.527/2011 (LAI) GSI Decreto nº 9.573/2018 TSE Portaria nº 263/2024 TSE Portaria nº 459/2021
4.4	Geração de Evidências para Auditorias Internas e Externas: O *SIEM* suporta auditorias internas e externas, fornecendo dados e relatórios que permitam aferir a eficácia dos controles de segurança, a conformidade com as políticas e o cumprimento das regulamentações aplicáveis?	CNJ Resolução nº 370/2021 GSI Instrução Normativa nº 3/2021 TSE Resolução nº 23.644/2021 TSE Portaria nº 263/2024 TSE Portaria nº 387/2024
4.5	Capacidade de Processamento: O *SIEM* possui a capacidade técnica (escalabilidade de ingestão e armazenamento) para processar e armazenar o alto volume de eventos gerados pela infraestrutura da Justiça Eleitoral, garantindo que todos os logs relevantes sejam coletados sem perdas?	GSI Norma Complementar nº 21/2014 Decreto nº 11.200/2022 TSE Portaria nº 263/2024 TSE Portaria nº 459/2021
4.6	Retenção e Integridade dos Logs para Fins Legais e Regulatórios: O *SIEM* garante a retenção dos logs por períodos adequados e sua integridade (imutabilidade), de modo que possam servir como evidências válidas em investigações ou fiscalizações, em conformidade com as exigências legais e as normas de gestão de registros?	Lei nº 8.159/1991 Lei nº 12.682/2012 CNJ Resolução nº 324/2020 CNJ Resolução nº 363/2021 CNJ Resolução nº 522/2023 GSI Norma Complementar nº 21/2014 GSI Portaria nº 93/2021 TSE Portaria nº 459/2021

- *Checkpoint* de Conformidade 4.1 e justificativas das normativas norteadoras:

Coleta e Gestão Centralizada de Logs: O SIEM centraliza a coleta, normalização, correlação e o armazenamento seguro de logs de sistemas e infraestrutura da Justiça Eleitoral, em conformidade com as diretrizes de registros do GSI e do Judiciário?

O embasamento normativo para a coleta e gestão centralizadas de logs é detalhado por um conjunto de normas técnicas e procedimentais. A Portaria TSE nº 459/2021 institui a norma de gerenciamento e monitoramento de logs para a Justiça Eleitoral, exigindo sua coleta, armazenamento seguro e verificação de integridade. Esta diretriz é complementada pela Portaria TSE nº 263/2024, que determina que os sistemas devem ser desenvolvidos para gerar logs detalhados e replicá-los em uma base centralizada. A necessidade de análise desses registros para fins de "diagnóstico contínuo" e de auditoria também é um requisito dos protocolos e manuais de segurança do Poder Judiciário, aprovados pela Portaria CNJ nº 162/2021. A utilização de uma ferramenta para a coleta e preservação de evidências alinha-se, ainda, às diretrizes da Administração Pública Federal, conforme a Norma Complementar GSI nº 21/IN01.

- *Checkpoint* de Conformidade 4.2 e justificativas das normativas norteadoras:

Auditoria de Sistemas de Gestão de Processos e Documentos: O SIEM possui capacidade de se integrar a sistemas de terceiros, como os de gestão processual e documental (p. ex., PJe, MoReq-Jus), assegurando a rastreabilidade de ações e a integridade de registros eletrônicos, conforme as normativas do CNJ e a legislação de arquivos?

O embasamento normativo para a auditoria de sistemas de gestão processual e documental é definido por um conjunto de diretrizes do Conselho Nacional de Justiça. O Modelo de Requisitos para Sistemas Informatizados Terceiros de Gestão de Processos e Documentos (MoReq-Jus), instituído pela Resolução CNJ Nº 522/2023, e o Programa Nacional de Gestão Documental (Proname), da Resolução CNJ Nº 324/2020, estabelecem a necessidade de garantir a integridade, autenticidade e rastreabilidade dos registros eletrônicos, sendo essa premissa detalhada no Manual de Gestão Documental do Poder Judiciário. Em nível técnico, a Portaria TSE nº 263/2024 exige que os sistemas sejam desenvolvidos com mecanismos de geração de logs detalhados. A capacidade de um SIEM de coletar e analisar os logs desses sistemas é, portanto, o instrumento para auditar os controles, verificar a manutenção da cadeia de custódia e assegurar a integridade das ações, em conformidade com este conjunto normativo.

- *Checkpoint* de Conformidade 4.3 e justificativas das normativas norteadoras:

Relatórios de Conformidade e Prestação de Contas: O SIEM gera relatórios analíticos de conformidade que evidenciam o cumprimento das políticas de segurança, acesso à informação e proteção de dados, apoiando a alta gestão na avaliação da postura de segurança e na prestação de contas?

O embasamento normativo para a geração de relatórios de conformidade e prestação de contas é estabelecido por diretrizes estratégicas e técnicas. A Política Nacional de Segurança das Infraestruturas Críticas (Decreto GSI nº 9.573/2018) e a Lei de Acesso à Informação (Lei nº 12.527/2011) requerem um sistema centralizado para gestão da informação de segurança e a demonstração de transparência no tratamento de dados. A capacidade de gerar tais relatórios depende da análise de logs detalhados, cuja produção e gestão íntegra são requisitos da Norma de Desenvolvimento Seguro de Sistemas (Portaria TSE Nº 263/2024) e da Norma de Gerenciamento e Monitoramento de Logs (Portaria TSE Nº 459/2021). A funcionalidade de um SIEM de analisar estes registros para criar relatórios analíticos é, portanto, o instrumento técnico que evidencia o cumprimento das políticas, apoia a alta gestão na avaliação da postura de segurança e viabiliza a prestação de contas.

- *Checkpoint* de Conformidade 4.4 e justificativas das normativas norteadoras:

Geração de Evidências para Auditorias Internas e Externas: O SIEM suporta auditorias internas e externas, fornecendo dados e relatórios que permitam aferir a eficácia dos controles de segurança, a conformidade com as políticas e o atendimento às regulamentações aplicáveis?

O embasamento normativo para o suporte a auditorias é estabelecido por diretrizes que exigem a comprovação da eficácia dos controles. A Instrução Normativa GSI/PR nº 3/2021 e a Resolução CNJ nº 370/2021 (ENTIC-JUD) determinam a necessidade de avaliações de conformidade e a manutenção de evidências documentais para subsidiar auditorias internas e externas no Poder Judiciário. No âmbito da Justiça Eleitoral, a Resolução TSE nº 23.644/2021 (PSI) eleva a "auditabilidade" à condição de princípio, enquanto normas como a Portaria TSE nº 387/2024 (ETIR) e a Portaria TSE nº 263/2024 (Desenvolvimento Seguro) requerem a coleta de evidências digitais e o registro de eventos para fins de auditoria. A capacidade de um SIEM de centralizar, armazenar e gerar relatórios a partir dos logs do sistema é, portanto, o instrumento técnico que fornece as evidências necessárias para atender a estas demandas de auditoria.

- *Checkpoint* de Conformidade 4.5 e justificativas das normativas norteadoras:

Capacidade de Processamento: O SIEM possui a capacidade técnica (escalabilidade de ingestão e armazenamento) para processar e armazenar o alto volume de eventos gerados pela infraestrutura da Justiça Eleitoral, garantindo que todos os logs relevantes sejam coletados sem perdas?

O embasamento normativo para a capacidade de processamento e armazenamento de um SIEM é definido por diretrizes estratégicas e técnicas. O Plano Nacional de Segurança de Infraestruturas Críticas (Decreto nº 11.200/2022) estabelece a necessidade de um "sistema centralizado de gestão da informação, robusto e eficaz", o que demanda elevada capacidade técnica. No âmbito do TSE, a Portaria Nº 459/2021 detalha esta exigência ao requerer "espaço de armazenamento adequado" para logs, enquanto a Portaria Nº 263/2024 determina a replicação de logs de todos os sistemas para uma base centralizada, gerando um alto volume de dados que a solução deve suportar. A utilização de uma ferramenta com capacidade técnica para a coleta e preservação de evidências é, ainda, uma diretriz para a Administração Pública Federal, conforme a Norma Complementar GSI nº 21/IN01.

- *Checkpoint* de Conformidade 4.6 e justificativas das normativas norteadoras:

Retenção e Integridade dos Logs para Fins Legais e Regulatórios: O SIEM garante a retenção dos logs por períodos adequados e sua integridade (imutabilidade), de modo que possam servir como evidências válidas em investigações ou fiscalizações, em conformidade com as exigências legais e as normas de gestão de registros?

O embasamento normativo para a retenção e integridade de logs como evidências válidas é fundamentado em leis federais e detalhado por resoluções e normas técnicas. As Leis nº 8.159/1991 (Lei Geral de Arquivos) e nº 12.682/2012 (Lei da Digitalização) estabelecem que os registros digitais têm valor probatório, desde que sua autenticidade, integridade e preservação sejam asseguradas. No Poder Judiciário, as Resoluções CNJ nº 324/2020 (Proname) e nº 522/2023 (MoReq-Jus) reforçam essa necessidade ao exigir a manutenção da cadeia de custódia e a garantia da integridade dos documentos digitais. Adicionalmente, a Resolução CNJ nº 363/2021 requer o registro dos prazos de conservação de dados, e a Norma Complementar GSI nº 21 orienta a preservação de logs como evidência. Em nível técnico, a Portaria TSE nº 459/2021 determina o uso de mecanismos, como resumos criptográficos, para verificar a integridade, conceito definido na Portaria GSI/PR nº 93/2021. A capacidade de um SIEM de garantir a retenção e a imutabilidade dos logs é, portanto, o meio técnico para atender a este conjunto de normas.

5.2.5 *Checkpoints* - Gestão de Incidentes e Resposta

O quinto e último domínio do *framework* aborda a dimensão operacional da cibersegurança, com foco nas capacidades da ferramenta SIEM para gerenciar o ciclo de vida completo de um incidente, desde a detecção em tempo real até a resposta e a investigação pós-incidente. Os *Checkpoints* avaliam funcionalidades avançadas, como a orquestração e automação da resposta (SOAR), a análise comportamental (UEBA), a integração com inteligência de ameaças e a garantia de soberania dos dados por meio da implantação em infraestrutura local. A Tabela 7 traz os *Checkpoints* e as normativas embasadoras.

Tabela 7 - *Checkpoints* do Domínio de Gestão de Incidentes e Resposta

Item	*Checkpoint* de Conformidade	Normativos de Referência
5.1	Detecção em Tempo Real de Ameaças: O *SIEM* é capaz de realizar a detecção de ameaças cibernéticas e atividades anômalas em tempo real, gerando alertas imediatos e acionáveis para a equipe de resposta a incidentes da Justiça Eleitoral?	CNJ Portaria nº 162/2021 (Anexo I) TSE Portaria nº 387/2024 TSE Portaria nº 459/2021
5.2	Capacidade de Resposta a Incidentes (Automação/Integração): O *SIEM* permite a integração com ferramentas ou processos de resposta a incidentes (SOAR), possibilitando ações de contenção ou mitigação automatizadas ou semiautomatizadas após a detecção de um incidente?	Decreto nº 10.222/2020 GSI Decreto nº 10.569/2020 CNJ Portaria nº 162/2021 (Anexo I) TSE Portaria nº 387/2024
5.3	Análise de Comportamento Anômalo (UEBA/AI): O *SIEM* emprega técnicas avançadas como Análise de Comportamento de Usuário e Entidades (UEBA) ou Inteligência Artificial para identificar ameaças internas ou ataques sofisticados, indo além da detecção baseada em assinaturas?	CNJ Resolução nº 332/2020 CNJ Resolução nº 615/2025
5.4	Integração com Fontes de Inteligência de Ameaças: O *SIEM* pode integrar-se com fontes de inteligência de ameaças (*Threat Intelligence*) para enriquecer os dados de log e melhorar a capacidade de detecção de Indicadores de Comprometimento (IoCs) de ataques conhecidos e emergentes?	CNJ Resolução nº 383/2021 CNJ Resolução nº 396/2021 CNJ Portaria nº 162/2021
5.5	Capacidade de Investigação e Busca Retrospectiva: O *SIEM* oferece funcionalidades robustas de busca e análise retrospectiva de logs, permitindo que a equipe de segurança investigue incidentes passados, identifique a linha do tempo de ataques e colete informações para remediação completa e análise forense?	GSI Instrução Normativa nº 21/2014 CNJ Portaria nº 162/2021 TSE Portaria nº 387/2024 TSE Portaria nº 459/2021
5.6	Capacidade de Implantação *On-Premises*: O *SIEM* opera integralmente em infraestrutura local (*on-premises*), assegurando o controle físico e lógico sobre os dados e logs de segurança, em conformidade com as exigências de soberania e tutela da informação governamental?	Lei nº 13.709/2018 (LGPD) CNJ Resolução nº 396/2021 GSI Norma Complementar nº 05/IN01/DSIC GSI Instrução Normativa nº 5/2021 TSE Portaria nº 459/2021

- *Checkpoint* de Conformidade 5.1 e justificativas das normativas norteadoras:

Detecção em Tempo Real de Ameaças: O SIEM é capaz de detectar ameaças cibernéticas e atividades anômalas em tempo real, gerando alertas imediatos e acionáveis para a equipe de resposta a incidentes da Justiça Eleitoral?

O embasamento normativo para a detecção de ameaças em tempo real é estabelecido pelo Protocolo de Prevenção a Incidentes Cibernéticos do Poder Judiciário (Portaria CNJ Nº 162/2021), que define a "detecção" como uma função básica de segurança e exige o "monitoramento contínuo para a detecção de anomalias e eventos". No âmbito da Justiça Eleitoral, a Portaria TSE nº 387/2024 atribui à Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR) a responsabilidade de identificar e tratar incidentes "em tempo hábil", atuando "imediatamente" ao identificar um risco. A capacidade de análise para essa detecção é fundamentada na Portaria TSE nº 459/2021, que exige que todos os eventos de segurança registrados em logs sejam formalmente analisados. A funcionalidade de um SIEM de correlacionar logs para detectar atividades anômalas e gerar alertas imediatos é, portanto, o mecanismo técnico que implementa o cumprimento dessas diretrizes.

- *Checkpoint* de Conformidade 5.2 e justificativas das normativas norteadoras:

Capacidade de Resposta a Incidentes (Automação/Integração): O SIEM permite a integração com ferramentas ou processos de resposta a incidentes (SOAR), possibilitando ações de contenção ou mitigação automatizadas ou semiautomatizadas após a detecção de um incidente?

O embasamento normativo para a automação da resposta a incidentes está estabelecido em diretrizes estratégicas nacionais. A Estratégia Nacional de Segurança Cibernética (Decreto nº 10.222/2020) menciona explicitamente a integração de SIEM com plataformas SOAR (*Security Orchestration, Automation and Response*) para aprimorar a eficácia da resposta, enquanto a Estratégia Nacional de Segurança de Infraestruturas Críticas (Decreto nº 10.569/2020) destaca o uso de soluções automatizadas como primordial. No Poder Judiciário, o Protocolo de Prevenção a Incidentes Cibernéticos (Portaria CNJ nº 162/2021) detalha as ações de contenção e mitigação passíveis de automação. A capacidade de automatizar a resposta é, ainda, um requisito operacional para que a Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR) do TSE possa atuar de forma "imediata" e "padronizada", conforme determina a Portaria TSE Nº 387/2024.

- *Checkpoint* de Conformidade 5.3 e justificativas das normativas norteadoras:

Análise de Comportamento Anômalo (UEBA/AI): O SIEM emprega técnicas avançadas, como Análise de Comportamento de Usuário e Entidades (UEBA) ou Inteligência Artificial, para

identificar ameaças internas ou ataques sofisticados, indo além da detecção baseada em assinaturas?

O embasamento normativo para o emprego de Inteligência Artificial (IA) e de Análise de Comportamento (UEBA) em um SIEM é definido por diretrizes do Conselho Nacional de Justiça. A Resolução CNJ nº 332/2020 estabelece os princípios para o uso de IA no Poder Judiciário, exigindo que as tecnologias atendam a critérios de transparência, imparcialidade e, fundamentalmente, a possibilidade de auditoria de seus resultados. Esta diretriz é aprofundada pela Resolução CNJ Nº 615/2025, a qual aprofunda a discussão ao mencionar implicitamente o uso de UEBA (*User & Entity Behavior Analytics*) ao classificar como uma finalidade de alto risco, para soluções de inteligência artificial, a "identificação de perfis e de padrões comportamentais de pessoas".

- *Checkpoint* de Conformidade 5.4 e justificativas das normativas norteadoras:

Integração com Fontes de Inteligência de Ameaças: O SIEM pode integrar-se a fontes de inteligência de ameaças (Threat Intelligence) para enriquecer os dados de log e aprimorar a capacidade de detecção de Indicadores de Comprometimento (IoCs) de ataques conhecidos e emergentes?

O embasamento normativo para a integração de um SIEM com fontes de inteligência de ameaças é estabelecido por diretrizes estratégicas do Conselho Nacional de Justiça. A Estratégia Nacional de Segurança Cibernética do Poder Judiciário (Resolução CNJ Nº 396/2021) determina explicitamente a necessidade de "utilizar tecnologia que permita a inteligência em ameaças cibernéticas". Esta diretriz alinha-se à finalidade do Sistema de Inteligência de Segurança Institucional do Poder Judiciário (Resolução CNJ Nº 383/2021), que visa a produção de conhecimento para identificar e acompanhar ameaças. Os protocolos e manuais aprovados pela Portaria CNJ Nº 162/2021 detalham essa necessidade ao preverem a criação de uma "base de conhecimento de defesa" e ao referenciarem *framework*s como o MITRE ATT&CK. A capacidade de um SIEM de se integrar a fontes de *Threat Intelligence* é, portanto, o mecanismo técnico que operacionaliza o cumprimento destas normas.

- *Checkpoint* de Conformidade 5.5 e justificativas das normativas norteadoras:

Capacidade de Investigação e Busca Retrospectiva: O SIEM oferece funcionalidades robustas de busca e análise retrospectiva de logs, permitindo que a equipe de segurança investigue incidentes passados, identifique a linha do tempo de ataques e colete informações para remediação completa e análise forense?

O embasamento normativo para a capacidade de investigação e de busca retrospectiva é definido por diretrizes federais e protocolos do Poder Judiciário. A Instrução Normativa GSI nº 21/2014 e os protocolos de investigação e prevenção da Portaria CNJ nº 162/2021 estabelecem a necessidade de coletar e preservar evidências para identificar as causas dos incidentes e subsidiar a análise de "lições aprendidas". No âmbito da Justiça Eleitoral, a Portaria TSE nº 387/2024 atribui à Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR) a competência de armazenar registros para a formação de séries históricas e para fins de auditoria. A capacidade de realizar tais investigações é tecnicamente amparada pela Portaria TSE nº 459/2021, que exige a retenção e a garantia de integridade dos logs para a execução de auditorias legais e forenses. A funcionalidade de um SIEM de permitir a busca e análise retrospectiva de logs é, portanto, o instrumento que viabiliza o cumprimento destas normas.

- *Checkpoint* de Conformidade 5.6 e justificativas das normativas norteadoras:

Capacidade de Implantação On-Premises: O SIEM opera integralmente na infraestrutura local (on-premises), assegurando o controle físico e lógico sobre os dados e logs de segurança, em conformidade com as exigências de soberania e de tutela da informação governamental?

O embasamento normativo para a implantação de um SIEM em infraestrutura local (*on-premises*) é sustentado pela necessidade de controle sobre dados e sistemas. A Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (Resolução CNJ nº 396/2021) exigem medidas de segurança rigorosas e a proteção de infraestruturas críticas. A preferência pela infraestrutura local é reforçada pela Instrução Normativa GSI nº 5/2021, que restringe o tratamento de informações sigilosas fora do território nacional, em atenção à tutela da informação governamental. Em nível operacional, a Norma Complementar GSI nº 05 define os requisitos para a adoção segura de computação em nuvem, enquanto a Portaria TSE Nº 459/2021 materializa essa exigência ao determinar que os logs devem ser mantidos em "localização física em área sujeita a controles de segurança".

5.3 Validação do *framework* FCAS-JE

A validação do *framework* de conformidade para sistemas de gerenciamento de eventos e de informações de segurança na Justiça Eleitoral fundamenta-se na análise técnica das soluções *Wazuh, Elastic Stack e Graylog*. A seleção dessas ferramentas justifica-se pela arquitetura e pela maturidade operacional no mercado de cibersegurança. O processo verifica a

viabilidade de implementação dos requisitos estabelecidos diante das capacidades de cada sistema.

O mapeamento analítico considerou somente as informações presentes nas documentações oficiais dos desenvolvedores. O estudo comparou cada critério do *framework* às funcionalidades documentadas para garantir uma validação baseada em especificações técnicas verificáveis.

Diante da documentação oficial, a análise contemplou exclusivamente as versões de código aberto ou gratuitas. Funcionalidades vinculadas a licenças comerciais ou camadas corporativas pagas foram excluídas do escopo. Essa restrição garante a aplicabilidade do modelo em cenários de gestão pública com limitações orçamentárias.

Os níveis de aderência técnica foram categorizados em duas classificações: Atende e Não atende. A classificação “Atende” foi aplicada quando a documentação oficial do fabricante descreve a implementação nativa da funcionalidade ou a viabilidade de sua configuração. A classificação “Não atende” foi atribuída aos requisitos cujos aspectos ou funcionalidades não foram encontrados nos manuais técnicos dos desenvolvedores. Essa categorização permite sistematizar os dados, evidenciando o grau de aderência das soluções *Wazuh, Elastic Stack* e *Graylog* aos domínios temáticos e conformidade estabelecidos.

A validação do instrumento, com o auxílio da ferramenta de IA NotebookLM, resultou no mapeamento de conformidade entre os *Checkpoints* extraídos das 41 normativas estudadas e as capacidades funcionais descritas pelos fabricantes. O mapeamento sistemático avaliou as soluções de tecnologia na Tabela 8 a seguir, evidenciando o grau de aderência às diretrizes de segurança e conformidade estabelecidas pelo *framework* FCAS-JE.

Tabela 8 – Aplicação do *Framework* FCAS-JE nas soluções SIEM *open source*

Domínio	***Checkpoint***	***Wazuh***	***Elastic Stack***	***Graylog***
Governança e Gestão Estratégica de TIC	**1.1**	✔	✔	✔
	1.2	✔	-	-
	1.3	✔	-	-
	1.4	✔	✔	✔
	1.5	✔	✔	-
Proteção e Governança de Dados (LGPD e IA)	**2.1**	✔	-	-
	2.2	✔	✔	✔
	2.3	-	-	-

	2.4	✔	✔	✔
	2.5	✔	✔	✔
	2.6	✔	✔	✔
Gestão de Riscos e Continuidade de Negócios	**3.1**	✔	-	-
	3.2	✔	-	-
	3.3	✔	✔	✔
	3.4	✔	✔	✔
	3.5	✔	✔	✔
Auditoria, *Logs* e Transparência	**4.1**	✔	✔	✔
	4.2	✔	✔	✔
	4.3	✔	-	-
	4.4	✔	✔	✔
	4.5	✔	✔	✔
	4.6	✔	✔	-
Gestão de Incidentes e Resposta	**5.1**	✔	✔	✔
	5.2	✔	-	-
	5.3	-	-	-
	5.4	✔	✔	-
	5.5	✔	✔	✔
	5.6	✔	✔	✔

A aplicação do framework de conformidade FCAS-JE às soluções *Wazuh*, *Elastic Stack* e *Graylog* revelou disparidades significativas em seus níveis de aderência regulatória. Com base nos dados consolidados na Tabela 8, a ferramenta Wazuh demonstrou ser a solução *open source* mais aderente às exigências da Justiça Eleitoral, especialmente pela integração nativa de controles que facilitam a conformidade com as diretrizes de auditoria e monitoramento. Essa distinção técnica reflete a capacidade da ferramenta em atender a uma maior quantidade de *checkpoints* extraídos das 41 normativas estudadas.

Entretanto, o levantamento técnico identificou lacunas de conformidade em todas as ferramentas analisadas, com destaque para o item 2.3, referente ao monitoramento e auditoria do uso de Inteligência Artificial. Embora as soluções utilizem algoritmos para detecção, as documentações oficiais das versões *open source* não descrevem mecanismos que assegurem a transparência e a explicabilidade exigidas pelas Resoluções do CNJ nº 332/2020 e nº 615/2025. A ausência de evidências documentais sobre a auditabilidade desses processos algorítmicos impede a validação plena da privacidade e segurança dos dados sob a ótica da conformidade institucional do Poder Judiciário.

Da mesma forma, as capacidades de análise de comportamento anômalo via UEBA ou IA, descritas no item 5.3, carecem de comprovação documental quanto à aderência às normas de cibersegurança do CNJ. Embora as ferramentas processem grandes volumes de dados, a ausência de descrições técnicas sobre a explicabilidade das detecções automatizadas impossibilita a validação desses controles sob a ótica da conformidade regulatória estrita. Tais achados indicam que a implementação dessas tecnologias na Justiça Eleitoral pode requerer o desenvolvimento de camadas metodológicas suplementares para garantir a integridade e a transparência do processo eleitoral.

Assim, este estudo reforça a utilidade do framework FCAS-JE como uma ferramenta padronizada para escolher soluções SIEM na Justiça Eleitoral. A validação e os achados demonstram que o *framework* funciona como uma conexão entre as exigências regulatórias e a aplicação prática dessas tecnologias de segurança.

6 CONSIDERAÇÕES FINAIS

Este capítulo apresenta a síntese dos resultados obtidos na investigação acerca dos desafios à implementação de sistemas SIEM no âmbito da Justiça Eleitoral. Expõe o desenvolvimento do *framework* FCAS-JE como solução para a lacuna identificada entre as demandas técnicas operacionais e o denso arcabouço normativo nacional. Estruturalmente, descreve-se primeiro a conclusão geral do estudo, fundamentada nas respostas às perguntas de pesquisa que nortearam o desenvolvimento do trabalho. Sequencialmente, detalha-se a principal contribuição técnico-científica e institucional gerada por esta pesquisa. Adicionalmente, discutem-se as limitações encontradas e propõem-se perspectivas para trabalhos futuros, visando a continuidade e o aprimoramento da temática frente às inovações tecnológicas. Por fim, apresentam-se os produtos acadêmicos e as publicações científicas resultantes desta investigação, que atestam a validação externa e a relevância do estudo para a comunidade científica.

6.1 Conclusão geral

A pesquisa se propôs a endereçar o complexo desafio da adoção de Sistemas de Gerenciamento de Eventos e Informações de Segurança (SIEM) no contexto da Justiça Eleitoral, um ambiente de alta criticidade e densa regulação. A pesquisa partiu da constatação de uma lacuna entre a necessidade técnica de monitoramento avançado e a ausência de um guia que traduzisse o vasto arcabouço normativo brasileiro em requisitos práticos. Como principal contribuição, foi desenvolvido o *Framework* de Conformidade para Adoção de SIEM na Justiça Eleitoral (FCAS-JE), um instrumento metodológico construído a partir da Análise de Conteúdo de documentos legais. Este capítulo final realiza uma análise sobre os resultados alcançados, avaliando o cumprimento dos objetivos traçados e a verificação das perguntas de pesquisa.

O Objetivo Geral, de "desenvolver um *framework* de conformidade para a adoção de SIEM na Justiça Eleitoral", foi consolidado integralmente no FCAS-JE. A concretização deste objetivo foi viabilizada pelo cumprimento sequencial e metódico dos objetivos específicos. Inicialmente, o primeiro objetivo específico de "identificar e sistematizar o arcabouço legal" foi também atendido integralmente. Realizou-se uma extensa pesquisa documental nas bases normativas do Conselho Nacional de Justiça (CNJ), do Tribunal Superior Eleitoral (TSE) e do Gabinete de Segurança Institucional (GSI), que, após a aplicação de critérios de pertinência e

relevância, resultou na constituição de um corpus final de 41 normativas, que serviu como alicerce para toda a análise subsequente.

Os objetivos específicos subsequentes, que correspondem à construção do artefato, foram igualmente alcançados. O segundo objetivo, de "estruturar as normativas em Domínios Temáticos", foi atendido integralmente por meio da fase de categorização da Análise de Conteúdo, na qual os requisitos legais codificados foram agrupados em macroáreas de obrigações. O terceiro objetivo, de "formular perguntas de verificação (*Checkpoints*)", foi atendido integralmente na fase de interpretação, na qual o conteúdo legal foi traduzido em questionamentos práticos e auditáveis. Por fim, o quarto objetivo, de "elaborar um *framework* de conformidade", foi atendido integralmente, sendo o resultado direto das etapas anteriores e a principal contribuição material deste trabalho, apresentado no capítulo de Resultados.

Quanto às perguntas de pesquisa (PP), seguem as análises dos resultados obtidos com o desenvolvimento deste trabalho:

Resumo da PP_1: A pesquisa confirmou a possibilidade de consolidar o arcabouço regulatório em controles objetivos por meio do desenvolvimento do FCAS-JE. A existência do *framework*, que mapeia domínios e checkpoints específicos a partir de 41 normativas distintas, demonstra que a consolidação é factível mediante a aplicação de um método sistemático de análise documental.

Resumo da PP_2: A estruturação do conhecimento em domínios simplifica o processo de tomada de decisão e reduz riscos operacionais. O *framework* atua na conversão de informações regulatórias difusas em um roteiro lógico e hierarquizado, o que mitiga o risco de não conformidade decorrente do desconhecimento ou da má interpretação das normas vigentes.

Resumo da PP_3: A aplicação do *framework* promove a elevação da maturidade em cibersegurança da organização. Ao fornecer uma abordagem estruturada, repetível e auditável para a adoção de tecnologias como o SIEM, o *framework* aprimora a governança institucional de um patamar reativo para um nível proativo e tecnicamente maduro.

Por fim, conclui-se que o *framework* desenvolvido cumpre seu propósito de servir como um instrumento de apoio à decisão, preenchendo a lacuna identificada entre as exigências de compliance e a implementação técnica de uma solução SIEM na Justiça Eleitoral. Como trabalho futuro, sugere-se a aplicação prática do FCAS-JE em um estudo de caso em um Tribunal Regional Eleitoral, a fim de validar empiricamente sua eficácia e coletar subsídios para seu refinamento. Outra possibilidade de continuação da pesquisa é a expansão do modelo para abranger outras tecnologias de segurança ou a sua adaptação para outros órgãos da administração pública que enfrentam desafios regulatórios semelhantes.

6.2 Principal contribuição

A principal contribuição deste trabalho em relação ao estado da arte reside na proposição de um *framework* FCAS-JE, contextualizado para o complexo arcabouço regulatório brasileiro e especificamente para a Justiça Eleitoral. A sua relevância técnico-científica manifesta-se na aplicação de uma metodologia sistemática de Análise de Conteúdo para traduzir a linguagem jurídica em um instrumento de governança tecnológica operacional, preenchendo a lacuna entre a teoria normativa e a prática de implementação de sistemas SIEM. No aspecto social, o fortalecimento da segurança do processo eleitoral contribui para a integridade da democracia e a confiança pública. O impacto econômico se reflete na otimização do investimento público, ao orientar a adoção de soluções de forma a mitigar riscos de implementações falhas ou não conformes, evitando desperdício de recursos e potenciais sanções.

Como um dos resultados da pesquisa e forma de validação de sua relevância, os achados deste trabalho foram consolidados em um artigo científico. O trabalho intitulado "DESAFIOS DE COMPLIANCE EM CIBERSEGURANÇA: UM *FRAMEWORK* PARA ADOÇÃO ESTRUTURADA DE SISTEMA DE GERENCIAMENTO DE EVENTOS E INFORMAÇÕES DE SEGURANÇA NA JUSTIÇA ELEITORAL", de autoria de Roberto César Rodrigues, Rafael Lima de Carvalho, foi aprovado e apresentado na modalidade Artigo no XXVIII Encontro Nacional de Modelagem Computacional, realizado em Montes Claros - Minas Gerais. A aceitação e apresentação do artigo em um evento nacional com revisão por pares confere validação externa à originalidade e à pertinência da pesquisa, atestando sua contribuição para a comunidade científica.

6.3 Trabalhos futuros

Uma limitação identificada durante este estudo reside na dependência temporal do arcabouço normativo utilizado como base para a construção do instrumento. As diretrizes institucionais e a legislação vigente, compostas pelas 41 normativas embasadoras, estão sujeitas a atualizações, revogações ou novas interpretações. Logo, a validade dos *checkpoints* estabelecidos é vinculada ao cenário jurídico do momento da pesquisa. Alterações no ordenamento jurídico podem modificar o embasamento do *framework* FCAS-JE, o que exige a revisão periódica dos critérios para manter a precisão dos diagnósticos de conformidade.

Adicionalmente, observou-se uma limitação metodológica no modelo de referência de Mokalled et al. (2020) adotado para a estruturação dos requisitos técnicos. Durante a validação, constatou-se que tal proposta não aborda de maneira direta o emprego de Inteligência Artificial (IA), Aprendizado de Máquina (*Machine Learning*) e outras técnicas avançadas nas funcionalidades de sistemas SIEM. Essa ausência de critérios específicos para tecnologias emergentes configura uma oportunidade para a atualização do *framework* proposto por Mokalled et at., visando incorporar requisitos que atendam à evolução da cibersegurança e às novas funcionalidades de sistemas SIEM.

As questões identificadas oferecem oportunidades para o desenvolvimento de trabalhos futuros na área de governança de TI. Sugere-se a atualização do *framework* de Mokalled et al. para incluir requisitos quantitativos/qualitativos que tratem da transparência e auditabilidade de algoritmos de IA e ML, alinhando-se às necessidades tecnológicas atuais. Além disso, a proposição de um mecanismo de atualização dinâmica dos *checkpoints*, baseado no monitoramento contínuo de novas resoluções, permitiria que o modelo de conformidade acompanhasse a celeridade tanto das inovações técnicas quanto das transformações no panorama regulatório brasileiro.

6.4 Produtos e publicações

Artigo em Congressos:
RODRIGUES, Roberto César; CARVALHO, Rafael Lima de; DESAFIOS DE COMPLIANCE EM CIBERSEGURANÇA: UM FRAMEWORK PARA ADOÇÃO ESTRUTURADA DE SISTEMA DE GERENCIAMENTO DE EVENTOS E INFORMAÇÕES DE SEGURANÇA NA JUSTIÇA ELEITORAL.. In: Anais do Encontro Nacional de Modelagem Computacional e Encontro de Ciência e Tecnologia de Materiais. Anais...Montes Claros (MG) Universidade Estadual de Montes Claros, 2025. Disponível em: https://www.even3.com.br/anais/enmc-2025/1253842-desafios-de-compliance-em-ciberseguranca--um-framework-para-adocao-estruturada-de-sistema-de-gerenciamento-de-ev. Acesso em: 09/03/2026

Congresso: V ENGEC - Encontro Internacional de Gestão e Comunicação
Artigo: CAMPOS, RAMON DE FREITAS ELIAS et al.. A RESOLUÇÃO 615/2025 DO CNJ E A AGENDA 2030: IMPACTOS E GOVERNANÇA.. In: Anais do V Encontro Internacional de Gestão e Comunicação. Anais...São Caetano do Sul(SP) USCS/UFCG/UniFACEF/UABC, 2025. Disponível em: https://www.even3.com.br/anais/v-engec/1330734-a-resolucao-6152025-do-cnj-e-a-agenda-2030--impactos-e-governanca. Acesso em: 09/03/2026

Congresso: V ENGEC - Encontro Internacional de Gestão e Comunicação
Artigo: ROCHA, Marcelo Lisboa et al.. APLICAÇÃO DE TÉCNICAS DE INTELIGÊNCIA COMPUTACIONAL NO CONTEXTO DA SAÚDE DOS SERVIDORES DO TRE-GO.. In: Anais do V Encontro Internacional de Gestão e Comunicação. Anais...São Caetano do Sul(SP) USCS/UFCG/UniFACEF/UABC, 2025. Disponível em: https://www.even3.com.br/anais/v-engec/1325820-aplicacao-de-tecnicas-de-inteligencia-computacional-no-contexto-da-saude-dos-servidores-do-tre-go. Acesso em: 09/03/2026

Congresso: International Conference on Software Engineering – ICSE 2026 / RAIE ‘26
Artigo: A Study of International Standards for Safe and Responsible AI for the Brazilian National Council of Justice

Revistas:
ARACÊ (ARE) ISSN 2358-2472 QUALIS CAPES 2017-2020 A2

Governança sustentável e contratações públicas responsáveis no Tribunal Regional Eleitoral de Goiás: alinhamento com os objetivos de desenvolvimento sustentável 12 e 16 da Agenda 2030 da Organização das Nações Unidas-**International Journal Of Development Research - Qualis A2 2023:**

REFERÊNCIAS

Apruzzese, G.; Laskov, P.; MONTES DE OCA, E.; MALLOULI, W.; BÚRDALO RAPA, L.; GRAMMATOPOULOS, A. V.; DI FRANCO, F. The Role of Machine Learning in Cybersecurity. In: SKIANIS, C. et al. (eds). Digital Transformation and Cybersecurity: A Synergistic Approach. Springer, Cham, p. 75-93, 2023.

González-Granadillo, G.; González-Zarzosa, S.; DIAZ, R. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Sensors, v. 21, n. 14, art. 4759, 2021.

Manzoor, J. et al. Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs. PLOS ONE, v. 19, n. 3, art. e0297645, 2024.

Mokalled, H. et al. The Guidelines to Adopt an Applicable SIEM Solution. Journal of Information Security, v. 11, n. 1, p. 46-70, 2020.

Bardin, L. Análise de Conteúdo. São Paulo: Edições 70, 2011.

Machado, Jeferson Barboza. Automação de tarefas de segurança e melhorias na resposta a incidentes cibernéticos: Como a automação impacta a eficácia da resposta a incidentes cibernéticos em termos de tempo e precisão? 2024. Ensaio Acadêmico (Curso Superior de Segurança e Defesa Cibernética) – Escola Superior de Guerra (ESG), Rio de Janeiro, 2024.

Menges, F.; Latzo, T.; Vielberth, M.; Sobola, S.; Pöhls, H. C.; Taubmann, B.; Köstler, J.; Puchta, A.; Freiling, F.; Reiser, H. P.; Pernul, G. Towards GDPR-compliant data processing in modern SIEM systems. Computers & Security, v. 103, 102165, 2021. DOI: 10.1016/j.cose.2020.102165.

Mokalled, H.; Catelli, R.; Casola, V.; Debertol, D.; Meda, E.; Zunino, R. The Guidelines to Adopt an Applicable SIEM Solution. Journal of Information Security, v. 11, n. 1, p. 46-70, 2020. DOI: 10.4236/jis.2020.111003.

Teixeira, Wesdres de Santana. Resposta a incidentes cibernéticos em sistemas ciberfísicos: estado da arte e análise de um caso no setor elétrico brasileiro. 2024. XIII, 140 p. Dissertação (Mestrado em Engenharia de Produção) – Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2024.

Vazão, A. P.; Santos, L.; Costa, R. L. De C.; Rabadão, C. Implementing and evaluating a GDPR-compliant open-source SIEM solution. Journal of Information Security and Applications, v. 75, 103509, 2023. DOI: 10.1016/j.jisa.2023.103509.

Vazão, A.; Santos, L.; Piedade, M. B.; Rabadão, C. Soluções SIEM *open source*: um estudo comparativo. In: IBERIAN CONFERENCE ON INFORMATION SYSTEMS AND TECHNOLOGIES (CISTI), 14., 2019, Coimbra. Anais.... Coimbra: IEEE, 2019. p. 1-5.

Bhatt, S.; Manadhata, P. K.; Zomlot, L. The Operational Role of Security Information and Event Management Systems. IEEE Security & Privacy, v. 12, n. 5, p. 35–41, Sept. 2014. DOI: 10.1109/MSP.2014.103

Tuyishime, Emmanuel et al. Enhancing cloud security: proactive threat monitoring and detection using a SIEM-based approach. Applied Sciences, [s. l.], v. 13, n. 22, p. 12359, 15 nov. 2023. DOI: 10.3390/app132212359. Disponível em: https://www.mdpi.com/2076-3417/13/22/12359. Acesso em: 7 nov. 2025.

On-premises vs. Cloud-Based SIEM: A Comprehensive Comparison. SearchInform, [s. l.], [s. d.]. Disponível em: https://searchinform.com/articles/cybersecurity/measures/SIEM/on-premises-vs-cloud-based-SIEM/. Acesso em: 7 nov. 2025.

Jhaveri, Mihan; Parmar, Viral. Cloud Security Information & Event Management. GIS Science Journal, [s. l.], v. 10, n. 3, 2023.

Ramakrishnan, Shanmugavelan; Chittibala, Dinesh Reddy. Enhancing Cyber Resilience: Convergence of SIEM, SOAR, and AI in 2024. International Journal of Computing and Engineering, [s. l.], v. 5, n. 2, p. 36-44, 2024. DOI: 10.47941/ijce.1754.

Perez, Gonzalez. Information Security Event Management (SIEM) Systems and AI for Enhancing Policy Deployment Effectiveness in Intrusion Detection. [S. l.: s. n.], 2023. DOI: 10.13140/RG.2.2.16106.94405.

Pulyala, Srinivas Reddy. The Future of SIEM in a Machine Learning-Driven Cybersecurity Landscape. Turkish Journal of Computer and Mathematics Education (TURCOMAT), [s. l.], v. 14, n. 3, p. 1309–1314, 8 jul. 2023. DOI: 10.61841/turcomat.v14i03.14392. Acesso em: 7 nov. 2025.

BRASIL. Tribunal Superior Eleitoral. **Você sabe o que é e o que faz o TSE?** 2024. Disponível em: https://www.tse.jus.br/comunicacao/noticias/2024/Dezembro/voce-sabe-o-que-e-e-o-que-faz-o-tse. Acesso em: 18 fev. 2026.

APÊNDICE A

Norma	Resumo
CNJ Manual de Gestão Documental do Poder Judiciário	É um material de consulta e orientação para o planejamento, implementação e execução da Gestão Documental no Poder Judiciário.
CNJ Portaria nº 1/2025	Estabelece o Plano Diretor de Tecnologia da Informação e Comunicação do Conselho Nacional de Justiça (PDTIC.CNJ) para o período de 2025.
CNJ Portaria Nº 162 de 10/06/2021	Aprova protocolos e manuais para prevenção, gerenciamento de crises e investigação de ilícitos cibernéticos no Poder Judiciário, incluindo o PPINC-PJ.
CNJ Resolução nº 324/2020	Institui diretrizes e normas de Gestão de Memória e Gestão Documental e dispõe sobre o Proname no Poder Judiciário.
CNJ Resolução nº 325/2020	Institui a Estratégia Nacional do Poder Judiciário 2021-2026 e dá outras providências.
CNJ Resolução Nº 332 de 21/08/2020	Dispõe sobre a ética, transparência e governança na produção e uso de Inteligência Artificial no Poder Judiciário.
CNJ Resolução nº 363/2021	Estabelece medidas para o processo de adequação dos tribunais à Lei Geral de Proteção de Dados (LGPD).
CNJ Resolução nº 370/2021	Estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD).
CNJ Resolução Nº 383 de 25/03/2021	Cria o Sistema de Inteligência de Segurança Institucional do Poder Judiciário (SInSIPJ).
CNJ Resolução Nº 396 de 07/06/2021	Institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).
CNJ Resolução nº 522/2023	Institui o Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário (MoReq-Jus).
CNJ Resolução Nº 615 de 11/03/2025	Estabelece diretrizes para o desenvolvimento, utilização e governança de soluções de inteligência artificial no Poder Judiciário.
GSI Decreto nº 10.569 de 09/12/2020	Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas.
GSI Decreto nº 10.748/2021	Institui a Rede Federal de Gestão de Incidentes Cibernéticos.
GSI Decreto nº 11.200/2022	Aprova o Plano Nacional de Segurança de Infraestruturas Críticas.
GSI Decreto nº 11.856/2023	Institui a Política Nacional de Cibersegurança [157, "Decreto Institui Política Nacional de Cibersegurança"].
GSI Decreto nº 12.572/2025	Institui a Política Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação no âmbito da administração pública federal.
GSI Decreto nº 12.573/2025	Institui a Estratégia Nacional de Cibersegurança.
GSI Decreto nº 7.845/2012	Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.
GSI Decreto nº 9.573/2018	Aprova a Política Nacional de Segurança de Infraestruturas Críticas (PNSIC).

GSI Instrução Normativa nº 1/2020	Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.
GSI Instrução Normativa nº 3/2021	Dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal.
GSI Instrução Normativa nº 5/2021	Dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal.
GSI Norma Complementar 05/IN01/2009	Estabelece diretrizes para a criação e funcionamento de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR).
GSI Norma Complementar nº 21/2014	Estabelece diretrizes para o registro de eventos, coleta e preservação de evidências de incidentes de segurança em redes na Administração Pública Federal.
Lei nº 12.527/2011 (LAI)	Regula o acesso a informações previsto na Constituição Federal.
Lei nº 12.682/2012	Disciplina a elaboração e o arquivamento de documentos em meios eletromagnéticos.
Lei Nº 13.709 de 14/08/2018 (LGPD)	Dispõe sobre a Lei Geral de Proteção de Dados Pessoais (LGPD).
Lei nº 13.853/2019	Altera a Lei nº 13.709/2018 (LGPD), que dispõe sobre a proteção de dados pessoais.
Lei nº 8.159/1991	Dispõe sobre a política nacional de arquivos públicos e privados e a gestão documental.
SGD/MGI Portaria nº 852/2023	Dispõe sobre o Programa de Privacidade e Segurança da Informação - PPSI.
TSE Portaria nº 262/2024	Dispõe sobre o Controle de Acesso Físico e Lógico Relativos à Segurança das Informações e Comunicações do Tribunal Superior Eleitoral.
TSE Portaria nº 263/2024	Dispõe sobre a instituição da Norma de Desenvolvimento Seguro de Sistemas, relativa à Política de Segurança da Informação do Tribunal Superior Eleitoral
TSE Portaria Nº 387/2024	Institui a Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR) no âmbito da Justiça Eleitoral.
TSE Portaria nº 388/2024	Dispõe sobre a Comissão e a Subcomissão de Segurança da Informação no âmbito do Tribunal Superior Eleitoral e dá outras providências.
TSE Portaria nº 444/2021	Institui a norma de termos e definições relativa à Política de Segurança da Informação do Tribunal Superior Eleitoral.
TSE Portaria nº 458/2021	Institui norma de gestão de ativos, relativa à Política de Segurança da Informação do Tribunal Superior Eleitoral.
TSE Portaria Nº 459/2021	Institui a norma de gerenciamento e monitoramento de logs (registros de eventos) relacionada à Política de Segurança da Informação do Tribunal Superior Eleitoral.
TSE Portaria nº 497/2021	Institui o Plano Estratégico do Tribunal Superior Eleitoral para o período 2021-2026 e dá outras providências.
TSE Resolução nº 23.644/2021	Institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral.
TSE Resolução nº 23.650/2021	Institui a Política Geral de Privacidade e Proteção de Dados Pessoais no âmbito da Justiça Eleitoral.