



UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO TECNOLÓGICO
DEPARTAMENTO ENGENHARIA DO CONHECIMENTO
CURSO DE PÓS-GRADUAÇÃO LATO SENSU EM INTELIGÊNCIA E INOVAÇÃO
APLICADAS NO ENFRENTAMENTO AO CRIME ORGANIZADO

Lucas Daniel Fernandes Cardozo
Renan Balbino Silva Araujo

**CONTRAINTELIGÊNCIA COMO INSTRUMENTO DE PROTEÇÃO
INSTITUCIONAL:** Uma análise de como o vazamento de informações, prejudicou
uma grande operação policial em Santa Catarina.

Lucas Daniel Fernandes Cardozo
Renan Balbino Silva Araújo

CONTRAINTELIGÊNCIA COMO INSTRUMENTO DE PROTEÇÃO

INSTITUCIONAL: Uma análise de como o vazamento de informações, prejudicou uma grande operação policial em Santa Catarina.

Trabalho de Conclusão de Curso submetido ao curso de Pós-Graduação em Inteligência e Inovação aplicadas no Enfrentamento ao Crime Organizado do Centro Tecnológico da Universidade Federal de Santa Catarina como requisito parcial para a obtenção do título de especialista em Inteligência e Inovação no Enfrentamento ao Crime Organizado

Orientador(a): Prof. Dr. HEROS HORST

Florianópolis

2026

ARAUJO, RENAN BALBINO SILVA
CONTRAINTELIGÊNCIA COMO INSTRUMENTO DE PROTEÇÃO
INSTITUCIONAL : Uma análise de como o vazamento de
informações, prejudicou uma grande operação policial em
Santa Catarina. / RENAN BALBINO SILVA ARAUJO, LUCAS DANIEL
FERNANDES CARDOZO ; orientador, PROF. HEROS HORST, DR.,
2026.
33 p.

Monografia (especialização) - Universidade Federal de
Santa Catarina, Centro Tecnológico, Curso de Inteligência
e Inovação no Enfrentamento ao Crime Organizado,
Florianópolis, 2026.

Inclui referências.

1. CONTRAINTELIGÊNCIA. 2. VAZAMENTO DE INFORMAÇÕES. 3.
INFILTRAÇÃO. 4. CRIME ORGANIZADO. 5. SEGURANÇA PÚBLICA. I.
CARDOZO, LUCAS DANIEL FERNANDES . II. HORST, DR., PROF.
HEROS. III. Universidade Federal de Santa Catarina.
Inteligência e Inovação no Enfrentamento ao Crime
Organizado. IV. Título.

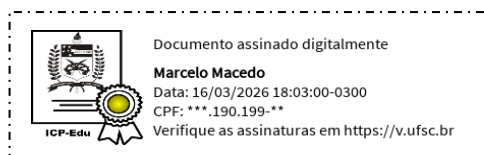
Lucas Daniel Fernandes Cardozo

Renan Balbino Silva Araújo

**CONTRAINTELIGÊNCIA COMO INSTRUMENTO DE PROTEÇÃO
INSTITUCIONAL:** Uma análise de como o vazamento de informações, prejudicou
uma grande operação em Santa Catarina.

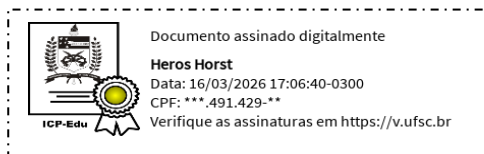
Este Trabalho de Conclusão de Curso foi julgado adequado para obtenção do título de
Inteligência e Inovação no Enfrentamento ao Crime Organizado e aprovado em sua forma
final pelo Curso Pós-Graduação em Inteligência e Inovação no Enfrentamento ao Crime
Organizado

Florianópolis, 02 de março de 2026

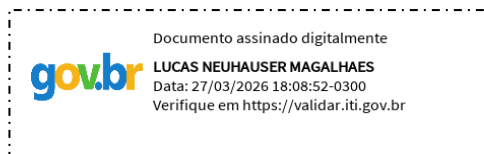


Prof. Marcelo Macedo, Dr.
Coordenação do Curso

Banca examinadora



Prof. Heros Horst, Dr.
Orientador



Prof.(a) Lucas Neuhauser Magalhães,
Instituição: Academia da Polícia Civil de Santa Catarina

Florianópolis, 2026.

RESUMO

Este artigo analisa a contrainteligência como instrumento estratégico de proteção institucional frente às ameaças de infiltração do crime organizado e ao vazamento de dados sensíveis no âmbito da segurança pública brasileira. O estudo tem como objetivo geral investigar em que medida essa atividade funciona como mecanismo estruturado de defesa para salvaguardar informações e a integridade das instituições. Emprega uma metodologia qualitativa de cunho descritivo, fundamentada em pesquisa bibliográfica, documental e no estudo de caso da "Operação Tio Patinhas", conduzida pela Polícia Civil de Santa Catarina. Utiliza a técnica de inteligência de fontes abertas (OSINT) e a triangulação de dados para superar as limitações impostas pelo sigilo de justiça e examinar a eficácia dos mecanismos de segurança orgânica. Os resultados indicam que a principal vulnerabilidade das instituições reside no fator humano, com destaque para a cooptação de agentes em cargos auxiliares, como estagiários e terceirizados, que frequentemente não são submetidos a escrutínios rigorosos. A análise empírica demonstra que falhas na gestão de acessos digitais e vínculos afetivos com lideranças criminosas permitiram o vazamento de informações que comprometeu cerca de 90% dos objetivos de uma operação de grande envergadura. O trabalho propõe a adoção de protocolos de investigação social contínua, a aplicação do princípio do menor privilégio no acesso a sistemas e o fortalecimento do gerenciamento de identidades (IAM). Conclui que a contrainteligência deve ser consolidada como política permanente de Estado para garantir o efeito surpresa das ações policiais e a preservação da legitimidade da persecução penal.

Palavras-chave: Contrainteligência; Crime Organizado; Segurança Pública; Proteção Institucional; Vazamento de Informações.

ABSTRACT

This article analyzes counterintelligence as a strategic instrument for institutional protection against organized crime infiltration and sensitive data leakage within the context of Brazilian public security. The study aims to investigate the extent to which this activity functions as a structured defense mechanism to safeguard information and institutional integrity. It employs a descriptive qualitative methodology based on bibliographic and documentary research, as well as a case study of "Operation Tio Patinhas," conducted by the Civil Police of Santa Catarina. Open Source Intelligence (OSINT) techniques and data triangulation were used to overcome judicial secrecy limitations and evaluate the effectiveness of organic security mechanisms. Results indicate that the primary institutional vulnerability lies in the human factor, specifically the co-option of auxiliary staff, such as interns and outsourced employees, who often lack rigorous vetting. Empirical analysis shows that failures in digital access management and emotional ties with criminal leaders facilitated information leaks that compromised approximately 90% of the objectives of a major operation. The study proposes the implementation of continuous social investigation protocols, the principle of least privilege for system access, and the strengthening of Identity and Access Management (IAM). It concludes that counterintelligence must be established as a permanent state policy to guarantee the element of surprise in police operations and preserve the legitimacy of criminal prosecution.

Keywords: Counterintelligence; Organized Crime; Public Security; Institutional Protection; Information Leakage.

SUMÁRIO

1. INTRODUÇÃO	08
2. REVISÃO BIBLIOGRÁFICA	12
2.1 FUNDAMENTOS TEÓRICOS E OPERACIONAIS DA INTELIGÊNCIA E CONTRAINTELIGÊNCIA	14
2.2 DESAFIOS E OPORTUNIDADES	15
3. METODOLOGIA	18
3.1 Procedimentos e etapas da pesquisa	18
3.2 Material analisado e origem das informações	19
3.3 Foco da análise: O caso da Operação "Tio Patinhas"	19
4. RESULTADO E DISCUSSÃO	21
4.1 SITUAÇÃO ILUSTRATIVA: A Infiltração do Crime Organizado e o Comprometimento de uma Operação Policial em Santa Catarina	23
5. CONCLUSÃO	27
6. REFERÊNCIA	30

1- INTRODUÇÃO

Este artigo analisa a importância da segurança nas instituições que combatem o crime organizado, um pilar fundamental diante da sofisticação das estratégias criminosas contemporâneas. Ameaças tangíveis, como o vazamento de informações sigilosas e a corrupção de agentes, transcendem problemas administrativos, elas representam um risco profundo à integridade do sistema de justiça criminal e à segurança coletiva, exigindo uma proteção constante e rigorosa dessas estruturas.

Nesse cenário, Coelho (2012) alerta que o crime organizado investe deliberadamente na infiltração de "espiões" nos quadros da segurança pública, chegando a financiar a preparação acadêmica para aprovação em concursos. Segundo o autor: *"No crime organizado, é possível que este patrocine a entrada de 'espiões' nas Instituições de Segurança Pública, inclusive com o pagamento de seus estudos para a aprovação dos mesmos em concursos de diversos órgãos que visem seus interesses escusos. Essa estratégia não é nova, e já faz parte da nossa realidade o grande número de pessoas infiltradas com a finalidade de obstruir a Segurança Pública no combate à criminalidade. É a corrupção de agentes públicos com metas empresariais ilícitas"*.

A infiltração não é um evento isolado, mas uma estratégia sistemática que visa comprometer a eficácia de investigações e criar ambientes de vulnerabilidade institucional. Diante desse panorama, a contrainteligência assume um papel estratégico indispensável, atuando como um dos principais mecanismo de defesa para proteger as missões constitucionais das instituições policiais contra ameaças internas e externas, garantindo a continuidade da repressão ao crime.

A contrainteligência tem um campo de aplicação cada vez mais relevante na segurança pública. Conforme o decreto 8.793 (Brasil, 2016) estabelece, e que podemos defini-la como *"a atividade que objetiva prevenir, detectar, obstruir e neutralizar a Inteligência adversa e as ações que constituam ameaça à salvaguarda de dados, conhecimentos, pessoas, áreas e instalações de interesse da sociedade e do Estado"* Diante de um panorama tão complexo, com tantas vulnerabilidades

institucionais e ameaças que não param de crescer, a pergunta central que se pretende responder é: de que forma a contrainteligência pode realmente servir como um escudo, um instrumento de proteção institucional, frente a essas tentativas de infiltração criminosa e ao vazamento de informações cruciais?

Para ilustrar essa complexidade, temos um exemplo marcante ocorrido no ano de 2024, o caso da “Operação Tio Patinhas”, conduzida pela Delegacia de Repressão ao Crime Organizado (DRACO) da Diretoria Estadual de Investigações Criminais (DEIC) de Santa Catarina. Essa operação, que estava investigando o crime organizado catarinense, foi seriamente comprometida por um vazamento de informações, resultando na frustração dos objetivos iniciais da operação.

A investigação do vazamento demonstrou que o sistema de persecução penal precisa de uma proteção muito mais abrangente, desde a contratação mais simples de um estagiário até o concurso para os cargos mais altos do poder judiciário.

É importante ressaltar que o trabalho não se dedicará à investigação inicial da “Operação Tio Patinhas” em si. O foco será o desdobramento do vazamento dessa operação, para tentar entender o papel da contrainteligência nesse combate aos vazamentos de informações e na proteção institucional. Assim, será possível identificar estratégias que funcionaram, os desafios enfrentados e os resultados que foram obtidos na neutralização de ameaças internas.

A escolha deste tema, *“Contrainteligência como Instrumento de Proteção Institucional”*, se justifica pela urgência e pela necessidade crescente de se compreender e desenvolver mecanismos eficazes para proteger as instituições de segurança pública contra ameaças que, no fim das contas, comprometem a sua missão fundamental. Assim como a relevância acadêmica desta pesquisa reside na escassez de estudos específicos sobre contrainteligência aplicada à segurança pública no contexto brasileiro. É um campo ainda pouco explorado, especialmente quando o objetivo é frear a entrada e a consolidação do crime organizado em nossas estruturas.

A metodologia adotada é qualitativa, com base em pesquisa bibliográfica e documental. Foram examinados referenciais normativos, doutrinários e técnicos sobre inteligência e contrainteligência, bem como relatórios institucionais e casos empíricos divulgados na imprensa que evidenciam o comprometimento de operações policiais por vazamentos internos. A análise incorpora ainda o exame de uma situação concreta, a “Operação Tio Patinhas”, conduzida pela Delegacia de Repressão ao Crime Organizado (DRACO) da Diretoria Estadual de Investigações Criminais (DEIC) do Estado de Santa Catarina, utilizada como estudo ilustrativo para compreender os impactos operacionais da infiltração e as limitações dos mecanismos preventivos existentes.

A relevância da pesquisa decorre da escassez de estudos específicos sobre contrainteligência aplicada à segurança pública no Brasil, especialmente sob a perspectiva da prevenção à captura institucional pelo crime organizado. A discussão proposta ultrapassa o âmbito administrativo e alcança a dimensão estratégica da governança pública, ao tratar da preservação da legitimidade, da confiança institucional e da eficácia da persecução penal frente a ameaças sofisticadas e persistentes.

O artigo organiza-se da seguinte forma: inicialmente, apresenta-se a revisão da literatura; em seguida, examina-se a metodologia com a infiltração criminosa nas instituições do Estado, com diagnóstico das vulnerabilidades identificadas na imprensa e desenvolvimento dos fundamentos teóricos e operacionais da inteligência e da contrainteligência, além dos desafios estruturais e das estratégias de integridade institucional. Posteriormente, analisa-se os resultados e discussão referente ao comprometimento de uma operação policial em Santa Catarina, da qual se extraem paradigmas e lições aprendidas. Por fim, é apresentada conclusão, com propostas voltadas ao aprimoramento da proteção institucional no âmbito da segurança pública brasileira.

O estudo tem como objetivo geral analisar em que medida a contrainteligência pode funcionar como mecanismo estruturado de proteção institucional frente às tentativas de infiltração criminosa e ao vazamento de informações estratégicas. Como objetivos específicos, busca-se identificar os

principais vetores de vulnerabilidade no sistema de justiça criminal, examinar ferramentas contemporâneas de inteligência e segurança orgânica aplicáveis ao contexto nacional, e propor diretrizes voltadas ao fortalecimento da integridade institucional e da integração interagências.

2. REVISÃO BIBLIOGRÁFICA

A infiltração da criminalidade organizada nas instituições do sistema de combate ao crime brasileiro deixou de ser uma possibilidade distante, tornando-se um perigo real e frequente, o que demanda políticas sólidas de controle e segurança na entrada de profissionais. O acesso a carreiras em segurança pública, no Judiciário e na política nacional deve ser fortalecido com critérios mais rigorosos em relação a habilidades técnicas, éticas e à integridade, capazes de identificar vulnerabilidades antes que se transformem em meios de cooptação. A questão não se restringe apenas a servidores públicos efetivos, alcançando funcionários terceirizados e estagiários os quais também representam riscos devido ao seu contato com informações sensíveis e processos administrativos. Em locais onde decisões, informações, dados e investigações são o foco, uma falha na seleção pode resultar em vazamentos de operações, destruição de provas e comprometimento de agentes.

A imprensa recente traz à tona a gravidade deste problema, com alertas de integrantes do Ministério Público, Delegados de Polícia e setores de inteligência, reforçando a necessidade urgente de respostas institucionais eficazes. (UOL, 2025).

A esse cenário soma-se a profissionalização da infiltração criminosa. Facções e milícias passaram a atuar com métodos estruturados, mapeando rotinas institucionais, explorando fragilidades humanas e tecnológicas e buscando cooptar indivíduos-chave. São as infiltrações silenciosas, planejadas e orientadas à obtenção de vantagem estratégica, ampliando a influência eleitoral, econômica e institucional das organizações criminosas (Congresso em Foco, 2025). A infiltração é gradual, e muitas vezes imperceptível, sendo preparada ao longo de meses ou anos.

Na área da segurança pública, aprimorar o processo de seleção deve envolver verificação de antecedentes abrangentes, avaliação da idoneidade moral e financeira, incluindo auditorias de estilo de vida e análise psicológica compatível com ambientes de alta pressão. Ferramentas de diligência e buscas em redes sociais e validação de referências profissionais contribuem para identificar potenciais riscos. Além disso, a certificação contínua em integridade e o monitoramento periódico de conflitos de interesse são práticas recomendadas. Terceirizados e estagiários devem assinar termos de confidencialidade e possuir acessos limitados, conforme boas práticas de “zero trust” que é um modelo de segurança no qual a arquitetura central

assume que nenhuma entidade, interna ou externa à rede, é confiável por padrão e requer verificação rigorosa (Cloudflare, 2025). Corregedorias atuantes e canais de denúncia se somam a esse modelo.

Outro elemento essencial é a cultura organizacional rígida. Ambientes onde há informalidade, confiança excessiva e falhas de supervisão tornam-se propícios à infiltração. Organizações criminosas exploram justamente essas brechas. Por isso, campanhas permanentes de conscientização, treinamentos práticos, exercícios simulados e reforço ético contínuo fortalecem a maturidade institucional e reduzem vulnerabilidades internas.

No Judiciário, os alvos potenciais incluem assessores, servidores de gabinete, analistas, técnicos de TI e equipes terceirizadas com acesso a áreas estratégicas. Adoção de práticas como distribuição aleatória de processos, trilhas de auditoria, controle de acesso a documentos sigilosos e monitoramento de consultas incomuns reduzem significativamente o risco de infiltração. A supervisão direta de estagiários e a limitação estrita de acessos também são fundamentais.

Além disso, cresce o número de ataques cibernéticos ao Judiciário (Valor, 2025), frequentemente atribuídos a grupos com vínculos criminosos. Esses ataques utilizam engenharia social, *ransomware* e vazamentos direcionados para beneficiar redes ilícitas. A combinação entre infiltração humana e tecnológica cria um risco especialmente perigoso. Assim, medidas de segurança digital, perícia forense e monitoramento automatizado tornam-se indispensáveis.

Na esfera política, a vulnerabilidade se manifesta na escolha de assessores, na distribuição de recursos, nas indicações para cargos de confiança e no financiamento eleitoral. Facções criminosas já foram identificadas financiando campanhas e posicionando representantes em gabinetes legislativos e executivos. *“A agência indica como fatores de vulnerabilidade a existência de milícias e facções criminosas que dominam territórios, financiam campanhas eleitorais, indicam candidatos próprios e coagem eleitores.” (...)* *“Chegando, em casos extremos, a eliminação de adversários políticos”* (O GLOBO, 2025). Medidas como auditorias de gastos eleitorais, verificação de beneficiários finais de doações, análise de vínculos suspeitos e monitoramento de evolução patrimonial são essenciais para a contenção desse movimento.

A infiltração política funciona como estratégia de longo prazo para obtenção de proteção institucional, influência em decisões governamentais e controle de contratos públicos. Em municípios pequenos, a captura de cargos políticos pode significar domínio sobre contratos de lixo, transporte, construção civil e segurança, o que fortalece economicamente o crime organizado e retroalimenta sua capacidade operacional.

2.1 FUNDAMENTOS TEÓRICOS E OPERACIONAIS DA INTELIGÊNCIA E CONTRAINTELIGÊNCIA

No sentido mais preciso, a contrainteligência em segurança orgânica é o segmento que preconiza a adoção de um conjunto de medidas destinado a prevenir e obstruir possíveis ameaças de qualquer natureza, dirigidas contra pessoas, dados, informações, materiais, áreas e instalações. (ABIN, 2020).

Divide-se ainda a contrainteligência em ativa e passiva, sendo que a primeira busca dissimular suas ações e confundir a inteligência adversária, levando o seu concorrente a ter uma interpretação errônea, e a segunda está relacionada à segurança das informações, salvaguarda dos conhecimentos e sistemas de interesse contra ações de forças adversas (ABIN, 2021). Convém que monitoramento e análise crítica ocorram em todos os estágios do processo. Monitoramento e análise crítica incluem planejamento, coleta e análise de informações, registro de resultados e fornecimento de retorno (ISO, 2018). A ética é determinante para evitar que a proteção institucional se transforme em vigilância inadequada, razão pela qual deve haver auditoria independente e normativos claros.

A antecipação é uma das capacidades mais valiosas da contrainteligência moderna. Instituições maduras conseguem identificar sinais precoces de infiltração: comportamentos atípicos, acessos incomuns, alterações súbitas de padrão de trabalho e vínculos externos suspeitos. Para isso, é essencial integrar bases de dados, treinar analistas e estimular o compartilhamento responsável de informações. Ambientes fragmentados favorecem a infiltração; já ambientes integrados permitem neutralizá-la antes que cause danos irreversíveis (ENAP, 2022).

As ameaças podem ser classificadas por origem, motivação, meio e grau de sofisticação. Ameaças internas incluem agentes mal-intencionados, negligentes ou

coagidos. Terceirizados e estagiários, por terem acesso operacional sem vínculo profundo, são vetores frequentes. Ameaças externas incluem infiltração humana, compra de acessos digitais, manipulação de servidores-chave e uso de intermediários políticos. A ameaça representada por crimes cibernéticos deverá aumentar ainda mais em volume e sofisticação nos próximos anos, o que representa riscos significativos (EUROPOL, 2021).

Em diversos casos investigados no Brasil, criminosos utilizaram servidores internos para fornecer senhas, orientar invasões tecnológicas ou facilitar o acesso físico a áreas restritas. Essa convergência entre espionagem digital e cooptação humana exige protocolos integrados de segurança da informação, prevenção de vazamentos, análise comportamental e controle rigoroso de credenciais (NIST, 2024).

Casos recentes revelados pela imprensa, como vazamentos de operações em tribunais, cooptação de agentes públicos e acessos indevidos a processos sigilosos, demonstram a necessidade urgente de modernizar políticas de segurança institucional (O GLOBO, 2022). Vazamentos de mandados e informações operacionais comprometem investigações, colocam em risco a vida de policiais e podem invalidar meses de trabalho investigativo (G1, 2022).

2.2 DESAFIOS E OPORTUNIDADES

A rede de terceirizados e estagiários exige atenção especial. Cláusulas de integridade nos contratos, auditorias periódicas, compliance obrigatório, verificação de antecedentes, controle físico de áreas sensíveis e expiração automática de credenciais são medidas essenciais. A ausência desses controles representa brechas exploradas repetidamente pelo crime organizado (OCDE, 2020).

Além disso, a rotatividade elevada nesses vínculos precários dificulta a consolidação de uma cultura institucional sólida, favorecendo a fragilização de protocolos de segurança. Muitas vezes, terceirizados e estagiários transitam entre diferentes órgãos, acumulando conhecimento sobre rotinas internas, sistemas e vulnerabilidades estruturais. Sem rastreabilidade adequada e sem um sistema integrado de controle de credenciais, o risco de reutilização indevida de acessos ou de cooptação posterior se intensifica. A gestão dessas relações deve transcender o

mero vínculo contratual, inserindo-se em uma política estruturada de segurança orgânica e proteção de ativos estratégicos.

Nesse sentido, um plano nacional de integridade e contrainteligência deve incluir padrões mínimos de seleção, certificação periódica, interoperabilidade entre órgãos, auditorias independentes e proteção a denunciantes, modelo amplamente recomendado em políticas internacionais (OCDE, 2020). A padronização de protocolos fortalece a previsibilidade institucional e reduz assimetrias entre entes federativos, especialmente em um país de dimensões continentais como o Brasil, onde municípios de pequeno porte podem apresentar maior vulnerabilidade estrutural.

Outro desafio relevante reside na fragmentação das informações institucionais. A ausência de interoperabilidade entre bases de dados de diferentes órgãos impede a identificação precoce de vínculos suspeitos, conflitos de interesse ou movimentações patrimoniais incompatíveis. A integração tecnológica, respeitando-se os limites legais de proteção de dados e garantias fundamentais, constitui oportunidade estratégica para a construção de um sistema preventivo mais eficiente. A utilização de ferramentas de análise de dados, inteligência artificial aplicada à detecção de padrões anômalos e cruzamento automatizado de informações pode representar avanço significativo na antecipação de riscos.

A proteção ao denunciante, por sua vez, revela-se elemento estruturante. Ambientes institucionais onde há medo de retaliação tendem a silenciar indícios de infiltração. Políticas claras de anonimato, canais seguros e proteção funcional incentivam a comunicação de irregularidades e ampliam a capacidade de resposta interna. Experiências internacionais demonstram que mecanismos de “*whistleblowing*” estruturados elevam o grau de integridade organizacional e reduzem a impunidade administrativa.

“*Whistleblowing*” consiste, portanto, na figura do denunciante ou dos canais de denúncia, metodologias nas quais um sujeito investiga e denuncia, ou há um portal de denúncias em certa empresa, devendo existir a utilização do “*whistleblowing*” para tornar um programa de “*compliance*” efetivo. (JusBrasil, 2019).

A integração entre corregedorias e setores de inteligência institucionais, bem como entre órgãos das forças de segurança, FICCO e GAECO, mostra-se fundamental no combate à infiltração. A atuação isolada limita a capacidade de identificação de redes complexas, enquanto a atuação coordenada permite análise sistêmica de padrões de cooptação, financiamento ilícito e captura institucional. A construção de protocolos conjuntos de troca de informações, com salvaguardas legais, fortalece a resposta estatal e reduz a sobreposição de esforços.

Ao mesmo tempo em que os desafios são significativos, as oportunidades também são evidentes. O fortalecimento da governança, a profissionalização da contrainteligência e a modernização tecnológica podem transformar a prevenção à infiltração em diferencial institucional. Instituições que investem em integridade, transparência e monitoramento estruturado não apenas reduzem riscos, mas ampliam sua legitimidade perante a sociedade.

Assim, enfrentar a infiltração criminosa não deve ser compreendido apenas como reação a crises pontuais, mas como política permanente de Estado, orientada por critérios técnicos, avaliação contínua de riscos e compromisso ético com a preservação das instituições democráticas.

3. METODOLOGIA

O trabalho se baseou em uma abordagem qualitativa, construída através do exame de, primordialmente, reportagens sobre o assunto retiradas de fontes jornalísticas confiáveis e da análise de um fato relacionado ao tema, tendo por finalidade exclusiva de aprofundar e complementar a pesquisa. Essa escolha se deve ao fato de que o assunto ainda é pouco tratado por escritores no Brasil, com informações dispersas em várias bases de dados, o que exige um estudo, em sua maioria esmagadora, apoiado em reportagens verificadas de fontes confiáveis. O método descritivo possibilita juntar ideias sobre proteção de instituições, contrainteligência e prevenção de vazamentos, criando uma base sólida para examinar informações de naturezas distintas.

3.1. Procedimentos e etapas da pesquisa

O trabalho seguiu um caminho organizado em quatro momentos principais. Inicialmente se tratou sobre os casos recentemente noticiados na imprensa, trazendo matérias jornalísticas com a opinião de jornalistas, promotores e policiais, demonstrando ainda a profissionalização das organizações criminosas para realizarem a infiltração nas estruturas de poder. Foram apontadas razões para a situação chegar ao ponto atual.

O próximo passo foi adentrar nos fundamentos teóricos da inteligência e da contrainteligência, sua subdivisão, as ameaças e sua classificação complementadas com outras matérias jornalísticas sobre o assunto, sugerindo as primeiras formas de ação para tentar minimizar os riscos de infiltração.

Ato contínuo, passou-se a tratar de uma situação problema, que foi justamente o vazamento da operação “Tio Patinhas”.

A coleta de textos e documentos priorizou publicações do período entre 2020 e 2025. As buscas utilizaram termos como "contrainteligência", "corrupção", "infiltração" e "crime organizado".

3.2. Material analisado e origem das informações

A consistência das análises depende do cruzamento de diferentes tipos de fontes, incluindo reportagens investigativas, nesse ponto foram selecionadas pelo menos oito matérias que exploram como grupos criminosos conseguiram penetrar na estrutura pública.

Houve a análise também de publicações técnicas de órgãos oficiais, tais como manuais da Agência Brasileira de Inteligência (ABIN), orientações do Ministério da Justiça, dados de organizações nacionais e internacionais como informações do Conselho Nacional de Justiça (CNJ), além de textos da EUROPOL, ONU e OCDE. Dentre trabalhos acadêmicos destaca-se o único livro encontrado que de fato trata do assunto, *"Contraineligência em Segurança Pública"*, escrito pelo ex-policial federal Paulo Cesar Coelho.

Vale destacar que analisar autos de processo foi inviável, já que a maioria dos casos tramita em segredo de justiça.

3.3. Foco da análise: O caso da Operação "Tio Patinhas"

Para dar mais profundidade prática à pesquisa, optou-se por examinar detalhadamente um caso específico: o vazamento de informações da Operação "Tio Patinhas", conduzida pela Delegacia de Repressão ao Crime Organizado (DRACO/DEIC/SC).

Esse caso foi estudado comparando quatro tipos de informação. Documentos institucionais, pois se teve acesso ao inquérito policial do caso com a devida autorização da chefia da Polícia Civil catarinense.

Depois disso, foi analisada a cobertura jornalística da época, com matérias investigativas que descreveram a sequência dos acontecimentos da infiltração e como funcionou o esquema de vazamento.

Outro passo importante foi o rastreamento do caminho da informação, com a reconstrução lógica de como os dados sigilosos saíram da custódia oficial e chegaram até membros do crime organizado.

Por fim, houve uma reunião e entrevista com o delegado responsável por apurar o vazamento do caso.

Essa forma de trabalhar permitiu estudar o problema do vazamento de informações em uma situação concreta, apontando onde foram identificados os pontos fracos no controle dessas informações. Mesmo que os documentos judiciais completos não estejam acessíveis por estarem protegidos por segredo de justiça, a análise de fontes públicas (método conhecido como OSINT - *Open Source Intelligence*).

Nesse ponto vale explicar que: *“Inteligência de código aberto (OSINT) é o processo de coleta e análise de informações publicamente disponíveis para avaliar ameaças, tomar decisões ou responder a perguntas específicas”* (<https://www.ibm.com/br-pt/think/topics/osint>), o que garante a validade científica da pesquisa ao se apoiar em fatos divulgados publicamente e confirmados, permitindo sugerir estratégias preventivas de contrainteligência.

4. RESULTADOS E DISCUSSÃO

Ao triangular fontes acadêmicas e registros práticos, identifica-se ao menos um padrão, de que o crime organizado não costuma "hackear" o sistema, ele "recruta" pessoas. A infiltração ocorre via vínculos afetivos ou financeiros, explorando as vulnerabilidades emocionais e sociais de quem já está dentro da estrutura estatal.

A investigação confirmou que a contrainteligência, conforme balizada pelos manuais da ABIN e pelas lições de Paulo Cesar Coelho, vai muito além de trancar portas ou criptografar dados. Trata-se de um sistema preventivo contra a infiltração e a cooptação. Restou evidente que a maior fragilidade das instituições públicas no Brasil não é tecnológica, mas humana. Como bem apontam organismos como a EUROPOL e a OCDE, o "fator humano" continua sendo o elo mais instável na custódia da informação.

Há um alinhamento entre o que recomendam órgãos internacionais (ONU, OCDE) e as diretrizes do Ministério da Justiça, todos pregam investigações sociais rígidas para servidores. No entanto, quando se olha para os relatos jornalísticos, a teoria não acompanha a prática. Enquanto os manuais exigem filtros para todos, a realidade brasileira mostra que o pessoal de suporte, como estagiários e terceirizados, muitas vezes passa pelo sistema sem o devido escrutínio, criando pontos cegos perigosos.

Outro ponto de convergência é o reconhecimento da sofisticação do crime organizado, que hoje opera com inteligência própria. A grande divergência, contudo, é temporal, as facções se adaptam com uma rapidez que os protocolos institucionais, engessados pela burocracia, não conseguem acompanhar.

O principal entrave encontrado para elaboração do trabalho foi o segredo de justiça, que blinda a maioria dos casos de infiltração criminosa e impediu o acesso direto aos autos. Por isso, a estratégia foi recorrer à análise de fontes abertas (OSINT).

OSINT significa "*Open Source Intelligence*", que em português se traduz como Inteligência de Código Aberto. É um processo de coleta, análise e utilização de dados públicos disponíveis de forma legal e acessível, com o objetivo de obter informações

valiosas para fins de investigação, segurança cibernética, negócios, pesquisas e tomada de decisão estratégica. Os dados utilizados em OSINT podem ser encontrados em diversas fontes, como websites, redes sociais, bancos de dados governamentais e repositórios acadêmicos (GRAN FACULDADE, 2023)

Embora esse método seja cientificamente robusto, detalhes cruciais de certos processos permanecem sob a sombra do sigilo.

Ademais, a fragmentação dos dados é um desafio real. As informações sobre vazamentos estão espalhadas entre relatórios do CNJ, notas de segurança estadual e imprensa investigativa. Cruzar esses dados exigiria um esforço de sistematização hercúleo, especialmente diante de um tema que ainda é pouco explorado pela academia brasileira, a infiltração "orgânica" em cargos auxiliares.

Os resultados forçam uma revisão de conceitos. Teoricamente, é necessário enxergar e priorizar a contrainteligência como uma defesa contra a cooptação interna de escalões inferiores.

Na prática, a urgência é por reformas em três pilares, começando pelo sigilo inegociável, mantendo o nível máximo de proteção em investigações sensíveis, eliminando "facilitadores" administrativos que criam brechas.

Adicionalmente, é necessário estabelecer um método de investigação social contínuo. O filtro deve ser para todos que tenham acesso ao sistema digital, não apenas para o servidor de carreira.

Além disso, estabelecer uma auditoria inteligente baseada em inteligência artificial, com sistemas que identifiquem acessos anômalos, como por exemplo consultas fora do horário ou pesquisas em processos sem conexão com o trabalho do usuário.

4.1. Situação Ilustrativa: A Infiltração do Crime Organizado e o Comprometimento de uma Operação Policial em Santa Catarina

Analisando o caso ilustrativo, o que se observa é um cenário de contrastes, se por um lado a literatura converge com os desafios reais das polícias, por outro, há lacunas críticas na forma como as informações sensíveis são protegidas no dia a dia.

Para ilustrar empiricamente os conceitos discutidos e evidenciar a materialização das vulnerabilidades identificadas na pesquisa, apresenta-se a análise de uma situação concreta ocorrida em Santa Catarina, envolvendo o comprometimento de uma investigação policial de grande envergadura.

Os dados relativos a esta situação foram obtidos através da triangulação de três fontes principais, que foi a entrevista técnica com a autoridade policial responsável pela investigação do vazamento, análise do inquérito policial sobre o caso e reportagens à época.

A operação em questão, denominada "Tio Patinhas", foi estruturada pela Delegacia de Repressão ao Crime Organizado (DRACO/DEIC/SC) para apurar crimes de tráfico de drogas e lavagem de dinheiro envolvendo lideranças do Primeiro Grupo Catarinense (PGC), facção caracterizada pela ostentação de patrimônio incompatível com atividades lícitas, e que atua dentro e fora dos presídios catarinenses.

A investigação revelou um grave comprometimento de informações sigilosas, confirmando empiricamente os principais conceitos discutidos na seção teórica desta pesquisa. O vazamento não resultou de ataque externo ou falha tecnológica, mas sim da ação de uma agente interna, que era uma estagiária de Direito lotada no Poder Judiciário.

A vulnerabilidade explorada residiu na própria arquitetura de permissões do sistema digital. Embora a estagiária estivesse formalmente alocada em uma vara de família, de competência completamente alheia à matéria criminal, possuía credenciais de acesso ao sistema Eproc com grande alcance. Quando o nível de sigilo da cautelar foi temporariamente reduzido do nível 4 (máximo) para o nível 2, a fim de permitir tramitações administrativas pelos servidores da vara, criou-se uma brecha que possibilitou o acesso transversal.

Eproc é o sistema de tramitação digital de processos judiciais utilizado pelo Tribunal de Justiça de Santa Catarina que substitui os autos físicos, permitindo acompanhamento, peticionamento e decisões totalmente online.

Registros eletrônicos do sistema Eproc e logs de acesso fornecidos pelo Núcleo de Inteligência do Tribunal de Justiça de Santa Catarina (TJSC) foram essenciais para se chegar até a autoria do vazamento.

A análise dos registros de acesso aos autos da operação “Tio Patinhas” demonstraram que a agente realizou aproximadamente 30 acessos indevidos aos autos da investigação. Para contornar os mecanismos de rastreabilidade que registram downloads de arquivos, utilizou-se de método rudimentar, porém eficaz, a captura fotográfica da tela do computador em sua residência, enviando as imagens diretamente a lideranças do PGC através de aplicativos de mensagens.

O impacto operacional foi significativo. Apesar da mobilização de aproximadamente 450 policiais civis e de planejamento logístico detalhado, cerca de 90% dos alvos encontravam-se vazios no momento da deflagração. A operação, que demandou investimento significativo de recursos públicos, foi tecnicamente frustrada em sua fase executória em razão da antecipação das informações por infiltrados do crime organizado.

A análise do processo de cooptação revelou aspectos que confirmam as preocupações levantadas neste estudo sobre o fator humano. A estagiária foi recrutada através de vínculos afetivos com lideranças faccionadas, evidenciando que a infiltração pode ocorrer de forma silenciosa através de relacionamentos pessoais desenvolvidos em ambientes sociais vinculados à subcultura criminosa.

A investigação demonstrou ainda que a transmissão de dados era recompensada com bens de consumo de alto valor e quantias em espécie, caracterizando a mercantilização do acesso à informação estatal.

Esta situação ilustra empiricamente diversos conceitos e deixa lições que não devem ser ignoradas, como a de que a infiltração orgânica em cargos de suporte confirma que a vulnerabilidade não está apenas em escalões superiores, mas de forma capilar em posições aparentemente secundárias (estagiários, servidores

administrativos), que, muitas vezes, não passam por filtros rigorosos de investigação social.

Houve falha na gestão de riscos internos, o que evidencia a necessidade, já preconizada pelos manuais de contrainteligência, de adoção de protocolos que incluam verificação contínua de todos os colaboradores, independentemente do tipo de vínculo (estatutários, terceirizados ou estagiários).

A inadequação dos controles de acesso evidencia que os níveis de sigilo não podem ser flexibilizados por conveniências administrativas, reforçando a necessidade de manutenção perene de proteções máximas em investigações sensíveis.

Evidencia-se a necessidade de adoção de modelo de verificação contínua (*continuous vetting*), no qual todos os indivíduos com acesso a informações sensíveis sejam periodicamente submetidos a avaliação de risco. Mudanças abruptas no padrão comportamental, patrimonial ou relacional devem ser tratadas como indicadores relevantes de possível vulnerabilidade.

A gestão de credenciais digitais deve ser orientada pelo princípio do menor privilégio, restringindo acessos às estritas necessidades funcionais. A flexibilização administrativa de níveis de sigilo, ainda que operacionalmente conveniente, pode gerar brechas incompatíveis com a natureza sensível de investigações de grande porte.

Os resultados reiteram que a tecnologia, embora essencial ao combate ao crime, cria novos flancos de vulnerabilidade quando não acompanhada de protocolos adequados de contrainteligência. A informação privilegiada em posse de organizações criminosas anula substancialmente a capacidade coercitiva do Estado, gerando não apenas prejuízos financeiros diretos pela mobilização infrutífera de recursos, mas principalmente o retardamento na desarticulação de estruturas responsáveis pelo crime organizado.

Assim, consolida-se a compreensão de que a investigação social rigorosa e o controle minucioso de identidades digitais são elementos tão vitais quanto o aparato

operacional de campo, constituindo-se como alicerces indispensáveis para a eficácia das ações estatais de combate ao crime organizado.

5. CONCLUSÃO

Conforme delineado na introdução deste artigo, buscou-se responder à seguinte indagação central: de que maneira a contrainteligência pode funcionar, de forma efetiva e sistematizada, como mecanismo de proteção institucional frente às tentativas de infiltração criminosa e ao vazamento de informações estratégicas no âmbito da segurança pública?

As soluções apresentadas não pretendem esgotar a matéria, mas oferecer diretrizes estruturantes coerentes com o problema de pesquisa enfrentado. Entre elas destacam-se: inclusão de cláusulas contratuais de integridade e auditoria para prestadores de serviço; capacitação obrigatória em segurança da informação e ética institucional; aplicação do princípio do menor privilégio na concessão de acessos; implementação de sistemas de gerenciamento de identidades com autenticação multifatorial e revisão automática de credenciais ao término dos vínculos; e auditorias regulares baseadas na análise de padrões de acesso e comportamento informacional.

Os resultados demonstram que a vulnerabilidade central do sistema não se concentra predominantemente na infraestrutura tecnológica, mas na dimensão humana. A infiltração criminosa manifesta-se, majoritariamente, por meio da cooptação interna, seja por vínculos afetivos, incentivos financeiros ou fragilidades pessoais, evidenciando que o risco informacional decorre da exploração de indivíduos legitimamente inseridos na estrutura estatal.

Verificou-se que o combate à vazamentos perpassa por algumas adequações, sobretudo internas ao sistema. Primeiro, o processo de integração de estagiários deve incluir treinamento obrigatório em segurança da informação, ética e confidencialidade, com supervisão ativa e acesso temporário e controlado. O controle físico de áreas sensíveis (como salas cofre, cartórios e centros de tecnologia da informação) deve incluir registro e acompanhamento aos prestadores de serviço.

Segundo, as formas das técnicas de contrainteligência podem ser readaptadas à realidade das forças de segurança para evitar o vazamento de informações.

E terceiro, ferramentas de gerenciamento de identidades (IAM sigla em inglês que significa “Identity and Access Management”, que se refere ao gerenciamento de identidade e acesso, especialmente em tecnologia e segurança da informação), com autenticação em múltiplos fatores e revisão automática de credenciais ao final dos contratos são essenciais. Paralelamente, campanhas educativas devem destacar que vazamentos são infrações graves e crimes, com implicações administrativas e penais.

Além disso, um plano nacional de integridade e contrainteligência para o setor público deveria definir padrões mínimos para a seleção, qualificação e acompanhamento de pessoal, incluindo indicadores de desempenho e transparência para a sociedade.

A implementação de protocolos sólidos de contrainteligência deve ser vista como o alicerce da liberdade de ação de uma força policial. A contrainteligência deve atuar como uma forma de blindagem contra a infiltração e o aliciamento, atuando na seleção e acompanhamento contínuo dos recursos humanos, evitando assim que organizações criminosas se infiltrem tal qual um cavalo de Tróia na estrutura.

É preciso garantir o efeito surpresa para a eficácia de uma operação policial, compartimentando as informações de forma a minimizar eventual vazamento e com segurança nas comunicações (criptografia e protocolos de rádio).

O uso de protocolos regulares, como varreduras eletrônicas e operações de desinformação servem para confundir e desinformar a inteligência alheia (do crime).

A proteção da instituição requer um equilíbrio entre os direitos individuais e o interesse público, com controles adequados e passíveis de revisão. Sem critérios rigorosos na admissão e sem uma contrainteligência bem estruturada, o Estado permanecerá em modo reativo, porém com eles, poderá retomar o controle e aumentar sua capacidade de resposta.

A preservação do efeito surpresa em operações policiais, a compartimentação informacional e a adoção de protocolos seguros de comunicação

— inclusive com uso adequado de criptografia e controle rigoroso de canais — constituem medidas estratégicas para redução da superfície de exposição. Da mesma forma, técnicas de contrainteligência voltadas à identificação de acessos anômalos, à detecção de desvios e à neutralização de inteligência adversa devem integrar a rotina institucional de proteção.

Cumprir destacar que a proteção informacional exige equilíbrio entre a salvaguarda dos direitos individuais e o interesse público na eficácia investigativa. Protocolos de monitoramento devem observar a legalidade, a proporcionalidade e os mecanismos de controle, dessa forma, evitando excessos. Entretanto, a ausência de critérios rigorosos na admissão e no acompanhamento contínuo de colaboradores mantém as instituições em posição vulnerável frente a organizações criminosas que operam com planejamento e capacidade adaptativa elevada.

Proteger informações sensíveis no Brasil, hoje, é mais um desafio de gestão de pessoas do que de tecnologia. O crime organizado não está apenas batendo à porta, ele está dentro ou tentando entrar através de quem opera o sistema. A informação privilegiada nas mãos de facções anula o poder do Estado e gera prejuízos que vão muito além do financeiro, atrasando o combate à crimes graves. A investigação social e o controle de identidades digitais não são apenas burocracia, são os pilares que sustentam a eficácia de qualquer operação policial.

REFERÊNCIAS

ABIN. Agência Brasileira de Inteligência. **Manual de Contraineligência**. Brasília: Escola de Inteligência, 2020. Disponível em: <https://www.gov.br/abin/pt-br/assuntos/inteligencia-e-contrainteligencia/CI>. Acesso em: 12 dez. 2025.

BRAGA, Vicente. O Estado sob ameaça: o avanço silencioso de organizações criminosas na política. **Congresso em Foco**, Brasília, 2025. Disponível em: <https://congressoemfoco.uol.com.br>. Acesso em: 12 dez. 2025.

BRASIL. Decreto nº 8.793, de 29 de junho de 2016. Fixa a Política Nacional de Inteligência (PNI). **Diário Oficial da União**: Brasília, DF: Presidência da República, 2016. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8793.htm. Acesso em: 9 fev. 2026.

CLOUDFLARE. **O que é uma rede Zero Trust? Segurança Zero Trust**. [S.l.]: Cloudflare, [2025]. Disponível em: <https://www.cloudflare.com/pt-br/learning/security/glossary/what-is-zero-trust/>. Acesso em: 12 dez. 2025.

CNJ. Conselho Nacional de Justiça. **Relatório de Fiscalização e Segurança Institucional**. Brasília: CNJ, 2022.

COELHO, Paulo Cesar. **Contraineligência em segurança pública**. Ed. rev. e ampl. Campo Grande: Clube de Autores, 2012.

ENAP. Escola Nacional de Administração Pública. **Integridade, ética e prevenção de conflitos de interesse no setor público**. Brasília: ENAP, 2022. EUROPOL. **EU Serious and Organised Crime Threat Assessment – SOCTA 2021**. The Hague: Europol, 2021.

G1. PF investiga vazamento de operações e cooptação de servidores públicos. **G1**, São Paulo, 2022. Disponível em: <https://g1.globo.com>. Acesso em: 20 nov. 2025.

GONÇALVES, Eduardo. Abin aponta atuação de facção e milícias na política e "interferência externa" como riscos para eleição de 2026. **O Globo**, Rio de Janeiro, 2 dez. 2025. Disponível em: <https://oglobo.globo.com/brasil/noticia/2025/12/02/abin-aponta-atuacao-de-faccao-e-milicias-na-politica-e-interferencia-externa-como-riscos-para-eleicao-de-2026.ghtml>. Acesso em: 12 dez. 2025.

GRAN FACULDADE. OSINT: o que é, como usar e suas principais técnicas. **Blog Gran Faculdade**, [S.l.], [2025]. Disponível em: <https://faculdade.grancursosonline.com.br/blog/osint/>. Acesso em: 24 fev. 2026.

IBM. O que é OSINT (inteligência de fontes abertas)? **IBM Think**, [S.l.]: IBM, [2025]. Disponível em: <https://www.ibm.com/br-pt/think/topics/osint>. Acesso em: 24 fev. 2026.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. **Normas de apresentação tabular**. Rio de Janeiro: IBGE, 1993. Disponível em: <http://biblioteca.ibge.gov.br/visualizacao/monografias/GEBIS%20-%20RJ/normastabular.pdf>. Acesso em: 20 jan. 2020.

ISO. International Organization for Standardization. **ISO 31000:2018 – Risk Management Guidelines**. Geneva: ISO, 2018.

MJSP. Ministério da Justiça e Segurança Pública. **Política Nacional de Segurança Pública e Defesa Social (PNSPDS)**. Brasília: MJSP, 2018.
NIST. National Institute of Standards and Technology. **Cybersecurity Framework 2.0**. Washington, D.C.: NIST, 2024.

O GLOBO. CNJ apura acessos indevidos a processos sigilosos e falhas de segurança. **O Globo**, Rio de Janeiro, 2022. Disponível em: <https://oglobo.globo.com>. Acesso em: 20 nov. 2025.

OCDE. Organisation for Economic Co-operation and Development. **OECD Public Integrity Handbook**. Paris: OECD Publishing, 2020.

OLIVEIRA, Suzana. Introdução ao conceito de whistleblower. **JusBrasil**, [S.l.], [2023]. Disponível em: <https://www.jusbrasil.com.br/artigos/introducao-ao-conceito-de-whistleblower/679304162>. Acesso em: 24 fev. 2026.

UNODC. United Nations Office on Drugs and Crime. **Global Study on Organized Crime**. Vienna: UNODC, 2023.

UOL NOTÍCIAS. "Tenho visto cada vez mais a infiltração de organização criminosa nos poderes do estado de SP", diz promotor. **UOL Notícias**, São Paulo, 1 set. 2025. Disponível em: https://cultura.uol.com.br/noticias/73507_tenho-visto-cada-vez-mais-a-infiltracao-de-organizacao-criminosa-nos-poderes-do-estado-de-sp-diz-promotor.html. Acesso em: 12 dez. 2025.

VALOR ECONÔMICO. Justiça sob ataque reforça papel da cibersegurança no Brasil. **Valor Econômico**, São Paulo, 11 ago. 2025. Disponível em: <https://valor.globo.com/patrocinado/dino/noticia/2025/08/11/justica-sob-ataque-reforca-papel-da-ciberseguranca-no-brasil-1.ghtml>. Acesso em: 12 dez. 2025.