PROPOSTA DE FRAMEWORK DE DISTRIBUIÇÃO SEGURA DE FEEDS DE INTELIGÊNCIA CIBERNÉTICA PARA INFRAESTRUTURAS CRÍTICAS - FDS-IC

Juliano Prestes Brum
Universidade de Brasília – UnB
juliano.brum@aluno.unb.br

Daniel Alves da Silva
Universidade de Brasília – UnB
daniel.alves@unb.br

João Gabriel Rossi de Borba
Universidade de Brasília – UnB
joaorossiborba@gmail.com

Georges Daniel Amvame Nze
Universidade de Brasília – UnB
georges@unb.br

Edna Dias Canedo
Universidade de Brasília – UnB
ednacanedo@unb.br

Fábio Lúcio Lopes de Mendonça
Universidade de Brasília – UnB
fabio.mendonca@redes.unb.br

RESUMO

A crescente sofisticação dos ataques cibernéticos direcionados a infraestruturas críticas, como energia, transportes, comunicações e saneamento impõe a necessidade de mecanismos avançados de compartilhamento e distribuição de informações de ameaça em tempo quase real. Contudo, o intercâmbio de feeds de inteligência cibernética (Cyber Threat Intelligence – CTI) entre entidades governamentais, operadoras e centros de resposta a incidentes enfrenta desafios relacionados à autenticidade, integridade, confidencialidade e governança dos dados compartilhados. Este artigo apresenta o Framework de Distribuição Segura de Feeds de Inteligência Cibernética (FDS-IC) para Infraestruturas Críticas (ICs) e seus ecossistemas. O FDS-IC integra princípios de criptografia assimétrica, autenticação federada, controle de acesso baseado em atributos (ABAC) garantindo a confiabilidade e a rastreabilidade das informações trocadas. Os resultados esperados incluem o aumento da resiliência cibernética, a redução do tempo de resposta a incidentes e o fortalecimento da cooperação interorganizacional sob diretrizes de segurança e conformidade, ancorado em princípios normativos e de governança e privacidade de dados (LGPD, PNSI, E-Ciber, PlanGIC). Além disso, através de uma revisão de literatura e outras soluções aplicadas em outros ecossistemas, como prova de conceito foi realizado um desenho arquitetural por camadas de nível gerencial do Comitê Nacional de Segurança de Infraestruturas Críticas (CGSIC) na governança e operacional do Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo do Brasil (CTIR Gov) como hub, rotulagem de Traffic Light Protocol 2.0 (TLP), canais seguros empregando ao

PGP/GPG, TAXII/TLS, além de demonstração prática no setor aéreo durante junto ao Fórum de Cooperação Econômica Internacional (G20), ocorrido no Brasil em 2024.

PALAVRAS-CHAVE
Inteligência Cibernética; Infraestruturas Críticas; Compartilhamento de Feeds; Cadeia de Suprimentos.

1. INTRODUÇÃO

O cenário global de segurança cibernética apresenta uma crescente complexidade impulsionada pela interconexão de sistemas industriais, redes de serviços essenciais e tecnologias emergentes como IoT, 5G e computação em nuvem. As infraestruturas críticas, responsáveis por serviços vitais ao funcionamento da sociedade e da economia, têm se tornado alvos estratégicos de ataques cada vez mais sofisticados, que exploram vulnerabilidades técnicas e falhas de coordenação entre organizações. Esse cenário é reforçado pelo crescimento significativo no número de incidentes cibernéticos que afetam redes governamentais (Cherdantseva et al., 2016). Esse cenário evidenciou a importância da tempestividade e da consciência situacional como fatores críticos para garantir uma resposta rápida e eficaz por parte das equipes do CTIR Gov e das Equipes de Tratamento de Incidentes de Rede (ETIR). O CTIR Gov, como CSIRT de responsabilidade nacional, tem como objetivo principal coordenar e integrar as ações destinadas à gestão de incidentes computacionais junto a outras Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos ETIR da Administração Pública Federal (APF).

O crescimento do número de incidentes e de fontes de indicadores ampliou o custo de filtrar, priorizar e distribuir sinais realmente úteis para a operação. Ainda que padrões e plataformas tenham melhorado a interoperabilidade, persiste uma lacuna entre disponibilidade de dados e relevância operacional. Cabe destacar que dados do painel 'CTIR Gov em Números' revelam que, em 2024, foram emitidas 5.147 notificações de segurança. Desse total, a grande maioria, 5.115 (99,4%), refere-se a vulnerabilidades identificadas, enquanto apenas 32 foram classificadas como incidentes, evidenciando o foco proativo do órgão na prevenção de ameaças (CTIR Gov, 2024). Estes dados podem ser observados com detalhe na Figura 1.

Figura 1 - Gráficos CTIR Gov em Números. Fonte: https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros

Considerando fatores externos, a crescente sofisticação dos ataques cibernéticos e o aumento exponencial das ameaças digitais impõem desafios sem precedentes à segurança das ICs. O cenário global demonstra uma perigosa convergência entre as táticas de atores estatais e as de cibercriminosos, onde ambos buscam ganhos

financeiros e desestabilização geopolítica. Segundo o Microsoft Digital Defense Report de 2024, que abrange o período de julho de 2023 a junho de 2024, a exposição global de equipamentos e sistemas de tecnologia operacional (OT), como os que controlam processos críticos em saneamento e energia, tornaram-se alvos centrais em guerras híbridas, explorados por grupos afiliados a nações como Irã e Rússia.

Nesse contexto, o compartilhamento de inteligência cibernética surge como uma ferramenta essencial para antecipar ameaças, identificar padrões de ataque e apoiar a tomada de decisão tática e estratégica. No entanto, a distribuição segura ainda constitui um desafio técnico e organizacional devido à diversidade de padrões, à ausência de protocolos de confiança e ao risco de exposição de informações sensíveis.

Este artigo apresenta a experiência na elaboração de descritores de desempenho e de indicadores utilizados para avaliar a segmentação por vínculo/criticidade e o processo de curadoria realizado pelas Infraestruturas Críticas (ICs). Também são descritos os mecanismos de fluxo de retorno bidirecional, desde os incidentes confirmados comunicados ao CTIR Gov até a mitigação de ruídos e falsos positivos, compartilhados com a CGSIC/SAGAE para o ajuste de filtros por *ranges* de IPs, ASNs e domínios. O objetivo central consiste em propor um framework de distribuição segura de *feeds* de inteligência cibernética (FDS-IC), que viabilize o compartilhamento confiável, rastreável e interoperável de informações sobre ameaças entre organizações responsáveis por infraestruturas críticas, contribuindo para o fortalecimento da resiliência cibernética e para uma resposta coordenada mais eficiente.

2. TRABALHOS RELACIONADOS

Os trabalhos relacionados concentram-se, majoritariamente, em soluções de distribuição e enriquecimento de feeds de inteligência cibernética voltadas a infraestruturas críticas. As iniciativas mapeadas variam desde mecanismos de contextualização da Cyber Threat Intelligence (CTI) com fontes abertas (OSINT) até propostas de arquiteturas de confiança e padronização de compartilhamento via STIX e TAXII. Em comum, tais estudos reforçam que a colaboração interorganizacional é o pilar essencial para aprimorar a detecção e a resposta a ameaças emergentes.

Para sistematizar essa análise, a Tabela 1 resume os principais objetivos e abordagens da literatura recente, contrastando-os com as limitações que o FDS-IC busca resolver.

Estudo Referências	Objetivo	Abordagem	Limitações e Soluções
Energies, at al. (2022)	Aborda o enriquecimento de CTI com OSINT	Adiciona uma camada contextual ao CTI, levando a uma avaliação de riscos mais abrangente e a uma detecção de ameaças mais precisa.	Propõe um *framework* para processos de confiança
Sun et al. (2023)	Complementam essa visão ao destacar que a CTI como os Indicadores de Comprometimento (IoCs)	Os dados são organizados e representados por meio de padrões como STIX e TAXII,	Falta de detalhes sobre automação
Osliak et al. (2023)	Informações contextuais sobre os agentes maliciosos, melhorar políticas de segurança com OSINT. Evidências técnicas como endereços IP, hashes de arquivos maliciosos e domínios comprometidos	Arquitetura baseada em contexto e risco.	Problemas com integração dinâmica de políticas.
Chaudhary, M.; Bansal, (2018)	Descreve um método baseado em teoria dos grafos no qual cada artefato é modelado como vértice e as relações entre eles são arestas ponderadas; o resultado é um “IoC de sistema”	Estruturar OSINT para cibersegurança.	Carece de validação em cenários reais.

Foco deste Artigo	Revisar e analisar técnicas de Privacidade de Dados aplicadas à CTI. um framework de compartilhamento para CII baseado em PDCA, o ambiente de governança, confiança e ferramentas.	Proposta de governança contínua, padrões e confidencialidade (PDCA), Curadoria ativa apoiada por ferramentas (EE-ISAC). Regra de envio com vínculo e criticidade, validação de vínculo curadoria (relevância, precisão, tempestividade) distribuição segmentada retorno (*feedback* voluntário)	Nenhuma das Limitações anteriores

Tabela 1: Trabalhos relacionados

Enquanto a Tabela 1 foca na revisão da literatura acadêmica, torna-se necessário posicionar o FDS-IC frente às ferramentas, padrões e modelos de governança já estabelecidos ou propostos internacionalmente. A Tabela 2 apresenta um quadro comparativo ampliado, confrontando o framework proposto com soluções de referência como o MISP (ferramenta), o padrão STIX/TAXII (protocolo) e modelos de governança (Indonésia e EE-ISAC).

Esta comparação evidencia os diferenciais do FDS-IC, especialmente no que tange à maturidade progressiva — permitindo a inclusão de atores com diferentes capacidades técnicas — e à segmentação por vínculo na cadeia de suprimentos, uma lacuna crítica nas soluções genéricas.

Aspecto	**FDS-IC** (Proposto)	**MISP** (Ferramenta)	**STIX/TAXII** (Padrão)	**Aferudin (Indonésia)** (Governança)	**EE-ISAC** (Setorial)
Foco	Distribuição Segura baseada em Vínculo	Plataforma de compartilhamento	Padrão de Estrutura e Transporte	Framework de Governança (PDCA)	Framework setorial (Energia)
Governança	Híbrida: Estratégica (SAGAE) e Operacional (CTIR)	Descentralizada (Comunidade)	N/A (Técnico)	Centralizada (Gestão de Risco)	Centralizada (Membros do setor)
Maturidade Progressiva	✅ 4 níveis (do E-mail ao STX)	❌ **Não** (Exige infraestrutura complexa)	❌ **Não** (Curva de aprendizado alta)	⚠️ **Parcial** (Foco em processos)	❌ **Não** (Requisito mínimo alto)
Análise de Tendências	✅ **Dinâmica** (Oscilação de vulns. em IPs/ASNs e dominios)	❌ **Estática** (Base de dados) estática	N/A (Formato de dados)	✅ **Gestão** (KPIs de Risco)	❌ **Estática** (Relatórios)
Fluxo Bidirecional	✅ **Feedback Voluntário** (Ajuste de filtros)	✅ Feedback Técnico (Correlacionado)	✅ Suporta (Se implementado)	✅ Ciclo PDCA (Melhoria)	✅ Feedback voluntário
Cadeia de Suprimento	✅ **Segmentação por Vínculo + Criticidade**	❌ Genérica (Broadcasting)	❌ Genérica (Depende da implementação)	⚠️ Menciona (Sem regra técnica)	⚠️ Apenas parceiros do setor
Alinhamento com Brasil	✅ Explícita (IC Curadora)	❌ Não abordado	❌ Internacional	❌ Foco Indonésia	❌ Foco Europeu

Atores Chave	✅ GSI/PR, SAGAE, CGSIC, CTIR Gov	Comunidade Open Source	OASIS Open	CSIRT Nacional (Indonésia)	Operadores de Energia (EU)

Tabela 2: Quadro Comparativo Completo (FDS-IC vs. Outros modelos)

A análise comparativa demonstra que, apesar dos avanços, as soluções atuais ainda enfrentam desafios significativos. Observam-se lacunas na curadoria e na validação contínua dos indicadores, dificuldades operacionais de segmentação por relevância e a ausência de mecanismos estruturados de retroalimentação para mitigar ruídos e falsos positivos.

Diante dessas limitações, torna-se evidente a necessidade de um modelo integrador. O FDS-IC foi desenvolvido justamente para preencher essas lacunas, promovendo um compartilhamento seguro e interoperável, assegurado por uma curadoria ativa (com critérios de vínculo e criticidade) e sustentado por um fluxo de retorno bidirecional que garante a melhoria contínua da inteligência cibernética nacional.

3. PROPOSTA DE FRAMEWORK

Diante das lacunas literárias e dos desafios operacionais explorados na Seção 2, apresentamos aqui o FDS-IC. Este framework foi desenhado para elevar o padrão de compartilhamento de CTI, conectando o CTIR Gov, as Infraestruturas Críticas e suas cadeias de suprimentos em um ambiente que preza pela confidencialidade, integridade e interoperabilidade.

A arquitetura do FDS-IC é estruturada em camadas e opera sob a supervisão estratégica da CGSIC/SAGAE, garantindo alinhamento com as normas de segurança vigentes. No pilar tecnológico, combinamos a robustez da criptografia assimétrica (PGP/GPG) e da autenticação federada com a versatilidade de scripts em Python. Essa escolha assegura não apenas um controle de acesso rigoroso baseado em atributos, mas também a modularidade necessária para adaptar o sistema a novas demandas.

Um elemento central do modelo é o fluxo de retorno bidirecional, que permite que incidentes confirmados reforcem a inteligência distribuída e que ruídos e falsos positivos sejam utilizados para ajuste fino de filtros e segmentação, reduzindo sobrecarga operacional e elevando a qualidade dos sinais compartilhados. Assim, o FDS-IC estrutura um mecanismo nacional de defesa colaborativa, que integra prevenção, curadoria ativa e resposta coordenada frente às ameaças que afetam as Infraestruturas Críticas.

A Figura 2 apresenta uma visão geral do fluxo operacional e de governança do FDS-IC, destacando os principais atores envolvidos e as interações entre as camadas do modelo. A seguir, descrevem-se as camadas que compõem o FDS-IC e seus respectivos papeis operacionais.

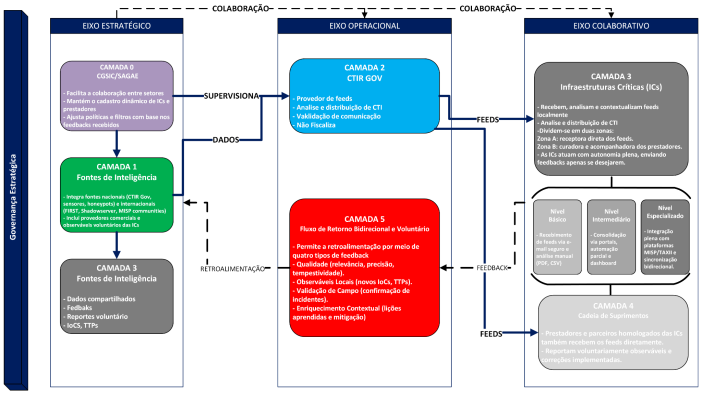

Figura 2: Fluxo operacional FDS-IC. Fonte: Elaboração própria (2025).

3.1 Camadas dos Framework

3.1.1 Camada 1: Fontes de Inteligência

As fontes de inteligência incluem: coleta nacional do CTIR Gov (*honeypots*, sensores de rede, análise de *malware*), parceiros internacionais (CERT.br, FIRST, *Shadowserver*, MISP *communities*), provedores comerciais de *threat intelligence* e observáveis locais reportados voluntariamente por ICs e prestadores. Esta última fonte é uma inovação do FDS-IC, transformando o *framework* de um sistema unidirecional em um ecossistema colaborativo de aprendizado contínuo, fundamentado em contribuições voluntárias, não obrigatórias.

3.1.2 Camada 2: Hub Central (CTIR Gov)

O CTIR Gov atua como hub central de processamento, análise e distribuição de inteligência cibernética, com foco na qualidade e autenticidade das informações, e não em fiscalização de conformidade. Na fase de processamento, os dados brutos passam por ingestão padronizada (conversão para STIX/TAXII, MISP e CSV), validação de autenticidade (assinaturas digitais e verificação de fontes confiáveis) e higienização dos formatos, incluindo deduplicação, enriquecimento com whois, geolocalização de IPs e verificação de reputação.

Na fase de análise, eventos são correlacionados para identificar campanhas coordenadas, Táticas, Técnicas e Procedimentos (TTPs) anteriormente mapeadas, e Indicadores de Ataque (IoAs) ou Indicadores de Compromisso (IoCs) são qualificados. A classificação utiliza Traffic Light Protocol (TLP) para definir níveis de confidencialidade, criticidade para priorização e relevância setorial para segmentação. Importante: a análise foca em identificação de tendências e padrões, oscilações de vulnerabilidades em IPs, ASNs e domínios, não em filtragem prévia baseada em ativos específicos de ICs.

A fase de distribuição implementa o modelo de fluxo único do FDS-IC. O CTIR Gov consulta a base da SAGAE/CGSIC para identificar destinatários relevantes com base em setor e tecnologias possivelmente vulneráveis, utilizando faixas (*ranges*) de IPs, ASNs e domínios vinculados às ICs. Esta abordagem parte de duas premissas:

1º As ICs tratam o "ruído" internamente. *Honeypots*, serviços legítimos anunciados em ASNs "suspeitos" e controles compensatórios são conhecidos pelo time local; a IC possui o melhor contexto para reconhecer falsos positivos, não cabendo ao CTIR Gov suprimir previamente esses sinais nem informar tais itens como "inventário oficial" à SAGAE.

2º Filtragem mínima e cadastro dinâmico. IPs/ASNs variam ao longo do tempo; deve-se manter cadastro atualizado dos blocos e itens mais relevantes, priorizando *ranges* e identificadores persistentes (ASNs, domínios corporativos) para garantir abrangência sem fragilizar a entrega.

O *feed* é enviado diretamente ao detentor do ativo (IC ou entidade do seu ecossistema), que é o responsável primário por decidir se e como agir. Quando o detentor for prestador/parceiro previamente declarado, o CTIR Gov envia cópia para a IC curadora (a organização que cadastrou o terceiro em seu ecossistema). Isso permite supervisão sem redistribuição manual, elimina gargalos operacionais, assegura mesma qualidade e tempestividade para todos os destinatários legítimos e preserva rastreabilidade centralizada: todos os envios ficam logados no CTIR Gov para auditoria de distribuição (não de conformidade).

Referente a segurança da transmissão, a distribuição utiliza PGP/GPG para email seguro e, quando aplicável, STIX 2.1/TAXII 2.1 e MISP para automação, respeitando a rotulagem TLP e mantendo trilhas de auditoria fim-a-fim.

3.1.3 Camada 3: Infraestruturas Críticas (ICs)

As ICs operam em duas zonas funcionais, podendo estar simultaneamente em ambas dependendo do contexto de cada *feed*. A característica fundamental é a autonomia: ICs decidem se e como agir com base em contexto local, sem obrigação de reportar ao CTIR Gov.

Na primeira zona, denominada **Zona A**, a IC atua como **receptora direta** sempre que um feed indica ameaça direcionada a seus próprios ativos. Nesse papel, a IC analisa e contextualiza localmente as informações recebidas, correlacionando-as com logs internos, avaliando o nível de exposição e identificando

possíveis falsos positivos ou honeypots próprios. Quando julga necessário, implementa controles de segurança, como aplicação de *patches*, definição de regras de *firewall* ou inclusão de *IoCs* em sistemas SIEM. Também pode, de forma voluntária, enviar *feedback* ao CTIR Gov sobre a relevância, precisão e tempestividade do feed. A ausência de *feedback* não é interpretada como não conformidade, mas apenas como ausência de contribuição naquele momento. Além disso, a IC pode solicitar à SAGAE a atualização de informações inconsistentes, incluindo a exclusão de indicadores incorretos dos filtros de envio.

Na segunda zona, denominada Zona B, a IC desempenha o papel de acompanhadora e curadora, quando o feed se refere a ativos de prestadores ou parceiros do seu ecossistema. Nesse caso, a IC recebe o conteúdo em cópia, mas não o redistribui, já que a entrega direta é feita pelo CTIR Gov. Sua função concentra-se no acompanhamento colaborativo das ações tomadas pelos prestadores. A IC pode monitorar a adoção de medidas corretivas, avaliar o risco e o potencial impacto em suas próprias operações, consolidar observáveis locais reportados por múltiplos prestadores, identificando padrões que um agente isolado não perceberia, e encaminhar ao CTIR Gov um *feedback* consolidado.

O papel de curadoria tem caráter facilitador, não fiscalizador. A IC não impõe respostas obrigatórias, mas pode oferecer suporte técnico, capacitação e assistência de engenheiros, quando solicitado ou quando identificar necessidade, inclusive com base em dispositivos legais ou cláusulas contratuais previamente definidas.

Essa dupla atuação, como receptora direta e como curadora, é essencial para o funcionamento do FDS-IC, pois equilibra autonomia local e cooperação voluntária entre as entidades do ecossistema de inteligência cibernética. Por exemplo, uma IC de telecomunicações pode atuar simultaneamente nas duas funções: como receptora direta, ao receber um feed sobre vulnerabilidade em seus próprios roteadores; e como curadora, ao acompanhar alertas relativos a equipamentos de um provedor regional parceiro. Em ambos os casos, a IC mantém visibilidade completa e autonomia para decidir como agir, reforçando o princípio de colaboração voluntária que sustenta o framework.

3.1.4 Camada 4: Cadeia de Suprimentos

Prestadores de serviço, fornecedores críticos, parceiros tecnológicos e empresas de manutenção escolhidas pela ICs, como membros de seu ecossistema, atuam sempre como receptores diretos do CTIR Gov, exatamente como as ICs. Eles recebem feeds sobre ameaças aos seus próprios ativos, implementam controles se julgarem necessário e podem, voluntariamente, reportar ações tomadas e observáveis locais à IC curadora (relação contratual/comercial) sem enviar validações de campo ao CTIR Gov.

Este modelo garante que prestadores sejam tratados como membros do ecossistema de inteligência. Eles têm acesso direto à fonte oficial (CTIR Gov), podem agir imediatamente sem depender de intermediários e são convidados a contribuir voluntariamente, não obrigados a reportar.

3.1.5 Camada 5: Fluxo de Retorno (Bidirecional e Voluntário)

O fluxo de retorno do FDS-IC é estruturado em quatro tipos de *feedback* voluntário, que permitem o aprimoramento contínuo da inteligência distribuída. A ausência de retorno não gera cobrança, acionamento ou penalização, uma vez que todo o processo se baseia em colaboração espontânea e não obrigatória.

O encaminhamento dos *feedbacks* segue duas regras principais: quando há exploração confirmada, ou seja, uma vulnerabilidade efetivamente explorada ou um *IoC* observado em produção, o informe é enviado ao CTIR Gov, com cópia para a IC curadora quando aplicável; quando se trata de sinais não relevantes, ruídos ou falsos positivos recorrentes, o informe é destinado à SAGAE/CGSIC, que realiza o ajuste dos filtros para suprimir tipos de alerta ou *ranges* específicos de IPs, ASNs ou domínios, evitando recirculação de informações que não agregam valor.

O primeiro tipo de *feedback*, denominado Qualidade, permite que ICs ou prestadores avaliem a relevância, precisão e tempestividade dos feeds recebidos, ou seja, se as informações foram úteis à operação, se houve falsos positivos e se chegaram a tempo de prevenir incidentes. As métricas de qualidade podem ser encaminhadas ao CTIR Gov, enquanto sinais sistematicamente não relevantes são comunicados à SAGAE/CGSIC para atualização dos filtros.

O segundo tipo, Observáveis Locais, ocorre quando receptores diretos identificam novos *IoCs*, *TTPs* ou vulnerabilidades em seus próprios ambientes. Esses dados são repassados à IC curadora, que consolida

insumos de múltiplos prestadores, evitando duplicações e identificando padrões mais amplos antes do encaminhamento ao destino adequado. Caso haja indícios de exploração real, o informe segue ao CTIR Gov. Sendo sinais benignos, testes internos ou *honeypots*, a IC curadora os envia à SAGAE/CGSIC para calibração dos filtros.

O terceiro tipo de retorno, Validação de Campo, corresponde à confirmação prática de que um *feed* se materializou em incidente ou exploração efetiva. Somente nesses casos o informe é direcionado ao CTIR Gov, com cópia para a IC curadora. Quando a validação confirma tratar-se de falso positivo, o encaminhamento é feito à SAGAE/CGSIC, contribuindo para reduzir a recorrência de alertas improdutivos.

Por fim, o Enriquecimento Contextual permite que receptores diretos compartilhem impactos reais, lições aprendidas e recomendações de mitigação. A IC curadora pode agregar contexto setorial antes do encaminhamento. Quando o enriquecimento confirma o impacto operacional, o envio é feito ao CTIR Gov. Caso seja demonstrada irrelevância para o setor, é remetido à SAGAE/CGSIC para refinamento da segmentação e supressão de sinais redundantes. O ciclo se completa quando o CTIR Gov incorpora validações e observáveis confirmados de volta às Fontes de Inteligência (Camada 1), enriquecendo continuamente a base de conhecimento. Paralelamente, a SAGAE/CGSIC ajusta filtros e políticas de distribuição, reduzindo ruído para ICs e seus ecossistemas. Esse processo opera sob o princípio da reciprocidade voluntária: quanto mais ICs e prestadores contribuem, maior é a qualidade e a relevância da inteligência para todos, sem imposição, mas com direcionamento preciso para cada tipo de retorno.

A Figura 3 fornece uma representação visual detalhada do esquema dos conteúdos observados, organizados de maneira a ilustrar claramente como cada um contribui para as diferentes dimensões de desempenho, os desempenhos específicos e os descritores associados. Este esquema é fundamental para entender a estrutura analítica do estudo, permitindo aos leitores identificarem a relação entre os conteúdos observados e os indicadores de desempenho.

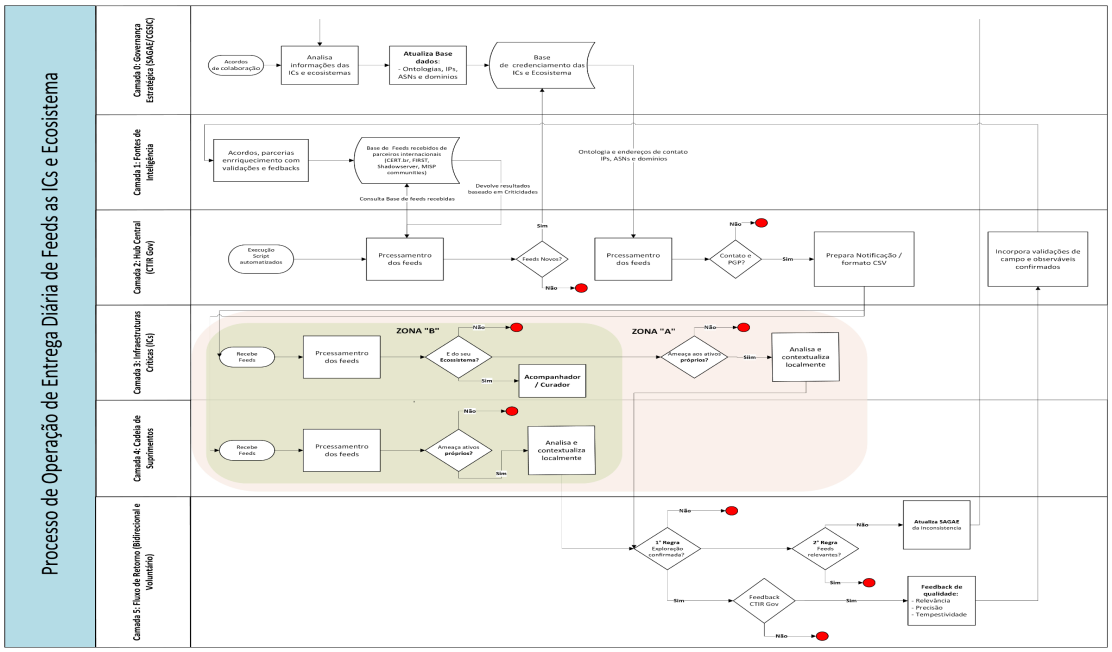

Figura 3: Fluxo Operacional Do FDS-IC. Fonte: Elaboração própria (2025).

4. RESULTADOS

A validação do framework foi conduzida através de cinco casos de uso em setores essenciais, abrangendo Transporte Aéreo, Telecomunicações, Energia e Petróleo & Gás. Liderei a implementação técnica,

desenvolvendo em Python as rotinas de automação responsáveis pela segmentação, distribuição e controle de segurança (TLP e ACK). Durante o G20 de 2024, esses ensaios demonstraram a eficácia do modelo em ambiente real, confirmando que é possível manter um fluxo preventivo e colaborativo que preserva a autonomia das Infraestruturas Críticas e se fortalece com o feedback estruturado.

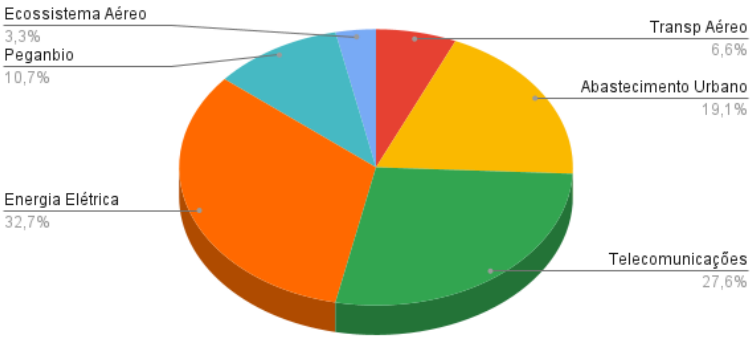

Figura 4 – Média de notificações enviadas por setor (G20/2024). Fonte: https://share.google/dlJjqCdjmYqzllrlU

Os resultados confirmam que a segmentação por vínculo é decisiva para tornar os alertas operacionalmente úteis. Essa constatação reforça o que a literatura preconiza sobre a necessidade de curadoria e filtros inteligentes para a troca de informações entre organizações distintas. No entanto, é importante reconhecer as limitações: a amostra de setores e a participação ainda incipiente de cadeias de suprimentos mais profundas (3º e 4º níveis) restringiram a granularidade das análises e o teste pleno dos mecanismos de retroalimentação. Para avançar, o caminho natural é expandir a base de ecossistemas e monitorar métricas de longo prazo, como a efetiva redução de falsos positivos e o enriquecimento da base de vulnerabilidades do CTIR Gov.

5. CONCLUSÃO E TRABALHOS FUTUROS

Este trabalho propôs e validou o Framework de Distribuição Segura de Feeds para Infraestruturas Críticas (FDS-IC) não apenas como um conceito, mas como um modelo operacional vivo, baseado em confiança e colaboração. A aplicação prática durante o G20 demonstrou seu valor real: protegemos o setor aéreo e seu ecossistema ao unir segmentação inteligente, curadoria ativa pelas ICs e entrega segura, sempre respeitando o princípio da necessidade de saber (need-to-know).

Aprendemos que a eficácia do FDS-IC não vem da fiscalização, mas da construção de um ecossistema de partilha genuína. Enquanto o CTIR Gov garante a qualidade da inteligência, as ICs atuam como curadoras — orientando seus parceiros em vez de coagí-los — e a SAGAE/CGSIC afina as políticas. Esse equilíbrio permitiu um fluxo ágil e auditável, garantindo confidencialidade e integridade sem criar burocracia desnecessária.

O coração desse modelo provou ser o fluxo de retorno bidirecional. A devolutiva qualificada — seja reportando um incidente real ao CTIR Gov ou sinalizando ruídos e falsos positivos à SAGAE/CGSIC — permitiu calibrar os filtros com precisão (por IPs, ASNs e domínios). Isso estancou a recirculação de alertas inúteis, provando que, sem colaboração ativa, a segmentação falha e o ruído volta a sobrecarregar as equipes.

Em suma, o FDS-IC mostrou-se viável e eficiente como mecanismo de defesa nacional. Ele funciona porque substitui a postura de fiscalização pela de parceria. Se mantivermos essa disciplina coletiva, o framework tem tudo para se consolidar como o padrão operativo capaz de elevar a resiliência não só das Infraestruturas Críticas, mas de todos os ecossistemas que dependem delas.

6. AGRADECIMENTOS

Gostaria de primeiramente agradecer a Deus, pela força, discernimento e saúde ao longo desta jornada. À minha família, pela compreensão nos momentos de ausência, pelo apoio incondicional e pela paciência que tornou possível a dedicação necessária a este trabalho. À Secretaria de Segurança da Informação e Cibernética e coordenadores do CTIR Gov, pela confiança depositada, pela orientação segura e pelo espaço para transformar experiência prática em aprendizado aplicado. Aos colegas e parceiros de trabalho e estudo, pelas brilhantes contribuições técnicas e discussões francas que nortearam este projeto — cada sugestão, crítica e colaboração foi essencial para a maturidade do framework aqui apresentado. Gostaria ainda de agradecer a orientação do Fábio Lúcio Lopes de Mendonça, apoio técnico e computacional do Laboratório LATITUDE, da Universidade de Brasília, ao TED junto Tribunal Regional Eleitoral do Distrito Federal – TRE/DF, ao TED 01/2021 da Secretaria Nacional de Assistência Social – SNAS/DGSUAS/CGRS, ao TED 01/2021 da Coordenação-Geral de Tecnologia da Informação (CGTI) da Procuradoria Geral da Fazenda Nacional – PGFN, ao Projeto SISTER City – Sistemas Inteligentes Seguros e em Tempo Efetivo Real para Cidades Inteligentes (Outorga 625/2022), ao Projeto "Sistema de Controle e Unificação de Projetos para o Governo Distrito Federal – Sispro-DF" (Outorga 497/2023), ao Decanato de Pesquisa e Inovação – DPI/UnB e a FAP/DF.

REFERÊNCIAS

[1] MICROSOFT. Defender Attack Surface Management: Microsoft Threat Intelligence. Redmond, WA: Microsoft, 2024. Disponível em: https://www.microsoft.com/security/blog. Acesso em: 14 out. 2025.

[2] CHECK POINT RESEARCH. The State of Cyber Security 2025. [S. l.]: Check Point Software Technologies, 2025. Disponível em: <https://www.checkpoint.com/research\>. Acesso em: 20 out. 2025.

[3] WALLIS, Tania; LESZCZYNA, Rafał. EE-ISAC—Practical Cybersecurity Solution for the Energy Sector. Energies, v. 15, n. 6, art. 2170, 2022. DOI: 10.3390/en15062170. Disponível em: https://www.mdpi.com/1996-1073/15/6/2170. Acesso em: 09 mar. 2025. MDPI+2MDPI+2

[4] AFERUDIN, Farouq; RAMLI, Kalamullah. The Development of Cybersecurity Information Sharing Framework for National Critical Information Infrastructure in Indonesia. Budapest International Research and Critics Institute (BIRCI-Journal), v. 5, n. 3, p. 22859–22872, ago. 2022. DOI: 10.33258/birci.v5i3.6297. Disponível em: https://www.researchgate.net/profile/Kalamullah-Ramli-2/publication/367598018_The_Development_of_Cybersecurity_Information_Sharing_Framework_for_National_Critical_Information_Infrastructure_in_Indonesia/links/6436d0e14e83cd0e2fab24f2/The-Development-of-Cybersecurity-Information-Sharing-Framework-for-National-Critical-Information-Infrastructure-in-Indonesia.pdf. Acesso em: 7 jun. 2025.

[5] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, p. 59, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 out. 2025.

[6] BRASIL. DECRETO Nº 9.573, DE 22 DE NOVEMBRO DE 2018. Aprova a Política Nacional de Segurança de Infraestruturas Críticas. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm. Acesso em: 10 Dez. 2024.

[7] BRASIL. Decreto nº 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Diário Oficial da União, Seção 1, Brasília, DF, p. 3, 27 dez. 2018a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/d9637.htm Acesso em: 8 set. 2024.

[8] BRASIL. Decreto nº 10.222, de 5 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética – E-Ciber. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm. Acesso em: 17 jul. 2024.

[9] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 27035-1:2016 - Information technology — Security techniques — Information security incident management — Part 1: Principles and process. Disponível em: https://www.iso.org/standard/63421.html. Acesso em: 6 abril. 2025.

[10] FIRST. Traffic Light Protocol (TLP) 2.0. [S.l.]: FIRST, 2022.. Disponível em: https://www.first.org/tlp/docs/v2/tlp-pt-br.pdf. Acesso em: 10 set. 2025.

[11] OASIS. STIX/TAXII 2.0 Interoperability Test Document: Part 1, v1.1. 16 ago. 2018. Disponível em: https://docs.oasis-open.org/cti/stix-taxii-2-interop-p1/v1.1/. Acesso em: 19 out. 2025. (Ver p. 1 e 9–10 para escopo/testes; p. 56 para requisitos de TIP.) docs.oasis-open.org

[12] OPEN SOURCE INTEL. MISP Project Documentation. CIRCL, 2019-2025. Disponível em: https://www.misp-project.org. Acesso em: 13 ago. 2025.

[13] THE MITRE CORPORATION. ATT&CK Framework. [S.l.]: MITRE, 2020-2025. Disponível em: https://attack.mitre.org. Acesso em: 5 jun. 2025.

[14] NIST. SP 800-61 Rev. 2/3 – Computer Security Incident Handling Guide. Gaithersburg, MD: NIST, 2012/2023. Disponível em: https://csrc.nist.gov/pubs/sp/800/61/r2/final. Acesso em: 17 jul. 2025.

[15] ABNT. NBR ISO/IEC 27001:2022. Rio de Janeiro: ABNT, 2022. Disponível em: https://intranetcomunix.com/wp-content/uploads/2024/07/ABNT_ISO_27001.pdf. Acesso em: 22 jun. 2025.

[16] ABNT. NBR ISO/IEC 27002:2022. Rio de Janeiro: ABNT, 2022. Disponível em: https://intranetcomunix.com/wp-content/uploads/2024/07/ABNT_ISO_27001.pdf. Acesso em: 30 jul. 2025.

[17] ABNT. NBR ISO/IEC 27001:2022. Rio de Janeiro: ABNT, 2022. Disponível em: https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros. Acesso em: 12 Dez. 2024.

[18] BRASIL. Gabinete de Segurança Institucional da Presidência da República (GSI). GSI participa da segurança integrada nos eventos do G20. Brasília, 2024. Disponível em: https://www.gov.br/gsi/pt-br/centrais-de-conteudo/noticias/2024/gsi-participa-da-seguranca-integrada-nos-eventos-do-g20. Acesso em: 5 nov. 2025.