FEBRABAN
/CYBER LAB

ESTUDO EXPLORATÓRIO EM INTELIGÊNCIA CIBERNÉTICA

COMPARTILHAMENTO E COLABORAÇÃO

Sumário

FEBRABAN
/CYBER LAB

1. Introdução

A colaboração em inteligência cibernética é reconhecida como mecanismo estratégico para aprimorar a prevenção, detecção e resposta a ameaças digitais. Porém, apesar do discurso favorável e da crescente oferta de plataformas de compartilhamento de dados, sua adoção permanece limitada e fragmentada. Diversos fatores **extra técnicos** ainda condicionam e restringem o engajamento colaborativo entre as equipes de segurança.

O conceito de **defesa coletiva** pressupõe que organizações que trocam informações sobre ataques, vulnerabilidades e táticas fortalecem sua própria resiliência e a de todo o ecossistema. Contudo, essa troca tende a ocorrer de forma reativa, informal ou superficial. Plataformas estruturadas de Threat Intelligence coexistem com redes pessoais de confiança, mas raramente são sustentadas por processos institucionais robustos ou incentivos claros que integrem o compartilhamento ao cotidiano dos analistas.

As limitações vão muito além de barreiras técnicas. Entraves **culturais e organizacionais** – como o receio de exposição, incertezas jurídicas, falta de governança definida, assimetria de capacidades entre participantes, baixa qualidade dos dados compartilhados e desconfiança quanto ao uso das informações recebidas – figuram entre os obstáculos à consolidação de práticas colaborativas. Poucas iniciativas conseguem equilibrar agilidade, segurança, relevância e padronização **simultaneamente**, sem depender de esforços isolados ou de relacionamentos pessoais pré-existentes.

Este estudo aprofunda essas questões, baseando-se em experiências REAIS no contexto brasileiro, mas **sem** citar instituições específicas ou fornecer prescrições normativas. Adota-se uma perspectiva crítica sobre as condições que favorecem ou limitam a cooperação em CTI, considerando não apenas as tecnologias disponíveis, mas também os processos, os modelos de governança e, sobretudo, a cultura organizacional subjacente a essas iniciativas.

Ao longo dos capítulos, exploram-se os benefícios potenciais da colaboração, os obstáculos observados na prática, as diferentes **práticas adotadas** conforme o nível de maturidade, os formatos de troca de dados e canais disponíveis, bem como os modelos de coordenação institucional já existentes. Busca-se, assim, propiciar uma compreensão mais precisa da complexidade envolvida no compartilhamento de inteligência cibernética em ambientes operacionais reais – nos quais decisões sobre **o quê**, **como** e **com quem** compartilhar são tomadas sob múltiplas pressões e condicionantes.

2. Benefícios do Compartilhamento de Inteligência Cibernética

Embora métricas para avaliar os benefícios do compartilhamento de inteligência sejam escassas, evidências sugerem que as organizações colaborativas são mais eficazes na identificação, prevenção e resposta às ameaças digitais. A experiência do setor financeiro, frequentemente citada como referência em modelos de compartilhamento estruturado, demonstra que a colaboração pode trazer benefícios tangíveis, incluindo maior eficiência operacional, redução de custos e melhoria significativa da capacidade preventiva e reativa. A seguir, são detalhados os principais benefícios identificados em experiências concretas e validadas por fontes de mercado, além de entrevistas realizadas com diferentes organizações.

2.1. Fortalecimento da Capacidade de Detecção e Resposta

O compartilhamento ágil e contínuo de informações sobre ameaças proporciona vantagem estratégica essencial às organizações. Ao acessar dados coletivos de inteligência, é possível identificar e mitigar ameaças antes mesmo que elas causem danos significativos, acelerando o processo de defesa. Entre os principais benefícios destacam-se:

Antecipação de ataques emergentes
Organizações ativas na troca de inteligência conseguem identificar rapidamente padrões, campanhas ou tendências emergentes, adotando medidas preventivas contra a ocorrência dos ataques;

Enriquecimento das análises internas
A inteligência compartilhada amplia o contexto das investigações internas, permitindo que as equipes identifiquem com mais precisão relações e padrões que passariam despercebidos sem essa cooperação;

Redução significativa dos tempos de resposta
Quando uma organização compartilha informações detalhadas sobre ameaça identificada, outras instituições conseguem responder com rapidez, implementando defesas eficazes baseadas em ações concretas validadas pelo mercado.

Esses benefícios são diretamente dependentes da qualidade, relevância e tempestividade das informações compartilhadas. Experiências práticas mostram que o simples compartilhamento de grandes volumes de dados sem curadoria ou contexto adequado pode comprometer os ganhos potenciais e até gerar sobrecarga operacional.

2.2. Uso Eficiente de Recursos e Redução de Custos

O compartilhamento estruturado de inteligência permite que as instituições financeiras utilizem seus recursos operacionais de forma mais eficiente, reduzindo retrabalhos e otimizando os investimentos em cibersegurança. Entre os benefícios concretos identificados estão:

Melhoria na gestão de equipes especializadas
Equipes com recursos limitados conseguem priorizar ameaças com maior impacto real, maximizando a eficácia das ações internas e evitando desperdícios em atividades redundantes.

Economia operacional
Ao compartilhar análises realizadas por equipes especializadas, evita-se duplicidade de esforços, permitindo que os analistas internos foquem em novas ameaças ou atividades;

Redução nos custos com inteligência externa
Instituições ativas em colaboração têm acesso a inteligência de alta qualidade sem precisar arcar integralmente com os custos de sua produção ou aquisição primária;

2.3. Conformidade com Regulamentações e Exigências Legais

Além dos benefícios técnicos, o compartilhamento de inteligência está cada vez mais relacionado às obrigações regulatórias específicas do setor financeiro brasileiro, contribuindo diretamente para:

Atendimento integral às normas regulatórias
Normativas como a Resolução Conjunta nº 6/2023 do Banco Central estabelecem claramente o dever de compartilhar informações sobre incidentes críticos entre instituições, tornando o compartilhamento não apenas desejável, mas obrigatório.

Transparência institucional perante reguladores
Instituições que demonstram participação ativa e estruturada em redes colaborativas são percebidas pelos órgãos reguladores como proativas e responsáveis, reduzindo riscos legais e fortalecendo sua reputação institucional.

No entanto, a mera adesão formal para cumprir exigências regulatórias mínimas, sem real engajamento, pode reduzir esses benefícios a meros procedimentos burocráticos, sem valor real, limitando o potencial de proteção coletiva.

FEBRABAN
/CYBER LAB

3. Obstáculos e Desafios do Compartilhamento

Embora o compartilhamento de inteligência cibernética seja amplamente reconhecido como estratégico para a defesa coletiva, sua operacionalização é atravessada por contradições, barreiras e assimetrias. As dificuldades vão além de limitações técnicas ou ausência de ferramentas apropriadas – residem, sobretudo, nos paradoxos que envolvem confiança, responsabilidade e valor percebido da informação.

Há consenso sobre a necessidade de colaboração para enfrentar ameaças cada vez mais interconectadas, porém persistem dinâmicas de contenção, silenciamento e seletividade que comprometem a eficácia dos esforços conjuntos.

3.1. Confiabilidade, Medo de Exposição e Riscos de Retaliação

A base de qualquer compartilhamento efetivo repousa na confiança– componente difícil de mensurar e ainda mais difícil de institucionalizar:

1 A organização que compartilha informações precisa garantir que seus dados não serão usados contra ela;

2 A organização que recebe os dados precisa confiar na integridade e precisão da informação;

No setor financeiro, onde a reputação constitui um ativo sensível e reguladores operam com rigor crescente, relatar vulnerabilidades ou ataques sofridos pode ser interpretado como um gesto de risco, mesmo quando mediado por protocolos como o TLP (Traffic Light Protocol) ou por acordos formais de confidencialidade (NDAs).

Principais Obstáculos Identificados

- Preocupação com a exposição reputacional
- Insegurança jurídica e risco de uso indevido das informações compartilhadas

3.2. Fragmentação Tecnológica e Interoperabilidade Reduzida

A coexistência de diferentes ferramentas, protocolos e formatos para o tratamento de inteligência cibernética dificulta a interoperabilidade e compromete a fluidez de troca de dados. Mesmo quando há boa vontade institucional para compartilhar, obstáculos técnicos e falta de padronização operacional geram gargalos, retrabalho e perda de valor analítico.

Principais Desafios

- Falta de padronização nos canais de transmissão
- Dependência de processos manuais de atualização
- Dificuldade para integrar plataformas legadas
- Adoção desigual de formato de dados, padrões e taxonomias

3.3. Receio de Irrelevância

A percepção de que apenas grandes instituições ou entidades com capacidades sofisticadas de monitoramento **possuem inteligência útil** acaba silenciando potenciais contribuições em redes colaborativas. O medo de não agregar valor leva organizações menores a não contribuírem, reforçando um ciclo de subparticipação. Essa **autolimitação** gera um paradoxo. Instituições que muitas vezes estão na linha de frente de ataques inovadores e servem de campo de testes para agentes maliciosos, deixam de compartilhar dados: a ausência de contribuição reforça a crença de que realmente "não há nada útil para compartilhar".

Principais Barreiras de Percepção

- Subestimação da própria visibilidade sobre ameaças
- Desconhecimento sobre o valor de eventos atípicos
- Insegurança quanto à qualidade das informações coletadas
- Falta de incentivo institucional para participação ativa
- Ausência de retorno sobre o impacto das informações enviadas

Mitos vs. Realidade:

Mito: Apenas grandes corporações e agências governamentais possuem inteligência útil

Realidade: Pequenas empresas frequentemente detectam novas ameaças antes das grandes, sendo alvos experimentais de novos ataques.

Mito: Se não houve impacto direto, não vale a pena compartilhar

Realidade: Muitos ataques são identificados por indícios preliminares que só se tornam evidentes quando analisados em conjunto com dados de outros participantes.

Mito: Contribuir exige ferramentas avançadas ou análise sofisticada

Realidade: Observações claras, mesmo que simples, podem ser valiosas para outras organizações que estejam enfrentando ameaças semelhantes

Mito: É melhor não compartilhar do que compartilhar algo que pareça trivial

Realidade: A cultura colaborativa se fortalece com o compartilhamento contínuo, mesmo que parcial ou contextual. O silêncio, por outro lado, não gera aprendizado coletivo.

3.4. Compartilhamento de Informações Públicas e Desatualizadas

Uma das ações mais recorrentes em redes de compartilhamento é o envio massivo de dados acessíveis em fontes abertas ou de indicadores que já perderam sua utilidade operacional. Essa prática, muitas vezes motivada por boa intenção, compromete a qualidade do fluxo de inteligência e gera um efeito cumulativo de saturação, dificultando a distinção do que é relevante.

A sobrecarga informacional sem curadoria reduz a confiança nos canais, desencoraja o engajamento e distorce a percepção de valor do compartilhamento. A repetição de IoCs amplamente conhecidos, listas de domínios já inativos ou alertas reaproveitados sem atualização contextual são manifestações frequentes desse fenômeno.

Problemas Associados:

- Reenvio de dados amplamente divulgados em fontes abertas, indicadores obsoletos ou já inativos
- Ausência de validação dos dados
- Sobrecarga das ferramentas e das equipes com volume irrelevante
- Falta de contextualização sobre a fonte e o objetivo do compartilhamento

3.5. Limitações de Recursos e Estrutura Organizacional

A capacidade de participar ativamente de iniciativas de compartilhamento de inteligência cibernética muitas vezes é comprometida por fatores internos, como ausência de equipes dedicadas, processos bem definidos ou fluxos de trabalho que incorporem o compartilhamento como atividade estratégica, comprometendo a regularidade e a consistência das contribuições.

Essa limitação não indica negligência, mas sim a predominância de gestão organizacional reativa, voltada à contenção de riscos imediatos. Nessas condições, mesmo quando há disposição institucional, faltam os meios para transformar o compartilhamento em prática recorrente.

Principais Barreiras Estruturais

- Falta de equipes exclusivas para atividades de CTI
- Ausência de processos institucionais que incorporem o compartilhamento
- Compartilhamento tratado como tividade periférica
- Dificuldade para justificar alocação de tempo e recursos

3.6. Capacitação Técnica e Barreiras Operacionais

Mesmo quando há recursos humanos disponíveis e boa vontade institucional, a baixa familiaridade com as plataformas, metodologias e terminologias empregadas em CTI representa um entrave significativo. A ausência de treinamento e de acúmulo prático em ambientes colaborativos leva a erros operacionais, contribuições mal formatadas e descontinuidade no uso dos canais de compartilhamento.

Além disso, muitos analistas enfrentam barreiras linguísticas, conceituais e instrumentais ao interagir com sistemas estruturados de inteligência. A curva de aprendizado das plataformas, aliada à falta de apoio técnico interno, limita a autonomia e reduz a fluidez da participação.

Principais Dificuldades Técnicas e Operacionais:

- Desconhecimento das funcionalidades das plataformas de compartilhamento
- Falta de capacitação em taxonomias, padrões e etiquetagem de dados
- Dificuldade de adaptação à lógica dos sistemas de CTI
- Ausência de programas internos de treinamento e simulação

3.7. Perspectiva Sobre Incentivos e Retornos

A prática de compartilhamento e colaboração é amplamente defendida como um bem coletivo. No entanto, no plano prático, **muitas instituições continuam a perceber o ato de compartilhar como um esforço pouco recompensado**. A ausência de incentivos claros, retornos visíveis ou reconhecimento institucional contribui para uma lógica de desengajamento silencioso. Mesmo entre participantes ativos de fóruns e plataformas, é comum a sensação de que a colaboração, embora importante, **não encontra mecanismos estruturados que sustentem sua continuidade**.

Um dos fatores críticos é a **assimetria entre esforço e retorno**. Compartilhar exige tempo, validação, curadoria, autorização interna – e muitas vezes isso ocorre sem qualquer tipo de retorno analítico, reciprocidade ou visibilidade. **O incentivo para colaborar é baixo porque os retornos raramente são claros ou imediatos.** Em algumas organizações, esse desalinhamento é agravado por métricas internas que valorizam a entrega operacional imediata, e não o fortalecimento da inteligência coletiva.

A ausência de mecanismos de reconhecimento ou valorização do compartilhamento também reforça a percepção de que **a contribuição é invisível e, portanto, dispensável**. Há quem sugira que **um sistema mais estruturado de reputação técnica, reciprocidade ou visibilidade setorial** poderia ajudar a reequilibrar a equação. Não se trata de *gamificar* a colaboração, mas de reconhecer que, **sem incentivos institucionais mínimos, ela tende a ser tratada como esforço extra, e não como parte da estratégia de segurança**.

Barreiras e oportunidades associadas ao tema dos incentivos

- Retorno pouco visível
- Ausência de reciprocidade clara
- Falta de reconhecimento técnico ou institucional
- Colaboração vista como esforço adicional
- Potencial para modelos de reconhecimento setorial

3.8. Outras Considerações

Além dos obstáculos já descritos, há fatores adicionais que, embora menos visíveis, impactam diretamente a capacidade das organizações de se engajarem de forma contínua e efetiva em iniciativas de compartilhamento de inteligência cibernética. Em muitos casos, esses fatores estão relacionados à escassez de recursos humanos especializados, ausência de processos internos consolidados ou sobreposição de prioridades operacionais que relegam a colaboração a um papel secundário, conforme demonstrado na Figura 1.

É importante reconhecer que, mesmo entre instituições que compreendem o valor estratégico do compartilhamento, a prática nem sempre é viável. Restrições orçamentárias, rotatividade de equipes e limitações técnicas são elementos que, isoladamente ou em conjunto, podem inviabilizar uma participação ativa e recorrente. Assim, entender esses limites é essencial para dimensionar expectativas e estruturar modelos de colaboração mais realistas e inclusivos.

Fatores Limitantes Adicionais

- Falta de equipes dedicadas à inteligência cibernética
- Baixa maturidade nos processos internos de segurança
- Concorrência com demandas operacionais urgentes
- Falta de familiaridade com plataformas de compartilhamento
- Ausência de incentivo institucional ou reconhecimento formal

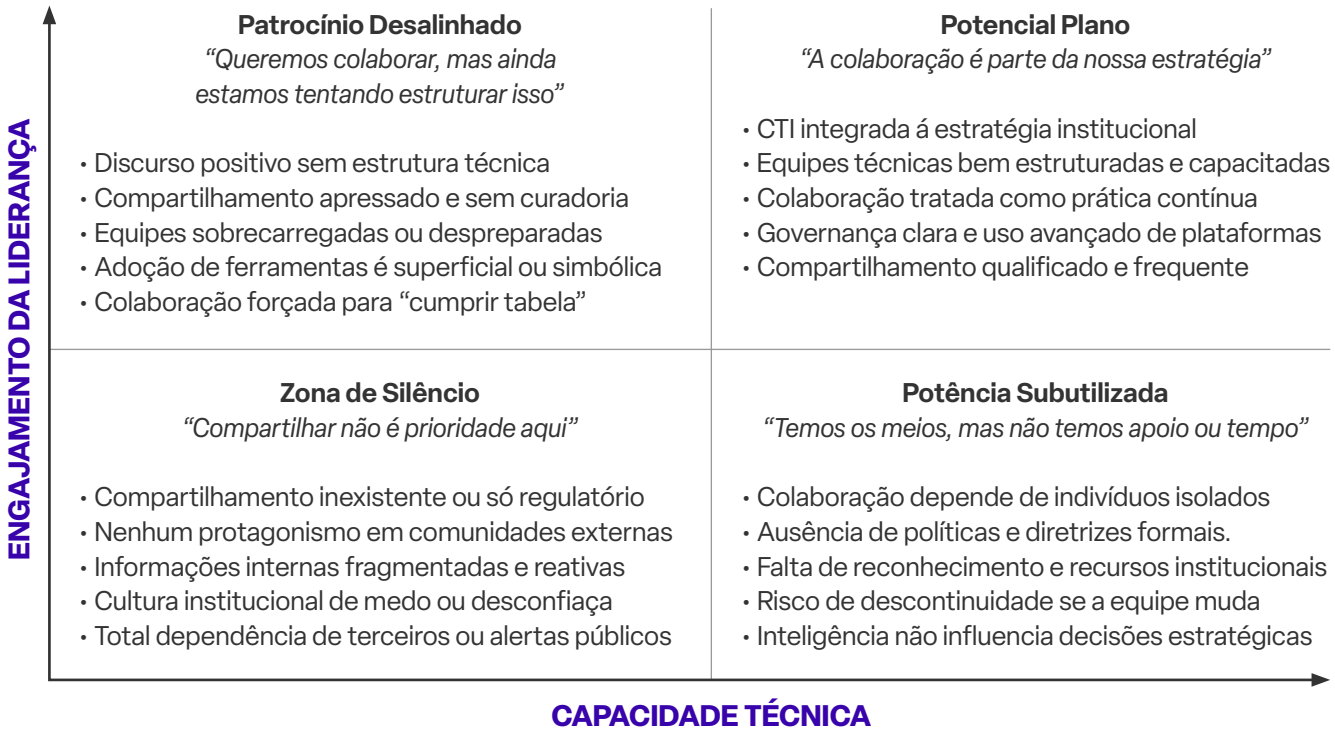


Figura 1: Quadrante de maturidade organizacional

4. Plataformas e Métodos de Compartilhamento

A escolha das ferramentas e canais por meio dos quais a inteligência cibernética é compartilhada influencia diretamente o alcance, a agilidade e a qualidade da colaboração entre organizações. Em teoria, a multiplicidade de soluções disponíveis – que vai de plataformas estruturadas a métodos tradicionais – deveria ampliar exponencialmente as possibilidades de integração. Na prática, porém, essa diversidade tem servido mais para evidenciar a distância entre intenção e execução do que para promover alinhamento real entre os envolvidos.

Ferramentas especializadas oferecem recursos avançados de automação, categorização e interoperabilidade. Contudo, sua utilização efetiva pressupõe níveis de maturidade técnica e organizacional que nem sempre estão presentes – ou sequer reconhecidos – pelas instituições. Por outro lado, métodos tradicionais, como e-mails e reuniões diretas entre analistas, permanecem surpreendentemente relevantes, não por sua eficácia comprovada, mas porque "funcionam" dentro das limitações operacionais conhecidas e da confiança pessoal construída ao longo do tempo.

Essa convivência entre meios formais e informais de colaboração expressa uma realidade em que cada organização adapta suas práticas ao próprio repertório, muitas vezes de forma pouco documentada e raramente reaplicável. A coexistência desses modelos não é, em si, problemática; torna-se crítica quando a informalidade suprime a rastreabilidade, ou quando a sofisticação técnica se esgota em dashboards pouco utilizados. As seções a seguir exploram os dilemas inclusos nessas escolhas e os efeitos dessa fragmentação sobre a eficácia do compartilhamento de inteligência cibernética.

4.1. Plataformas de Compartilhamento em Inteligência Cibernética

As chamadas Threat Intelligence Platforms (TIPs) foram concebidas para estruturar, automatizar e padronizar o compartilhamento de dados de ameaça entre organizações. Elas permitem consolidar indicadores, aplicar filtros e taxonomias, enriquecer automaticamente os dados recebidos e integrá-los a sistemas internos de defesa, como SIEMs e ferramentas de resposta a incidentes. Em ambientes maduros, essas plataformas funcionam como o eixo técnico das redes de colaboração, viabilizando a interoperabilidade entre fontes diversas.

Na prática, contudo, sua adoção enfrenta obstáculos recorrentes: uso parcial das funcionalidades, ausência de governança interna, falta de integração com sistemas legados e fragmentação semântica entre instâncias. Mesmo ferramentas amplamente reconhecidas como o MISP, ThreatConnect ou OpenCTI, quando não acompanhadas de processos institucionais claros, acabam se tornando repositórios estáticos ou de uso restrito a poucos analistas.

Exemplos de Plataformas Utilizadas

MISP (Malware Information Sharing Platform): Plataforma open-source amplamente utilizada para troca de IOCs. Oferece dashboards interativos, integração via APIs e suporte a padrões abertos como STIX/TAXII

ThreatConnect e ThreatQ: Soluções comerciais para gerenciamento integrado de inteligência e automação de respostas a incidentes. Possuem interfaces amigáveis e integrações robustas, sendo ideais para grandes organizações que necessitam de suporte dedicado

OpenCTI: Plataforma open-source altamente customizável para análise e gestão de ameaças. Embora com curva de aprendizado acentuada, é extremamente flexível para atender a necessidades específicas de cada organização

EclecticIQ Platform: Solução comercial voltada à coleta, análise e disseminação de inteligência cibernética. Oferece suporte a padrões como STIX/TAXII e é projetada para atender a demandas de organizações que exigem alta customização e escalabilidade

Cyware Threat Intelligence eXchange (CTIX): Plataforma comercial focada em agregação, análise e compartilhamento colaborativo de inteligência de ameaças. Facilita a colaboração entre equipes e organizações com painéis interativos e recursos de automação.

4.2. Métodos Tradicionais de Compartilhamento

Apesar do avanço das plataformas especializadas, métodos tradicionais seguem amplamente utilizados em redes de inteligência cibernética, seja por facilidade de acesso, familiaridade operacional ou pela baixa exigência técnica para sua adoção. Em muitos casos, esses canais atuam como soluções contingenciais, especialmente em contextos em que as relações de confiança são baseadas mais em vínculos pessoais do que em mecanismos institucionais formalizados.

No entanto, a prevalência desses métodos expõe limitações significativas: ausência de padronização, dificuldade de rastreamento, dependência de esforço humano contínuo e vulnerabilidade à perda de contexto. Em ambientes com alta rotatividade ou baixa maturidade, tornam-se não apenas um meio alternativo, mas o canal principal de troca, o que compromete a escalabilidade e a sustentabilidade da colaboração ao longo do tempo.

Principais Formas Utilizadas

- E-mails e planilhas informais
- Reuniões presenciais ou virtuais entre analistas
- Listas de e-mail restritas e fóruns técnicos especializados
- Publicações em plataformas abertas (GitHub, X/Twitter, fóruns OSINT)
- Mensagens instantâneas e canais informais
- Grupos de Discussão e Reuniões Presenciais

4.3. Flexibilidade vs. Especialização nas Plataformas de Compartilhamento

A escolha de uma plataforma de Threat Intelligence costuma oscilar entre **soluções abertas e flexíveis** – como o MISP, amplamente adotado globalmente – e **produtos comerciais especializados**, mais focados em padrões e casos de uso específicos (por exemplo, ThreatQ, OpenCTI, OTX etc). É comum que organizações implementem plataformas sob medida para determinadas **verticais** (como prevenção a fraudes bancárias) e, diante de incidentes **híbridos**, por exemplo em um ataque de phishing que envolva extorsão e uso de infraestrutura maliciosa em múltiplos setores, percebam a necessidade de ferramentas adicionais para correlacionar dados fora do escopo restrito de sua solução principal.

As equipes de segurança precisam optar entre **manter múltiplas plataformas distintas** (uma para ameaças cibernéticas, outra para fraudes financeiras, outra para engenharia social, etc), **adotar uma única plataforma versátil** que exija maior esforço humano de curadoria e governança, ou então **desenvolver uma solução própria**, sob custo e complexidade potencialmente elevados.

Exemplo: Uma empresa focada em segurança de cartões que utiliza uma plataforma comercial extremamente eficiente na detecção de fraudes financeiras. Quando surge um novo grupo de ransomware atacando também sistemas de varejo e expondo dados de clientes, essa plataforma dedicada não consegue abranger o perfil mais amplo do ataque. A equipe, então, é obrigada a migrar parte das informações para o MISP ou outra ferramenta generalista, gerando **trabalho duplicado** e aumentando o risco de inconsistências e desencontro de dados.

FEBRABAN
/CYBER LAB

5. A Dinâmica dos Padrões de Compartilhamento

O compartilhamento estruturado de inteligência cibernética exige mais do que boa vontade ou ferramentas tecnicamente robustas – exige alinhamento semântico. Para que a colaboração entre diferentes organizações funcione de forma escalável e confiável, é necessário que todos falem a mesma língua, ou pelo menos uma variação mutuamente compreensível. Padrões e frameworks como STIX (Structured Threat Information Expression), TAXII (Trusted Automated eXchange of Indicator Information), OpenIOC, MITRE ATT&CK e o MISP Standard foram criados com esse propósito: permitir que diferentes atores descrevam ameaças de forma interoperável e acionável, mesmo operando em realidades institucionais distintas.

Apesar dessa base amplamente reconhecida, sua aplicação segue limitada por uma série de práticas inconsistentes. Em muitos casos, a adoção é superficial: configura-se a plataforma para "suportar" os padrões, mas sem que isso se traduza em rotinas consolidadas de uso. Como observou um profissional durante entrevista, "*a ferramenta até permite usar tudo isso, mas ninguém quer ser o primeiro a fazer certo*". A padronização vira promessa latente – sempre disponível, mas raramente ativada. O problema, ao que tudo indica, não está na ausência de frameworks, mas na ausência de compromisso com a curadoria, o preenchimento consistente de campos e o uso disciplinado dos recursos já existentes.

Essa dissociação entre a sofisticação dos modelos e a prática cotidiana expõe um paradoxo estrutural: embora os padrões estejam tecnicamente maduros, sua efetividade continua refém da cultura organizacional e da governança coletiva. A padronização, ao contrário do que se supõe, não é um atributo técnico, e sim uma disciplina operacional. A ironia, nesse caso, é que os sistemas já são plenamente capazes de conversar entre si; o problema é que muitos ainda insistem em falar de forma isolada, ou em dialetos improvisados que só fazem sentido dentro de suas próprias fronteiras institucionais. A seguir, exploram-se dois elementos centrais dessa problemática: a utilização (ou ausência) de taxonomias e galaxies, e os erros recorrentes que comprometem a eficácia dos padrões na prática.

5.1. Taxonomias e Galaxies como Padrão de Compartilhamento

Taxonomias e galaxies são mecanismos fundamentais para que os dados compartilhados em ambientes de inteligência cibernética sejam **compreensíveis, comparáveis e reutilizáveis**. Enquanto as taxonomias permitem classificar eventos, atributos e níveis de confiança com precisão formal, as galaxies estruturam relacionamentos entre atores de ameaça, campanhas, técnicas e famílias de malware. Em conjunto, essas ferramentas permitem transcender o dado bruto e situar o incidente em um contexto analítico mais amplo, essencial para resposta coordenada, aprendizado coletivo e correlação automatizada.

Ainda que essas estruturas estejam mais visivelmente associadas a sistemas como o MISP**, seus princípios se aplicam a múltiplas formas de compartilhamento – inclusive em contextos informais, bilaterais ou analógicos**. Sempre que se compartilha uma ameaça sem um vocabulário comum, aumenta-se a ambiguidade, dificulta-se a validação e enfraquece-se a possibilidade de correlação entre eventos. Padronizar não é apenas uma exigência de sistemas sofisticados, mas uma **condição para qualquer forma de colaboração que pretenda ser reprodutível e eficaz**.

Ainda assim, seu uso prático permanece limitado em muitas organizações. É comum encontrar instâncias em que os eventos são registrados com campos vazios ou com classificações genéricas, mesmo quando os recursos estão tecnicamente disponíveis. Um profissional de uma instituição resumiu com franqueza: "*A gente até sabe como deveria usar, mas entre o ideal e o que dá tempo de fazer, fica o campo em branco*". Esse tipo de escolha, entre fazer direito e fazer rápido, evidencia que a padronização depende menos da tecnologia e mais da cultura operacional. Sem governança clara, processos incorporados à rotina e valorização institucional do rigor analítico, taxonomias e galaxies seguem tratadas como acessórios opcionais, quando deveriam ser alicerces do compartilhamento eficaz.

Principais fragilidades observadas

- Campos obrigatórios ignorados ou mal preenchidos
- Taxonomias divergentes entre instâncias
- Atualizações e curadoria negligenciadas
- Desconhecimento das taxonomias e galaxies padronizadas já disponíveis
- Prejuízo à automação e à análise por IA
- Ativação indiscriminada de múltiplas taxonomias redundantes
- Uso simbólico sem aplicação efetiva
- Criação de taxonomias personalizadas fora dos padrões existentes

5.2. Problemas Comuns na Prática

Mesmo com a existência de padrões técnicos consolidados e recursos avançados disponíveis em plataformas especializadas, o compartilhamento de inteligência ainda é permeado por distorções operacionais que limitam seu potencial. Muitos desses problemas não derivam de falhas tecnológicas, mas sim de **práticas enraizadas no cotidiano institucional, de hábitos de trabalho que priorizam a velocidade sobre a qualidade** e de **estruturas organizacionais que ainda tratam o compartilhamento como exceção**, e não como fluxo regular.

Na prática, observa-se uma tendência à simplificação: prioriza-se o envio de **indicadores técnicos pontuais**, como IPs ou hashes, enquanto se negligenciam elementos críticos como **contexto, motivação do atacante, vetores de exploração ou contramedidas eficazes**. O resultado é uma inteligência fragmentada, difícil de correlacionar e de utilidade reduzida para quem a recebe. Em paralelo, muitos dados são compartilhados com duplicidade, redundância ou ausência de validação, criando sobrecarga cognitiva e exigindo retrabalho por parte dos analistas destinatários.

A persistência desses problemas reflete uma cultura que prioriza volume em detrimento da qualidade.

Práticas recorrentes que comprometem a efetividade do compartilhamento

1. Foco desproporcional em IOCs técnicos isolados
2. Ausência de dados contextuais
3. Baixa qualificação ou curadoria das informações enviadas
4. Redundância e reenvio de dados públicos
5. Compartilhamento reativo, sem continuidade

Essas distorções não anulam o valor da colaboração, mas revelam uma maturidade ainda em construção. A persistência de práticas pouco eficazes evidencia que a inteligência compartilhada só alcança seu potencial quando é acompanhada por critérios mínimos de qualidade, contexto e curadoria. Corrigir esses desvios exige mais do que ajustes técnicos - requer compromisso institucional com a consistência, a utilidade e a inteligibilidade do que se escolhe colocar em circulação. Conforme demonstrado na Figura 2, há uma clara diferença entre dados realmente valiosos - bem contextualizados, validados e com metadados - e aqueles que, apesar de fáceis de obter, pouco contribuem para a análise, como dumps genéricos ou indicadores obsoletos.

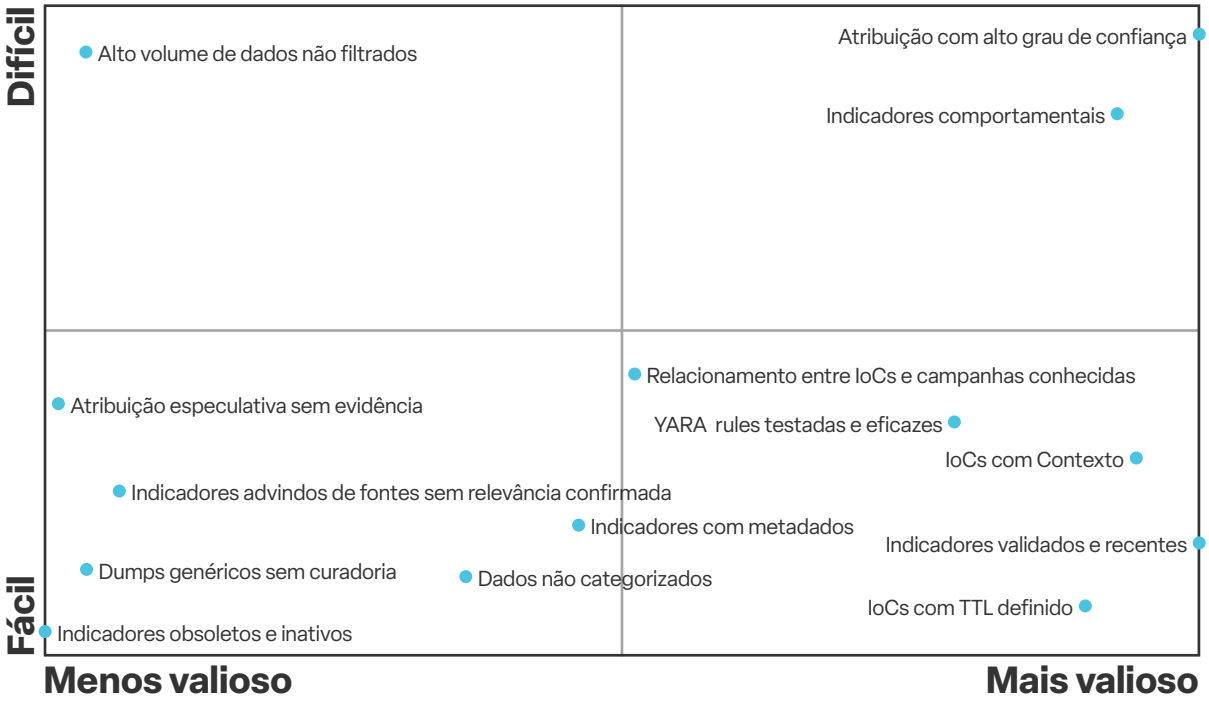
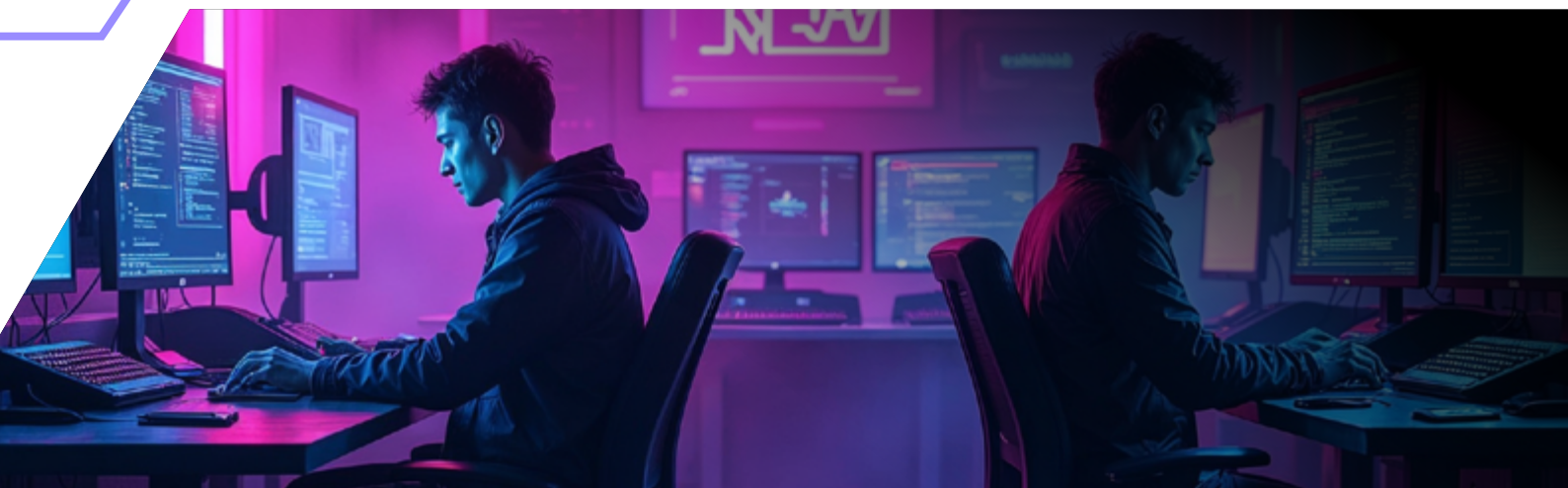


Figura 2: Quadrante de classificação de indicadores de inteligência



6. Contexto Certo para Cada Tipo de Inteligência

A eficácia do compartilhamento de inteligência cibernética não depende apenas da qualidade dos dados ou da maturidade da plataforma utilizada, mas também da **adequação do conteúdo ao público** e ao **momento certo de uso**. Nem toda informação serve para todos os perfis de destinatários, nem todo dado técnico deve circular da mesma forma que uma análise estratégica. **Ignorar essa diferenciação compromete a utilidade da inteligência e a fluidez da colaboração.**

Costuma-se dividir a inteligência em **três níveis complementares**: **estratégico**, **tático** e **operacional**. Cada um desses níveis responde a perguntas distintas, atende a públicos específicos e exige formatos próprios de compartilhamento. **Tratar essas camadas como intercambiáveis** – por exemplo, enviando relatórios executivos para analistas de SOC, ou IOCs crus para conselhos de administração – leva à desconexão entre **produção** e **uso da informação**. Mais do que classificar o dado, é necessário entender **para quem ele será útil**, **quando**, e **com qual finalidade**.

Em diversas entrevistas, essa falta de distinção surgiu como fonte de frustração: *"Compartilham coisa demais, mas nada do que eu preciso para agir"*; *"Recebi um hash malicioso sem saber nem de onde veio nem o que causava"*. Esses relatos ilustram que, além de compartilhar, é necessário **contextualizar**: ajustar o nível de detalhamento, explicitar o propósito e alinhar o formato da inteligência ao tipo de decisão que ela pretende informar.

A tabela a seguir sintetiza as diferenças centrais entre os três níveis de inteligência, com base em sua definição, formato ideal e propósito no ecossistema de defesa cibernética:

Tipo de Inteligência	Definição	Formato Ideal	Objetivo
Inteligência Estratégica	Relatórios detalhados que analisam cenários de longo prazo, motivações e impactos gerais das ameaças	Relatórios gerenciais, apresentações e reuniões executivas	Fornecer insights para a tomada de decisões estratégicas e planejamentos de longo prazo
Inteligência Tática	Informações sobre TTPs (Táticas, Técnicas e Procedimentos) e campanhas associadas a grupos maliciosos	Documentos estruturados, relatórios e plataformas como MISP e ThreatConnect	Ajudar equipes de segurança a entender e responder de forma mais eficaz às ameaças específicas
Inteligência Operacional	Indicadores técnicos (IOCs) compartilhados para resposta imediata a incidentes	MISP, e-mails rápidos e canais de comunicação instantânea, como Slack	Permitir respostas rápidas e eficazes a incidentes em andamento, minimizando danos e restaurando operações o mais rápido possível.

Importante observar que a clareza sobre o tipo de inteligência a ser compartilhada não é um exercício técnico abstrato, é o que determina se a informação gerará ação ou será ignorada. Compartilhar no nível errado, com o público errado, no momento errado, é um dos erros mais recorrentes e evitáveis nas iniciativas de colaboração em CTI.

6.1. O Risco do Nivelamento Excessivo

Com o objetivo de facilitar o compartilhamento ou reduzir barreiras internas, muitas organizações adotam uma abordagem simplificadora: tratam toda informação como se fosse inteligência operacional. Essa tendência à uniformização se manifesta em planilhas de IOCs genéricos, arquivos padronizados para todos os casos ou modelos de reporte únicos, independentemente do público-alvo. Embora essa prática possa parecer funcional em curto prazo, ela dilui o valor analítico do que está sendo compartilhado. **Ao reduzir a inteligência ao que é mais fácil de transmitir – e menos sensível – se compartilha o que é possível, mas não o que é necessário.**

Esse nivelamento não apenas empobrece o conteúdo, como também limita o engajamento dos diferentes perfis de profissionais. Executivos não se beneficiam de blocos de indicadores técnicos desconectados de contexto estratégico. Analistas de defesa, por sua vez, não conseguem agir com base em documentos abstratos ou excessivamente gerais. O resultado é um ciclo de baixa efetividade: todos compartilham, mas poucos aproveitam. A colaboração se mantém ativa apenas no volume, não no impacto.

6.2. Formato Desalinhado ao Propósito

Mesmo quando o conteúdo da inteligência é relevante, ele frequentemente chega ao destinatário em formato ineficaz. Indicadores operacionais são enviados por capturas de tela ou dentro de documentos não estruturados; relatórios táticos vêm em arquivos que não permitem extração automatizada; alertas estratégicos circulam como mensagens rápidas em chats informais, sem contexto ou autoria clara. **Nessa desconexão entre forma e função, perde-se a utilidade da informação, por mais valiosa que ela seja.**

Esse desalinhamento não decorre apenas de erro técnico, mas da ausência de uma lógica editorial que considere o destinatário e a finalidade da comunicação. Assim como uma boa apresentação exige pensar no público, o compartilhamento de inteligência exige pensar no uso pretendido. **Compartilhar o certo da forma errada é tão disfuncional quanto não compartilhar.** O ganho real está em alinhar o conteúdo, o formato e o momento de entrega, uma articulação que exige mais do que tecnologia: exige intenção e curadoria.

FEBRABAN
/CYBER LAB

7. Melhor Momento e Melhor Forma de Compartilhar

Em teoria, compartilhar inteligência cibernética deve ser um processo contínuo, calibrado e oportuno. Na prática, –a definição do “melhor momento” para compartilhar é frequentemente determinada por pressões contextuais, e não por estratégia. Muitas organizações compartilham **tarde demais, cedo demais** ou **de maneira imprecisa**. O desafio real não está apenas em ter o que compartilhar, mas em saber **quando e como fazê-lo para que a informação seja útil, acionável e confiável para quem a recebe**.

Modelos como o **FAIR (Factor Analysis of Information Risk)** e o **Cynefin Framework** ajudam a compreender por que uma abordagem única para o compartilhamento tende ao fracasso. O Cynefin, por exemplo, distingue contextos simples, complicados, complexos e caóticos – cada um exigindo respostas distintas em termos de fluxo de decisão e comunicação. Já o modelo FAIR enfatiza a necessidade de análise probabilística e sensível ao risco para avaliar a utilidade da informação. Apesar dessas referências estarem disponíveis, muitas organizações continuam a **replicar procedimentos padronizados, independentemente da natureza do incidente**, o que compromete tanto a eficácia da resposta quanto a qualidade do aprendizado organizacional. A rigidez processual transforma incidentes dinâmicos em burocracias estáticas, com efeitos colaterais como atrasos críticos ou compartilhamentos descontextualizados.

Adaptar a forma e o tempo do compartilhamento à realidade do evento é uma competência ainda rara, mas essencial. Organizações que conseguem modular sua atuação conforme o estágio do incidente (detecção, resposta, investigação, revisão) tendem a responder melhor, errar menos e aprender mais. Essa flexibilidade não significa improvisação: trata-se de **alinhar os métodos aos diferentes graus de complexidade e urgência** que cada situação impõe.

A tabela a seguir sintetiza e exemplifica os **momentos ideais para o compartilhamento**, os **canais recomendados** e as **finalidades associadas**, com base nos graus de complexidade e risco indicados por frameworks como **FAIR** e **Cynefin**. Embora muitos desses canais e meios sejam tecnicamente estruturados, as entrevistas revelaram que, na prática, **métodos informais, como grupos fechados de WhatsApp, mensagens diretas e contatos interpessoais, continuam sendo os mais acionados em situações críticas**. Esse uso não autorizado oficialmente, mas amplamente tolerado, revela tanto a agilidade buscada quanto a lacuna de canais institucionais adequados para cada cenário.

Cenário / Situação	Momento Ideal para Compartilhar	Meio/Plataforma Recomendado	Objetivo / Notas
Incidente Ativo	Imediatamente, durante a detecção e resposta ao incidente.	E-mails instantâneos, canais de chat (ex: Slack, Microsoft Teams).	Permitir a contenção rápida e a comunicação ágil para mitigar os danos; crítico em contextos caóticos.
Fase de Investigação	Durante a coleta e análise de evidências.	Plataformas colaborativas (ex: MISP, OpenCTI).	Facilitar a correlação de dados e o enriquecimento das informações; essencial em situações complexas.
Detecção de Atividade Suspeita	Logo após a verificação inicial e confirmação de padrões ou IOCs.	Relatórios rápidos via e-mail, dashboards temporários ou alertas em plataformas.	Alertar parceiros e reforçar defesas, garantindo que informações preliminares sejam avaliadas corretamente.
Compartilhamento de OSINT	Periodicamente, conforme novas informações forem coletadas e validadas.	Repositórios online (ex: GitHub), fóruns especializados, redes sociais.	Divulgar informações contextuais e atualizadas de fontes abertas, ampliando a visão do cenário.
Sessões de Treinamento e Workshops	Durante eventos programados, exercícios simulados ou sessões de capacitação.	Reuniões presenciais/virtuais, workshops, fóruns de discussão.	Disseminar lições aprendidas, compartilhar melhores práticas e fortalecer a cultura colaborativa.
Revisões Pós-Incidente	Após a resolução do incidente e conclusão de análises de lições aprendidas.	Relatórios formais, dashboards consolidados, apresentações em reuniões executivas.	Documentar insights, atualizar procedimentos e aprimorar estratégias de resposta e prevenção.

8. Limites da Inteligência Compartilhada: O que (não) se compartilha

Em todos os fóruns, guias e declarações públicas, o discurso sobre compartilhamento de inteligência cibernética enfatiza os benefícios da colaboração e a importância da troca de dados para fortalecer a defesa coletiva. No entanto, pouco se discute sobre **o que fica de fora dessa troca**. As entrevistas revelaram que, mesmo entre instituições que participam ativamente de redes colaborativas, há um conjunto significativo de informações que **não é compartilhado**, seja por estratégia, por receio, por limitação técnica ou por simples pragmatismo.

Entre os conteúdos sistematicamente omitidos estão dados sensíveis sobre falhas internas, falhas de detecção, erros operacionais e incidentes parcialmente contidos. Também são raros os compartilhamentos de **lições aprendidas de forma estruturada**, avaliações críticas sobre medidas que falharam, ou reflexões sobre dificuldades institucionais em lidar com ameaças complexas. Em muitos casos, o compartilhamento se restringe ao que já é público, genérico ou tecnicamente "seguro" de divulgar. O resultado é um fluxo de dados que, embora contínuo, **carece de profundidade analítica e valor estratégico**.

Esse silêncio seletivo não é fruto de descuido. Ele decorre de uma série de barreiras reais, como o medo de exposição, restrições legais, disputa de reputação e falta de mecanismos para anonimização robusta. Há também componentes culturais: **compartilhar inteligência ainda é, em muitas instituições, um gesto defensivo**, não uma prática natural. Saber o que não se compartilha – e por quê – é tão importante quanto mapear o que circula. Reconhecer esses limites é passo necessário para construir modelos de governança que não apenas incentivem a colaboração, mas compreendam suas zonas de silêncio e saibam como lidar com elas.

Conteúdos frequentemente excluídos do compartilhamento

- Lições aprendidas operacionais consideradas "básicas"
- Incidentes parcialmente contidos ou sob investigação
- Erros táticos ou falhas de mitigação
- Análises internas não classificadas como "estratégicas"
- Observações preliminares com potencial de correlação
- Boas práticas na correção de problemas ou implementação de soluções

O que se deixa de compartilhar é tão revelador quanto aquilo que circula. A ausência de conteúdos considerados “sensíveis”, “óbvios” ou “irrelevantes” por quem os detém não significa que essas informações sejam inúteis para os demais. **O que parece trivial para uma organização pode ser um alerta crítico para outra, especialmente em um ecossistema marcado por assimetrias de maturidade, visibilidade e capacidade de resposta.**

No entanto, é importante não confundir essa constatação com uma defesa do compartilhamento indiscriminado. Nem tudo que se sabe precisa ser repassado, e nem todo dado técnico é relevante fora do seu contexto. **O valor da inteligência compartilhada não está apenas no volume, mas na sua utilidade potencial para quem a recebe.** O desafio está em identificar aquilo que, mesmo básico para uns, pode ser essencial para outros – e compartilhá-lo com discernimento, curadoria e propósito. Esse tipo de julgamento exige não só sensibilidade técnica, mas também uma cultura de colaboração genuína, capaz de equilibrar generosidade com responsabilidade analítica.

FEBRABAN
/CYBER LAB

9. Mecanismos de Coordenação e Governança

A colaboração em inteligência cibernética não se sustenta apenas em tecnologia, confiança ou intenção. Ela requer **mecanismos de coordenação estáveis**, que definam regras, papéis, critérios de adesão, fluxos de decisão e processos de responsabilização. Quando múltiplas organizações interagem sem um arranjo comum de governança, o que se observa é a fragmentação do esforço coletivo, a sobreposição de iniciativas paralelas e a dificuldade de sustentar qualquer prática colaborativa no longo prazo.

As entrevistas revelaram uma realidade marcada por **iniciativas bem-intencionadas, mas desarticuladas**, que dependem fortemente de indivíduos específicos, que não se conversam entre si e raramente se transformam em estruturas duradouras. Em muitos casos, falta clareza sobre **quem deve liderar, convocar ou manter os canais de colaboração vivos**. Alguns defendem a criação de um intermediário neutro e institucionalizado, com legitimidade para operar entre os bancos e mediar o compartilhamento de forma segura, estruturada e anonimizada. Outros valorizam a informalidade entre pares, desde que haja mínima coordenação e comprometimento mútuo. Essa divergência reflete diferentes visões sobre confiança, risco e maturidade organizacional.

Não há um modelo universal. Centralização, descentralização ou arranjos híbridos são opções legítimas, mas sua efetividade depende de como são implantadas e, sobretudo, mantidas. A falta de governança prática, aquela que define o que é feito na rotina, e não apenas no papel, tem sido uma barreira invisível, mas persistente, à consolidação da inteligência colaborativa no setor financeiro. A seguir, são descritas abordagens de referência, observadas em experiências nacionais e internacionais.

9.1. Modelos Observados: Centralizado, Descentralizado e Híbrido

As formas de coordenação em redes de inteligência cibernética variam amplamente. Alguns setores optam por **modelos centralizados**, com uma entidade responsável por consolidar, filtrar e redistribuir a inteligência. Outros preferem **arranjos descentralizados**, baseados na autonomia e na troca direta entre os participantes. Há ainda os **modelos híbridos**, que combinam diretrizes centrais com liberdade local de ação. Nenhum desses formatos é superior por definição. Sua adequação depende do contexto: grau de regulação, cultura institucional, maturidade técnica e capacidade de manutenção contínua.

No setor financeiro, essas diferenças aparecem com clareza. Enquanto algumas instituições expressam desconforto com a ausência de uma instância clara de coordenação, outras demonstram resistência a estruturas centralizadoras, por receio de burocracia ou exposição. Há também quem aponte que, mesmo onde existe um modelo nominalmente definido, a governança de fato é informal e reativa. Em outras palavras, o desafio **não é desenhar o modelo, mas fazê-lo funcionar na prática**: garantir adesão, continuidade e legitimidade.

A tabela a seguir resume as características principais desses três modelos, incluindo exemplos reais, vantagens esperadas e limitações identificadas. Mais do que uma tipologia, ela serve como referência para avaliar as escolhas institucionais frente à realidade de colaboração que se pretende construir.

Modelo	Vantagens	Desafios	Exemplos Reais / Grupos	Comentários Adicionais
Centralizado	• Estabelece padrões rigorosos e uniformes em todos os processos. • Proporciona maior controle na disseminação de informações sensíveis.	• Pode se tornar burocrático e limitar a agilidade na resposta a incidentes. • Risco de sobrecarga no ponto central, comprometendo a eficiência da rede.	• **FS-ISAC** (Financial Services ISAC) • **US-CERT** • **CERT-EU** • **Interpol** Cybercrime Directorate	É mais utilizado como gateway de informações, onde cada organização pode compartilhar com a entidade central, mas a entidade central que irá definir, unificar e estruturar as informações necessárias do que e como deve ser compartilhado com os demais membros. Esse modelo é recomendado para setores altamente regulados, onde a consistência e o controle são essenciais. Embora facilite auditorias e conformidade, a dependência de um único ponto pode gerar vulnerabilidades e perda de informações relevantes.
Descentralizado	• Oferece maior flexibilidade e agilidade na atualização e disseminação de informações. • Concede autonomia para respostas rápidas a incidentes específicos.	• A ausência de padronização pode resultar em inconsistências na qualidade e integração dos dados. • Exige esforços adicionais para validação dos dados.	• **FIRST** (Forum of Incident Response and Security Teams) • **CIRCL** Private Sector Information Sharing Community • **X-ISAC**	Incentiva a inovação e permite que cada entidade veja e compartilhe de forma comunitária entre os demais envolvidos, adaptando seus processos conforme seu contexto. Contudo, a falta de controle centralizado pode gerar redundâncias e principalmente falta de padrões.
Híbrido	• Equilibra a padronização com a flexibilidade, integrando diretrizes mínimas e espaço para inovação.	• Necessita de uma coordenação robusta para alinhar diretrizes centrais com a autonomia local, evitando conflitos e divergências.	• **CTA** (Cyber Threat Alliance) • **ENISA** • **SABRIC** (South African Banking Risk Information Centre)	Combina os pontos fortes dos modelos centralizado e descentralizado, facilitando a interoperabilidade entre setores e regiões. Requer investimentos contínuos em treinamento, comunicação e atualização dos padrões para manter sua eficácia.

As entidades mencionadas exemplificam como a governança pode ser adaptada para fomentar comunidades colaborativas e integradas. Cada modelo apresenta benefícios específicos, mas também limitações que devem ser consideradas.

A escolha do modelo mais adequado deve levar em conta as características do setor, a natureza das ameaças e o nível de maturidade dos processos internos. Mais do que um desenho institucional, trata-se de criar condições para que as organizações se reconheçam como parte de uma comunidade ativa. O sucesso do compartilhamento depende, antes de tudo, da capacidade coletiva de sustentar essa comunidade ao longo do tempo, com clareza, segurança e compromisso mútuo.

9.2. O Papel de Colaboração Intermediada

Em um ecossistema onde as instituições compartilham riscos e ameaças semelhantes, mas não compartilham inteligência com regularidade, há um ruído que não se deve apenas à falta de ferramentas. Discussões revelaram uma realidade fragmentada: **maioria das pessoas e organizações não se conhecem, não mantêm canais abertos entre si e, muitas vezes, sequer sabem com quem falar em caso de necessidade**. Em um ambiente assimétrico, marcado por desconfianças e reservas, é compreensível que o compartilhamento não aconteça de forma fluida.

A confiança, como já discutido, segue associada a vínculos pessoais. Quando alguém pergunta sobre uma ameaça em um grupo, corre o risco de ser interpretado como **vítima daquela ameaça**. Quando uma instituição compartilha informação sem contextualizar, há quem questione: por que está compartilhando isso agora? Está acontecendo com ela? O receio de exposição bloqueia a circulação da informação antes mesmo que ela se torne útil. Isso cria um ciclo em que **a ausência de familiaridade entre os indivíduos leva ao silêncio**, e o silêncio aprofunda a ausência de relacionamento.

Essa desarticulação cotidiana alimenta um senso comum: mesmo quando há disposição para colaborar, falta estrutura para transformar intenção em prática. Não existe um canal institucional confiável, não há clareza sobre formatos, e o julgamento sobre "o que pode ou não ser dito" recai sempre sobre o indivíduo, que tende a optar pela omissão. **Nesse vazio prático, emerge a expectativa de uma figura mediadora** – não como ideal normativo, mas como consequência de um sistema que ainda não se comunica por si só.

O papel de intermediário não surge como inovação recente, tampouco como proposta elaborada em comitês. Trata-se de uma figura frequentemente mencionada, em diferentes setores e regiões, como uma **resposta recorrente a ambientes de colaboração pouco estruturados, baseados em confiança interpessoal e marcados por lacunas operacionais**. A ideia de contar com alguém que organize o que não está coordenado, que preencha os vazios entre instituições que não se falam diretamente, que proteja o compartilhamento quando o risco de exposição paralisa a iniciativa, **não é exclusiva do setor financeiro – é um padrão comum em ecossistemas onde a colaboração não amadureceu plenamente**.

Nesse contexto, o intermediário costuma ser imaginado não como uma entidade formal ou permanente, mas como uma função legitimada, que transita entre organizações com discrição e critério técnico, capaz de receber dados sensíveis, aplicar anonimização quando necessário, e redistribuir a informação com base em relevância e responsabilidade. Sua função não é substituir os canais existentes, mas **atuar precisamente onde esses canais se mostram ausentes, frágeis ou inoperantes**.

O fato dessa figura ser frequentemente invocada, mesmo que de maneira informal, **é sintoma de algo mais profundo**: a percepção de que, sozinhas, muitas instituições, inclusive no setor financeiro, **ainda não conseguem sustentar um fluxo confiável e contínuo de inteligência compartilhada**. A dúvida sobre a quem recorrer, como compartilhar ou sob qual formato, revela que o problema não está apenas na informação, mas nas estruturas que deveriam viabilizá-la.

9.3. Desejo de Colaboração Intersetorial: Entre a Intenção e a Maturidade

Colaboração entre diferentes setores econômicos, como financeiro, telecomunicações, nuvem e varejo, é frequentemente mencionada como um objetivo desejável, capaz de ampliar a visibilidade sobre ameaças, fortalecer a resposta coordenada e reduzir vulnerabilidades sistêmicas. Em tese, a integração entre setores permitiria rastrear campanhas complexas, identificar vetores cruzados e antecipar riscos compartilhados. **Na prática, porém, esse tipo de colaboração ainda está distante da realidade.**

Um dos primeiros entraves é estrutural: **muitos setores, especialmente no Brasil, sequer consolidaram internamente práticas básicas de compartilhamento**. Não há políticas claras, equipes preparadas, governança ou cultura que favoreça a troca de informações, mesmo entre instituições do mesmo segmento. Tentar construir pontes intersetoriais nessas condições se torna uma tentativa de antecipar a maturidade que ainda não foi alcançada internamente.

Além disso, **a confiança, que já é escassa entre pares de um mesmo setor, se torna ainda mais frágil quando atravessa fronteiras institucionais, regulatórias e operacionais**. O receio de exposição, o desconhecimento mútuo e a ausência de padrões comuns tornam a colaboração entre setores uma prática de alto risco percebido. Sem canais neutros, sem atores legitimados para intermediar a troca e sem vocabulário compartilhado, a aproximação tende a se restringir a fóruns genéricos ou iniciativas com pouco impacto prático.

Ainda assim, os ganhos potenciais da colaboração intersetorial são evidentes. Em cenários como ataques DDoS, campanhas de phishing massivo ou incidentes que envolvem infraestrutura crítica, **as fronteiras entre setores são mais artificiais do que técnicas**. Um ataque que afeta o setor financeiro pode passar por uma operadora de telecomunicações. Uma ameaça detectada por um provedor de nuvem pode estar prestes a atingir serviços públicos, e sem integração mínima, as ações de resposta ocorrem de forma isolada, descoordenada e, por vezes, redundante.

A colaboração intersetorial não deve ser tratada apenas como tendência ou oportunidade. Ela deve ser reconhecida como uma lacuna que, se não for preenchida com cuidado, pode comprometer toda a resiliência do ecossistema.

Principais barreiras e oportunidades da colaboração intersetorial

- Descompasso de maturidade e confiança entre setores
- Ausência de padrões e canais comuns
- Inexistência de fóruns neutros ou mecanismos confiáveis de mediação
- Falta de clareza sobre papéis e benefícios mútuos
- Oportunidade de resposta mais coordenada
- Integração potencial com “law enforcement”

10. Uma Questão Mais Cultural do Que Tecnológica

As questões anteriores mostram que os principais desafios do compartilhamento de inteligência não estão nas ferramentas, nos padrões ou nos modelos. Eles residem nas posturas, prioridades institucionais e relações estabelecidas (ou não) entre os atores do ecossistema. Apesar do avanço técnico, da existência de plataformas sofisticadas e da maior visibilidade sobre os riscos cibernéticos, **compartilhar segue sendo uma decisão essencialmente humana, contextual e carregada de implicações não técnicas**.

O que ainda predomina em muitos ambientes é uma lógica de contenção: compartilha-se o mínimo necessário, com o menor grau de exposição possível, em canais que nem sempre foram desenhados para isso. A colaboração, quando acontece, é episódica e frequentemente impulsionada por indivíduos, e não por processos estruturados. Isso gera dependência de vínculos informais, rotinas improvisadas e uma oscilação constante entre períodos de engajamento intenso (geralmente durante crises) e longos intervalos de silêncio. **A cultura da segurança ainda é defensiva, orientada pela prudência individual e pela preservação institucional – e não por uma mentalidade coletiva de resiliência setorial**.

Superar esse quadro exige mais do que ajustes técnicos. Implica revisar incentivos, reconhecer os bloqueios simbólicos e reorganizar a colaboração como parte do funcionamento regular das instituições. Isso passa por treinamento, liderança engajada, rituais de troca e, sobretudo, por tempo. Cultura não se impõe, se cultiva, e sem ela qualquer tecnologia de compartilhamento continuará funcionando abaixo de seu potencial – ou apenas servindo de vitrine para boas intenções que nunca se concretizam por inteiro.

Elementos culturais críticos para sustentar a colaboração

- Confiança mútua
- Clareza de propósito e responsabilidade interna
- Visão de longo prazo
- Engajamento institucional real (não apenas individual)
- Rituais organizados e sustentáveis

10.1. A Importância da Alta Gestão no Compromisso com a Colaboração

Ao longo deste estudo, tornou-se evidente que muitas das barreiras culturais à colaboração em inteligência cibernética não decorrem apenas de resistência operacional, mas da **ausência de patrocínio ativo por parte da alta gestão**. Em diversas organizações, o compartilhamento é percebido como um esforço técnico, secundário, que pode (ou não) acontecer dependendo da disponibilidade e do interesse dos profissionais envolvidos. **A colaboração, nesses contextos, não é uma política institucional estratégica – é uma prática operacional, invisível para os níveis decisórios mais altos.**

Essa invisibilidade gera efeitos estruturais. Sem posicionamento claro da liderança, o tema **não ganha prioridade nem legitimidade interna**. Iniciativas são criadas de forma experimental, sem recursos dedicados, sem tempo protegido nas agendas das equipes e sem respaldo para enfrentar resistências internas – como as que vêm de áreas jurídicas ou de compliance. A falta de sinalização da diretoria também limita a articulação externa: profissionais hesitam em representar sua instituição em fóruns, evitam assumir protagonismo e se retraem diante de dúvidas sobre o que podem ou não compartilhar em nome da organização.

A ausência de engajamento executivo é interpretada como desinteresse. Onde não há apoio estratégico, **as iniciativas de colaboração tendem a serem tratadas como esforços voluntários, dependentes da energia pessoal de poucos indivíduos**. Essa dependência é frágil. Quando esses profissionais mudam de área, saem da empresa ou perdem fôlego, o trabalho coletivo se desfaz. O apoio institucional da alta gestão é essencial para garantir a escalabilidade, a sustentabilidade e a relevância da colaboração.

Efeitos da ausência da alta gestão

- Falta de prioridade institucional
- Ausência de recursos e continuidade
- Inviabilidade de criar políticas internas claras
- Isolamento de áreas técnicas

Esse descompasso se torna mais visível nos momentos de tensão. Quando um incidente significativo repercute no setor, ou quando há indícios de uma ameaça que possa afetar diretamente a organização, **é justamente a alta gestão, quem exige com mais urgência relatórios, contatos, validações e comparações com outros players do mercado**. A colaboração, que antes parecia periférica, passa a ser tratada como peça central da resposta. E quando o corpo técnico não consegue obter informações suficientes ou entregá-las em tempo hábil, **não são raras as cobranças de agilidade de uma rede que nem sempre recebe investimento, atenção ou priorização institucional**. **Espera-se retorno imediato de uma estrutura pouco incentivada fora dos contextos de crise;** quando ela falha, a ausência de estratégia tende a recair sobre a área operacional.

10.2. O Silêncio Pós-Compartilhamento e o Esgotamento do Engajamento

Em muitos ambientes colaborativos, compartilhar inteligência ainda é um ato de confiança, esforço e tempo. Demanda seleção do que é relevante, organização da informação, aplicação de critérios de segurança e, muitas vezes, negociação interna para autorizar a divulgação. Porém, uma vez compartilhado, **o que acontece depois raramente é discutido**, e é justamente no "depois" que reside uma das barreiras mais silenciosas à continuidade da colaboração.

A ausência de retorno, seja ele um simples reconhecimento, uma pergunta, um comentário ou uma confirmação de recebimento, **é percebida como indiferença**. Aos poucos, o silêncio se acumula e se transforma em sinal. Compartilhar passa a parecer irrelevante. Profissionais relatam, em diversos contextos, que após enviar relatórios, indicadores ou alertas, **não houve qualquer tipo de resposta ou engajamento visível**. Com o tempo, isso desestimula. A colaboração, que deveria ser uma via de mão dupla, **vira monólogo**.

Em última instância, a ausência de resposta enfraquece, de forma sutil e cumulativa, o principal combustível da colaboração: a percepção de que o esforço teve algum impacto.

Consequências frequentes desse silêncio recorrente

- Desvalorização simbólica do esforço de colaborar
- Redução gradual do engajamento por parte de quem compartilha
- Adoção de postura mais reativa e contida
- Perda de senso de comunidade

10.3. Colaboração não é Conformidade

O avanço da regulação em temas de segurança cibernética tem levado muitas organizações a institucionalizarem processos de relatório, adoção de padrões técnicos e resposta a incidentes. Embora essas obrigações normativas sejam fundamentais, é importante reconhecer que **cumprir exigências formais não equivale a colaborar de forma genuína**. A colaboração pressupõe engajamento voluntário, abertura informacional e disposição para contribuir com o fortalecimento do ecossistema como um todo.

Quando o compartilhamento é tratado apenas como desdobramento do compliance, ele tende a ser restrito, reativo e desprovido de intencionalidade analítica. O foco se desloca do valor coletivo da inteligência para a simples entrega documental, muitas vezes dissociada do contexto mais amplo de proteção interinstitucional. **A prática do compartilhamento, nesse cenário, corre o risco de se esvaziar, não por falta de mecanismos, mas por ausência de propósito**.

Em muitos contextos e indústrias, especialmente nas instâncias superiores de gestão, se observa a expectativa de que a colaboração em inteligência cibernética possa – ou deva – ser inteiramente normatizada. Há quem deseje regras detalhadas sobre **o que compartilhar, com quem, em que momento, por qual canal e sob quais níveis de autorização**. Embora essa expectativa seja compreensível frente à insegurança jurídica e à preocupação com riscos reputacionais, ela **revela uma leitura equivocada da natureza da colaboração genuína**. Práticas colaborativas eficazes dependem de confiança construída, julgamento contextual e capacidade de adaptação. Esses elementos não se submetem facilmente a protocolos rígidos. **Tentar regular todos os aspectos da colaboração pode transformá-la em um exercício burocrático: previsível, mas estéril.**

Padrões observáveis quando colaboração é confundida com obrigação:

Envio de dados descontextualizados
com foco apenas na entrega formal e não na utilidade da informação

Participação limitada a fluxos exigidos por norma
sem envolvimento em fóruns ou redes que operam por confiança e reciprocidade

Compartilhamento técnico desvinculado de análise tática ou estratégica
o que compromete sua aplicabilidade mais ampla

Fragmentação interna entre áreas técnicas e jurídicas
dificultando a construção de uma postura colaborativa integrada

Reverter esse quadro não exige apenas revisão regulatória, mas **reconhecimento de que a colaboração é uma prática deliberada, não um reflexo automático da conformidade**. Ela começa onde termina a obrigação, e só se sustenta quando há clareza sobre seu valor para além do cumprimento normativo.

FEBRABAN
/CYBER LAB

11. A Influência do Setor e da Localização Geográfica

A colaboração em inteligência costuma ser abordada como um desafio técnico ou organizacional. No entanto, sua efetividade é profundamente moldada por fatores externos à operação direta das instituições. **O setor em que a organização atua, o ambiente regulatório a que está submetida, sua posição no mercado e a geografia institucional à sua volta condicionam, muitas vezes de forma invisível, o que é possível, aceitável e sustentável em termos de compartilhamento.** Colaborar não é apenas uma escolha operacional, é também uma construção contextual.

É comum ouvir referências a modelos internacionais tidos como exemplares – alianças globais, centros europeus, comunidades maduras em outros setores – como se fossem soluções universais. Frases como "*precisamos ser como aquela iniciativa*" aparecem com frequência nos debates. No entanto, **pouco se discute sobre as condições que tornam esses modelos viáveis**: marcos legais estáveis, tradição de cooperação público-privada, homogeneidade de maturidade entre os participantes, infraestrutura técnica consolidada e, sobretudo, tempo de maturação institucional. A tentativa de importar formatos sem considerar esses fatores costuma gerar frustração e desalinhamento. **É como querer replicar o comportamento de um ecossistema sem reconhecer o solo onde ele foi cultivado.**

Essas variáveis não devem ser vistas como barreiras, mas como coordenadas. **Elas definem os contornos de onde e como a colaboração pode prosperar.** Compreender essas diferenças é fundamental para evitar expectativas irrealistas e desenhar arranjos de compartilhamento que sejam coerentes com a realidade local, não apenas inspirados em boas práticas externas, mas ajustados à maturidade, ao risco e à capacidade do ecossistema em questão. A seguir, são destacados alguns dos principais fatores setoriais e geográficos que influenciam as práticas de compartilhamento.

Fatores Setoriais

- Regulamentação e Conformidade
- Natureza dos Ativos e Riscos
- Capacidade de Investimento: Fatores Geográfico
- Diferenças Regulatórias Regionais
- Cultura e Cooperação Regional
- Infraestrutura tecnológica e maturidade digital

Esses fatores destacam que a colaboração em inteligência cibernética **não acontece no vácuo técnico**, ela é moldada por contextos institucionais, culturais e geográficos que determinam até onde a colaboração pode ir e o que ela precisa contornar para existir. Compreender essas variáveis é essencial para definir estratégias realistas, sustentáveis e ajustadas à realidade de cada organização.

12. Conclusão

Falar em colaboração e compartilhamento de inteligência cibernética tornou-se um mantra institucional. Fóruns, documentos estratégicos, palestras e normas repetem com fluidez que é necessário colaborar, urgente compartilhar, fundamental integrar. O vocabulário já está assentado. **O problema é outro.** Muito se diz sobre o **porquê colaborar**, e muito também sobre **como colaborar**. O que falta, com frequência, é dizer com clareza **por que essa colaboração, mesmo tão defendida, quase nunca se sustenta com a robustez que se espera.**

Este estudo não se propõe a responder como compartilhar, mas a entender **por que não se compartilha**. Seu objetivo não é a formulação de boas práticas ou o desenho de modelos operacionais, mas sim **provocar reflexão**.

Mais ainda, **provocar desconforto**.

O desconforto de reconhecer que, por trás da aparente concordância em torno da colaboração, há **contradições não verbalizadas, tensões institucionalizadas e obstáculos que todos conhecem de forma intuitiva, mas poucos conseguem nomear com precisão**. Quando a crítica é evitada ou silenciada, o que sobra são **tentativas mal formuladas, iniciativas que falham sem autocrítica e a repetição de fórmulas que não respondem à realidade concreta**.

Ao longo da análise, observou-se que os maiores entraves **não são técnicos**. Plataformas existem. Padrões foram definidos. Modelos de governança estão amplamente documentados. O que falta **não é ferramenta, mas disposição política, clareza estratégica, suporte institucional e, sobretudo, coerência entre discurso e prática**. Muitos dos dilemas examinados neste estudo não são desconhecidos. Eles estão presentes no cotidiano das instituições, nas conversas de bastidores, nos projetos que se iniciam com entusiasmo e terminam no esvaziamento silencioso. Falta apenas organizá-los, torná-los visíveis e, portanto, discutíveis.

Um dos objetivos centrais deste estudo é justamente esse: **transformar o desconforto difuso em crítica estruturada**. Dar forma ao que incomoda, mas raramente é dito com todas as letras. Quando se diz, por exemplo, que as iniciativas falham por falta de adesão, raramente se pergunta por que ninguém adere. Quando se afirma que os fóruns não funcionam, raramente se discute o que os inviabiliza. E quando se tenta replicar modelos externos bem-sucedidos, quase nunca se reconhece que o contexto regulatório, institucional e cultural, possui particularidades que exigem **adaptações muito mais profundas** do que copiar boas práticas externas.

Este estudo parte da constatação de que a colaboração **não falha por má vontade, mas por ausência de estrutura real para sustentá-la**. Falta clareza sobre responsabilidades, processos internos bem definidos, políticas de validação e tratamento, proteção jurídica e, sobretudo, uma cultura institucional que trate a colaboração como prática estratégica, e não como exceção emergencial. Ao contrário do que se imagina, muitos dos fracassos colaborativos não vêm da falta de iniciativa, mas do excesso dela. O setor está repleto de **iniciativas paralelas que não se coordenam, plataformas que não conversam, fóruns que existem, mas não se comunicam**. Não por desorganização, mas por **ausência de alinhamento prévio, escuta crítica e disposição para o desacordo produtivo**.

A ideia recorrente de que um intermediário neutro resolveria a fragmentação do ecossistema revela esse cenário. Ela emerge não como proposta institucionalizada, mas como tentativa de preencher um **vazio de governança, de coordenação e de legitimidade entre os atores**. Quando se busca um canal confiável externo para fazer circular informações, o que se evidencia é a dificuldade da comunicação direta. **O intermediário é uma solução, mas também um sintoma. Ele aparece quando a rede, por si só, não se sustenta.**

Há ainda outro paradoxo pouco discutido: o **desejo por normatização total da colaboração**. É recorrente a expectativa de que tudo seja regulado – **o conteúdo, o canal, o momento, o destinatário, a frequência**. Embora compreensível diante das inúmeras incertezas jurídicas, essa visão ignora o fato de que **colaboração genuína não é construída com base apenas em dispositivos legais ou mecanismos formais de compliance**. A colaboração começa **muito antes disso**: **nas organizações, nas comunidades profissionais, nas lideranças que decidem se comprometer e nos indivíduos que têm coragem de agir mesmo diante das incertezas**. Regras ajudam, mas **não criam cultura**. E sem cultura, o risco é transformar a prática colaborativa em um protocolo tecnicamente correto, mas vazio de engajamento real.

Este estudo também reforça que **a colaboração é um fenômeno situado**. Cada setor, cada país, cada grupo opera sob diferentes incentivos, riscos, capacidades e histórias. Replicar modelos externos sem considerar o solo em que se pisa tem levado, com frequência, a novas frustrações. O que funcionou em outro lugar talvez não funcione aqui – **não por resistência, mas por incompatibilidade estrutural**. E adaptar exige **humildade, tempo e escuta**.

Em última instância, este estudo não oferece soluções prontas, mas **clareza crítica**. Ao nomear os problemas, **não os multiplica – busca organizá-los**. Ao iluminar as contradições, **não as condena – as torna visíveis**. E ao provocar desconforto, **não paralisa – prepara o terreno para que propostas reais, consistentes e adequadas possam surgir**, sem depender de improvisos, atalhos ou interferências mal-informadas. Às vezes é necessário falar o óbvio.

A colaboração, como se viu, não é fácil nem automática. Mas ela é possível. E será tanto mais possível quanto maior for a honestidade dos envolvidos em reconhecer os problemas que estão diante de todos, mas que poucos têm coragem ou vocabulário para enfrentar. **Este estudo entrega, portanto, o que se propôs a fazer: um ponto de partida mais lúcido, mais denso e mais exigente para que o futuro da colaboração em inteligência cibernética não se limite a intenções.** Mas se transforme, gradualmente, **em prática consciente, estruturada e sustentável.**

FEBRABAN
/CYBER LAB

13. Referências de Suporte

Documentos oficiais e frameworks de referência

- NIST SP 800-150 (2016) – Guide to Cyber Threat Information Sharing
- E-Ciber (Estratégia Nacional de Cibersegurança)
- Resolução Conjunta nº 6/2023 – Banco Central do Brasil
- Manual de Compartilhamento de Informações de Cibersegurança na Aviação Civil – ANAC
- FAIR Institute – Factor Analysis of Information Risk

Guias setoriais e publicações institucionais

- ANBIMA – Ebook: Orientações para Compartilhamento de Informações de Incidentes Cibernéticos
- Security Leaders – A importância do compartilhamento de informações para o setor financeiro
- FS-ISAC – Intelligence Sharing 2.0: Beyond Threat Intelligence
- Concordia H2020 – Threat Intelligence Sharing
- CISA – Information Sharing Hub

Artigos científicos e acadêmicos

- Open Access – Cyber Threat Intelligence Sharing Survey and Research Directions
- ScienceDirect – Factors influencing cyber threat intelligence sharing

- ACM Digital Library – Multiple articles
  - The practice of CTI sharing: trust, incentives, and barriers
  - Interorganizational Intelligence Sharing
  - Automating threat intelligence validation
- Oxford Academic – Cybersecurity Journal
  - The effect of interorganizational trust on CTI sharing
  - CTI frameworks: operational and legal gaps
- JSTOR – Sharing Security Information
- NDSS Symposium – Threat sharing architectures
- Arxiv – Distributed Threat Intelligence Models
- PMC – Interoperability and CTI
- Scholarworks – Institutional Barriers to CTI
- Nano Journal – Barriers to Cyber Collaboration
- Kalahari Journals – CTI Adoption Challenges

Artigos analíticos, técnicos e de opinião

- NIC.br – Colaboração e compartilhamento de inteligência
- XLabs – Falta de compartilhamento prejudica a segurança cibernética no Brasil
- Lockton – 10 tendências de segurança e risco cibernético
- Cisco + Distrito – Panorama de segurança cibernética no Brasil
- Chambers Practice Guide – Cybersecurity 2025: Brazil
- Cybersecurity Magazine – Improving Threat Intelligence Collaboration

FEBRABAN
/CYBER LAB