DEFININDO ESCOPO DE PROJETOS DE SEGURANÇA CIBERNÉTICA COM O MÉTODO FAIR-MAM™

GIANFRANCO MUNCINELLI – g.muncinelli@pucpr.edu.br
PONTIFICIA UNIVERSIDADE CATÓLICA DO PARANÁ – PUC-PR
FUNDAÇÃO GETULIO VARGAS - FGV

WILSON MENDES LAURIA - ext.wilson.lauria@prof.fgv.edu.br
FUNDAÇÃO GETULIO VARGAS - FGV

ALEXANDRE ANTONIO URIOSTE VASCONCELLOS -
alexandre.urioste@grciber.com.br
FUNDAÇÃO GETULIO VARGAS - FGV

ÁREA: *06.ENGENHARIA ORGANIZACIONAL*
SUBÁREA: *6.2- GERENCIAMENTO DE PROJETOS*

RESUMO: *A DEFINIÇÃO DE ESCOPO EM PROJETOS DE SEGURANÇA CIBERNÉTICA É UM DESAFIO CRESCENTE, ESPECIALMENTE DIANTE DA SOFISTICAÇÃO DAS AMEAÇAS E DA NECESSIDADE DE JUSTIFICAR INVESTIMENTOS COM BASE EM VALOR PARA O NEGÓCIO. ESTE ARTIGO PROPÕE O USO DO MÉTODO FAIR™ (FACTOR ANALYSIS OF INFORMATION RISK) E SUA EXTENSÃO FAIR-MAM™ (MATERIALITY ASSESSMENT MODEL) COMO ABORDAGEM QUANTITATIVA PARA DELIMITAR ESCOPOS DE FORMA OBJETIVA, ESTRATÉGICA E FINANCEIRAMENTE JUSTIFICÁVEL. APÓS CONTEXTUALIZAÇÃO TEÓRICA E APRESENTAÇÃO DAS LIMITAÇÕES DAS ABORDAGENS TRADICIONAIS, O ESTUDO APLICA OS MÉTODOS AO CASO DO ATAQUE NOTPETYA À MAERSK EM 2017, DEMONSTRANDO COMO O FAIR™ PODE TRADUZIR RISCOS TÉCNICOS EM IMPACTOS FINANCEIROS E ORIENTAR A PRIORIZAÇÃO DO ESCOPO. A CONCLUSÃO RESSALTA A RELEVÂNCIA DESSAS METODOLOGIAS PARA AUMENTAR A MATURIDADE EM SEGURANÇA CIBERNÉTICA E FACILITAR DECISÕES MAIS ALINHADAS COM OS OBJETIVOS ORGANIZACIONAIS.*

PALAVRAS-CHAVES: *SEGURANÇA CIBERNÉTICA; FAIR-MAM; ESCOPO DE PROJETOS.*

1. INTRODUÇÃO

A definição de escopo é um processo crítico em qualquer tipo de projeto. Em projetos de segurança cibernética, especialmente quando se busca garantir que os recursos sejam alocados com base na materialidade do risco isso se reveste de importância excepcional. O escopo define os limites do que será entregue, influenciando diretamente os custos, o cronograma e o valor gerado.

Entretanto, a abordagem tradicional da gestão de riscos — baseada em classificações qualitativas de probabilidade e impacto, apresenta limitações significativas quando aplicada ao contexto da Segurança Cibernética. A ausência de métricas quantitativas robustas e a dificuldade em traduzir riscos técnicos em impactos concretos para o negócio podem comprometer a eficácia do processo decisório, resultando em decisões subótimas na priorização do escopo.

Em ambientes de negócios cada vez mais expostos a riscos cibernéticos, definir com precisão o escopo de um projeto de segurança tornou-se uma tarefa altamente complexa e estratégica. Ao contrário de projetos tradicionais, em que os objetivos são concretos e mensuráveis — como a implementação de um novo sistema ou processo — os projetos de segurança lidam com ativos intangíveis, ameaças incertas e impactos altamente voláteis.

Segundo o Global Cybersecurity Outlook 2024 do World Economic Forum (WEF), 91% das organizações acreditam que um ciberataque com impacto catastrófico é provável nos próximos dois anos, no entanto menos da metade se sente preparada. Essa dissonância entre percepção de risco e capacidade de resposta está diretamente associada à dificuldade da estruturação do escopo: o que proteger primeiro?; como justificar investimentos?; quais riscos são materialmente relevantes para o negócio? (WEF, 2024)

A consultoria Gartner, em seu relatório de 2023, destaca que 60% dos projetos de segurança que fracassam o fazem por erro na delimitação de escopo, geralmente por se fundamentarem em suposições subjetivas ou pressões reativas. A ausência de uma abordagem sistemática para análise de risco e priorização de requisitos pode comprometer o valor entregue (GARTNER, 2024).

É nesse cenário que o modelo FAIR™ (Factor Analysis of Information Risk) se apresenta como um diferencial: ele permite a transição de uma abordagem qualitativa e genérica para uma estrutura quantitativa, analítica e baseada em valor financeiro do risco, favorecendo decisões mais alinhadas com os objetivos estratégicos da organização. Com base

quantitativa e estrutura probabilística, o FAIR™ permite que riscos cibernéticos sejam avaliados em termos financeiros. O anexo FAIR-MAM (Materiality Assessment Model) aprofunda essa abordagem ao estabelecer critérios objetivos para avaliar a materialidade de eventos cibernéticos (JONES, 2021).

O pano de fundo deste trabalho será um evento em que uma das maiores empresas de logística do mundo, a Maersk, foi vítima do ransomware NotPetya, que criptografou dados e paralisou operações globalmente no ano de 2017 (MAERSK, 2018) (GREENBERG, 2018) (BAREHAM, 2020).

Este artigo pretende fornecer uma visão de estrutura robusta para definição de escopo de um projeto de cibersegurança, com base no valor a ser protegido e avaliado em termos financeiros.

2. REVISÃO DE LITERATURA

Projetos de segurança cibernética se inserem em uma categoria particular de empreendimentos estratégicos: são movidos por risco, mas seu sucesso é medido pela não-ocorrência de eventos ou quando eles ocorrem não são capazes de causar um dano significativo. Essa inversão conceitual desafia os modelos tradicionais de escopo, que se concentram na entrega de produtos tangíveis e na medição de benefícios diretos. A seguir, aprofundamos os principais fatores que tornam essa definição um obstáculo recorrente para gerentes de projeto (NIST, 2022).

2.1. A intangibilidade dos ativos e dos resultados

Em projetos convencionais, o escopo é definido com base em entregas concretas (ex: software implantado, processo redesenhado, infraestrutura finalizada). Já nos projetos de segurança, o objetivo primário é reduzir a exposição a eventos negativos — como vazamentos de dados, indisponibilidades, fraudes internas ou violações regulatórias — cujos impactos são muitas vezes latentes ou difíceis de quantificar baseado em suposição e prognóstico, sendo fundamentalmente subjetivo e estimativo (PMI, 2021).

Além disso, os ativos envolvidos (dados sensíveis, imagem institucional, confiança do consumidor) são intangíveis e não aparecem nos balanços patrimoniais, o que dificulta a justificação de investimentos do ponto de vista financeiro (WEF, 2024b).

2.2. Ambiente de ameaça adaptativo e volátil

A definição de escopo se torna frágil quando se baseia em uma fotografia estática do ambiente de risco. O cenário cibernético é caracterizado por (FAIR INSTITUTE, 2022):

- Ações intencionais e adaptativas de agentes maliciosos;
- Surgimento contínuo de vulnerabilidades (zero-days, exploits em cadeia de suprimentos, IA generativa maliciosa);
- Ataques dirigidos por grupos com capacidade quase-estatal (APT – Advanced Persistent Threats).

Dessa forma, escopos de projeto definidos sem o apoio de ferramentas que possibilitem a modelagem de riscos com granularidade e capacidade de atualização contínua tendem a se tornar obsoletos ainda durante o ciclo de vida do projeto, comprometendo sua efetividade e aderência às necessidades reais do contexto cibernético dinâmico (FAIR INSTITUTE, 2022).

2.3. Multiplicidade de pressões e stakeholders

Além da volatilidade técnica, o escopo de um projeto de segurança é pressionado por múltiplos interesses, como:

- Demandas de compliance (LGPD, GDPR, SOX, ISO/IEC 27001);
- Auditorias internas e externas;
- Riscos regulatórios setoriais (ex: ANS, Bacen, ANPD);
- Requisitos comerciais (ex: exigências contratuais de grandes clientes ou parceiros);
- Expectativas da alta gestão por "resolução rápida" principalmente após um incidente de segurança.

Esses vetores geram sobreposição de prioridades, frequentemente desconectadas da materialidade dos riscos, o que leva à inclusão de requisitos arbitrários ou à omissão de áreas críticas (FAIR INSTITUTE, 2022).

2.4. Lacuna entre linguagem técnica e executiva

Gerentes de projeto frequentemente se veem entre duas linguagens inconciliáveis: a tecnologia fala em vulnerabilidades, vetores, CVEs e firewalls, enquanto a alta gestão exige indicadores financeiros, Key Performance Indicators (KPI) e impacto no negócio.

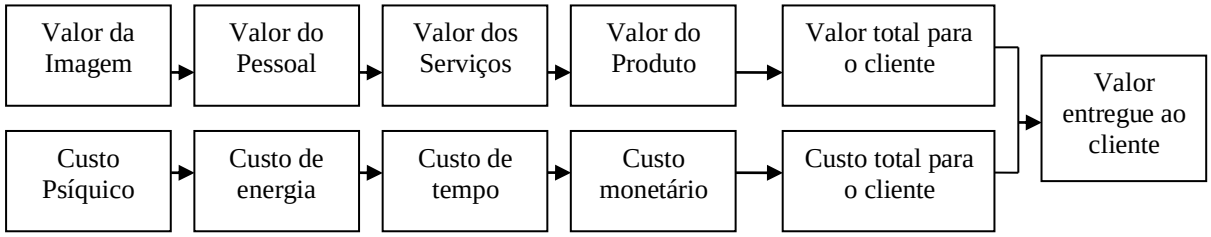
Na ausência de uma ponte entre esses dois domínios, o escopo tende a ser definido por "melhores práticas genéricas", frameworks genéricos ou por percepção subjetiva de risco. Isso cria um escopo desalinhado com os objetivos estratégicos e sem critérios objetivos para priorização (GOYAL, 2025).

2.5. O paradoxo do sucesso silencioso

Projetos de segurança bem-sucedidos são aqueles em que "nada acontece" — o ataque foi evitado, a violação não ocorreu, a multa não foi aplicada. No entanto, essa invisibilidade de

resultado dificulta a percepção de valor e reduz o apoio para escopos mais ambiciosos (GOYAL, 2025).

FIGURA 1 - Valor entregue ao cliente.



Fonte: Kotler (2000).

TABELA 1 - Flutuações dos níveis de produção ao longo da cadeia de suprimentos.

Mês	Fornecedor		Montadora		Distribuidor		Varejista		Mercado
	Produção	Est. Inic. Est. final	Produção	Est. Inic. Est. final	Compra	Est. Inic. Est. final	Compra	Est. Inic. Est. final	Demanda
1	100	100 100	100	100 100	100	100 100	100	100 100	100
2	20	100 60	60	100 80	80	100 90	90	100 95	95
3	180	60 120	120	80 100	100	90 95	95	95 95	95
4	60	120 90	90	100 95	95	95 95	95	95 95	95
5	100	90 95	95	95 95	95	95 95	95	95 95	95
6	95	95 95	95	95 95	95	95 95	95	95 95	95

Fonte: Slack et al. (1999).

3. METODOLOGIA

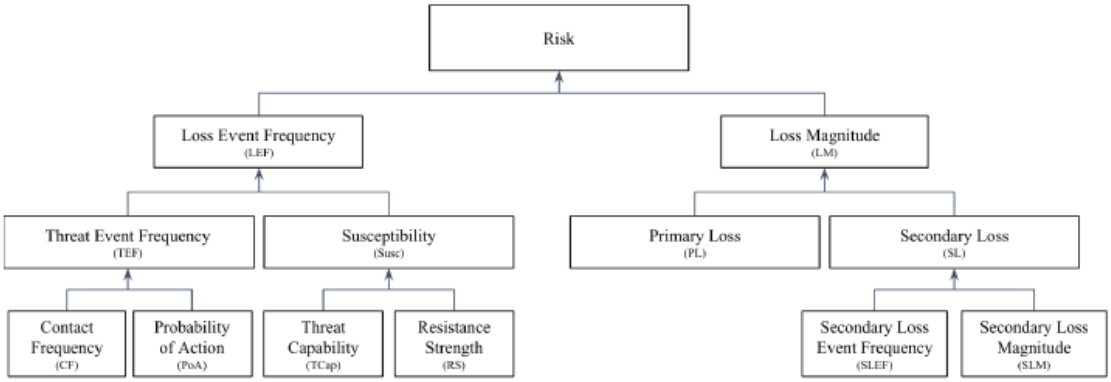
A crescente complexidade e sofisticação das ameaças cibernéticas exige que a definição de escopo em projetos de segurança se baseie em critérios objetivos de risco. Para gerentes de projeto acostumados a lidar com análise de riscos operacionais, financeiros ou estratégicos, o contexto cibernético apresenta desafios singulares: incerteza extrema, ausência de histórico estatístico confiável, dependência de variáveis técnicas e a necessidade de priorização baseada em impacto ao negócio, e não apenas em vulnerabilidades técnicas (GOYAL, 2025).

Neste cenário, o FAIR™ (Factor Analysis of Information Risk) se destaca como a principal metodologia quantitativa para análise e modelagem de riscos cibernéticos. Reconhecido internacionalmente por instituições como o NIST, ISACA e a Open Group, o FAIR™ fornece uma estrutura lógica e matemática para decompor, quantificar e comunicar

riscos com base em probabilidade e impacto em termos financeiros (NIST, 2022) (JONES, 2021) (FAIR INSTITUTE, 2022).

O Modelo FAIR descreve os fatores subjacentes que compõem o risco e podem ser quantificados para estimá-lo. Tradicionalmente, analistas de risco realizam essa quantificação com base em estimativas do assunto. Os analistas podem trabalhar em diferentes níveis do modelo, dependendo da disponibilidade de dados. Com dados históricos robustos, eles podem operar em um nível mais alto de abstração. Quando os dados são escassos, eles podem precisar trabalhar em níveis mais granulares dentro do modelo, conforme a figura 1 abaixo (GOYAL, 2025):

FIGURA 1 – NÍVEIS GRANULARES DO FAIR-MAM



Fonte: Goyal, 2025

Diferente de frameworks qualitativos baseados em “matrizes de calor” ou escalas subjetivas de severidade, o FAIR™ promove a convergência entre risco técnico e risco de negócio, traduzindo ameaças cibernéticas em potenciais perdas monetárias. Essa capacidade é crucial para fundamentar o escopo de projetos de segurança em prioridades verdadeiramente materiais (GOYAL, 2025).

3.1 FAIR-MAM™: Avaliação de Materialidade como Âncora para o Escopo

O FAIR-MAM™ (Materiality Assessment Model), lançado pelo FAIR Institute em colaboração com especialistas de mercado, é um modelo complementar que orienta a aplicação do FAIR™ com foco na avaliação da materialidade de cenários de risco. Seu objetivo é oferecer critérios objetivos e consistentes para determinar quais riscos cibernéticos são materialmente relevantes e devem ser endereçados por meio de projetos, planos de resposta ou estratégias de mitigação (FAIR INSTITUTE, 2022).

Para o contexto de gerenciamento de projetos, o FAIR-MAM™ atua como filtro estratégico para delimitar escopos excessivamente amplos ou mal priorizados, fornecendo um processo estruturado com as seguintes etapas principais:

a) Estrutura de Materialidade Baseada em Stakeholders

O FAIR-MAM™ parte da premissa de que a materialidade não é apenas técnica, mas relacional — ou seja, um risco só é material se tiver o potencial de afetar negativamente os interesses legítimos de partes relevantes, como (FAIR INSTITUTE, 2022):

- Investidores e conselhos;
- Reguladores e autoridades de supervisão;
- Clientes e usuários;
- Parceiros comerciais;
- Imprensa e opinião pública.

Com isso, o modelo propõe um framework para mapear fontes de preocupação material associadas a diferentes categorias de stakeholders, agrupadas em seis domínios principais (FAIR INSTITUTE, 2022):

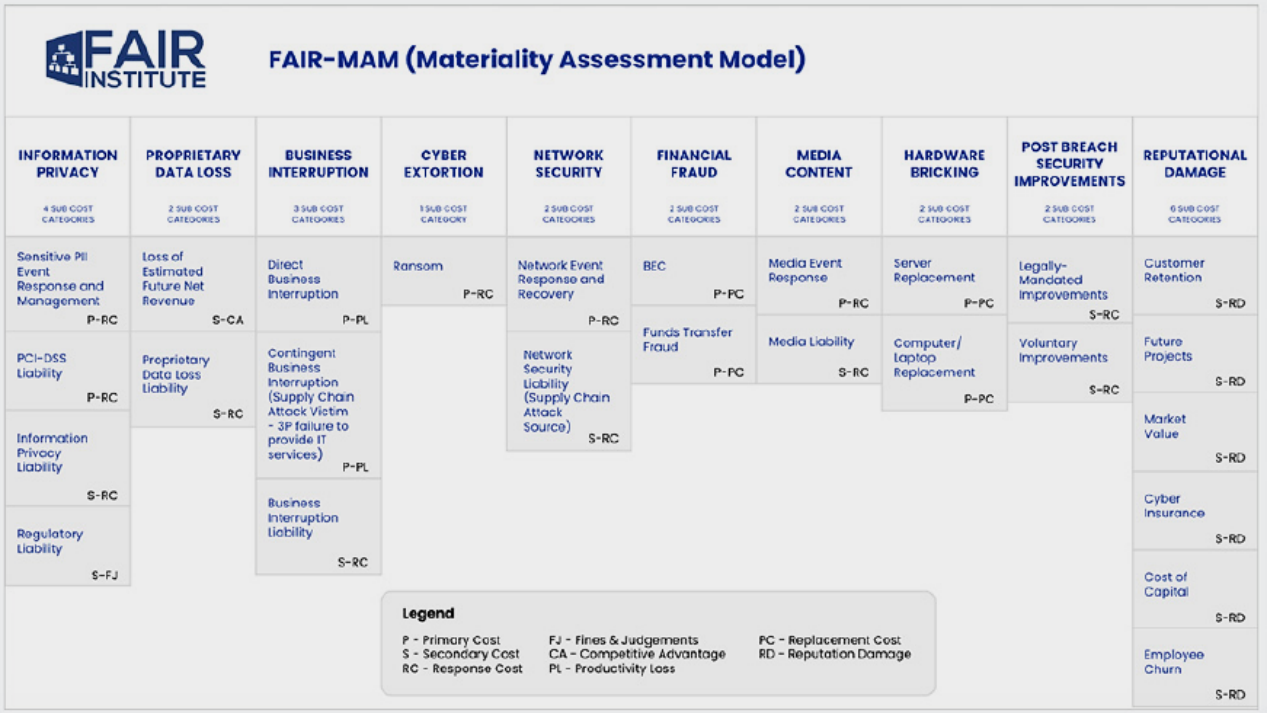
1. Viabilidade Financeira
2. Estabilidade Operacional
3. Legalidade e Compliance
4. Reputação
5. Expectativas da Liderança
6. Bem-Estar Humano e Social

b) Identificação de Triggers de Materialidade

Conforme apresentado no documento "An Introduction to the FAIR Materiality Assessment Model", o diagrama sintetiza de maneira estruturada e precisa o encadeamento lógico das etapas analíticas do modelo – mostrado na figura 2 (FAIR INSTITUTE, 2022):

- Início com um evento adverso hipotético, como um vazamento de dados, interrupção operacional ou ataque ransomware.
- Identificação dos vetores de impacto associados (ex: perda de receita, ações legais, queda de produtividade).
- Verificação de "gatilhos de materialidade", como violações contratuais, quebras de confidencialidade, ou impactos ao bem-estar social.
- Mapeamento das fontes de materialidade ativadas por esses gatilhos.
- Determinação da significância material com base em critérios como magnitude financeira, severidade normativa e repercussão reputacional.

FIGURA 2 - FAIR-MAM



Fonte: FAIR INSTITUTE, 2022

Os termos utilizados na figura 2 são explicados e traduzidos no quadro 1, abaixo.

Quadro 1 - Termos do FAIR-MAM

Sigla	Inglês (significado)	Português (tradução)	Explicação prática no contexto de risco cibernético e escopo de projeto
P	Primary Cost	Custo Primário	Impacto financeiro direto decorrente de um incidente (ex: perdas operacionais imediatas).
S	Secondary Cost	Custo Secundário	Custos indiretos ou subsequentes ao evento, como perda de clientes ou aumento no seguro.
RC	Response Cost	Custo de Resposta	Gastos com contenção e mitigação (ex: mobilização de equipes, horas extras, investigação forense).
FJ	Fines & Judgements	Multas e Julgamentos	Penalidades legais ou sanções regulatórias que podem surgir após o incidente.
CA	Competitive Advantage	Vantagem Competitiva	Potencial comprometimento da diferenciação da empresa no mercado devido ao incidente.
PL	Productivity Loss	Perda de Produtividade	Redução da eficiência operacional (ex: sistemas indisponíveis, desvio de recursos).
PC	Replacement Cost	Custo de Reposição	Investimentos necessários para restaurar ativos danificados ou comprometidos.
RD	Reputational Damage	Dano Reputacional	Prejuízos à imagem institucional, confiança de clientes e stakeholders.

Fonte: FAIR INSTITUTE, 2022

O FAIR-MAM permite que gerentes de projeto analisem e priorizem os impactos não apenas sob a ótica do risco, mas da materialidade financeira e estratégica. Cada um desses elementos (P, S, RC, etc.) contribui para uma compreensão aprofundada do que realmente constitui uma perda material para a organização, ajudando a justificar por que determinados controles ou ações devem estar dentro do escopo do projeto de segurança cibernética (FAIR INSTITUTE, 2022).

Esse fluxo permite aos gerentes de projeto responder com precisão à pergunta crítica: “Este risco cibernético é material o suficiente para justificar alocação de recursos em um projeto?”.

c) Contribuição para a Definição do Escopo

Ao aplicar o FAIR-MAM™ antes da definição de escopo, o gerente de projetos obtém (PMI, 2021):

- Priorização orientada por valor: foco em cenários que, de fato, impactam os objetivos organizacionais.
- Justificativa transparente de exclusões: permitindo documentar por que certos riscos foram deliberadamente deixados fora do escopo.
- Alinhamento com os critérios de governança da organização, ao adotar definições de materialidade consistentes com aquelas utilizadas em ESG, auditoria e compliance.

Em suma, o FAIR-MAM™ substitui a abordagem genérica do “vamos cobrir tudo que pudermos” por uma lógica clara: mitigar o que importa, com base em impacto e relevância para o negócio.

3. RESULTADOS

Em 2017, a Maersk, uma das maiores empresas de logística do mundo, foi vítima do ransomware NotPetya, que criptografou dados e paralisou operações globalmente (US CONGRESS, 2018). Esse incidente é emblemático e vamos utilizá-lo para demonstrar a aplicação da metodologia FAIR™ e seu anexo FAIR-MAM™ na avaliação e gestão de riscos cibernéticos.

4.1 Aplicação da Metodologia FAIR™

1. Identificação do Cenário de Risco:

• Ativo em Risco: Sistemas de TI críticos para operações logísticas.

• Ameaça: Ransomware NotPetya.

• Forma de Perda: Interrupção operacional e perda de dados.

2. Avaliação dos Fatores de Risco:

• Frequência de Evento de Perda (Loss Event Frequency - LEF): Considerando o histórico da Maersk e o ambiente de ameaças em 2017, a frequência estimada para ataques de ransomware era moderada.

• Magnitude da Perda (Loss Magnitude - LM):

Perda Primária: Custos diretos de recuperação de sistemas e dados.

Perda Secundária: Impactos financeiros devido à interrupção de serviços, penalidades contratuais e danos à reputação.

3. Cálculo do Risco:

• Risco Inerente: LEF x LM = Risco Financeiro Estimado.

• Risco Residual: Após implementação de controles e medidas de mitigação, recalcula-se o risco considerando a eficácia desses controles.

4.2 Aplicação da Metodologia FAIR-MAM™

Utilizando o modelo FAIR-MAM™, podemos detalhar as perdas materiais específicas associadas ao incidente, mostradas no quadro 2:

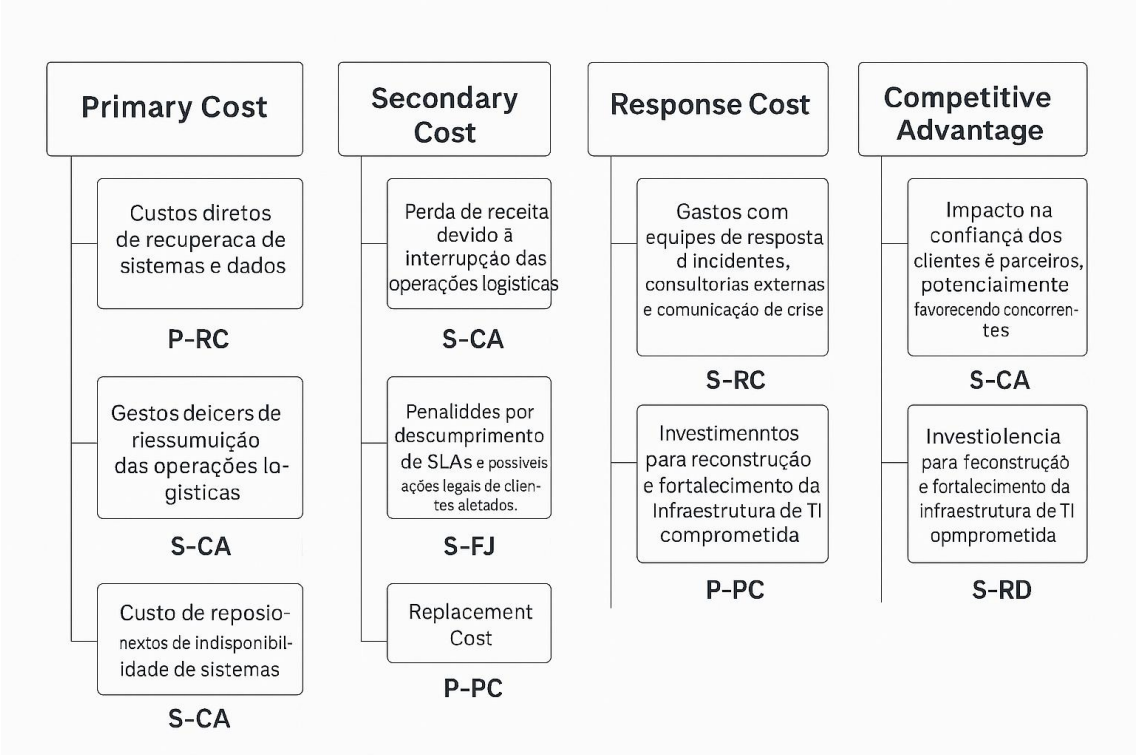
QUADRO 1 - Perdas materiais específicas associadas ao incidente

Sigla	Significado	Descrição no Contexto Maersk
P	Custo Primário	Custos diretos de recuperação de sistemas e dados.
S	Custo Secundário	Perda de receita devido à interrupção das operações logísticas.
RC	Custo de Resposta	Gastos com equipes de resposta a incidentes, consultorias externas e comunicação de crise.
FJ	Multas e Julgamentos	Penalidades por descumprimento de SLAs e possíveis ações legais de clientes afetados.
CA	Vantagem Competitiva	Impacto na confiança dos clientes e parceiros, potencialmente favorecendo concorrentes.
PL	Perda de Produtividade	Ineficiência operacional durante e após o incidente devido à indisponibilidade de sistemas.
PC	Custo de Reposição	Investimentos para reconstrução e fortalecimento da infraestrutura de TI comprometida.
RD	Dano Reputacional	Danos à imagem da Maersk no mercado, afetando futuras oportunidades de negócio.

Fonte: Os autores

Pode-se transformar o quadro no modelo encontrado no modelo FAIR-MAM™, conforme a figura 3 abaixo:

FIGURA 3 - Aplicação do método FAIR-MAM



Fonte: Os autores

4.3 Estrutura Analítica de Projeto (EAP)

Objetivo do Projeto: Fortalecer a resiliência cibernética da Maersk para prevenir e mitigar impactos de futuros ataques de ransomware.

1. Planejamento e Análise:

•1.1. Avaliação de Riscos: Aplicação das metodologias FAIR™ e FAIR-MAM™ para identificar e priorizar riscos.

•1.2. Definição de Escopo: Determinar os ativos críticos e processos a serem protegidos.

2. Implementação de Controles:

•2.1. Melhoria de Infraestrutura: Atualização de sistemas, aplicação de patches e reforço de medidas de segurança.

•2.2. Backup e Recuperação: Estabelecimento de rotinas robustas de backup e planos de recuperação de desastres.

•2.3. Treinamento e Conscientização: Programas de capacitação para funcionários sobre boas práticas de segurança.

3. Monitoramento e Resposta:

•3.1. Detecção de Ameaças: Implementação de sistemas de monitoramento contínuo e detecção de intrusões.

•3.2. Plano de Resposta a Incidentes: Desenvolvimento e testes regulares de planos de resposta a incidentes cibernéticos.

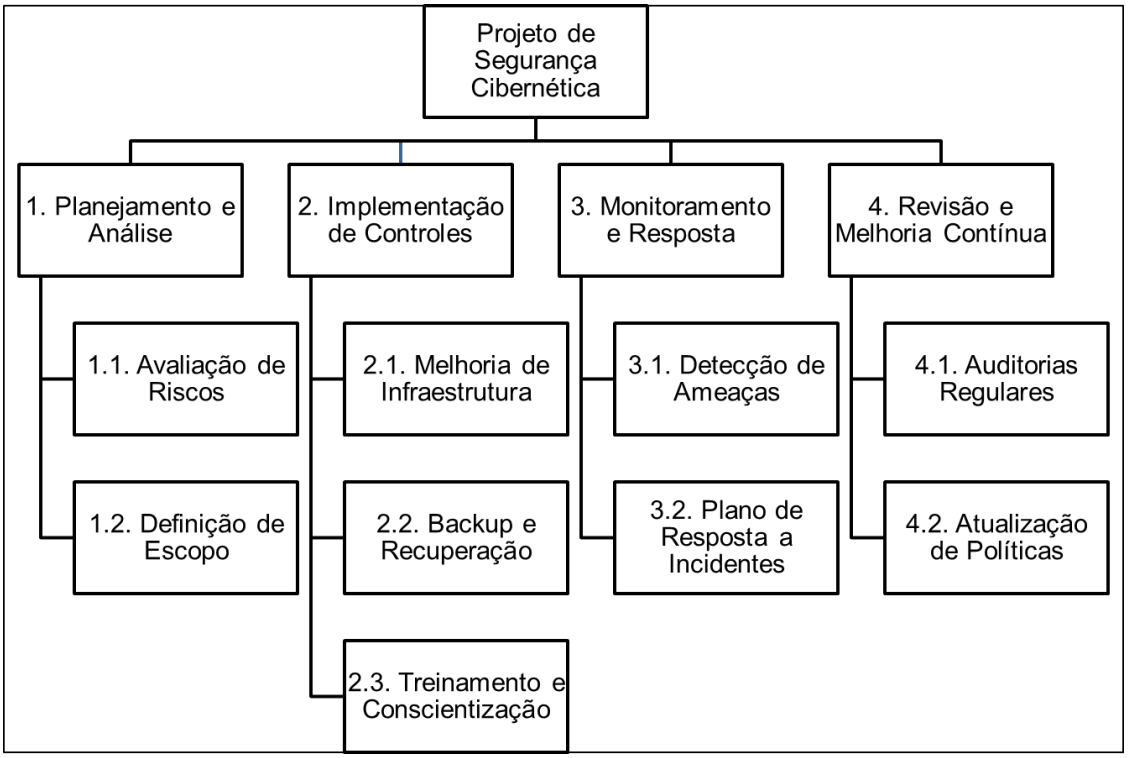
4. Revisão e Melhoria Contínua:

•4.1. Auditorias Regulares: Condução de auditorias periódicas para avaliar a eficácia dos controles implementados.

•4.2. Atualização de Políticas: Revisão e atualização contínua das políticas de segurança conforme novas ameaças emergem.

A figura 4 traz a EAP de forma gráfica.

FIGURA 4 - Estrutura Analítica de Projeto



Fonte: Os autores

Esta aplicação ilustra como as metodologias FAIR™ e FAIR-MAM™ podem ser aplicadas para avaliar e mitigar riscos cibernéticos de forma estruturada e quantitativa, fornecendo uma base sólida para a tomada de decisões informadas em projetos de segurança da informação.

3. CONCLUSÕES

A delimitação do escopo em projetos de segurança cibernética representa um desafio crítico na contemporaneidade, marcado pela complexidade dos ativos protegidos, pela

volatilidade do ambiente de ameaças e pela necessidade de justificar investimentos com base em critérios de valor para o negócio. Neste contexto, os métodos tradicionais, de natureza essencialmente qualitativa e subjetiva, mostram-se insuficientes para lidar com a exigência crescente por racionalidade decisória, transparência e alinhamento estratégico.

O presente artigo apresentou o método FAIR™ e sua extensão FAIR-MAM™ como alternativas metodológicas robustas e consistentes, capazes de superar essas limitações ao introduzirem uma abordagem quantitativa para análise de risco e avaliação de materialidade. A aplicação prática das metodologias ao caso Maersk evidenciou sua capacidade de traduzir ameaças técnicas em impactos financeiros concretos, permitindo que gestores e profissionais de projetos fundamentem decisões com maior precisão, previsibilidade e aderência às prioridades organizacionais.

Além de oferecer uma contribuição teórica relevante para o campo da gestão de riscos cibernéticos, o trabalho também propõe um avanço prático ao demonstrar como a definição de escopo pode ser orientada por critérios objetivos, integrando perspectivas técnicas e executivas. A utilização do FAIR-MAM™, em especial, reforça a importância de considerar a materialidade como vetor central na priorização de ações e alocação de recursos, promovendo maior eficiência e governança nos projetos de cibersegurança.

Conclui-se, portanto, que a adoção do FAIR™ e do FAIR-MAM™ representa não apenas uma inovação técnica, mas um novo paradigma para a concepção, planejamento e comunicação de projetos de segurança cibernética, especialmente em ambientes corporativos de alta criticidade e exposição a riscos digitais.

REFERÊNCIAS

BAREHAM, David. How NotPetya Cost Maersk Hundreds of Millions. Medium, 18 set. 2020. Disponível em: https://medium.com/swlh/how-notpetya-cost-maersk-hundreds-of-millions-1a5cbd3f3f4b. Acesso em: 06 abr. 2025.

FAIR INSTITUTE. FAIR-MAM: Materiality Assessment Model. [S.l.], 2022. Disponível em: https://www.fairinstitute.org/. Acesso em: 06 abr. 2025.

GARTNER. How to manage cybersecurity threats, not episodes. Stamford, CT, 2024. Disponível em: https://www.gartner.com/en/articles/how-to-manage-cybersecurity-threats-not-episodes. Acesso em: 06 abr. 2025.

GOYAL, Pankaj; SANNA, Nick; TUCKER, Todd. A FAIR framework for effective cyber risk management: leveraging the FAIR Model, FAIR-CAM, and FAIR-MAM to align

cybersecurity efforts with business priorities and regulatory compliance. [S.l.]: FAIR Institute, 2025. Disponível em: https://www.fairinstitute.org. Acesso em: 09 abr. 2025.

GREENBERG, Andy. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Wired, 22 ago. 2018. Disponível em: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ Acesso em: 06 abr. 2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 27005:2018 – Information technology – Security techniques – Information security risk management. Geneva, 2018.

JONES, Jack; COPELAND, Jack Freund. Measuring and managing information risk: a FAIR approach. 2. ed. Spokane Valley, WA: RiskLens Press, 2021.

MAERSK. Annual Report 2017. Copenhagen: A.P. Moller - Maersk, 2018. Disponível em: https://www.maersk.com/news/articles/2018/03/maersk-2017-annual-report. Acesso em: 06 abr. 2025.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Framework for improving critical infrastructure cybersecurity. Gaithersburg, MD, 2022. Disponível em: https://www.nist.gov/cyberframework. Acesso em: 06 abr. 2025.

PROJECT MANAGEMENT INSTITUTE. A guide to the Project Management Body of Knowledge (PMBOK® Guide). 7. ed. Newtown Square, PA: PMI, 2021.

UNITED STATES CONGRESS. Hearing on Cybersecurity: Lessons from the NotPetya Attack. Washington, D.C.: U.S. Senate Committee on Homeland Security, 2018. Disponível em: https://www.hsgac.senate.gov/hearings/cybersecurity-lessons-from-the-notpetya-attack/. Acesso em: 06 abr. 2025.

WORLD ECONOMIC FORUM. Global Cybersecurity Outlook 2024. Cologny/Geneva, 2024. Disponível em: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf. Acesso em: 06 abr. 2025.

WORLD ECONOMIC FORUM. Global Cybersecurity Outlook 2025. Cologny/Geneva, 2025. Disponível em: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf. Acesso em: 06 abr. 2025.

WORLD ECONOMIC FORUM. Stronger cybersecurity requires reducing complexity. Geneva, 2024. Disponível em: https://www.weforum.org/stories/2024/10/strong-cybersecurity-reduce-complexity-risk-cyber/. Acesso em: 06 abr. 2025.

WORLD ECONOMIC FORUM. Unpacking Cyber Resilience. Cologny/Geneva, 2024. Disponível em: https://www3.weforum.org/docs/WEF_Unpacking_Cyber_Resilience_2024.pdf. Acesso em: 06 abr. 2025.