Adversarial Risk Mapping & Assessment

Technical Guide

Document Type: Standard Technical

Document Version: 1.0

Date: 28/03/2025

Authors: Joas Antonio dos Santos

Table of Contents

Executive Summary

O avanço contínuo das ameaças cibernéticas, aliado à crescente complexidade dos ambientes tecnológicos e à rigorosidade das legislações regulatórias globais, impõe uma necessidade urgente de evolução nas metodologias de teste de segurança ofensiva. Embora práticas tradicionais como o Penetration Testing Execution Standard (PTES), o NIST SP800-115 e guias como o OWASP Testing Guide ofereçam diretrizes valiosas, observa-se que grande parte dos testes de intrusão ainda permanece limitada à identificação pontual de vulnerabilidades técnicas, sem estabelecer uma conexão robusta entre a exploração de falhas e o impacto real sobre o negócio, os ativos críticos e a conformidade regulatória.

A metodologia **A.R.M.A. - Adversarial Risk Mapping & Assessment** surge como uma resposta estruturada a essa lacuna, propondo um modelo técnico-operacional que transcende o simples checklist técnico e a execução de ferramentas automatizadas. Fundamentada na simulação comportamental de adversários reais, a A.R.M.A. proporciona uma abordagem de avaliação ofensiva orientada ao risco, capaz de mapear não apenas falhas individuais, mas toda a cadeia de exploração e seus desdobramentos sobre a continuidade operacional e a exposição legal da organização.

No contexto das ameaças modernas, ataques raramente ocorrem por meio de uma única vulnerabilidade isolada. O conceito de **Risk Chain Mapping**, central na A.R.M.A., permite demonstrar como falhas aparentemente triviais, quando encadeadas de forma estratégica, resultam em cenários de comprometimento total de ativos críticos. A metodologia conduz o executor do teste a explorar múltiplas superfícies de ataque — desde ambientes web, APIs, sistemas internos, cloud e infraestruturas legadas — sempre guiando suas decisões por um raciocínio adversarial e não apenas pelo reconhecimento superficial de vulnerabilidades.

Um dos diferenciais fundamentais da A.R.M.A. é a capacidade de quantificar tecnicamente cada etapa do processo ofensivo, atribuindo pesos e pontuações que refletem a dificuldade técnica, o nível de profundidade alcançado, o potencial de impacto financeiro e reputacional, bem como o risco regulatório gerado pela exploração de cada vetor. Tal quantificação culmina na geração de um **score de risco consolidado**, estruturado para ser compreendido tanto por equipes técnicas quanto por executivos e conselhos de administração, permitindo uma visão holística da exposição da organização.

A estrutura da metodologia prevê a **integração direta com frameworks de ameaça e compliance reconhecidos globalmente**, como o MITRE ATT&CK para o mapeamento de técnicas e táticas adversariais, o CWE Top 25 para categorização das fraquezas exploradas, e os principais referenciais regulatórios como PCI DSS, LGPD, DORA e GDPR. Cada vulnerabilidade validada e cada pivotagem bem-sucedida são automaticamente associadas aos requisitos de conformidade violados, proporcionando um relatório final que extrapola o simples inventário de falhas e apresenta um verdadeiro mapa de riscos, com impactos financeiros, técnicos e legais bem definidos.

Diferentemente das práticas convencionais, a A.R.M.A. não se encerra com a entrega de um relatório técnico. A metodologia estabelece um **ciclo contínuo de aprendizado e melhoria**, onde cada exercício de ataque conduz a uma análise das deficiências defensivas

identificadas, das falhas nos mecanismos de detecção e resposta e das oportunidades para fortalecimento da postura cibernética da organização. Este ciclo de realimentação permite que a organização amadureça seus processos de defesa proporcionalmente à complexidade dos ataques simulados, saindo da zona de conforto das verificações periódicas para adotar uma mentalidade de evolução contínua.

O relatório final gerado sob a ótica A.R.M.A. apresenta um **balanceamento entre profundidade técnica e visão executiva**, oferecendo desde detalhes específicos sobre as ferramentas utilizadas e os vetores explorados até análises de impacto sobre linhas de negócios, ativos críticos e cadeias de fornecimento. Esta característica torna a metodologia aplicável não apenas a avaliações técnicas de ambientes de TI, mas também a setores sensíveis como ICS/SCADA, ambientes cloud multi-região, operações financeiras críticas e infraestruturas estratégicas sob regulamentação específica.

Outro fator relevante da A.R.M.A. é a **adaptabilidade a cenários de Purple Teaming**, possibilitando a execução de operações ofensivas coordenadas com as equipes de defesa da organização. Essa sinergia viabiliza a validação em tempo real dos mecanismos de detecção, resposta e contenção, promovendo o fortalecimento prático das capacidades defensivas e proporcionando insights sobre o tempo de resposta a incidentes complexos.

Dentro do escopo de **risk management e compliance**, a metodologia permite o mapeamento direto de cada vulnerabilidade a artigos específicos de normativos legais, como o artigo 46 da LGPD referente à proteção de dados pessoais, ou os requisitos técnicos da PCI DSS 6.5 voltados à validação de segurança em aplicações. Com isso, A.R.M.A. habilita a organização a antecipar violações de compliance antes que estas se concretizem em sanções, multas ou incidentes públicos de grande repercussão.

A metodologia também se mostra altamente aplicável à realidade de **empresas de grande porte, instituições financeiras, entes governamentais e operadores de infraestrutura crítica**, cenários onde os impactos de uma exploração bem-sucedida transcendem o ambiente tecnológico e reverberam diretamente sobre o valor de mercado, a confiança do público e a estabilidade operacional.

No tocante à mensuração do risco, a A.R.M.A. propõe um **modelo quantitativo robusto**, capaz de atribuir pontuações diferenciadas a cada fase da exploração adversarial, levando em consideração a complexidade técnica da exploração, a profundidade do acesso conquistado, o impacto potencial no negócio e o grau de exposição frente às legislações aplicáveis. Essa abordagem oferece uma alternativa concreta e mais realista aos modelos tradicionais de severidade baseados apenas em CVSS, permitindo à organização entender quais cadeias de ataque realmente configuram riscos estratégicos e devem ser priorizadas.

Importante destacar que a A.R.M.A. foi concebida para **ser evolutiva e integrável a futuras tecnologias e práticas de cibersegurança**, incluindo o uso de inteligência artificial para tomada de decisões ofensivas, a integração em pipelines de DevSecOps e a adaptação a cenários emergentes como a segurança de dispositivos IoT e ambientes de computação quântica. O arcabouço metodológico proposto prevê, inclusive, a possibilidade de execução automatizada parcial, garantindo escalabilidade para operações contínuas e em larga escala.

Em termos de documentação e entrega, a A.R.M.A. estabelece o formato de **relatórios executivos e técnicos altamente visuais**, incluindo mapas de cadeia de risco, gráficos de pontuação de risco e representações visuais de mapeamento de compliance. Esses artefatos não apenas facilitam o entendimento técnico das descobertas como também permitem o consumo direto por comitês de risco, conselhos e órgãos reguladores, elevando o valor estratégico das entregas.

Em síntese, a A.R.M.A. se posiciona como uma evolução natural das metodologias de pentest tradicionais, propondo um **modelo ofensivo orientado ao risco, ao negócio e à conformidade**, capaz de fornecer às organizações uma visão clara, quantificável e acionável sobre sua real exposição cibernética. Ao adotar essa abordagem, as empresas não apenas elevam seu nível de maturidade em segurança ofensiva, mas também fortalecem sua capacidade de antecipação a cenários adversos complexos, tornando-se mais resilientes frente ao panorama de ameaças modernas.

Portanto, a A.R.M.A. se estabelece como uma **metodologia ofensiva robusta, estruturada e orientada ao risco**, capaz de preencher lacunas críticas das abordagens tradicionais de pentest. Ao conduzir o profissional de segurança por uma jornada adversarial realista, mapeando cadeias de risco, quantificando impactos e correlacionando diretamente cada exploração aos requisitos regulatórios aplicáveis, a metodologia proporciona um novo patamar de maturidade e valor para as operações de segurança cibernética.

Sua aplicabilidade transversal, aliada à capacidade de geração de relatórios ricos, visuais e orientados à decisão, torna a A.R.M.A. uma ferramenta essencial não apenas para equipes técnicas, mas também para os gestores de risco, compliance e executivos responsáveis pela governança corporativa e pela continuidade dos negócios.

Frente a um cenário global onde a **complexidade dos ataques aumenta proporcionalmente às exigências legais e regulatórias**, a adoção da A.R.M.A. representa um avanço significativo no fortalecimento da resiliência cibernética organizacional, alinhando as práticas de segurança ofensiva à real demanda do mercado por **inteligência de risco integrada, precisa e acionável**.

References and Applicable Documents

Este documento técnico da metodologia **A.R.M.A. - Adversarial Risk Mapping & Assessment** foi desenvolvido com base nas principais normas, padrões internacionais, frameworks de segurança cibernética e legislações de proteção de dados que regem as práticas de testes de intrusão, análise de risco e conformidade regulatória. A seguir, são relacionadas as referências consideradas essenciais para a compreensão, aplicação e validação da metodologia proposta.

Entre os principais documentos de referência técnica, destacam-se os guias e normas amplamente reconhecidos nas áreas de segurança da informação, engenharia reversa, modelagem de ameaças e simulação adversarial. O **Penetration Testing Execution Standard (PTES)**, por exemplo, fornece uma base estruturada para o planejamento e

execução de testes de penetração, cobrindo desde a coleta de informações até a modelagem de ameaças e o reporte de resultados. Complementarmente, o **NIST Special Publication 800-115** oferece diretrizes detalhadas para condução de avaliações técnicas de segurança, reforçando a necessidade de processos auditáveis e metodologias consistentes.

O framework **MITRE ATT&CK** é uma referência indispensável para o mapeamento das táticas, técnicas e procedimentos (TTPs) utilizados por agentes maliciosos em cenários reais, sendo incorporado na A.R.M.A. como base para o planejamento das ações ofensivas e o alinhamento com modelos de ameaça conhecidos. Ainda na esfera técnica, o **Common Weakness Enumeration (CWE Top 25)** fornece a classificação das principais fraquezas de software exploradas por atacantes, servindo como guia para a identificação e exploração de vulnerabilidades durante a execução da metodologia.

No que tange à conformidade regulatória, a A.R.M.A. estabelece correlação direta com normas e legislações de ampla aplicabilidade internacional. A **Payment Card Industry Data Security Standard (PCI DSS v4.0)** orienta os requisitos de segurança para ambientes que processam, armazenam ou transmitem dados de cartões de pagamento, sendo essencial para o mapeamento de falhas que representem risco de não conformidade financeira. Por sua vez, legislações de privacidade como a **Lei Geral de Proteção de Dados Pessoais (LGPD - Brasil)**, o **Regulamento Geral sobre a Proteção de Dados (GDPR - Europa)** e a **Digital Operational Resilience Act (DORA - União Europeia)** fundamentam a avaliação dos riscos regulatórios e de exposição legal decorrentes das vulnerabilidades exploradas.

Além dos documentos normativos, a A.R.M.A. reconhece como referência o conjunto de boas práticas publicadas por organizações como a **OWASP Foundation**, cujo Testing Guide v4 é amplamente utilizado na validação de aplicações web e APIs, fornecendo parâmetros técnicos de avaliação da segurança de sistemas expostos à internet.

Os documentos abaixo listados compõem, portanto, o arcabouço técnico e regulatório que fundamenta a construção da metodologia A.R.M.A.:

- **PTES - Penetration Testing Execution Standard**
- **NIST SP 800-115 - Technical Guide to Information Security Testing and Assessment**
- **MITRE ATT&CK Framework**
- **CWE Top 25 Most Dangerous Software Weaknesses**
- **OWASP Web Security Testing Guide (WSTG v4)**
- **PCI DSS v4.0 - Payment Card Industry Data Security Standard**
- **LGPD - Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018 - Brasil)**

- **GDPR - General Data Protection Regulation (Regulation EU 2016/679)**
- **DORA - Digital Operational Resilience Act (EU Regulation 2022/2554)**
- **ISO/IEC 27001:2022 - Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems**

Adicionalmente, a metodologia permanece aberta à integração com novas regulamentações emergentes e normativas setoriais específicas, garantindo sua evolução contínua e aderência aos desafios regulatórios de diferentes setores e jurisdições.

Introduction

O cenário global de segurança cibernética tem testemunhado um crescimento exponencial na sofisticação e na frequência dos ataques direcionados a infraestruturas críticas, sistemas financeiros, ambientes corporativos e dados sensíveis de cidadãos e organizações. A evolução constante das técnicas de ataque, impulsionada por grupos de ameaças avançadas (APTs), cibercriminosos e atores estatais, demanda das organizações uma postura proativa e metodologicamente sólida para a identificação, mapeamento e mitigação de riscos cibernéticos.

Diante desse contexto, as metodologias tradicionais de **testes de penetração (pentesting)**, ainda majoritariamente ancoradas em modelos lineares e baseadas na simples verificação de vulnerabilidades técnicas, mostram-se insuficientes para refletir a complexidade dos cenários adversariais modernos. Grande parte dos testes conduzidos no mercado permanece restrita à identificação de falhas isoladas, sem uma visão ampla da cadeia de exploração e, principalmente, sem a devida conexão entre os vetores técnicos explorados e o impacto efetivo sobre o negócio, a continuidade operacional e o atendimento às legislações e normativas vigentes.

Além disso, a crescente adoção de arquiteturas distribuídas, ambientes híbridos, serviços em nuvem, e a interconexão de sistemas legados com aplicações modernas ampliam significativamente a superfície de ataque das organizações, tornando obsoletas as abordagens ofensivas que desconsideram a visão de risco encadeado e de impacto estratégico. Neste contexto, não basta mais ao profissional de segurança identificar vulnerabilidades pontuais: é imprescindível que o processo de avaliação ofensiva seja capaz de simular o raciocínio e as tomadas de decisão de um atacante real, percorrendo cadeias complexas de exploração até alcançar ativos de alto valor estratégico ou provocar rupturas operacionais significativas.

Outro fator determinante é a intensificação dos requisitos regulatórios relacionados à privacidade de dados, resiliência operacional e proteção de infraestruturas críticas. Normas como a **PCI DSS v4.0**, **LGPD**, **GDPR** e **DORA** impõem obrigações explícitas às organizações no que se refere à identificação e tratamento de vulnerabilidades que possam comprometer a integridade, a confidencialidade e a disponibilidade de dados e sistemas. Nesse cenário, metodologias limitadas à geração de laudos técnicos desconectados da realidade de negócios e do risco regulatório perdem relevância e efetividade.

Diante dessas demandas, surge a necessidade de uma metodologia que alinhe a execução ofensiva com a lógica de risco, a visão de impacto estratégico e a aderência regulatória. É neste ponto que se insere a proposta da **A.R.M.A. - Adversarial Risk Mapping & Assessment**: um modelo metodológico que transforma o pentest tradicional em uma operação ofensiva orientada a objetivos adversariais reais, com foco em demonstrar o impacto de negócios, a materialização de riscos e a violação de obrigações regulatórias.

A metodologia A.R.M.A. foi concebida para conduzir o executor do teste por um fluxo estruturado de ações ofensivas, desde a descoberta de contexto, passando pelo planejamento tático e pela execução iterativa das explorações, até a consolidação das descobertas em um mapa de risco encadeado e um relatório robusto de impacto. Essa abordagem não apenas amplia a profundidade técnica da avaliação, mas também garante que cada descoberta seja contextualizada frente aos ativos de negócio, aos processos críticos e às exigências legais aplicáveis.

Diferentemente das abordagens convencionais, a A.R.M.A. incorpora o conceito de **Risk Chain Mapping**, que permite demonstrar como múltiplas vulnerabilidades, quando exploradas de forma encadeada, podem resultar em cenários de comprometimento total da infraestrutura ou em violações severas de privacidade e conformidade. Ao invés de simplesmente reportar vulnerabilidades técnicas, a metodologia expõe as potenciais consequências de sua exploração em um fluxo lógico e visual, oferecendo subsídios claros para a tomada de decisão por parte da alta gestão.

Adicionalmente, a metodologia propõe um modelo de **pontuação de risco (Risk Scoring)** robusto e multidimensional, capaz de atribuir pesos às descobertas com base na complexidade técnica, na profundidade do acesso obtido, no potencial de impacto financeiro e reputacional e na gravidade da exposição regulatória. Esse modelo promove uma priorização objetiva das vulnerabilidades e das cadeias de ataque, permitindo à organização concentrar esforços de remediação nos pontos de maior risco estratégico.

Outro diferencial importante da A.R.M.A. é sua capacidade de gerar relatórios integrados, que não se restringem a aspectos técnicos, mas oferecem uma visão executiva, com destaque para o mapeamento das violações aos principais normativos e legislações aplicáveis. Tal característica posiciona a metodologia como uma ferramenta não apenas para os times de segurança da informação, mas também para áreas de compliance, jurídico, governança e gestão de riscos corporativos.

A A.R.M.A. também foi projetada para ser compatível com práticas modernas de **Purple Teaming** e **Continuous Security Validation**, integrando-se a fluxos de DevSecOps e a processos contínuos de validação da resiliência cibernética. A metodologia prevê, inclusive, a possibilidade de automação parcial dos ciclos de ataque e de geração de relatórios, ampliando sua aplicabilidade em ambientes dinâmicos e de larga escala.

A proposta da A.R.M.A. não é substituir padrões consagrados como o PTES ou o NIST SP 800-115, mas sim evoluir o conceito de testes ofensivos, incorporando à prática de pentest uma visão holística e estratégica da segurança cibernética. Ao adotar essa metodologia, as organizações passam a ter uma ferramenta eficaz para medir sua real exposição a ataques avançados, compreender os impactos potenciais sobre o negócio e priorizar investimentos e

ações corretivas de forma alinhada à sua matriz de risco e aos requisitos regulatórios de sua indústria.

Além das questões técnicas e da crescente complexidade dos ambientes tecnológicos, o cenário atual impõe uma pressão adicional sobre as organizações no que se refere à **demonstração de due diligence** em segurança da informação. Regulatórios e normativas globais exigem que as organizações não apenas implementem controles técnicos, mas também sejam capazes de **evidenciar o conhecimento de seus riscos cibernéticos** e as ações concretas tomadas para mitigá-los. Dentro desse contexto, a **simulação de adversários reais** e a modelagem de cadeias de risco tornam-se elementos indispensáveis para garantir uma visão holística sobre a real exposição da organização.

A **A.R.M.A.** nasce justamente para suprir esta necessidade: oferecer uma metodologia estruturada que vá além da detecção de vulnerabilidades, promovendo uma **leitura estratégica do ambiente sob a ótica adversarial**. Ao adotar essa abordagem, a organização consegue não apenas verificar falhas, mas também entender o que um atacante real poderia fazer a partir daquelas falhas, quais cadeias de exploração poderiam ser formadas, e, sobretudo, quais impactos técnicos, financeiros e regulatórios poderiam ser concretizados.

O **mapeamento da cadeia de risco (Risk Chain Mapping)** proposto pela A.R.M.A. é um diferencial que permite às áreas de gestão de risco e à alta direção visualizarem, de forma clara, o encadeamento de vulnerabilidades exploráveis e como cada uma delas contribui para o aumento da exposição organizacional. Essa visão permite, por exemplo, entender como um erro de configuração aparentemente trivial em um ativo de baixa criticidade pode, quando encadeado com outras falhas, resultar no comprometimento de sistemas core de negócio ou na exposição de dados sensíveis sob regulação.

No contexto atual, em que **vazamentos de dados** e incidentes cibernéticos tornaram-se recorrentes, a capacidade de demonstrar conhecimento sobre as próprias fragilidades e o tratamento efetivo dessas falhas torna-se fator diferencial em processos de auditoria, due diligence e em negociações de mercado, incluindo processos de M&A (Fusões e Aquisições). A A.R.M.A. permite, neste sentido, que a organização eleve sua **maturidade em cibersegurança**, saindo da visão reativa e pontual para uma abordagem **estratégica, contínua e orientada a riscos reais**.

Outro ponto crucial abordado pela metodologia é a **integração entre os aspectos ofensivos e o cumprimento regulatório**. A A.R.M.A. mapeia cada vulnerabilidade validada e cada exploração bem-sucedida a artigos específicos das principais legislações e normativos do setor. Isso significa que, ao final de um ciclo de execução da metodologia, a organização terá não apenas um inventário técnico de vulnerabilidades, mas um relatório completo apontando **quais dispositivos da PCI DSS foram violados, quais artigos da LGPD foram expostos, e quais requisitos do DORA ou GDPR foram diretamente impactados** pelas fragilidades exploradas.

Em tempos em que sanções regulatórias podem atingir cifras milionárias, e em que o não cumprimento de normativos como o DORA implica risco direto à continuidade de operações financeiras e críticas, essa capacidade de **vincular falhas técnicas a impactos regulatórios diretos** é um dos grandes diferenciais da A.R.M.A. A metodologia torna o

laudo técnico um documento estratégico, **utilizável não apenas por times de segurança**, mas também por **áreas de compliance, jurídico, auditoria e gestão de risco corporativo**.

Importante destacar ainda que o modelo proposto não é restrito a um setor específico. A.R.M.A. foi desenhada para operar **em qualquer vertical de mercado**, seja em instituições financeiras altamente reguladas, seja em ambientes industriais e de OT, onde o risco físico se sobrepõe ao risco digital, passando por operadoras de telecomunicação, setores de energia, saúde, governo, ou mesmo startups e ambientes de inovação.

A flexibilidade do framework permite sua aplicação **desde simulações adversariais controladas**, como exercícios de Red Team e Purple Team, até avaliações mais amplas, em processos de Continuous Security Validation, integrando-se a ferramentas de CI/CD e pipelines de DevSecOps. Isso habilita o uso da A.R.M.A. **tanto de forma periódica quanto contínua**, permitindo à organização validar sua resiliência de forma dinâmica, sempre considerando as ameaças mais recentes e as mudanças constantes na infraestrutura tecnológica.

Vale ressaltar que a A.R.M.A. também propõe **um modelo de pontuação e priorização de riscos distinto dos tradicionais modelos baseados apenas em CVSS**. Enquanto o CVSS considera essencialmente aspectos técnicos, a A.R.M.A. pondera, além da dificuldade de exploração, o **nível de acesso conquistado, a relevância dos ativos impactados, o potencial de dano financeiro e reputacional, e a exposição frente aos principais normativos aplicáveis**. Esse modelo de scoring multidimensional permite uma visão realista do risco, facilitando a priorização de ações corretivas com base não apenas no aspecto técnico, mas também na materialidade do impacto.

Outro elemento inovador da metodologia é a **previsão de ciclos de aprendizado e melhoria contínua**. Cada execução da A.R.M.A. deve gerar não apenas o mapeamento das falhas exploradas, mas também uma reflexão sobre as deficiências dos mecanismos de defesa, a capacidade de detecção e resposta, e os pontos cegos da arquitetura de segurança. Esses ciclos de feedback garantem que a metodologia contribua diretamente para o fortalecimento da defesa, transformando cada ofensiva em uma oportunidade de crescimento organizacional.

Por fim, a A.R.M.A. propõe **um padrão de entrega de resultados estruturado**, capaz de atender simultaneamente aos públicos técnicos e executivos. Os relatórios produzidos contemplam **detalhamento técnico das explorações**, **visualizações gráficas das cadeias de risco**, **painéis de pontuação e priorização**, e **mapas de exposição regulatória**, oferecendo uma visão 360° da avaliação realizada. Esta riqueza de informações torna os laudos gerados documentos de alto valor agregado, aptos a serem utilizados como base para planejamento estratégico de segurança, como insumos para auditorias externas e até mesmo como peças de defesa em eventuais processos legais ou investigações regulatórias.

Em suma, a **A.R.M.A. se apresenta como uma evolução natural e necessária das metodologias de testes de intrusão**, alinhando a prática ofensiva ao risco de negócio, à conformidade regulatória e à inteligência estratégica. Ao adotar esta metodologia, a organização dá um passo importante rumo à **maturidade plena em cibersegurança**,

ganhando capacidade real de compreender, mapear e reduzir sua superfície de exposição, não apenas tecnicamente, mas de forma integrada aos seus objetivos de negócio e às obrigações legais e regulatórias às quais está submetida.

Methodology Overview (A.R.M.A. Phases):

A Metodologia A.R.M.A. - Adversarial Risk Mapping & Assessment foi estruturada em seis fases interdependentes, cada uma delas concebida para garantir uma execução ofensiva com foco em adversarialidade real, avaliação do impacto estratégico e mapeamento preciso do risco organizacional. Estas fases permitem que o ciclo de testes de intrusão deixe de ser uma mera verificação pontual de falhas técnicas e passe a constituir um processo robusto de simulação de ameaças e materialização de riscos, com forte aderência às demandas de governança, risco e compliance.

Cada fase da A.R.M.A. possui objetivos claros, entradas bem definidas e entregáveis que alimentam as etapas subsequentes. A seguir, detalha-se cada uma dessas fases:

Context Discovery

A fase de Context Discovery marca o início da operação ofensiva sob a ótica A.R.M.A., distinguindo-se das abordagens convencionais por seu foco na coleta e na interpretação do contexto de negócios, e não apenas na identificação técnica de ativos expostos. Aqui, o objetivo não é meramente mapear superfícies de ataque, mas compreender a organização-alvo como um ecossistema operacional, regulatório e estratégico.

Essa fase contempla a identificação dos ativos críticos de negócio, mapeamento de fluxos de dados sensíveis, entendimento das dependências de terceiros, além da caracterização das obrigações legais e regulatórias que incidem sobre cada processo de negócio. Essa leitura inicial permite que o pentester assuma um papel mais próximo de um adversário real, direcionando suas ações não pela oportunidade técnica mais óbvia, mas pelos alvos de maior valor estratégico.

Dentro do escopo técnico, realiza-se também o mapeamento tradicional de ativos, endereços IP, domínios, subdomínios, APIs e quaisquer interfaces de comunicação expostas. Contudo, a análise vai além, incorporando variáveis como perfil de usuários, jornadas digitais, interações de sistemas e possíveis pontos de pivotagem.

Ao final da fase, a equipe ofensiva deverá possuir uma cartografia completa do ambiente, incluindo ativos-alvo priorizados, mapa de fluxos de dados e lista de normativos e legislações aplicáveis, configurando um plano tático para a fase subsequente.

Adversarial Planning

Com o contexto devidamente mapeado, a metodologia segue para a fase de **Adversarial Planning**, onde se estabelece a estratégia ofensiva a ser adotada. Nesta etapa, a equipe atua como um agente de ameaça, tomando decisões racionais sobre quais caminhos seguir, que técnicas aplicar e quais vetores possuem maior potencial de gerar um efeito cascata sobre o ambiente-alvo.

O planejamento não se limita à escolha de ferramentas, mas abrange a definição de **cenários de ataque realistas**, simulando desde o comportamento de grupos de cibercrime organizado até **ameaças persistentes avançadas (APTs)** ou **insiders maliciosos**. Utiliza-se o **MITRE ATT&CK** como framework de referência para seleção das táticas e técnicas mais aderentes ao ambiente-alvo e aos objetivos adversariais definidos.

Cada cenário é descrito com:

- Objetivo adversarial;
- Vetores de entrada estimados;
- Técnicas de exploração previstas;
- Possíveis pivotagens;
- Caminhos esperados de escalonamento.

Essa fase também define o **limiar de impacto desejado**, ou seja, até onde a simulação poderá avançar — seja até a exposição de dados sensíveis, o comprometimento de sistemas de missão crítica ou a violação de um normativo específico.

O planejamento adversarial é documentado, formando a base do que será executado nas iterações ofensivas seguintes.

Offensive Iterative Loops

Diferente dos modelos tradicionais, que executam o pentest de forma linear, a A.R.M.A. propõe a execução ofensiva por meio de **ciclos iterativos e adaptativos**. A fase de **Offensive Iterative Loops** é o núcleo da operação, onde cada ação ofensiva alimenta a inteligência para o ciclo seguinte, permitindo correções de rota e exploração de novas oportunidades de ataque.

Cada iteração consiste em:

- Execução de uma técnica previamente planejada;
- Validação dos resultados e impactos obtidos;
- Reavaliação do cenário;

- Planejamento da próxima ação com base nas descobertas.

Essa abordagem simula com fidelidade o comportamento de um adversário real, que ajusta suas estratégias com base na resposta do ambiente. Por exemplo, a exploração de uma SQL Injection pode revelar credenciais que, por sua vez, habilitam um novo ciclo ofensivo com foco em movimento lateral e escalonamento de privilégios.

O loop só é finalizado quando se atinge o impacto definido ou esgotam-se os vetores de exploração. Toda movimentação adversarial é registrada, compondo o material que será utilizado no mapeamento da cadeia de risco.

Esse ciclo iterativo garante não apenas maior profundidade técnica, mas também o **encadeamento de vulnerabilidades**, elemento essencial para a próxima fase.

Risk Chain Mapping

O **Risk Chain Mapping** é a espinha dorsal da A.R.M.A., representando o momento em que as ações ofensivas são organizadas logicamente para evidenciar a formação de uma cadeia de exploração. Aqui, não se analisam vulnerabilidades isoladamente, mas sim **como cada falha técnica se conecta a outra**, formando um caminho crítico até o ativo ou o impacto final.

O grande diferencial desta fase é a **capacidade de visualizar e documentar o efeito cascata** de vulnerabilidades menores que, isoladamente, não seriam consideradas críticas, mas que, encadeadas, podem levar a um cenário de colapso organizacional ou de grave violação legal.

Essa fase gera como entregável um **diagrama da cadeia de risco**, evidenciando:

- Pontos de entrada;
- Técnicas utilizadas;
- Pivotagens;
- Escalonamentos de privilégio;
- Impactos alcançados;
- Normativos potencialmente violados.

O Risk Chain Mapping é um artefato visual poderoso, permitindo que executivos e áreas técnicas compreendam, de forma gráfica e objetiva, a jornada adversarial e os pontos críticos de risco.

Impact & Compliance Report

Com a cadeia de risco mapeada, a A.R.M.A. avança para a consolidação dos resultados na fase de **Impact & Compliance Report**. Este não é um mero relatório técnico, mas um **documento multidimensional**, estruturado para atender às necessidades de diferentes públicos dentro da organização.

O relatório é dividido em três grandes eixos:

1. **Técnico**: Detalhamento das técnicas, ferramentas, explorações bem-sucedidas e provas de conceito.

2. **Negócios**: Análise dos impactos sobre processos críticos, estimativa de perdas financeiras, interrupções e danos reputacionais.

3. **Regulatório**: Mapeamento das falhas exploradas frente às exigências de normativos como PCI DSS, LGPD, GDPR e DORA.

Este modelo de entrega possibilita que o mesmo relatório seja utilizado simultaneamente por:

- Times técnicos para correção;

- Executivos para tomada de decisão;

- Jurídico e compliance como material de evidência.

A **pontuação de risco (Risk Score)** calculada durante o ciclo ofensivo também é apresentada nesta etapa, permitindo a priorização das correções e investimentos.

Adversary-Driven Learning

Encerrando o ciclo metodológico, a A.R.M.A. estabelece a fase de **Adversary-Driven Learning**, responsável por garantir que cada ofensiva gere aprendizado organizacional e fortalecimento da postura defensiva.

Esta etapa consiste em:

- Revisão dos pontos de falha na detecção e resposta;

- Análise das oportunidades de melhoria na arquitetura defensiva;

- Definição de ações corretivas e estratégicas.

O objetivo é **transformar cada ataque em um ciclo de evolução**, refinando continuamente os controles de segurança e a capacidade de resiliência organizacional.

Além disso, o aprendizado é utilizado para retroalimentar a própria A.R.M.A., garantindo que os próximos ciclos sejam mais eficazes, explorando novos vetores e técnicas adversariais ainda mais complexas.

Detalhamento Operacional — Inputs, Outputs, Toolsets e Exemplos por Fase

1. Context Discovery

Inputs:

- Escopo definido (domínios, ranges de IP, ativos conhecidos);
- Briefing executivo e matriz de criticidade dos ativos;
- Mapas de processos críticos e fluxos de dados (quando fornecidos);
- Requisitos de compliance aplicáveis.

Outputs:

- Inventário técnico de ativos expostos (hosts, aplicações, APIs);
- Identificação de ativos de alto valor (HVTs);
- Lista de possíveis vetores de ataque;
- Mapeamento preliminar de requisitos regulatórios aplicáveis.

Toolsets:

- OSINT Framework, Recon-ng, Shodan, Censys, SpiderFoot;
- Ferramentas DNS (Sublist3r, DNSenum);
- Cloud Asset Discovery (AWS Prowler, ScoutSuite).

Exemplos:

- Mapeamento de uma API não documentada exposta no subdomínio `api.internal.company.com`, permitindo futuras explorações;
- Identificação de servidor legado com sistema operacional obsoleto.

2. Adversarial Planning

Inputs:

- Inventário técnico e de ativos críticos (da fase anterior);
- Frameworks como MITRE ATT&CK, CWE Top 25;
- Objetivos de negócios e requisitos de compliance.

Outputs:

- Cenários de ataque modelados (ex.: acesso inicial, persistência, movimento lateral);
- Lista de técnicas adversariais a empregar;
- Definição das regras de engajamento e limiares de impacto.

Toolsets:

- ATT&CK Navigator, Threat Modeling tools (Microsoft SDL);
- Desenho de cenários adversariais no Miro, Lucidchart ou Threat Dragon.

Exemplos:

- Definição de um cenário focado em vazamento de dados financeiros por meio de exploração de injeção em API;
- Planejamento da exploração de SAML Injection para sequestro de sessão.

3. Offensive Iterative Loops

Inputs:

- Cenários adversariais modelados;
- Lista de técnicas selecionadas.

Outputs:

- Vulnerabilidades validadas e exploradas;

- Credenciais, tokens e artefatos coletados;
- Novos vetores descobertos para exploração.

Toolsets:

- Burp Suite Pro, SQLmap, Nmap, BloodHound;
- Metasploit Framework, Cobalt Strike, Empire;
- Ferramentas customizadas para exploits.

Exemplos:

- Exploração de SQLi resultando na extração de hashes de senhas;
- Escalonamento de privilégios após coleta de token OAuth em API.

4. Risk Chain Mapping

Inputs:

- Logs e artefatos das iterações ofensivas;
- TTPs utilizadas e resultados obtidos.

Outputs:

- Diagrama visual da cadeia de risco (Risk Flow);
- Identificação das pivotagens e escalonamentos;
- Priorização dos riscos encadeados.

Toolsets:

- Mindmaps (XMind), Draw.io, Maltego;
- Geradores de gráficos (Chart.js, Graphviz).

Exemplos:

- Cadeia mapeada: **Exposição de Docker API → Acesso a container → Escalonamento → Comprometimento de banco de dados financeiro**;
- Mapeamento visual das dependências entre vulnerabilidades.

5. Impact & Compliance Report

Inputs:

- Risk Chain Mapping completo;
- Matriz de impacto e severidade calculada.

Outputs:

- Relatório executivo e técnico;
- Painel de priorização de riscos;
- Mapeamento das violações de compliance.

Toolsets:

- Geradores de PDF (LaTeX, Pandoc, html2pdf.js);
- Templates de relatórios executivos (Word, Markdown).

Exemplos:

- Relatório com impacto financeiro estimado de 1,5 milhão por exploração da falha X;
- Mapeamento de SQL Injection diretamente violando PCI DSS 6.5.1 e LGPD Art.46.

6. Adversary-Driven Learning

Inputs:

- Relatório final consolidado;
- Registro das técnicas que bypassaram defesas.

Outputs:

- Lista de melhorias defensivas recomendadas;
- Relatório de gaps de detecção e resposta;
- Recomendações de novos cenários para o próximo ciclo.

Toolsets:

- SIEM (Splunk, ELK, QRadar);
- Purple Team platforms (MITRE Caldera, Prelude Operator).

Exemplos:

- Identificação de falha na monitoração de logs de API, sugerindo integração de WAF;
- Recomendação de incluir CTI (Cyber Threat Intelligence) nas próximas execuções.

O ciclo metodológico da **A.R.M.A.** se consolida como uma abordagem robusta, modular e escalável, estruturando cada fase com entradas claras, entregáveis tangíveis e o suporte das melhores ferramentas técnicas disponíveis no mercado. Essa granularidade operacional não só garante a repetibilidade e auditabilidade do processo, mas também posiciona a metodologia como um **padrão de referência aplicável a ambientes complexos e altamente regulados**.

Cada fase contribui diretamente para a materialização dos objetivos estratégicos da metodologia: **mapear o risco de forma encadeada**, **simular o comportamento real de adversários** e **produzir inteligência de segurança acionável para todos os níveis da organização**. A força da A.R.M.A. está na sua capacidade de evoluir o teste de intrusão clássico para um verdadeiro exercício de avaliação de riscos cibernéticos, **integrando aspectos técnicos, de negócios e de conformidade em um único fluxo de trabalho estruturado**.

Com o ciclo completo — da descoberta contextual até o aprendizado organizacional —, a A.R.M.A. garante não apenas o mapeamento das fragilidades exploráveis, mas também o fortalecimento contínuo da postura de defesa, transformando cada execução em um passo concreto rumo à **maturidade cibernética e à resiliência organizacional**.

Scoring System Design Quantitative model covering:

O sistema de pontuação da metodologia **A.R.M.A.** representa um dos seus pilares fundamentais, garantindo que cada cadeia de exploração não seja avaliada apenas sob a ótica da severidade técnica isolada, mas sob uma perspectiva holística que incorpora variáveis de impacto financeiro, regulatório e operacional.

Diferente de modelos tradicionais como o **CVSS**, que focam exclusivamente na severidade técnica das vulnerabilidades, o **Risk Scoring Model da A.R.M.A.** foi projetado para refletir o real risco estratégico enfrentado pela organização, ponderando cinco dimensões principais:

Technical Complexity (TC)

Reflete o nível de habilidade técnica, conhecimento e recursos necessários para executar a exploração. Ataques triviais recebem menor peso, enquanto explorações sofisticadas — como correntes multi-exploit, chaining de CVEs ou bypass de hardening — elevam o score.

Exemplos de variação:

- TC Baixo (1-3): Exploração via SQLi simples ou brute-force;
- TC Médio (4-6): Exploração de vulnerabilidade lógica ou RCE em aplicações customizadas;
- TC Alto (7-10): Cadeias complexas envolvendo exploração de 0-day, bypass de sandbox, ou pivotagens internas.

Formulação: `TC = Complexidade Técnica atribuída (1 a 10)`

Business Impact (BI)

Calcula o impacto direto ou potencial sobre os negócios da organização, considerando perda financeira, paralisação de operações, dano reputacional e riscos estratégicos.

Parâmetros analisados:

- BI Baixo (1-3): Exposição de dados não sensíveis ou de impacto operacional mínimo;
- BI Médio (4-6): Vazamento de informações estratégicas, paralisação de serviços não críticos;
- BI Alto (7-10): Vazamento massivo de dados pessoais, paralisação de processos core, interrupção de negócios.

Formulação: `BI = Escala de impacto operacional e financeiro (1 a 10)`

Compliance Risk (CR)

Mensura o risco de não conformidade regulatória, mapeando as explorações às normativas aplicáveis como PCI DSS, LGPD, GDPR, HIPAA, DORA. Quanto maior a exposição à sanção regulatória, maior o score.

Exemplos de atribuição:

- CR Baixo (1-3): Exposição sem relação direta com normativos;
- CR Médio (4-6): Possível violação de controle técnico exigido;
- CR Alto (7-10): Violação direta de requisitos de privacidade ou segurança regulamentar.

Formulação: `CR = Gravidade da exposição regulatória (1 a 10)`

Detection/Stealth (DS)

Avalia o grau de evasão dos mecanismos de detecção e resposta da organização. Quanto mais furtivo o ataque e menos perceptível pelas defesas, maior o peso atribuído.

Considerações:

- DS Baixo (1-3): Atividades detectadas e alertadas;
- DS Médio (4-6): Detecção parcial ou atrasada;
- DS Alto (7-10): Totalmente stealth, bypass completo de EDR/SIEM.

Formulação: `DS = Capacidade de evasão do ataque (1 a 10)`

Fórmula Recomendada — Weighted Risk Score

O cálculo final do **Risk Score A.R.M.A.** pode seguir a fórmula ponderada abaixo, permitindo personalização por setor ou organização:

```
Risk Score = (TC * 0.15) + (DC * 0.25) + (BI * 0.25) + (CR * 0.2) + (DS * 0.15)
```

Justificativa das Pesagens:

- **Technical Complexity (15%)**: Relevante, mas não determina sozinha o risco;
- **Depth of Compromise (25%)**: Reflete a gravidade do avanço adversarial;
- **Business Impact (25%)**: Priorização pelo potencial de dano financeiro e operacional;
- **Compliance Risk (20%)**: Reflete a exposição legal, muitas vezes mais impactante que o técnico;

- **Detection/Stealth (15%)**: Importância de entender se o ataque passou despercebido.

Exemplo de Aplicação Real (Case)

Cenário: Acesso inicial via exposed API + SQL Injection + movimento lateral → acesso à base de dados financeira e vazamento de dados sensíveis.

Métrica	Score	Justificativa
Technical Complex	7	Uso de encadeamento de técnicas e exploração manual
Depth Compromise	9	Controle total de sistema crítico
Business Impact	8	Vazamento de dados financeiros
Compliance Risk	9	Violação direta à LGPD e PCI DSS
Detection/Stealth	6	Parte da atividade não foi detectada

Cálculo Final:

```
Risk Score = (7*0.15) + (9*0.25) + (8*0.25) + (9*0.2) + (6*0.15)
Risk Score = 1.05 + 2.25 + 2 + 1.8 + 0.9 = **8.0 (Escala 0 a 10)**
```

Resultado: Exploração considerada **CRÍTICA**, alta prioridade de remediação e reporte imediato ao comitê de risco.

Customização e Escalabilidade

O modelo A.R.M.A. permite:

6. Ajustes de pesos conforme setor (bancário, saúde, industrial);
7. Integração com dashboards dinâmicos;
8. Alimentação de sistemas de GRC e SIEM;
9. Uso em cálculos de probabilidade de sucesso de Red Team / APT.

O modelo de pontuação proposto pela **A.R.M.A.** eleva o conceito de mensuração de risco em operações ofensivas, integrando variáveis críticas que extrapolam a visão puramente técnica. Ao ponderar complexidade, profundidade do comprometimento, impacto nos negócios, risco regulatório e capacidade de detecção, o sistema fornece uma **visão multidimensional do risco cibernético real**, permitindo priorizações mais assertivas e tomadas de decisão estratégicas.

Esse mecanismo de scoring torna a metodologia adaptável a diferentes cenários, setores e ambientes regulatórios, sendo capaz de suportar desde avaliações pontuais até integrações com **frameworks de GRC (Governança, Risco e Conformidade)** e **plataformas de SIEM**, consolidando-se como uma ferramenta de alto valor para a **gestão integrada de risco cibernético**.

Com o modelo validado e aplicado, o **Risk Score A.R.M.A.** fornece ao decisor não apenas o entendimento do que pode ser explorado tecnicamente, mas o que realmente ameaça o core business da organização, **colocando o risco cibernético em perspectiva com os objetivos estratégicos e regulatórios** da entidade avaliada.

Risk Chain Mapping Visualization

O **Risk Chain Mapping** representa o núcleo visual e estratégico da metodologia A.R.M.A., sendo o elo crítico entre a exploração técnica e a materialização real dos riscos cibernéticos para o negócio. Trata-se da construção gráfica e lógica da jornada adversarial, evidenciando como vulnerabilidades isoladas se conectam, formam caminhos de exploração e, encadeadas, resultam em impactos significativos para a organização.

Diferentemente dos relatórios tradicionais de pentest que listam vulnerabilidades de forma descritiva e isolada, o Risk Chain Mapping proporciona **uma visão dinâmica, encadeada e visual**, permitindo ao público técnico e executivo entender **como cada falha contribuiu para o avanço do agente de ameaça dentro do ambiente corporativo**.

Objetivos do Risk Chain Mapping

O principal objetivo do mapeamento da cadeia de risco é traduzir o caminho real percorrido por um atacante, demonstrando:

- Como um vetor de entrada inicial possibilitou acessos subsequentes;

- Como vulnerabilidades de baixa severidade, quando combinadas, resultaram em cenários de alto risco;

- Onde houve falhas nos controles defensivos e oportunidades de mitigação.

Essa visualização permite ainda identificar pontos de ruptura da cadeia, onde **uma melhoria de controle específica** impediria o avanço da exploração, funcionando como **insight direto para estratégias de hardening e melhoria contínua**.

Componentes Essenciais do Risk Chain

O Risk Chain Mapping é composto por:

- **Nó de Entrada:** Vetor inicial de exploração (ex: exposed API, spear-phishing);

- **Exploit Points:** Vulnerabilidades efetivamente exploradas;

- **Pivot Points:** Pontos onde o atacante amplia seu acesso ou altera o vetor;

- **Assets Impactados:** Sistemas ou dados de alto valor atingidos;

- **Compliance Flags:** Indicação visual dos requisitos regulatórios violados;

- **Kill Chain Milestones:** Pontos relevantes da cadeia de ataque, mapeados conforme o framework ATT&CK ou Lockheed Martin Cyber Kill Chain.

Ferramentas e Modelos de Visualização

A metodologia A.R.M.A. recomenda o uso de ferramentas capazes de gerar diagramas dinâmicos e interativos, como:

- **Graphviz, Draw.io ou Lucidchart:** Para fluxogramas e mapas hierárquicos;

- **Maltego ou Mind Maps (XMind, Miro):** Para representações exploratórias e pivotagens;

- **Chart.js ou D3.js:** Para dashboards dinâmicos em plataformas integradas.

Cada vulnerabilidade é representada como um nó no diagrama, conectado por setas que indicam a progressão do ataque. Pontos de decisão (forks) e escalonamentos de privilégio são destacados, permitindo identificar rapidamente os caminhos críticos.

Exemplo de Cadeia de Risco (Ilustração Conceitual)

Entrada: `API exposta sem autenticação (Technical Complexity 4)`
⬇

Exploração: `SQL Injection → Dump de credenciais (Depth 6)`
⬇
Pivot: `Acesso à rede interna → Scanning → Falha em serviço SMB (BI 7)`
⬇
Escalonamento: `Remote Code Execution via serviço vulnerável (Compliance LGPD Art. 46)`
⬇
Impacto Final: Acesso à base de dados financeiros e PII → Risco regulatório e financeiro extremo (Risk Score 8.5)

Esta visualização conecta todos os nós, demonstrando claramente **como o impacto foi construído pela soma das explorações**.

Benefícios Estratégicos do Risk Chain Mapping

Ao consolidar a exploração adversarial de forma encadeada, o Risk Chain Mapping entrega valor estratégico ao permitir:

- **Tomada de decisão executiva baseada em impacto e risco real, não apenas em severidade técnica isolada**;
- Identificação dos **"single points of failure"** — ativos ou controles cuja falha permitiu a materialização do risco;
- Mapeamento visual de **possíveis violações regulatórias**, permitindo ação preventiva junto às áreas de compliance;
- Estímulo à **integração entre Red Teams e Blue Teams**, facilitando o entendimento da jornada do atacante;
- Criação de uma **linha do tempo visual da ofensiva**, útil para treinamentos e lições aprendidas.

Integração com Compliance e Negócio

Cada nó ou etapa da cadeia pode e deve ser enriquecido com dados complementares:

- **Valor do ativo impactado** (financeiro, reputacional);
- **Normativo ou artigo de lei violado**;
- **Probabilidade de detecção no momento da execução**;
- **Tempo estimado para execução da etapa**.

Esse enriquecimento torna o Risk Chain Mapping uma ferramenta **multidimensional**, que serve não apenas ao time técnico, mas também como **artefato de reporte executivo** e até como **evidência documental** em processos de auditoria ou defesa regulatória.

Outputs Esperados

Ao final da fase, a A.R.M.A. entrega:

- Diagrama completo da cadeia de risco;
- Lista de vulnerabilidades encadeadas e seus pesos;
- Pontos de mitigação estratégica identificados;
- Relatório visual integrável a painéis de risco corporativo.

O Risk Chain Mapping se consolida, assim, como **o principal diferencial visual e estratégico** da metodologia A.R.M.A., materializando o conceito de que **o verdadeiro risco não está na falha individual, mas na forma como o adversário a utiliza para atingir seus objetivos dentro do negócio**.

O **Risk Chain Mapping** dentro da metodologia **A.R.M.A.** representa a **transformação visual e estratégica do processo de exploração ofensiva**, oferecendo uma visão encadeada e lógica da jornada adversarial. Ao construir essa representação gráfica, a organização deixa de enxergar vulnerabilidades como pontos isolados e passa a compreendê-las como **partes de uma cadeia dinâmica de risco**, onde o real impacto decorre do encadeamento e da exploração contínua.

Essa visão permite, de forma inédita, **integrar o técnico ao estratégico**, oferecendo às lideranças um entendimento claro dos vetores de risco, dos ativos mais críticos e das deficiências defensivas que permitiram a materialização da ameaça. Ao conectar cada etapa da exploração com **normativos violados, ativos impactados e falhas de detecção**, o Risk Chain Mapping se torna **uma ferramenta poderosa para priorização de remediações, planejamento de investimentos e gestão de crises**.

Por fim, essa fase consolida a A.R.M.A. como uma **metodologia de ofensiva cibernética orientada ao risco real e ao negócio**, permitindo que a segurança da informação saia da esfera puramente técnica e atue como **instrumento estratégico de proteção e resiliência corporativa**.

Compliance Mapping Model

No contexto da metodologia **A.R.M.A.**, o **Compliance Mapping Model** é uma das fases mais estratégicas e diferenciais, pois estabelece a **conexão direta entre os vetores**

técnicos explorados e as obrigações regulatórias e legais aplicáveis à organização avaliada.

Diferentemente de abordagens ofensivas tradicionais que se restringem à análise de vulnerabilidades sob a ótica técnica, a A.R.M.A. assegura que **cada exploração, cada cadeia de ataque e cada ativo comprometido sejam avaliados também sob o prisma da conformidade regulatória**, fornecendo uma visão clara dos riscos de não conformidade, das potenciais sanções envolvidas e dos requisitos legais violados.

Objetivos do Compliance Mapping

O principal objetivo desta fase é **traduzir tecnicamente os resultados da exploração adversarial em um mapa de risco regulatório e legal**, permitindo que o relatório final da A.R.M.A. seja utilizado não apenas por equipes técnicas, mas também por:

- **Departamentos Jurídicos**;
- **Áreas de Compliance e Auditoria**;
- **Comitês de Risco**;
- **Alta Direção e Conselho**.

O modelo fornece insumos objetivos para que a organização compreenda **não só o impacto técnico das falhas exploradas, mas principalmente o impacto legal, financeiro e reputacional** de cada incidente simulado.

Integração com Normas e Regulamentações Globais

A A.R.M.A. estabelece a **integração direta e contínua com as principais regulamentações e normas de segurança e privacidade**, tais como:

- **PCI DSS v4.0**
- **LGPD (Brasil)**
- **GDPR (Europa)**
- **DORA (Europa)**
- **HIPAA (EUA)**
- **ISO/IEC 27001 e 27002**
- **NIST Privacy Framework**

- **Basel III e regulatórios financeiros setoriais**

Cada uma dessas normas possui requisitos explícitos quanto à proteção de dados, integridade de sistemas, privacidade e resiliência operacional. Ao explorar uma vulnerabilidade, o pentester A.R.M.A. já aponta **quais artigos, cláusulas ou controles normativos foram potencialmente violados**.

Funcionamento do Compliance Mapping

A fase se desenvolve em três grandes etapas:

a) Mapeamento de Explorações x Normativos

Cada vulnerabilidade validada ou cadeia de risco é analisada e mapeada em uma matriz de correlação com os requisitos regulatórios impactados.

Exemplo:

- **SQL Injection explorada em aplicação de pagamento:** Viola **PCI DSS 6.5.1**;
- **Exfiltração de dados pessoais:** Configura violação de **LGPD Art. 46** e **GDPR Art. 32**;
- **Comprometimento de sistema financeiro:** Potencial infração ao **DORA - Continuidade Operacional**.

b) Cálculo do Compliance Risk Score

Cada violação regulatória é pontuada conforme:

- Severidade da norma;
- Probabilidade de sanção;
- Impacto financeiro potencial.

Esse score compõe a métrica **Compliance Risk (CR)** do modelo de scoring geral da A.R.M.A.

c) Produção do Compliance Map Visual

O relatório final contém:

- Gráficos de pizza ou barras mostrando **% de risco por norma**;
- Tabelas detalhadas cruzando **cada falha técnica x artigo violado**;

- Análise das multas potenciais e das implicações legais.

Exemplo Prático de Compliance Mapping Aplicado

Vulnerabilidade: Exposed API com endpoint desprotegido → SQL Injection → Dump de dados pessoais.

Normativos Violados:

Normativo	Artigo / Controle	Descrição da Violação
LGPD	Art. 46	Falha na proteção de dados pessoais
GDPR	Art. 32	Medidas técnicas e organizacionais insuficientes
PCI DSS v4.0	Req. 6.5.1	Falha de validação de entrada em aplicação
DORA	Continuidade Operacional	Risco à resiliência de sistema financeiro

Compliance Risk Score calculado: 9 (Crítico)

Impacto: Potencial multa LGPD de até 2% do faturamento anual; Violação PCI sujeita a bloqueio de operação com cartões.

Benefícios Estratégicos do Compliance Mapping A.R.M.A.

✅ **Integração real entre segurança ofensiva e governança corporativa;**
✅ **Materialização objetiva do risco regulatório em cada exploração;**
✅ **Priorização de correções baseadas não apenas na severidade técnica, mas no potencial de sanção financeira e regulatória;**
✅ **Fortalecimento das defesas jurídicas da organização em caso de incidentes ou auditorias externas;**
✅ **Transparência total para comitês e conselhos sobre a situação de risco regulatório.**

Entregáveis da Fase

Ao final da fase, a A.R.M.A. entrega:

- **Matriz de Compliance Completa (Técnica x Normativa);**
- **Tabela de potenciais exposições regulatórias;**
- **Estimativa de impacto financeiro por norma violada;**
- **Painéis visuais para reporte executivo.**

Essa capacidade de gerar um mapeamento de compliance robusto torna a A.R.M.A. **uma ferramenta essencial não apenas para a cibersegurança, mas para o compliance e a governança das organizações**, especialmente em mercados regulados como financeiro, saúde, telecomunicações e energia.

O **Compliance Mapping Model** da A.R.M.A. eleva a metodologia a um novo patamar, integrando a ofensiva cibernética ao universo da **governança, risco e conformidade (GRC)**. Ao estabelecer a correlação direta entre cada exploração técnica e os normativos regulatórios aplicáveis, a A.R.M.A. permite que a organização **visualize de maneira clara e objetiva suas fragilidades legais e regulatórias**, indo além da simples dimensão técnica.

Essa abordagem fornece um mecanismo robusto para que **áreas jurídicas, de compliance e auditoria corporativa** possam atuar de forma proativa, antecipando riscos legais, estimando potenciais sanções financeiras e priorizando as correções com base no impacto regulatório.

Ao final deste ciclo, a A.R.M.A. transforma o pentest tradicional em um **instrumento estratégico de gestão de risco regulatório**, tornando-se essencial para organizações expostas a normativas como PCI DSS, LGPD, GDPR, DORA e outras legislações setoriais.

Practical Case Study (DVWA Simulation)

Com o objetivo de demonstrar a aplicação prática da metodologia **A.R.M.A.**, foi conduzida uma simulação completa sobre o ambiente do **Damn Vulnerable Web Application (DVWA)**, uma plataforma amplamente utilizada no mercado para treinamentos e provas de conceito em segurança ofensiva.

O exercício teve como foco **não apenas explorar vulnerabilidades técnicas conhecidas**, mas principalmente **aplicar integralmente os princípios da A.R.M.A.**, encadeando falhas, mapeando o risco real e avaliando o impacto técnico, regulatório e de negócios, simulando um cenário corporativo realista.

Context Discovery no DVWA

Objetivos e Premissas:

- Mapear o DVWA como se fosse uma aplicação produtiva de uma empresa;

- Identificar fluxos de dados sensíveis;
- Correlacionar possíveis impactos a normativos como LGPD, PCI DSS e GDPR.

Atividades Realizadas:

- Mapeamento da aplicação, funcionalidades e fluxos;
- Identificação de pontos de entrada: forms, uploaders, APIs REST simuladas;
- Simulação de ativos críticos: base de dados, painel administrativo, funcionalidades de login e upload de arquivos.

Saídas (Outputs):

- Áreas mais críticas mapeadas: **SQL Injection**, **File Upload**, **Command Injection**;
- Definido como objetivo adversarial **o acesso e vazamento da base de dados simulada**.

Adversarial Planning (Modelagem da Ameaça)

Planejamento de Cadeias de Exploração:

- Acesso inicial via SQL Injection;
- Extração de credenciais;
- Movimento lateral até o módulo de upload;
- Escalada para execução remota de comandos;
- Extração completa da base de dados simulada.

Referência: MITRE ATT&CK ID T1505.003 - Server Software Component: Web Shell previsto na fase final.

Regras de Engajamento:

- Não derrubar a aplicação;
- Priorizar stealth e evasão.

Offensive Iterative Loops Executados

Ciclo 1 — Exploração de SQL Injection (SQLi):

- Ferramenta: **SQLMap / Burp Suite Pro**
- Resultado: Acesso à tabela de usuários com hashes de senhas.

Ciclo 2 — Credential Stuffing e Movimentação Lateral:

- Utilização dos hashes obtidos para login;
- Mapeamento das permissões administrativas.

Ciclo 3 — Exploração do módulo File Upload (Web Shell):

- Envio de payload PHP malicioso;
- Bypass de validação de extensão;
- Execução remota de comandos.

Ciclo 4 — Risk Chain Completion:

- Escalonamento via shell;
- Dump completo da base de dados.

Risk Chain Mapping Resultante

Encadeamento Realizado:

Exposed Input Field → SQL Injection → Credential Dump → Privilege Escalation → File Upload Exploitation → Remote Shell → Full Database Compromise

Visualização: Construída cadeia de risco com todas as pivotagens e técnicas.

Impacto: Comprometimento total da aplicação e extração de dados simulados sensíveis.

Impact & Compliance Report (Simulado)

Business Impact:

- Vazamento de dados simulados representando PII;

- Simulação de impacto financeiro superior a 2 milhões (por extrapolação de LGPD/GDPR multas).

Compliance Mapping:

Vulnerabilidade	Compliance Violado	Detalhe
SQL Injection	PCI DSS 6.5.1	Falha na validação de entrada
File Upload / RCE	LGPD Art. 46 / GDPR Art. 32	Falha na proteção de dados
Privilege Escalation	DORA / ISO 27001	Comprometimento de ambiente crítico

Risk Score Calculado (Simulação):

- **Technical Complexity:** 7
- **Depth of Compromise:** 9
- **Business Impact:** 8
- **Compliance Risk:** 9
- **Detection/Stealth:** 6

Risk Score Final: 8.2 (Crítico)

Lessons Learned — Adversary Driven Learning

- Identificação de gaps na validação de entrada e no controle de upload;
- Falhas de monitoração: Explorações passaram sem alertas;
- Recomendação de implementação de WAF e hardening de permissões de upload.

Conclusão da Simulação Prática

O estudo de caso aplicado no **DVWA** demonstrou de forma clara o **potencial da A.R.M.A. em transformar um exercício técnico em uma análise estratégica de risco**. A capacidade de encadear falhas, visualizar a jornada do atacante e produzir um relatório que conecta técnica, negócio e compliance **valida a metodologia como um diferencial frente ao mercado de pentest tradicional**.

Mesmo em um ambiente de laboratório, a A.R.M.A. revelou como vulnerabilidades pequenas, quando ignoradas ou mal priorizadas, podem resultar em **cenários catastróficos** que extrapolam o âmbito técnico e colocam a **continuidade operacional e a conformidade regulatória em risco real**.

Recommendations and Use Cases

A metodologia **A.R.M.A. - Adversarial Risk Mapping & Assessment** foi desenhada para atender às demandas de organizações que buscam uma **abordagem ofensiva avançada, orientada a risco e compliance**, superando as limitações dos modelos tradicionais de pentest.

Sua flexibilidade permite aplicação transversal em diversos cenários críticos, sendo recomendada como framework de referência para operações cibernéticas estratégicas, com foco em **impacto real de negócios e materialização do risco regulatório**.

A seguir, detalham-se os principais cenários de uso e recomendações de aplicação:

Red Teaming & Adversarial Simulations

O A.R.M.A. se encaixa de forma nativa em operações de **Red Teaming**, onde o objetivo não é apenas explorar vulnerabilidades, mas sim **simular o raciocínio, o comportamento e os objetivos de um adversário real**.

Benefícios Diretos:

- Permite modelar ataques complexos encadeados;
- Facilita o mapeamento de impactos sobre ativos de alto valor;
- Gera artefatos visuais que enriquecem o pós-mortem técnico e executivo;
- Integra perfeitamente **Purple Team exercises**, retroalimentando os controles defensivos testados.

Aplicação Recomendada:

- APT Simulations;
- Insider Threat Scenarios;
- Ransomware Kill Chain Testing;
- Testes de Controles de Deteção e Resposta (EDR/SIEM).

ICS / SCADA Environments

Em ambientes industriais e de controle de processos (ICS/SCADA), onde a **indisponibilidade ou falha técnica pode resultar em riscos físicos e catastróficos**, o A.R.M.A. oferece um modelo seguro para execução de simulações ofensivas.

Principais Aplicações:

- Mapeamento de cadeias de risco que possam levar à parada operacional;
- Avaliação de pontos de falha crítica e rotas de pivotagem entre TI e OT;
- Quantificação de impacto financeiro de downtime ou sabotagem;
- Testes controlados com limitação de payloads destrutivos.

Diferencial A.R.M.A.:

Integração da camada técnica com a **avaliação de impacto sobre linhas de produção**, reforçando o link entre TI e chão de fábrica.

Cloud Security Assessments

Com a adoção massiva de serviços em nuvem, A.R.M.A. se adapta perfeitamente a cenários **AWS, Azure, GCP** e multi-cloud, explorando vetores modernos de risco como:

- **Exposição de buckets e blobs;**
- **Exploração de falhas de IAM (Identity and Access Management);**
- **Cross-region pivoting e tenant attacks.**

Recomendações:

- Avaliações contínuas de arquiteturas serverless e containers;
- Mapeamento de impactos sobre SLA e compliance em nuvem (SOC 2, LGPD, GDPR);
- Simulações de abusos de permissões em nuvem (ex: privilege escalation via STS).

Continuous Validation & DevSecOps Pipelines

O ciclo iterativo da A.R.M.A. permite sua **integração direta com fluxos de DevSecOps**, oferecendo às organizações a capacidade de:

- Validar continuamente as superfícies de ataque;
- Automatizar parte dos loops ofensivos;
- Ajustar a postura defensiva com base em risco real e não em detecção de CVE isolado.

Cenários de Aplicação:

- Validação de cada nova feature ou deploy crítico;
- Monitoramento contínuo de mudanças na superfície de exposição;
- Teste de resiliência após updates ou mudanças de arquitetura.

Auditing, Risk and Compliance Alignment

A.R.M.A. proporciona um ganho estratégico para **auditorias de segurança, avaliações de risco e mapeamento de compliance**, especialmente para setores regulados:

- Bancário / Financeiro;
- Telecomunicações;
- Saúde;
- Governo;
- Energia.

Principais Benefícios:

- Materializa a violação de normativos como PCI DSS, LGPD, DORA, GDPR;
- Oferece artefatos técnicos como prova de exposição real;
- Suporta due diligence em processos de M&A ou auditorias externas;
- Alimenta diretamente sistemas GRC.

Considerações Estratégicas Finais sobre Aplicação

Ao adotar a A.R.M.A., a organização ganha **capacidade real de antecipação de riscos estratégicos**, passando de um modelo reativo e técnico para uma **gestão ofensiva integrada ao negócio**.

A metodologia é altamente recomendada para qualquer organização que:

- Lide com dados sensíveis ou infraestrutura crítica;
- Esteja submetida a regimes regulatórios complexos;
- Busque maturidade em **Cyber Threat Intelligence (CTI)**;
- Precise justificar investimentos em cibersegurança com base em riscos reais e quantificados.

A **metodologia A.R.M.A.** se consolida como uma solução robusta, versátil e aderente a múltiplos cenários críticos da segurança cibernética moderna. Sua aplicação transcende o pentest tradicional, proporcionando **valor estratégico real** em operações de Red Teaming, ambientes industriais (ICS/SCADA), nuvem, auditorias regulatórias e processos contínuos de validação de segurança.

Ao alinhar simulação ofensiva, avaliação de risco e mapeamento de compliance, a A.R.M.A. permite que as organizações **visualizem, priorizem e mitiguem seus riscos cibernéticos de forma prática, visual e diretamente conectada aos impactos sobre o negócio**.

Com capacidade de integração a **GRC, DevSecOps, SOCs e frameworks de Purple Team**, a A.R.M.A. torna-se um elemento chave para empresas que buscam **maturidade cibernética**, visão holística de risco e resiliência frente às ameaças modernas.

Conclusion

O desenvolvimento da metodologia **A.R.M.A. — Adversarial Risk Mapping & Assessment** representa um avanço significativo nas práticas de segurança ofensiva e gestão de risco cibernético. Ao longo deste documento, foi demonstrado como a A.R.M.A. transcende as limitações das abordagens tradicionais de pentest, introduzindo uma visão estratégica e multidimensional que permite às organizações **compreenderem o risco de forma encadeada, quantificável e diretamente correlacionada ao impacto sobre o negócio e à conformidade regulatória**.

No cenário atual, onde as ameaças cibernéticas evoluem em complexidade e sofisticação, o mercado demanda abordagens que não apenas apontem falhas técnicas, mas que **evidenciem como essas falhas se conectam em cadeias de risco capazes de comprometer a continuidade operacional, expor dados sensíveis e gerar penalidades financeiras e reputacionais severas**.

A A.R.M.A. responde a essa demanda com um ciclo metodológico estruturado, composto por fases que conduzem o profissional ofensivo desde a descoberta do contexto organizacional até o aprendizado adversarial, passando por:

- Modelagem da ameaça;

- Execução iterativa das explorações;
- Mapeamento visual das cadeias de risco;
- Relatório técnico, de negócios e regulatório integrado.

O grande diferencial da A.R.M.A. está na sua capacidade de **unificar a visão técnica e a executiva**, entregando relatórios que servem tanto como artefatos de melhoria contínua para as áreas de tecnologia quanto como **instrumentos estratégicos de tomada de decisão para lideranças, conselhos e comitês de risco**.

Além disso, o modelo de **pontuação multidimensional** proposto permite às organizações abandonar métricas genéricas como o CVSS, oferecendo uma visão muito mais realista das suas prioridades de correção e investimento, baseada no **impacto efetivo de cada cadeia de risco**.

Do ponto de vista regulatório, a A.R.M.A. também se diferencia ao **mapear automaticamente as violações de normas como PCI DSS, LGPD, GDPR, DORA e outras**, permitindo uma gestão proativa da conformidade e evitando que falhas técnicas se transformem em passivos legais ou financeiros.

Sua aplicabilidade transversal — seja em Red Teaming, ICS/SCADA, ambientes em nuvem, ou auditorias de compliance — reforça o caráter flexível e escalável da metodologia, tornando-a **uma ferramenta essencial para organizações que buscam atingir ou manter um alto grau de maturidade em segurança cibernética e gestão de riscos**.

Por fim, a A.R.M.A. não deve ser vista apenas como uma metodologia ofensiva, mas como um **framework de inteligência cibernética ofensiva**, capaz de fornecer **visibilidade estratégica da superfície de ataque**, apoiar **planos de resposta a incidentes**, orientar **decisões de investimento em segurança** e fortalecer a **resiliência organizacional frente às ameaças modernas**.

Appendices

Esta seção apresenta os **materiais de apoio técnico, templates e referências complementares** que sustentam a aplicação prática da metodologia **A.R.M.A. - Adversarial Risk Mapping & Assessment**.

Os apêndices têm o propósito de **facilitar a adoção da metodologia**, promover a padronização das entregas e assegurar a reprodutibilidade dos processos por diferentes equipes e organizações.

Sample Risk Chain Diagram (Modelo Visual de Cadeia de Risco)

Representação gráfica sugerida para visualizar a progressão do ataque:

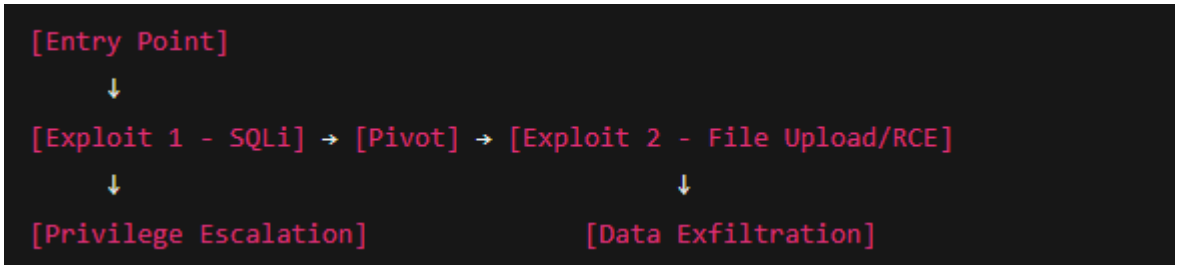

Figura 1 - Progressão de Ataque

Legenda:

- Cada bloco representa uma vulnerabilidade explorada;
- Linhas indicam a sequência e dependência entre os vetores;
- Pontos de pivotagem são destacados como momentos críticos da cadeia.

Example Compliance Mapping Table

Vulnerability	Normative Framework	Article / Control	Description of Violation
SQL Injection	PCI DSS v4.0	6.5.1	Input validation failure
File Upload RCE	LGPD	Art. 46	Data protection failure
Privilege Escalation	GDPR	Art. 32	Lack of technical/organizational controls
Lateral Movement	DORA	Continuity Risk	Operational resilience compromise

Sample Risk Scoring Table

Metric	Score (1-10)	Weight	Weighted Score
Technical Complexity	7	15%	1.05
Depth of Compromise	9	25%	2.25
Business Impact	8	25%	2.00
Compliance Risk	9	20%	1.80

Stealth / Detection	6	15%	0.90
Total Risk Score			**8.0**

Glossary of Terms and Acronyms

Term / Acronym	Description
A.R.M.A.	Adversarial Risk Mapping & Assessment
DC	Depth of Compromise
BI	Business Impact
CR	Compliance Risk
TC	Technical Complexity
DS	Detection/Stealth
ATT&CK	Adversarial Tactics, Techniques & Common Knowledge (MITRE)
CVSS	Common Vulnerability Scoring System
ICS/SCADA	Industrial Control Systems / Supervisory Control and Data Acquisition
DORA	Digital Operational Resilience Act

Bibliographic References

NIST SP 800-115 — Technical Guide to Information Security Testing and Assessment. National Institute of Standards and Technology.

MITRE ATT&CK Framework — Adversarial Tactics, Techniques, and Common Knowledge. MITRE Corporation. Available at: https://attack.mitre.org

CWE Top 25 Most Dangerous Software Weaknesses — MITRE Corporation. Available at: https://cwe.mitre.org/top25/

OWASP Web Security Testing Guide (WSTG) — Open Web Application Security Project (OWASP). Available at: https://owasp.org/www-project-web-security-testing-guide/

PCI DSS v4.0 — Payment Card Industry Data Security Standard. PCI Security Standards Council. Available at: https://www.pcisecuritystandards.org

LGPD (Lei Geral de Proteção de Dados Pessoais) — Brazilian General Data Protection Law (Law No. 13,709).

GDPR (General Data Protection Regulation) — European Parliament and Council Regulation (EU) 2016/679.

DORA (Digital Operational Resilience Act) — European Union Regulation on digital operational resilience for the financial sector.

ISO/IEC 27001 & 27002 — International Standards for Information Security Management Systems and Controls.

The Diamond Model of Intrusion Analysis — Center for Cyber Intelligence Analysis and Threat Research. Available at: https://apps.dtic.mil/sti/pdfs/ADA586960.pdf

Purple Team Tactics and Exercises — SANS Institute.

Common Vulnerability Scoring System (CVSS) v3.1 — Forum of Incident Response and Security Teams (FIRST). Available at: https://www.first.org/cvss

Cloud Security Alliance (CSA) Controls Matrix — Cloud Security Alliance.

NIST Privacy Framework — A Tool for Improving Privacy through Enterprise Risk Management.

Basel Committee on Banking Supervision — Principles for the Sound Management of Operational Risk — Bank for International Settlements (BIS).

Com diagramas, matrizes de compliance, modelos de scoring e glossário, a A.R.M.A. entrega às organizações **ferramentas práticas para transformar a simulação ofensiva em um exercício estratégico de gestão de risco e conformidade**.