CYBER CONF EDU

Conferência Internacional Cibersegurança e Educação Digital

Conferência Internacional Cibersegurança e Educação Digital, Volume I. Número 1. Ano 1 – 2025/1 – ISSN: XXXX-XXXX

Anais do IWCS

Volume 1 (2025)

Workshop Internacional de Cibersegurança: Fronteiras Digitais

São Paulo - Brasil
Faculdade IBPTECH
ibptech.edu.br

FACULDADE IBPTECH

CYBER CONF EDU

Conferência Internacional de Cibersegurança e Educação Digital

Anais do I Workshop Internacional de Cibersegurança: Fronteiras Digitais

ISSN: XXXX-XXXX

São Paulo

2025

Créditos:

Comissão Organizadora do I Workshop Internacional de Cibersegurança: Fronteiras Digitais:

Profª. Drª. Angela Mazzeo

Prof. Dr. Giuliano Giova

Organização da publicação:

Profª. Drª. Angela Mazzeo

Prof. Dr. Giuliano Giova

Vitória Regina Michelli

Capa:

Vitória Regina Michelli

Sumário

Inteligência Artificial na Cibersegurança: Aliada ou Ameaça?

Palestrante:
Prof. Dr. Jefferson Jesus Hengles Almeida

Resumo

A palestra abordou a análise detalhada dos principais aspectos forenses aplicados a dados armazenados em serviços de computação em nuvem. Foram discutidos conceitos fundamentais, desafios técnicos e metodológicos, bem como as implicações legais envolvidas na aquisição e preservação de evidências digitais nesse ambiente. O conteúdo destacou a importância de compreender a estrutura da nuvem, a responsabilidade compartilhada entre provedores e usuários, e os processos de autenticação e auditoria que garantem a integridade dos dados. Além disso, foram apresentadas ferramentas e estratégias utilizadas para rastreamento e extração de informações de diferentes camadas, como infraestrutura, plataforma e software. A abordagem multidisciplinar, que combina aspectos técnicos, jurídicos e operacionais, foi ressaltada como essencial para o sucesso das investigações. O estudo reforçou que a perícia em ambientes de nuvem requer atualização constante, alinhada à evolução das tecnologias e das regulamentações. Com isso, enfatizou-se a necessidade de preparo técnico avançado e análise criteriosa para garantir a validade e confiabilidade das provas obtidas.

Palavras-chave: computação em nuvem; forense digital; preservação de evidências; segurança da informação; serviços online.

ABSTRACT

The session focused on a detailed analysis of the main forensic aspects applied to data stored in cloud computing services. It discussed fundamental concepts, technical and methodological challenges, as well as legal implications related to the acquisition and preservation of digital evidence in this environment. The content highlighted the importance of understanding the cloud structure, the shared responsibility between providers and users, and the authentication and auditing processes that ensure data integrity. In addition, tools and strategies used for tracking and extracting information from different layers, such as infrastructure, platform, and software, were presented. The multidisciplinary approach, combining technical, legal, and operational aspects, was emphasized as essential for the success of investigations. The study reinforced that forensic analysis in cloud environments requires constant updates, aligned with the evolution of technologies and regulations. Therefore, it stressed the need for advanced technical preparation and critical analysis to ensure the validity and reliability of the evidence obtained.

Keywords: cloud computing; digital forensics; evidence preservation; information security; online services.

Criptografia na Era Quântica: Estamos preparados?

Palestrante:
Prof. Esp. Rodrigo Moura

Resumo

Algoritmos quânticos específicos, como o de Shor, são projetados para resolver eficientemente a fatoração de números inteiros grandes e o problema do logaritmo discreto, que são as bases matemáticas da segurança da criptografia assimétrica (chave pública-privada) amplamente utilizada. O algoritmo de Grover, por sua vez, acelera a busca em bancos de dados não estruturados, reduzindo pela metade a força efetiva das chaves de criptografia simétrica. Foi destacado o ataque "armazene agora, decifre depois" (*store now, decrypt later*), onde dados criptografados interceptados hoje podem ser armazenados até que computadores quânticos potentes estejam disponíveis para quebrá-los, tornando a ameaça imediata para dados sensíveis de longo prazo. A resposta a essa ameaça é a Criptografia Pós-Quântica (PQC), que consiste no desenvolvimento de novos algoritmos criptográficos baseados em problemas matemáticos que se acredita serem resistentes tanto a computadores clássicos quanto quânticos. As principais abordagens incluem criptografia baseada em reticulados (lattices), códigos, isogenias e funções de hash. A transição para a PQC apresenta desafios significativos, incluindo a necessidade de padronização (liderada por instituições como o NIST), a atualização de infraestruturas legadas e o aumento do tamanho das chaves e assinaturas, com impacto no desempenho. A palestra enfatizou a urgência de as organizações iniciarem o planejamento, realizando um inventário de seus ativos criptográficos e adotando uma "agilidade criptográfica" para facilitar futuras migrações. A computação quântica não é uma evolução incremental, mas uma revolução que exige uma reavaliação completa da segurança digital. Embora um computador quântico capaz de quebrar os padrões criptográficos atuais ainda não seja uma realidade generalizada, a janela de vulnerabilidade já está aberta. A preparação para a era pós-quântica é uma tarefa complexa e urgente, que demanda colaboração internacional, investimento em pesquisa e a adoção proativa de novas estratégias e tecnologias para garantir a privacidade e a segurança das informações no futuro.

Palavras-chave: criptografia pós-quântica; computação quântica; algoritmo de Shor.

ABSTRACT

Digital security, a cornerstone of modern society, is based on cryptographic algorithms whose robustness relies on mathematical problems that are computationally complex for classical computers. However, the rise of quantum computing represents a paradigm shift, threatening to invalidate decades of development in information security. This lecture analyzed the fundamentals of current cryptography, the disruptive impact of quantum computing, and the strategies needed to transition to a quantum-resistant security infrastructure. The presentation began with a review of the three pillars of cryptography—confidentiality, integrity, and authenticity—and its historical evolution, from ancient methods to the asymmetric (RSA, ECC) and symmetric (AES) algorithms that protect the vast majority of today's digital communications, such as HTTPS traffic. The core of the threat lies in the ability of quantum computers to exploit principles like superposition and entanglement of qubits to achieve massive computational parallelism. Specific quantum algorithms, such as Shor's, are designed to efficiently solve the factorization of large integers and the discrete logarithm problem, which are the mathematical foundations of widely used asymmetric (public-key) cryptography. Grover's algorithm, in turn, accelerates searches in unstructured databases, effectively halving the strength of symmetric encryption keys. The "store now, decrypt later" attack was highlighted, where encrypted data intercepted today can be stored until powerful quantum computers are available to break them, making the threat immediate for long-term sensitive data. The answer to this threat is Post-Quantum Cryptography (PQC), which involves the development of new cryptographic algorithms based on mathematical problems believed to be resistant to both classical and quantum computers. The main approaches include lattice-based, code-based, isogeny-based, and hash-based cryptography. The transition to PQC presents significant challenges, including the need for standardization (led by institutions like NIST), the update of legacy infrastructures, and the increase in key and signature sizes, which impacts performance. The lecture emphasized the urgency for organizations to begin planning by conducting an inventory of their cryptographic assets and adopting "crypto-agility" to facilitate future migrations. Quantum computing is not an incremental evolution but a revolution that demands a complete reassessment of digital security. Although a quantum computer capable of breaking current cryptographic standards is not yet a widespread reality, the window of vulnerability is already open. Preparing for the post-quantum era is a complex and urgent task that requires international collaboration, investment in

research, and the proactive adoption of new strategies and technologies to ensure the privacy and security of information in the future.

Keywords: post-quantum cryptography (PQC); quantum computing; Shor's algorithm.

Gestão de Incidentes de Cibersegurança: A Importância da Preparação e Cultura Organizacional

Palestrante:
Eng. Gustavo Batistuzzo

Resumo

A crescente sofisticação das ameaças cibernéticas, exacerbada pela digitalização acelerada e pelo trabalho remoto, tornou os incidentes de segurança uma inevitabilidade para as organizações. Este estudo aborda a criticidade da preparação prévia em tempos de "paz" para mitigar os impactos de um ataque cibernético, focando nos custos associados, nos desafios da resposta a incidentes e na necessidade de uma cultura de segurança robusta. A análise de incidentes cibernéticos revela que a falta de preparação adequada resulta em custos financeiros substanciais, como evidenciado por um estudo da IBM de 2024, que aponta um custo médio de quase US$ 5 milhões por vazamento de dados. A escassez de profissionais qualificados em cibersegurança ("cyber skills") agrava esse cenário, contribuindo significativamente para os custos totais. A demora na identificação e contenção de incidentes, especialmente aqueles decorrentes de engenharia social, phishing ou credenciais roubadas (podendo levar mais de 250 dias), permite que atacantes permaneçam indetectados, mapeando ambientes e coletando dados sensíveis antes de deflagrar ataques destrutivos. A palestra categoriza os incidentes em tipos como intrusão de sistemas, engenharia social, ataques a aplicações web, erro humano, negação de serviço, ativos perdidos/roubados e uso indevido de privilégios. É enfatizado que a cultura de cibersegurança é a primeira linha de defesa, exigindo comprometimento da liderança, comunicação clara, treinamentos contínuos, simulações e integração da segurança desde o *onboarding* de novos colaboradores. A implementação de um plano de resposta a incidentes (IRP) é crucial, definindo papéis e responsabilidades, procedimentos de comunicação (interna e externa, incluindo órgãos reguladores como a ANPD/GDPR), e a preservação de logs íntegros e centralizados para análise forense e conformidade regulatória. A importância de testes regulares de backups e a adoção de frameworks de segurança (NIST, ISO 27000) e modelos de avaliação de maturidade são destacadas como ferramentas essenciais para identificar e preencher lacunas na postura de segurança. A gestão eficaz de incidentes de cibersegurança transcende a mera implementação de ferramentas tecnológicas; ela reside na construção de uma

cultura organizacional resiliente e na preparação proativa. A negligência na preparação pode resultar em sanções regulatórias e danos reputacionais irreparáveis. A colaboração entre equipes internas e, quando necessário, com especialistas externos, é fundamental para garantir uma resposta coordenada e eficaz, minimizando o impacto dos inevitáveis incidentes cibernéticos e transformando-os em oportunidades de aprendizado e aprimoramento contínuo da segurança.

Palavras-chave: gestão de incidentes de segurança cibernética; plano de resposta a incidentes (IRP); cultura organizacional.

ABSRACT

The increasing sophistication of cyber threats, exacerbated by accelerated digitalization and remote work, has made security incidents an inevitability for organizations. This study addresses the criticality of prior preparation during "peace" times to mitigate the impacts of a cyberattack, focusing on associated costs, incident response challenges, and the need for a robust security culture. The analysis of cybersecurity incidents reveals that a lack of adequate preparation results in substantial financial costs, as evidenced by a 2024 IBM study, which points to an average cost of nearly US$5 million per data breach. The scarcity of qualified cybersecurity professionals ("cyber skills") exacerbates this scenario, significantly contributing to total costs. Delays in identifying and containing incidents, especially those stemming from social engineering, phishing, or stolen credentials (which can take over 250 days), allow attackers to remain undetected, mapping environments and collecting sensitive data before launching destructive attacks. The lecture categorizes incidents into types such as system intrusion, social engineering, web application attacks, human error, denial of service, lost/stolen assets, and misuse of privileges. It is emphasized that cybersecurity culture is the first line of defense, requiring leadership commitment, clear communication, continuous training, simulations, and the integration of security from the onboarding of new employees. The implementation of an incident response plan (IRP) is crucial, defining roles and responsibilities, communication procedures (internal and external, including regulatory bodies like ANPD/GDPR), and the preservation of integral and centralized logs for forensic analysis and regulatory compliance. The importance of regular backup testing and the adoption of security frameworks (NIST, ISO 27000) and maturity assessment models are highlighted as essential tools to identify and fill gaps in the security posture. Effective cybersecurity incident management transcends the mere implementation of technological tools; it lies in building a resilient organizational culture and proactive preparation. Negligence in preparation can result in regulatory sanctions and irreparable reputational damage. Collaboration between internal teams and, when necessary, with external specialists, is fundamental to ensuring a coordinated and effective response, minimizing the impact of inevitable cyber incidents and transforming them into opportunities for continuous learning and security improvement.

Keywords: cybersecurity incident management; incident response plan (IRP); organizational culture.

Cibersegurança em Infraestruturas Críticas e Nucleares

Palestrante:
Profa. Dra. Angela Mazzeo

Resumo

A guerra cibernética, operando como um "quinto domínio" de conflito, representa uma ameaça constante e invisível à segurança nacional. Este estudo analisa as vulnerabilidades de infraestruturas críticas, com foco especial nos setores energético e nuclear, que são fundamentais para a estabilidade social e econômica. A interrupção desses serviços por meio de ataques cibernéticos pode gerar consequências sistêmicas devastadoras. Infraestruturas críticas como sistemas de energia, água, saúde, transporte e finanças, destacando a matriz energética como um ponto central de vulnerabilidade, cuja falha impacta todos os outros setores. A automação e a digitalização, especialmente através de sistemas SCADA e PLCs, criam novos vetores de ataque. Foram detalhados ataques comuns a subestações elétricas, como injeção de malware, exploração de acesso remoto, manipulação de firmware e ataques de negação de serviço (DDoS), que podem levar a sobrecargas e apagões coordenados. No contexto nuclear, a segurança é multifacetada, combinando proteção física robusta com cibersegurança. Ameaças como o malware Stuxnet demonstraram a capacidade de ataques cibernéticos causarem danos físicos diretos a equipamentos críticos, como centrífugas de enriquecimento de urânio, explorando vulnerabilidades através de mídias removíveis (USB) mesmo em sistemas isolados (*air-gapped*). A Agência Internacional de Energia Atômica (AIEA) estabelece diretrizes rigorosas (série NSS), preconizando uma abordagem de defesa em profundidade, segmentação de rede, gestão de riscos, e a crucial integração entre equipes de Tecnologia da Informação (TI) e Tecnologia Operacional (TO) para proteger esses ambientes. A proteção de infraestruturas críticas e nucleares exige uma abordagem de segurança integrada e dinâmica, que vai além das defesas físicas tradicionais. É imperativo que a cultura organizacional incorpore a cibersegurança como um pilar, com treinamentos contínuos, simulações de incidentes e adesão estrita a normativas internacionais. A convergência entre TI e TO é essencial para gerenciar os riscos associados à automação industrial e garantir a resiliência contra um cenário de ameaças em constante evolução.

Palavras-chave: cibersegurança; infraestrutura crítica; segurança nuclear.

ABSTRACT

Cyber warfare, operating as a "fifth domain" of conflict, poses a constant and invisible threat to national security. This study analyzes the vulnerabilities of critical infrastructures, with a special focus on the energy and nuclear sectors, which are fundamental to social and economic stability. The disruption of these services through cyberattacks can lead to devastating systemic consequences. The lecture identifies critical infrastructures such as energy, water, health, transport, and financial systems, highlighting the energy grid as a central point of vulnerability whose failure impacts all other sectors. Automation and digitalization, especially through SCADA systems and PLCs, create new attack vectors. Common attacks on electrical substations were detailed, including malware injection, remote access exploitation, firmware manipulation, and denial-of-service (DDoS) attacks, which can lead to overloads and coordinated blackouts. In the nuclear context, security is multifaceted, combining robust physical protection with cybersecurity. Threats like the Stuxnet malware have demonstrated the ability of cyberattacks to cause direct physical damage to critical equipment, such as uranium enrichment centrifuges, by exploiting vulnerabilities through removable media (USB) even in air-gapped systems. The International Atomic Energy Agency (IAEA) establishes strict guidelines (NSS series), advocating for a defense-in-depth approach, network segmentation, risk management, and the crucial integration of Information Technology (IT) and Operational Technology (OT) teams to protect these environments. The protection of critical and nuclear infrastructures requires an integrated and dynamic security approach that extends beyond traditional physical defenses. It is imperative that organizational culture incorporates cybersecurity as a pillar, with continuous training, incident simulations, and strict adherence to international standards. The convergence of IT and OT is essential to manage the risks associated with industrial automation and ensure resilience against an ever-evolving threat landscape.

Keywords: cybersecurity; critical infrastructure; nuclear security.

O Papel da Forense Computacional no Tratamento de Incidentes Cibernéticos

Palestrante:
Profa. Esp. Taciana Eugênia Duarte

Resumo

No âmbito processual, a elucidação de questões técnicas complexas frequentemente demanda a intervenção de especialistas. O Parecer Técnico emerge como um documento fundamental, emitido por um perito de parte, para fornecer análises e conclusões sobre uma matéria específica, contrapondo-se ou complementando o Laudo Pericial oficial. O Parecer Técnico é um documento formal solicitado por uma das partes envolvidas em um processo judicial ou administrativo. Sua estrutura é análoga à do Laudo Pericial, diferenciando-se pelo signatário, que atua em nome da parte contratante. A elaboração do documento exige uma metodologia rigorosa, incluindo a identificação do solicitante, a definição clara do objetivo da análise, a descrição detalhada dos objetos periciados e seu estado atual, e a especificação dos métodos técnicos empregados. A apresentação dos resultados deve ser feita em linguagem clara e acessível, culminando em uma conclusão sucinta que responda aos quesitos formulados. A elaboração de um Parecer Técnico eficaz transcende a mera competência técnica na área de conhecimento. Requer, adicionalmente, habilidades de redação e formatação textual, bem como a estrita observância dos princípios éticos e técnicos inerentes à prática pericial. O documento serve como uma ferramenta crucial para a defesa dos interesses da parte, contribuindo para o contraditório e a ampla defesa ao oferecer uma perspectiva especializada sobre a matéria em análise, podendo, inclusive, fundamentar a solicitação de uma nova perícia judicial, conforme previsto no Art. 480 do Código de Processo Civil.

Palavras-chave: Parecer técnico; Laudo pericial; Perícia forense.

ABSTRACT

Within the procedural scope, the elucidation of complex technical issues often requires the intervention of specialists. The Technical Opinion emerges as a fundamental document, issued by a party-appointed expert, to provide analysis and conclusions on a specific matter, either opposing or complementing the official Expert Report (Laudo Pericial). The Technical Opinion is a formal document requested by one of the parties involved in a judicial or administrative process. Its structure is analogous to that of the Expert Report, differing in its signatory, who acts on behalf of the contracting party. The elaboration of the document demands a rigorous methodology, including the identification of the requesting party, a clear definition of the analysis's objective, a detailed description of the objects under examination and their current state, and the specification of the technical methods employed. The presentation of the findings must be in clear and accessible language, culminating in a succinct conclusion that addresses the formulated questions. The creation of an effective Technical Opinion transcends mere technical competence in the field of knowledge. It also requires skills in writing and textual formatting, as well as strict adherence to the ethical and technical principles inherent in forensic practice. The document serves as a crucial tool for defending the party's interests, contributing to the principles of contradiction and full defense by offering a specialized perspective on the matter under analysis. It can also substantiate a request for a new judicial expert examination, as provided for in Art. 480 of the Brazilian Conde of Civil Procedure.

Keywords: Technical Opinion; Expert Report; Forensic Expertise.

Mesa Redonda: Criminologia digital no Brasil e na Espanha

Palestrantes:
Profa. MSc. Rubia Ferrão
Profa. MSc. Julia Machi Navarro
Eng. Gustavo Batistuzzo

Resumo

Esta mesa redonda promoveu um diálogo interdisciplinar entre especialistas em Direito Digital e Criminologia do Brasil e da Espanha, com o objetivo de analisar e comparar os cenários do cibercrime, os desafios regulatórios e as estratégias de combate em ambas as regiões. A discussão destacou como diferentes contextos geopolíticos e sociais moldam as prioridades e abordagens na luta contra a criminalidade digital. A análise do cenário brasileiro, apresentada pela Professora Rúbia Ferrão, focou nos crimes contra o patrimônio (estelionato, fraude eletrônica), na exploração sexual online e na disseminação de desinformação, especialmente através de *deepfakes*. Foi ressaltada a evolução da legislação brasileira, como a Lei Carolina Dieckmann e as recentes alterações no Código Penal, para tipificar crimes digitais "puros" e "impuros". Os principais desafios apontados foram a extraterritorialidade, a dificuldade de investigação devido ao anonimato, a necessidade de cooperação internacional (reforçada pela adesão à Convenção de Budapeste) e a escassez de profissionais qualificados. A importância da "autópsia digital" (análise forense imediata) e da inteligência preventiva foi enfatizada como crucial para a identificação de autores. Em contraponto, a Professora Julia, da Universidade de Valência, descreveu o panorama espanhol e europeu, onde as principais ameaças cibernéticas estão intrinsecamente ligadas a questões geopolíticas, como o ciberterrorismo, a radicalização violenta online e a desestabilização de processos democráticos por meio de campanhas de desinformação. A estratégia europeia de cibersegurança, alinhada à OTAN, foca na resiliência de infraestruturas críticas e na defesa contra ameaças híbridas. Foi discutido que, embora crimes patrimoniais existam, a prioridade recai sobre ameaças à segurança do Estado. A digitalização acelerada de serviços na Europa também foi citada como um vetor crescente de vulnerabilidades, embora a percepção de risco ainda seja ofuscada pelas ameaças de terrorismo. A mesa redonda concluiu que, apesar das diferenças de foco — patrimonial no Brasil e geopolítico/terrorista na

Espanha —, ambos os contextos enfrentam desafios comuns, como a necessidade de mais profissionais qualificados, a importância da cooperação internacional e o fomento a uma cultura de cibersegurança. A discussão sobre o compartilhamento de informações sobre ameaças entre entidades públicas e privadas (como proposto pelo DORA na UE) revelou-se um ponto de convergência, sendo essencial para a construção de uma defesa cibernética mais resiliente e proativa em um mundo globalizado e interconectado.

Palavras-chave: Criminologia; Cibersegurança e Direito Digital.

ABSTRACT:

This round table facilitated an interdisciplinary dialogue between experts in Digital Law and Criminology from Brazil and Spain, aiming to analyze and compare the cybercrime landscapes, regulatory challenges, and combat strategies in both regions. The discussion highlighted how different geopolitical and social contexts shape priorities and approaches in the fight against digital crime. The analysis of the Brazilian scenario, presented by Professor Rúbia Ferrão, focused on crimes against property (fraud, electronic scams), online sexual exploitation, and the dissemination of disinformation, especially through deepfakes. The evolution of Brazilian legislation, such as the "Carolina Dieckmann Law" and recent amendments to the Penal Code to classify "pure" and "impure" digital crimes, was emphasized. The main challenges identified were extraterritoriality, the difficulty of investigation due to anonymity, the need for international cooperation (reinforced by adherence to the Budapest Convention), and the scarcity of qualified professionals. The importance of "digital autopsy" (immediate forensic analysis) and preventive intelligence was stressed as crucial for identifying perpetrators. In contrast, Professor Julia from the University of Valencia described the Spanish and European landscape, where the main cyber threats are intrinsically linked to geopolitical issues, such as cyberterrorism, online violent radicalization, and the destabilization of democratic processes through disinformation campaigns. The European cybersecurity strategy, aligned with NATO, focuses on the resilience of critical infrastructures and defense against hybrid threats. It was discussed that while property crimes exist, the priority lies with threats to state security. The accelerated digitalization of services in Europe was also cited as a growing vector of vulnerabilities, although the perception of risk is still overshadowed by terrorist threats. The round table concluded that, despite differences in focus—patrimonial in Brazil and geopolitical/terrorist in Spain—both contexts face common challenges, such as the need for more qualified professionals, the importance of international cooperation, and the promotion of a cybersecurity culture. The discussion on sharing threat intelligence between public and private entities (as proposed by DORA in the EU) emerged as a point of convergence, being essential for building a more resilient and proactive cyber defense in a globalized and interconnected world.

Keywords: Criminology; Cybersecurity; Digital Law.