Curso de Especialização em *Segurança da Informação e Resiliência Digital*

1. Estrutura Curricular – componente curricular/carga horária.

MÓDULO 1 - Governança de Segurança e Segurança Digital	
Segurança Digital nas Organizações	32
Conformidade e Controles	32
Continuidade de Negócios	32
Arquitetura e Projetos Digitais	32
Carga horária total do módulo	**128 horas-aula**
MÓDULO 2 - Cyber Security	
Desenvolvimento Seguro	32
Inteligência de Ameaças	32
Ethical Hacking	32
Segurança Ofensiva	32
Carga horária total do módulo	**128 horas-aula**
MÓDULO 3 - Operação e Defesa Cibernética	
Implantação e Tecnologias de Segurança	32
Inteligência na detecção de ataques	32
Resposta à incidentes	32
Análise Forense	32
Carga horária total do módulo	**128 horas-aula**
MÓDULO 4 -Aplicação de Conhecimento	48 horas-aulas à distância
Total da carga horária do curso	**432 horas-aula**

IDENTIFICAÇÃO DO COMPONENTE CURRICULAR - 1

1. Nome do Componente Curricular: **Segurança Digital nas Organizações**

2. Carga Horária: 32 horas

3. Ementa:

Importância da Segurança Digital nas organizações. Abordagens da Segurança Digital em Sistemas Operacionais, Banco de Dados e Redes de Computadores. Linguagens de Programação Web. Conceitos de Criptografia.

4. Objetivo:

Compreender a importância e os principais fundamentos de Segurança Digital nas Organizações demonstrando sua aplicabilidade em sistemas computacionais (sistemas operacionais e banco de dados), bem como apresentar os conceitos essenciais de disciplinas (rede de computadores, programação web e criptografia) para que os alunos possam equalizar o conhecimento e prosseguir no curso.

5. Conteúdo Programático:

- Fundamentos da Segurança da informação
  - Princípios de Segurança: confiabilidade, Integridade e Disponibilidade;
  - Controle de Acesso;
  - Modelos de Segurança;
  - Identificação e Autenticação
- Segurança em sistemas operacionais e Banco de dados

- Conceitos de Redes de Computadores (Modelo OSI, TCP/IP e Principais Protocolos)
- Linguagem de programação para Web (HTTP, HTML, CSS, PHP)
- Conceitos de Criptografia
- Exercício prático: Análise de Pacotes de rede utilizando Wireshark
- Exercício prático: Geração de Hash - Utilização de criptografia simétrica e assimétrica em arquivo.
- Exercício prático: Controle de acesso no Linux e Windows

6. Bibliografia:

- Básica:
  Dieter Gollmann. Computer Security. 3rd Edition. Wiley, 2011.
  Michael T. Goodrich; Roberto Tamassia. Introdução à Segurança de Computadores. Bookman, 2013.
  Lawrie Brown; William Stallings. Segurança de Computadores - Princípios e Práticas. 2a. edição. Campus, 2014.
- Complementar:
  John R. Vacca. Computer and Information Security Handbook. 3rd Edition. Morgan Kaufmann, 2017.
  Georgia Weidman. Testes de Invasão: uma Introdução Prática ao Hacking. 1a edição. Novatec Editora, 2017.
  William Stallings. Criptografia e Segurança de Redes: Princípios e Práticas. 6ª edição. Pearson, 2014.
  Chris Sanders. Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems. 3rd Edition. No Starch Press, 2017.
  Chris McNab. Avaliação de Segurança de Redes: Conheça a sua Rede. 1ª edição. Novatec, 2017.

IDENTIFICAÇÃO DO COMPONENTE CURRICULAR – 2

1. Nome do Componente Curricular: **Conformidade e Controles**

2. Carga Horária: 32 horas

3. Ementa:

Gerenciamento de risco de segurança. Frameworks de Gerenciamento de Riscos. Padrões de Segurança (ISO 27000, NIST Cybersecurity Framework e Center for Internet Security (CIS). Privacidade de dados. Políticas de Segurança.

4. Objetivo:

Apresentar ao aluno os principais conceitos de gerenciamento de risco de segurança, controles de segurança e privacidade dos dados de forma que possam ser implantados em conformidade com as políticas e normas da organização.

5. Conteúdo Programático:

- Introdução a Gerenciamento de risco de segurança;
  - Tipos de Riscos;
  - Processo de Gerenciamento de Riscos
- Frameworks de Gerenciamento de Riscos
- Padrões de Segurança
  - Família ISO 27000
  - NIST Cybersecurity Framework
  - Center for Internet Security (CIS)
- Privacidade dos Dados -
  - Lei Geral de Proteção de Dados (LGPD)
  - General Data Protection Regulation (GDPR)

- Privacidade dos Dados - Implantação/Framework
    - NIST Privacy Framework;
    - ISO 27001 - PIMS (Privacy Information Management System);
    - Frameworks brasileiro
- Políticas de Segurança
- Exercício prático: Elaboração de uma política de segurança com base em um framework
- Exercício prático: Elaboração de um plano diretor de segurança com base em um framework

6. Bibliografia:

- Básica:

Anne Kohnke; Ken Sigler; Dan Shoemaker. Implementing Cybersecurity: A Guide to the National Institute of Standards and Technology Risk Management Framework. Auerbach Publications, 2017.
Omar Santos. Developing Cybersecurity Programs and Policies. 3rd Edition. Pearson IT Certification, 2018.
John Warsinske, et al. The Official (ISC)2 Guide to the CISSP CBK Reference. Wiley; 5th edition, 2019.
James Broad. Risk Management Framework: A Lab-Based Approach to Securing Information Systems. Syngress, 2013.

- Complementar:

Daniel Donda. Guia prático de implementação da LGPD. Editora Labrador, 2020.
Maldonado, Viviane Nóbrega, Opice Blum, Renato - LGPD – Lei Geral de Proteção de Dados comentada, São Paulo, Thomsom Reuters, 2019
BAARS, Hans. HINTZBERGEN, Kees. HINTZBERGEN, Jule, Smulders, André. Fundamentos de Segurança da Informação. Com Base na ISO 27001 e na ISO 27002. Rio de Janeiro: Brasport, 2018.
FONTES, Edison. Políticas e Normas para a Segurança da Informação. Brasport, 2012.
TEIXEIRA FILHO, Sócrates Arantes. Segurança da Informação Descomplicada. Rio de Janeiro: Clube de Autores, 2019.
SANTOS, Cleórbete. Segurança Digital. Amazon, 2019.

IDENTIFICAÇÃO DO COMPONENTE CURRICULAR - 3

1. Nome do Componente Curricular: Continuidade de Negócios

2. Carga Horária: 32

3. Ementa

Avaliação de riscos. Continuidade dos Negócios. Planos de Continuidade de Negócios, de Crise e de recuperação de desastres. Norma ISO 22301.

4. Objetivo:

Compreender os processos e procedimento para o sucesso da implementação do plano de continuidade de negócios, formalizando as ações a serem tomadas para que, em momentos de crise, a recuperação, a continuidade e a retomada possam ser efetivas, evitando que os processos críticos de negócio da organização sejam afetados, o que pode acarretar perdas financeiras.

5. Conteúdo Programático:

- Análise de impacto nos negócios e processo de avaliação de riscos
- Estratégia de Continuidades dos Negócios
- Desenvolvimento e implantação de Planos:
    - Planos de Continuidade de Negócios (PCN)
    - Planos de Crise
    - Plano de recuperação de Desastres
- Programa de Treinamento e Conscientização para Companhia e Fornecedores
- Exercício Prático: Desenvolver um plano de continuidade operacional
- Exercício Prático: Desenvolver um plano de continuidade negócio.

6. Bibliografia:

a. Básica:

Marinho Fernando. Guia de plano de continuidade de negócios (PCN). Elsevier, 2018.

William William Alevate. Gestão da Continuidade de Negócios. Elsevier, 2013.

John Warsinske, et al. The Official (ISC)2 Guide to the CISSP CBK Reference. Wiley; 5th edition, 2019.

b. Complementar:

Dejan Kosutic. Becoming Resilient – The Definitive Guide to ISO 22301 Implementation. PublishDrive, 2017.

_____ ISO 22301:2019 - Security and resilience - Business continuity management systems - Requirements. International Organization for Standardization (ISO), 2nd Edition, 2019.

Willson, David, Dalziel, Henry. Cyber Security Awareness for CEOs and Management, Syngress; 1st edition, 2015

IDENTIFICAÇÃO DO COMPONENTE CURRICULAR - 4

1. Nome do Componente Curricular: **Arquitetura e Projetos Digitais**

2. Carga Horária: 32h/a

3. Ementa

Conceitos de Computação em Nuvem. Principais Serviços da Nuvem e custos. Proteção de Dados na Nuvem. Segurança de rede. Arquitetura de Nuvem Segura.

4. Objetivos

Habilitar o aluno a implementar ambientes mais seguros de infraestrutura baseado em Nuvem. Fomentar discussões e insights sobre modelos de negócio usando Nuvem Híbrida. Realizar o desenho e modelos arquitetônicos para proteção dos dados independente de onde estejam localizados.

5. Conteúdo Programático:

- Conceitos de Computação em Nuvem
  - Características da Nuvem
  - Modelos de serviço (IaaS, PaaS, SaaS)
  - Modelos de implantação (público, privado, Híbrido)
  - Compartilhamento de responsabilidade
- Principais Serviços da Nuvem e custos
  - Computação, armazenamento, rede e transferência de dados.
  - Tendências de Segurança e fornecedores
- Proteção de Dados na Nuvem
  - Gerenciamento do ciclo de vida dos Dados
  - Criptografia de dados em repouso
  - Disponibilidade
  - Criptografia de dados em trânsito
  - Gerenciamento de Chaves

- Segurança de rede
    - Rede on-premise, Rede de nuvem privada, Rede de nuvem pública, Segmentação de Rede, Serviços de proteção de rede.
- Arquitetura de Nuvem Segura
    - AWS Well-Architected Framework
    - Google 5 Principles for Cloud Native Architecture
- Exercício prático: Controle e Acesso as informações na Nuvem (IAM)
- Exercício prático: Criptografia de dados em repositório de objetos (Bucket) na Nuvem
- Exercício prático: Regras Firewall na Nuvem (Security Group e NACL)

6. Bibliografia:

● Básica:

Anthony Velte. Cloud Computing – Computação Em Nuvem: Uma Abordagem Pratica. 1. ed. [*S. l.*]: Alta Books, 2011. 352 p. ISBN 9788576085362.

Chris Dotson. Practical Cloud Security: A Guide for Secure Design and Deployment. 1st Edition. O'Reilly Media, 2019.

O'Hara & Malisow. CCSP (ISC)2 Certified Cloud Security Professional Official Study Guide, Sybex, 2017.

● Complementar:

Frank Kim et al. Practical Guide to AWS Cloud Security Security in the AWS Cloud. SANS, 2020.

Documentação dos provedores de Computação em Nuvem (e.g. Amazon Web Services, Microsoft Azure e Google Cloud Platform).

IDENTIFICAÇÃO DO COMPONENTE CURRICULAR – 5

1. Nome do Componente Curricular: **Desenvolvimento Seguro**

2. Carga Horária: 32h

3. Ementa

Ciclo de desenvolvimento Seguro. Segurança para aplicativos móveis e dispositivos autônomos conectados à internet (IoTs). Metodologia de Defesa e Ataque de aplicação Web. Ataques de Injeção. Validação de Entradas. Injeção de Código. Execução Remota de Código (RCE).

4. Objetivo:

Explorar estratégias para incorporar a segurança aos ciclos de disponibilização rápida, típicos do desenvolvimento e implantação de aplicações modernas. Adotando a mentalidade de shift-left testing, que exige que as organizações corrijam as fragilidades durante o processo de desenvolvimento.

5. Conteúdo Programático:

- Ciclo de desenvolvimento Seguro, DevOps, DevSecOps
- Segurança para aplicativos móveis
- Segurança em tecnologia de dispositivos autônomos conectados à internet (IoTs)
- Metodologia de Defesa e Ataque de aplicação Web
    - Metodologia Desenvolvimento de Software Seguro

- Metodologia para Teste de Invasão de aplicação Web.
- OWASP top 10

- Ataques de Injeção
  - Validação de Entrada, Web Application Firewall, Injeção SQL; Blind SQL Injection; Injeção de Comandos; Entidades Externas de XML (XXE).
- CTF de Validação de Entradas
  - Cross-site Scripting (XSS) e Cross Site Request Forgery (CSRF)
- CTF de Injeção de Código
  - SQLi, Blind SQL Injection.
  - Utilização de ferramenta de automatização (e.g. SQLmap)
- CTF de Execução Remota de Código (RCE)

6. Bibliografia:

- Básica:

Michael Howard; David LeBlanc. Escrevendo Código Seguro. Bookman, 2 edição, 2005.
Daniel Moreno. Pentest em Aplicações web. 1ª edição. Novatec, 2017.
Dafydd Stuttard, Marcus Pinto. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2nd Edition. Willey, 2011.

- Complementar:

Julien Vehent. Securing DevOps: Security in the Cloud. Manning Publications, 1st edition, 2018.
Peter Kim. The Hacker Playbook 3: Practical Guide To Penetration Testing Paperback. 1st edition. Independently published, 2018.
Bergman, Neil, Stanfield, Mike, Rouse, Jason , Scambray, Joel, Geethakumar, Sarath Deshmukh, Swapnil, Matsumoto, Scott, Steven, John, Price, Mike. Hacking Exposed Mobile: Security Secrets & Solutions, McGraw-Hill Education; 1st edition, 2013.
Gupta, Aditya. The IoT Hacker's Handbook: A Practical Guide to Hacking the Internet of Things, Apress; 1st ed. Edition, 2019.

Rehberger, Johann. Cybersecurity Attacks – Red Team Strategies: A practical guide to building a penetration testing program having homefield advantage, Packt Publishing; 1st edition, 2020.

IDENTIFICAÇÃO DO COMPONENTE CURRICULAR – 6

1. Nome do Componente Curricular: **Inteligência de Ameaças**

2. Carga Horária: 32h

3. Ementa:

Inteligência na antecipação de ataques. Gestão de vulnerabilidades. Conhecendo os adversários. Ciclo das ameaças cibernéticas. Técnicas de proteção.

4. Objetivo:

Capacitar o discente para que seja capaz de identificar novas falhas de segurança e tomar precauções para evitar que elas sejam exploradas, a partir do entendimento da motivação dos adversários, dos seus possíveis ataques e da utilização de mecanismos de prevenção, tais como gestão de vulnerabilidades e técnicas de proteção de sistemas.

5. Conteúdo Programático:

- Inteligência na antecipação de ataques
  - Modelagem de ameaças, cenário de ameaças e evolução
- Gestão de Vulnerabilidades
  - Tipos Vulnerabilidades x Patches
  - Gerenciamento de Patch
- Conhecendo os adversários
  - Tipos de ataques e motivações.
  - Técnicas, táticas e procedimentos (TTPs).
- Ciclo das ameaças cibernéticas
  - Cyber KillChain, MITRE ATT&CK.
- Técnicas de proteção

- *Hardening*

- Exercício Prático: Pesquisar Indicador de Compromisso (IoC) e construir uma assinatura para IPS/IDS e antivírus.
- Exercício Prático: Desenvolver *hardening* para Linux
- Exercício Prático: Desenvolver *hardening* para Windows

6. Bibliografia:

- Básica

  Palacín, Valentina. Practical Threat Intelligence and Data-Driven Threat Hunting: A hands-on guide to threat hunting with the ATT&CK™ Framework and open source tools, Packt Publishing; 1st edition, 2021.

  Troia, Vinny Hunting Cyber Criminals: A Hacker's Guide to Online Intelligence Gathering Tools and Techniques, Wiley; 1st edition, 2020.
- Complementar

  Alleyne, Nik . Learning by Practicing - Hack & Detect: Leveraging the Cyber Kill Chain for Practical Hacking and its Detection via Network Forensics. N3Security. 2018

  DunkerleyM, Mark. Mastering Windows Security and Hardening: Secure and protect your Windows environment from intruders, malware attacks, and other cyber threats, Packt, 2020.

IDENTIFICAÇÃO DO COMPONENTE CURRICULAR – 7

1. Nome do Componente Curricular: **Ethical Hacking**

2. Carga Horária: 32 horas

3. Ementa:

Ética Hacker. Fases do Testes de invasão. Técnicas de Evasão, de exploração, de movimentação lateral, de escalação de privilégios e de execução de códigos remotos. Ataques de Rede.

4. Objetivo

Capacitar o aluno a explorar as vulnerabilidades técnicas nas aplicações e infraestrutura, respeitando os princípios éticos, privacidade e legais.

5. **Conteúdo Programático**:

- Conceitos de Ética Hacker
- Reconhecimento
    - Open Source Intelligence (OSINT),
    - Engenharia Social
- Equipes de Segurança
    - RedTeam, BlueTeam, PurpleTeam
- Técnicas de evasão
- Técnicas de exploração, movimentação lateral, escalação de privilégios e execução de códigos remotos
- Exercício prático: Ataque - Falsificação ARP (ARP Spoofing)
- Exercício prático: Ataques - Falsificação de IP (IP Spoofing) e espionagem de Pacotes (Packet Sniffing).
- Exercício prático: Ataque - Sequestro de Sessão TCP (TCP Session Hijacking)

6. Bibliografia:

- **Básica**:

Georgia Weidman. Testes de Invasão: uma Introdução Prática ao Hacking. 1a edição. Novatec Editora, 2017.
Daniel Moreno. Introdução ao Pentest. 2ª edição. Novatec, 2019.
Raymond Nutting, Mirza Ahmed, William MacCormack. GPEN GIAC Certified Penetration Tester All-in-One Exam Guide. McGraw-Hill, 2020.

- **Complementar**:

Peter Kim. The Hacker Playbook 2: Practical Guide To Penetration Testing. 1st edition. CreateSpace Independent Publishing Platform, 2015
Peter Kim. The Hacker Playbook 3: Practical Guide To Penetration Testing Paperback. 1st edition. Independently published, 2018.
Michael T. Goodrich; Roberto Tamassia. Introdução à Segurança de Computadores. Bookman, 2013.

IDENTIFICAÇÃO DO COMPONENTE CURRICULAR – 8

1. Nome do Componente Curricular: **Segurança Ofensiva**

2. Carga Horária: 32h/a

3. Ementa

Identificação de Alvos. Tipos de varredura. Enumeração. Cracking de Senha. Hacking de aplicações web e de Redes sem fios. Ataques com a ferramenta Metasploit.

4. Objetivo

Habilitar o aluno para realizar ataques direcionados a determinadas infraestruturas e aplicações, dentro de um ambiente controlado e seguindo as metodologias apresentadas anteriormente.

5. Conteúdo Programático:

- Identificação de Alvos
- Varredura de portas, Evasão, Varredura de Vulnerabilidades;
- Técnicas de Enumeração
- Hacking de aplicações web
  - Injeções SQL (SQLi),
  - Scripts Cruzados entre Sites (XSS),
  - Inclusões de Arquivos Remotos (RFI)
- Hacking de Redes Sem Fio
- Exercício prático: Ataques e varreduras utilizando Nmap
- Exercício prático: CTF de Cracking de Senha
- Exercício prático: Ataques com Metasploit - ransomware, execução remota de comandos

6. Bibliografia:

- Básica:

Georgia Weidman. Testes de Invasão: uma Introdução Prática ao Hacking. 1a edição. Novatec Editora, 2017.
Daniel Moreno. Introdução ao Pentest. 2ª edição. Novatec, 2019.
Raymond Nutting, Mirza Ahmed, William MacCormack. GPEN GIAC Certified Penetration Tester All-in-One Exam Guide. McGraw-Hill, 2020.

- Complementar:

Peter Kim. The Hacker Playbook 2: Practical Guide To Penetration Testing. 1st edition. CreateSpace Independent Publishing Platform, 2015.
Peter Kim. The Hacker Playbook 3: Practical Guide To Penetration Testing Paperback. 1st edition. Independently published, 2018.
Michael T. Goodrich; Roberto Tamassia. Introdução à Segurança de Computadores. Bookman, 2013.

IDENTIFICAÇÃO DO COMPONENTE CURRICULAR - 9

1. Nome do Componente Curricular: **Implantação e Tecnologias de Segurança**

2. Carga Horária: 32 ha

3. Ementa

Tendências de tecnologias de Segurança; Estratégia de implantação e sustentação; Utilização das tecnologias de proteção

4. Objetivo

Capacitar o aluno a desenvolver estratégias, implementaras tecnologias de segurança das informações, bem como fazer a boa utilização dos recursos já existentes. Avaliar as tendências e melhores soluções de mercado.

5. Conteúdo Programático:

- Tendências de tecnologias de Segurança;
  - Cenários de tecnologias
  - Gartner (Magic Quadrant e HypeCicle)
- Estratégia de implantação e sustentação
  - Proteção do perímetro e controle de acesso
  - Proteção de aplicações, integrações e banco de dados
  - Soluções de análise comportamental
- Utilização das tecnologias de proteção
  - Retorno sobre os investimentos (ROI)
- Exercício prático: Criação de regras em firewall (pfsense e iptables)
- Exercício prático: Elaborar solução de segurança para uma empresa de acordo com orçamento
- Exercício prático: estipulado e com as prioridades do negócio.

6. Bibliografia:

- Básica:

Watts, Andrew. Firewall (The Firewall Spies Book 1), Severn River Publishing, 2021

Wilson, Yvonne. Solving Identity Management in Modern Applications: Demystifying OAuth 2.0, OpenID Connect, and SAML 2.0, Apress; 1st ed., 2019.

- Complementar:

Gilman, Evan. Zero Trust Networks: Building Secure Systems in Untrusted Networks, O′Reilly, 2017

D. Brian Roulstone, Jack J. Phillips. ROI for Technology Projects: Measuring and Delivering Value, Elsevier, 2008

IDENTIFICAÇÃO DO COMPONENTE CURRICULAR - 10

1. Nome do Componente Curricular: **Inteligência na detecção de ataques**

2. Carga Horária: 32 horas

3. Ementa

Detecção e Prevenção de Intrusão. Análise, monitoramento e correlação de eventos. Centro de Operações de Segurança (SOC) e seus tipos. Automação de processos e de indicadores.

4. Objetivo

Capacitar o aluno a desenvolver estratégias para ajustes técnicos nas ferramentas de detecção, bem como os processos para o monitoramento adequado da rede e dos negócios da empresa.

5. Conteúdo Programático

- Introdução à Detecção de Intrusão
  - Sistema de Prevenção de Intrusão (IPS) e Sistema de Detecção de Intrusão (IDS)
  - Ciclo: Coleta, detecção e análise,
  - Tipos de analista.
- Análise de eventos
  - Rede, Aplicações, banco de dados e negócios
- SOC x Business SOC
- Correlação de eventos e *tuning* de soluções
- Automação de processos e de indicadores
- Exercício prático: Detecção de ameaças em pacotes de redes (Aprofundamento da ferramenta Wireshark)
- Exercício prático: Aplicação de regras para detecção de Intrusos (ferramenta Snort)
- Exercício prático: Criação de ambiente para monitoria de eventos de deteção de ameaças (ferramentas Elastic Search e Kibana)

6. Bibliografia:

- Básica:

Don Murdoch. Blue Team Handbook: Soc, Siem, and Threat Hunting Use Cases: A Condensed Field Guide for the Security Operations Team. Createspace Independent Publishing Platform, 2018.

Chris Sanders; Jason Smith. Applied Network Security Monitoring: Collection, Detection, and Analysis. Syngress, 2013.

Richard Bejtlich. The Practice of Network Security Monitoring: Understanding Incident Detection and Response. 1st Edition. No Starch Press, 2013.

- Complementar:

Stephen Northcutt; Judy Novak. Network Intrusion Detection. 3rd Edition. Sams Publishing, 2002.

Matt Fearnow. Karen Federick, Mark Cooper, Stephen Northcutt. Intrusion Signatures and Analysis, Sams, 2001.

Sherri Davidoff; Jonathan Ham. Network Forensics: Tracking Hackers through Cyberspace. 1st Edition, Pearson, 2012.

IDENTIFICAÇÃO DO COMPONENTE CURRICULAR -11

1. Nome do Componente Curricular: **Resposta à incidentes**

2. Carga Horária: 32 horas

3. Ementa

Preparação/Adequação do CSIRT. Detecção de ameaças. Contenção. Erradicação. Recuperação do ambiente. Indicadores e Lições aprendidas.

4. Objetivo

Apresentar aos alunos os conceitos e tecnologias necessárias para o tratamento e respostas à incidentes de Segurança da Informação garantindo dessa forma a resiliência adequada aos negócios.

5. Conteúdo Programático:

- Preparação/Adequação do CSIRT
    - Categorização e priorizações
    - Incidentes de Privacidades
    - Estratégia de um CSIRTs
- Detecção de ameaças
    - Evento de arquivos de Logs
    - Coleta de evidências
    - SIEM
- Contenção
    - Análise dinâmica, Análise Estática, Depuração, Codificação de Dados
    - SandBoxing
- Erradicação
    - Remoção de ameaças

- Movimentação lateral
- Recuperação do ambiente
  - Testar, monitorar e validar sistemas
  - Tomada de decisões
- Indicadores e Lições aprendidas
  - Automação de processos e indicadores
  - Conscientização

Laboratório: Análise de ameaças utilizando ferramentas de Sandboxing (ferramentas any.run)

- Exercício prático: Elaboração de um processo de resposta à incidentes
- Exercício prático: Análise de memória (Ferramenta Mandiant Redline)

6. Bibliografia:

- Básica:

N. K. McCarthy. Resposta a Incidentes de Segurança em Computadores: Planos para Proteção de Informação em Risco. Bookman, 2014.
Gerard Johansen. Digital Forensics and Incident Response: A practical guide to deploying digital forensic techniques in response to cyber security incidents. Packt Publishing, 2017.

7. Complementar:

Gerard Johansen. Digital Forensics and Incident Response: A practical guide to deploying digital forensic techniques in response to cyber security incidents. Packt Publishing, 2017.
Cory Altheide; Harlan Carvey. Digital Forensics with Open Source Tools. 1st Edition, Syngress, 2011.
Steve Anson. Applied Incident Response. 1st Edition. Wiley, 2020.

IDENTIFICAÇÃO DO COMPONENTE CURRICULAR - 12

1. Nome do Componente Curricular: **Análise Forense**

2. Carga Horária: 32h

3. Ementa

Conceito de computação forense. Análise de arquivos e artefatos de Internet. Engenharia Reversa. Elaboração do laudo.

4. Objetivo:

Apresentar e habilitar o aluno para os principais conceitos e procedimentos para coleta e exame de evidências digitais, reconstrução de dados e ataques, identificação e rastreamento de invasores.

5. Conteúdo Programático:

- Conceito de computação forense,
  - Perícia, preservação de evidências e provas digitais
  - Volatilidade de evidências e coleta de dados em um sistema em execução
- Análise
  - Engenharia reversa de códigos maliciosos
  - Reconstrução da linha temporal dos eventos
  - Análise de arquivos: imagens, documento, esteganografia
  - Análise artefatos de Internet: análise de e-mail, rede interna, nuvem
- Elaboração do laudo.
- Exercício prático: Análise de arquivo malicioso (ferramentas: winhex, process monitor).
- Exercício prático: Engenharia reversa de phishing.
- Exercício prático: Análise Forense de Imagens (ferramentas: Caine, Autopsy, Deft Linux ou SIFT)

6. Bibliografia:

- Básica:

Pedro Monteiro da Silva Eleutério, Marcio Pereira Machado. Desvendando a Computação Forense. Novatec, 2011.

Nihad A. Hassan. Perícia forense digital: Guia prático com uso do sistema operacional Windows. Novatec, 2019.

Cory Altheide; Harlan Carvey. Digital Forensics with Open Source Tools. 1st Edition, Syngress, 2011.

- Complementar:

Jesus Antonio Velho. Tratado de Computação Forense. Millennium, 2016.

Gerard Johansen. Digital Forensics and Incident Response: A practical guide to deploying digital forensic techniques in response to cyber security incidents. Packt Publishing, 2017.

Michael Sikorski e Andrew Honig. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. 1st Edition. No Starch Press, 2012.

William Oettinger. Learn Computer Forensics: A beginner's guide to searching, analyzing, and securing digital evidence. Packt Publishing, 2020.

Jason T. Luttgens et al. Incident Response & Computer Forensics. 3rd Edition. McGraw-Hill Education, 2014.

IDENTIFICAÇÃO DO COMPONENTE CURRICULAR - 13

1. Nome do Componente Curricular: **Aplicação de Conhecimento**

2. Carga Horária: 48 horas/aula na modalidade EAD

3. Ementa

A disciplina promove o desenvolvimento do Trabalho de Aplicação de Conhecimento, com base no método prático e aplicado, o qual direciona o aluno para a resolução de um desafio ou problema real vivenciado em um contexto institucional/pessoal, utilizando os conceitos e práticas abordados ao longo do curso.

4. Objetivo

Capacitar o participante para investigar, analisar e compreender as causas e as implicações dos desafios em um contexto institucional/pessoal; e com base no diagnóstico e na pesquisa bibliográfica, propor soluções e ações detalhadas, visando à resolução de problemas ou oportunidades reais e pontuais enfrentadas nesse contexto institucional/pessoal.

5. Conteúdo Programático:

- Definição do problema/oportunidade/desafio a ser resolvido;
- Descrição das características gerais do contexto institucional/pessoal;
- Diagnóstico das origens e implicações do desafio a ser resolvido;
- Pesquisa bibliográfica sobre os temas relacionados com o desafio do contexto institucional/pessoal;
- Proposição de soluções e ações detalhadas para a resolução do desafio.

6. Bibliografia

- Básica:

MARCONI, Marina de Andrade. Fundamentos de metodologia científica. 8. Rio de Janeiro Atlas 2017 1 recurso online

MARCONI, Marina de Andrade. Técnicas de pesquisa. 8. Rio de Janeiro Atlas 2017

YIN, Robert K. Estudo de caso: planejamento e métodos. 5. Porto Alegre Bookman 2015

GIL, Antonio Carlos. Estudo de caso: fundamentação científica; subsídios para coleta e análise de dados; como redigir o relatório. São Paulo Atlas 2009.

- Complementar:

GIL, Antonio Carlos. Como elaborar projetos de pesquisa. 6. Rio de Janeiro Atlas 2017

FLICK, Uwe. Introdução à pesquisa qualitativa. 3. Porto Alegre ArtMed 2008

MATTAR, João. Metodologia científica na era digital. 4. São Paulo Saraiva 2017

FACHIN, Odília. Fundamentos de metodologia. 6. São Paulo Saraiva 2017

SILVA, Anielson Barbosa da. Pesquisa qualitativa em estudos organizacionais: paradigmas, estratégias e métodos. 2. São Paulo Saraiva 2011.

THIOLLENT, Michel. Metodologia da pesquisa-ação. 10. ed. São Paulo: Cortez, 2000.

SEVERINO, Antonio Joaquim. Metodologia do trabalho científico. 24. ed. rev. e atual. São Paulo: Cortez, 2017. 317 p. ISBN 9788524924484.