MBA em Segurança da Informação e Resiliência Digital

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**

DISCIPLINA 01

Nome da Disciplina: **Segurança Digital nas Organizações**

Carga Horária: 32 h/aula

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.

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.

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

DISCIPLINA 02

Nome da Disciplina: **Conformidade e Controles**

Carga Horária: 32 h/aula

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.

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.

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

DISCIPLINA 03

Nome da Disciplina: **Continuidade de Negócios**

Carga Horária: 32 h/aula

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

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.

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.

DISCIPLINA 04

Nome da Disciplina: **Arquitetura e Projetos Digitais**

Carga Horária: 32 h/aula

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

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.

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)

DISCIPLINA 05

Nome da Disciplina: **Desenvolvimento Seguro**

Carga Horária: 32 h/aula

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).

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.

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)

DISCIPLINA 06

Nome da Disciplina: **Inteligência de Ameaças**

Carga Horária: 32 h/aula

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

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.

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
-

DISCIPLINA 07

Nome da Disciplina: **Ethical Hacking**

Carga Horária: 32 h/aula

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.

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

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)

DISCIPLINA 08

Nome da Disciplina: **Segurança Ofensiva**

Carga Horária: 32 h/aula

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.

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

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

DISCIPLINA 09

Nome da Disciplina: **Implantação e Tecnologias de Segurança**

Carga Horária: 32 h/aula

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

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.

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.

DISCIPLINA 10

Nome da Disciplina: **Inteligência na detecção de ataques**

Carga Horária: 32 h/aula

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.

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.

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)

DISCIPLINA 11

Nome da Disciplina: **Resposta à incidentes**

Carga Horária: 32 h/aula

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

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.

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)

DISCIPLINA 12

Nome da Disciplina: **Análise Forense**

Carga Horária: 32 h/aula

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

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.

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)

DISCIPLINA 13

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

Carga Horária: 48 horas/aula na modalidade EAD

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.

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.

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.