ESCOLA DO FUTURO

PLANO DE ENSINO

1. IDENTIFICAÇÃO DO CURSO

NOME DO CURSO		QTP3 Cibersegurança *Como terceiro componente da Habilitação Profissional Técnica em Desenvolvimento Web e Cibersegurança*	
MODALIDADE		Concomitante Intercomplementar ao Ensino Médio Integral	
CATEGORIA		Presencial	
EIXO TECNOLÓGICO		Informação e Comunicação	
COMPONENTE CURRICULAR		Cibersegurança	
DATA INÍCIO	19/01/2026	**DATA FIM**	18/12/2026
CARGA HORÁRIA		120h (120 aulas de 60 minutos)	

2. PLANO DE ENSINO

EMENTA:

Fundamentos da Segurança da Informação e a Tríade CIA (Confidencialidade, Integridade e Disponibilidade). Governança, Risco e Compliance (**White Team**): Ética Hacker, Legislação vigente (LGPD, Marco Civil), Normas ISO 27001 e elaboração de Políticas de Segurança. Segurança Defensiva (**Blue Team**): Arquitetura de segurança em profundidade, *Hardening* (endurecimento) de Sistemas Operacionais Linux e Windows, configuração de Firewalls, IDS/IPS, Criptografia aplicada (PKI), Backup e Recuperação de Desastres. Segurança Ofensiva (**Red Team**): Metodologias de Teste de Intrusão (Pentest), Inteligência de Fontes Abertas (OSINT), Varredura de Vulnerabilidades, Exploração de Redes e Aplicações Web (OWASP Top 10). Ameaças Avançadas (**Black Team**): Engenharia Social, Phishing, Análise de Malware e Segurança Física. Operações Integradas (**Purple Team**): Monitoramento de Logs (SIEM), Forense Computacional, Resposta a Incidentes

UFG UNIVERSIDADE FEDERAL DE GOIÁS

ESCOLA DO FUTURO

OBJETIVOS:

- Compreender a Cibersegurança não apenas como tecnologia, mas como um ecossistema que envolve pessoas, processos e leis, internalizando a ética profissional (*White Hat*) e a responsabilidade social ;
- Desenvolver a capacidade de trabalhar em equipes multidisciplinares (Squads), aplicando metodologias ágeis (Scrum) para planejar, executar e revisar ciclos de defesa e ataque ;
- Promover a comunicação assertiva e a capacidade de traduzir riscos técnicos complexos em linguagem de negócios para tomadores de decisão (Diretoria/Stakeholders) através de *Pitches* e relatórios executivos ;
- Demonstrar autonomia e criatividade na resolução de incidentes críticos sob pressão, simulando o ambiente real de um Centro de Operações de Segurança (SOC);
- Elaborar e Implementar Políticas de Segurança da Informação (PSI) e Planos de Continuidade de Negócios (PCN), alinhados a normas internacionais (ISO 27001) e legislação vigente (LGPD);
- Realizar a classificação de ativos de informação e mapeamento de riscos, criando Matrizes de Risco (Probabilidade x Impacto) para priorizar investimentos em defesa;
- Auditar processos e configurações técnicas realizadas pelos outros times, garantindo a conformidade com *checklists* de segurança (ex: CIS Benchmarks) e documentação técnica detalhada ;
- Projetar e Configurar arquiteturas de rede seguras, implementando segmentação (VLANs/DMZ), Firewalls (Iptables/Windows) e controles de acesso rigorosos baseados no princípio do menor privilégio;
- Executar o *Hardening* (endurecimento) avançado em Sistemas Operacionais Linux e Windows, desabilitando serviços desnecessários, configurando auditoria de logs e aplicando *patches* de segurança ;
- Implementar sistemas de monitoramento contínuo e detecção de intrusão (IDS/IPS e SIEM), criando regras de correlação para identificar anomalias de tráfego e comportamento de usuário ;
- Responder a incidentes de segurança seguindo protocolos padronizados (NIST/SANS), realizando a contenção, erradicação da ameaça e recuperação dos serviços com o menor *downtime* possível;
- Configurar mecanismos de criptografia para dados em repouso e em trânsito (VPNs, PKI, HTTPS), garantindo a confidencialidade e integridade das informações .

UFG UNIVERSIDADE FEDERAL DE GOIÁS

ESCOLA DO FUTURO

COMPETÊNCIA:

1. Defesa Cibernética e Operações de Segurança (Blue Team):

- **Projetar e blindar** infraestruturas de TI, implementando técnicas avançadas de *Hardening* em sistemas operacionais e configurando perímetros de rede seguros (Firewalls, VPNs, DMZ);
- **Monitorar e Responder** a incidentes em tempo real, operando centros de comando (SIEM) para detectar intrusões, conter ameaças e recuperar serviços críticos com agilidade.

2. Segurança Ofensiva e Análise de Vulnerabilidades (Red Team):

- **Executar testes de intrusão (*Pentest*)** completos, utilizando metodologias éticas e ferramentas de mercado (Kali Linux, Metasploit) para explorar falhas em redes e aplicações Web (OWASP Top 10);
- **Mapear superfícies de ataque** através de técnicas de Inteligência de Fontes Abertas (*OSINT*) e varreduras de vulnerabilidade, identificando portas de entrada antes de adversários reais.

3. Governança, Risco e Conformidade (White Team):

- **Elaborar e gerenciar** Políticas de Segurança da Informação (PSI) e matrizes de risco, alinhando as práticas técnicas às normas internacionais (ISO 27001) e à legislação vigente (LGPD);
- **Auditar** processos e configurações, garantindo que as estratégias de defesa estejam em conformidade com os requisitos de negócio e privacidade de dados.

4. Inteligência de Ameaças e Fator Humano (Black/Purple Team):

- **Analisar táticas adversárias**, incluindo o comportamento de *malwares* e campanhas de Engenharia Social (*Phishing*), para desenvolver contramedidas proativas;
- **Integrar defesa e ataque** (*Purple Teaming*), utilizando o conhecimento ofensivo para aprimorar continuamente as regras de detecção e a cultura de segurança da organização.

METODOLOGIA DA APRENDIZAGEM:

Durante as aulas, o professor utilizará diversas metodologias para garantir o máximo aprendizado de todos os alunos. As explicações teóricas serão acompanhadas de atividades participativas, como rodas de conversa e debates, permitindo que os alunos tirem dúvidas e contribuam com suas próprias experiências culturais.
Os alunos serão incentivados a participar ativamente, através de projetos, trabalhos em grupo e jogos, promovendo um ambiente de aprendizado colaborativo e

UFG UNIVERSIDADE FEDERAL DE GOIÁS

dinâmico. A ideia é envolver os alunos de forma integral na construção do conhecimento e no desenvolvimento de suas habilidades.

Aulas Expositivas: Serão realizadas apresentações dos conteúdos de forma clara e objetiva, utilizando recursos visuais como slides e vídeos para facilitar a compreensão dos temas abordados.

Atividades Práticas: Serão propostas atividades práticas individuais e em grupo, como estudos de casos, simulações e resolução de problemas, que permitam aos alunos aplicar os conceitos teóricos na prática e desenvolver habilidades práticas relacionadas à prática profissional.

Discussões Dirigidas: Serão promovidas discussões em sala de aula sobre casos reais e situações do cotidiano profissional, incentivando os alunos a compartilharem suas experiências e pontos de vista, e estimulando o debate e a reflexão crítica.

Estudos de Caso: Serão apresentados casos práticos relacionados aos conteúdos abordados, para que os alunos possam analisar, interpretar e propor soluções, desenvolvendo assim habilidades de análise crítica e tomada de decisão.

Feedback Construtivo: Serão fornecidos feedbacks individualizados aos alunos, tanto durante as atividades em sala de aula quanto nas avaliações, com o objetivo de identificar pontos fortes e áreas de melhoria, e promover o desenvolvimento contínuo do aprendizado.

Metodologias Ativas: Serão utilizadas metodologias que coloquem o aluno como protagonista do seu próprio aprendizado, como aprendizagem baseada em problemas, aprendizagem colaborativa e aprendizagem baseada em projetos, promovendo assim a autonomia e o engajamento dos estudantes.

Tecnologias Educacionais: Serão exploradas ferramentas e recursos tecnológicos, como plataformas de ensino online, aplicativos educacionais e ambientes virtuais de aprendizagem, para enriquecer as atividades de ensino e oferecer diferentes formas de acesso ao conteúdo.

CONTEÚDOS PROGRAMÁTICOS:

1. Fundamentos e Governança (White Team)

- Tríade CIA (Confidencialidade, Integridade, Disponibilidade);
- Legislação (LGPD, Crimes Cibernéticos) e Ética Hacker;
- Gestão de Riscos, Normas ISO 27001 e Políticas de Segurança.

2. Defesa e Infraestrutura Segura (Blue Team)

- Virtualização e Laboratórios Seguros;
- *Hardening* de Sistemas Operacionais (Linux/Windows);
- Criptografia Aplicada (PKI/Hash) e Backup;

2: Arquitetura Defensiva e Hardening

Foco: Blindagem de infraestrutura e proteção de dados.

- **Segurança de Redes e Perímetro:**
  - **Arquitetura:** Zonas de Segurança, DMZ (Bastion Hosts), VLANs (Segmentação L2) e Microsegmentação.
  - **Firewalls:** Filtragem de Pacotes (Stateless), Inspeção de Estado (Stateful), Proxies e Next-Gen Firewalls (Conceitos).
  - **Prática de Firewall:** Configuração de cadeias INPUT/OUTPUT/FORWARD no iptables e regras de entrada/saída no Windows Defender Firewall.
  - **Acesso Remoto Seguro:** VPNs (IPSec vs SSL/TLS), Túneis SSH e Zero Trust Network Access (Intro).
- **Hardening de Sistemas Operacionais (Linux):**
  - **Gestão de Acesso:** Usuários, Grupos, Permissões especiais (SUID, SGID, Sticky Bit) e sudoers.
  - **Serviços e Rede:** Desativação de serviços xinetd/inetd, proteção da pilha TCP/IP (sysctl.conf).
  - **SSH Hardening:** Desabilitar root login, uso de chaves RSA/Ed25519, AllowUsers, Banner Grabbing.
  - **Auditoria:** Configuração do auditd para monitorar chamadas de sistema e alterações em arquivos críticos.
- **Hardening de Sistemas Operacionais (Windows Server):**
  - **Políticas de Grupo (GPO):** Configuração de políticas de senha, bloqueio de conta e direitos de usuário.
  - **Controles de Acesso:** UAC (User Account Control), LAPS (Local Administrator Password Solution) e BitLocker.
  - **Monitoramento:** Event Viewer (Security, System, Application) e Sysmon (System Monitor) da Sysinternals.
- **Criptografia Aplicada:**
  - **Algoritmos:** Simétricos (AES, ChaCha20), Assimétricos (RSA, ECC) e Hashing (SHA-256, bcrypt, argon2).
  - **PKI (Infraestrutura de Chaves Públicas):** Autoridades Certificadoras (CA), CSR, emissão e revogação (CRL/OCSP) de Certificados Digitais (X.509).

ESCOLA DO FUTURO

RECURSOS DIDÁTICOS:

- **Hardware:** Laboratório de informática com computadores e acesso à internet.
- **Software:** VirtualBox/VMware, Kali Linux, Metasploitable, Windows Server (Trial), VS Code, Wireshark, Burp Suite.
- **Plataformas de Apoio:** Ambientes de treino como TryHackMe, HackTheBox ou PortSwigger Academy.
- **Ferramentas de Apoio:** Datashow, Quadro Branco para desenho de vetores de ataque.

CRITÉRIOS DE AVALIAÇÃO:

1. Avaliação Diagnóstica

- Realizada no início do curso e Sprints. Instrumentos: Quizzes sobre redes/Linux e levantamento de conhecimentos prévios .

2. Avaliação Formativa

- Realizada continuamente.
- **Qualitativa:** Participação nas cerimônias Scrum e colaboração nas Squads de defesa/ataque.
- **Quantitativa:** Entrega dos Laboratórios Práticos (*Labs*) e progresso nos CTFs.

3. Avaliação Somativa

- Realizada ao final dos ciclos.
- **Provas Teóricas/Práticas:** Testes sobre conceitos de segurança e desafios práticos (*flags*).
- **Projeto Integrador:** Avaliação da infraestrutura segura ou do relatório de pentest entregue.
- **Pitch Final:** Avaliação da apresentação oral e defesa técnica no *War Game*.

UFG UNIVERSIDADE FEDERAL DE GOIÁS

ESCOLA DO FUTURO

1º Bimestre (30 Aulas)

- **Aula 01:** Apresentação da Ementa e Formação das Squads (Color Teams).
- **Aula 02:** Dinâmica: O Cenário de Guerra Cibernética e regras de engajamento.
- **Aula 03:** Tríade CIA, Autenticidade e Não-Repúdio.
- **Aula 04:** Legislação: Crimes Cibernéticos e LGPD na prática.
- **Aula 05:** Governança: Normas ISO 27001 e Políticas de Segurança (PSI).
- **Aula 06:** Gestão de Riscos: Matriz de Risco e Classificação de Ativos.
- **Aula 07:** Lab: Setup do Laboratório (VirtualBox, Kali, Alvos).
- **Aula 08:** Linux Hardening I: Permissões (chmod/suid) e Usuários.
- **Aula 09:** Linux Hardening II: Proteção SSH e Auditoria (auditd).
- **Aula 10:** Windows Hardening I: Contas, Grupos e UAC.
- **Aula 11:** Windows Hardening II: Políticas de Grupo (GPO) locais.
- **Aula 12:** Windows Hardening III: Logs de Eventos e Sysmon.
- **Aula 13:** Lab: Aplicando Checklist CIS Benchmark em servidores.
- **Aula 14:** Criptografia I: Simétrica, Assimétrica e Hashing.
- **Aula 15:** Criptografia II: PKI, Certificados Digitais e HTTPS.
- **Aula 16:** Lab: Uso de GPG e Veracrypt.
- **Aula 17:** Redes Seguras: DMZ, VLANs e Segmentação.
- **Aula 18:** Firewalls I: Teoria (Packet Filter, Stateful, Proxy).
- **Aula 19:** Lab Firewall: Configurando iptables e UFW.
- **Aula 20:** Lab Firewall: Windows Firewall com Segurança Avançada.
- **Aula 21:** Backup e Recuperação: Estratégia 3-2-1.
- **Aula 22:** Lab Backup: Scripts de automação de backup.
- **Aula 23:** Auditoria Cruzada: Squad A audita Squad B.
- **Aula 24:** Relatórios: Documentação de Conformidade Técnica.
- **Aula 25:** Revisão Geral da Sprint I (Governança e Hardening).
- **Aula 26:** Estudo de Caso: Análise de incidentes por falha de configuração.
- **Aula 27:** Lab Extra: Reforço em Linux/Windows CLI.
- **Aula 28:** Sprint Review I: Apresentação da Infraestrutura Segura.
- **Aula 29:** Avaliação Somativa 1 (Teórica): Fundamentos e Defesa.
- **Aula 30: Feedback e Fechamento do 1º Bimestre.**

2º BIMESTRE (30 Aulas)

- **Aula 31:** Compute na Nuvem: O serviço EC2 (Instâncias Virtuais).
- **Aula 32:** Famílias de Instâncias: General Purpose vs Compute Optimized.
- **Aula 33: Lab:** Launch Instance (Subindo o primeiro servidor Linux na Nuvem).
- **Aula 34:** Acesso Seguro: Criação e gerenciamento de Key Pairs (.pem/.ppk).
- **Aula 35:** Conexão Remota na Nuvem: Acessando a instância via terminal.
- **Aula 36:** VPC (Virtual Private Cloud): O conceito de isolamento lógico.
- **Aula 37:** Endereçamento IP na Nuvem: Blocos CIDR.
- **Aula 38:** Subnets: Diferença prática entre Subnet Pública e Privada.
- **Aula 39:** Roteamento: Internet Gateway (IGW) e Route Tables

UFG UNIVERSIDADE FEDERAL DE GOIÁS

ESCOLA DO FUTURO

- **Aula 40: Lab:** Criando uma VPC personalizada "do zero" (Manual).
- **Aula 41:** Firewalls de Nuvem I: Security Groups (Stateful).
- **Aula 42:** Firewalls de Nuvem II: NACLs (Stateless).
- **Aula 43: Lab:** Configurando Security Groups para liberar Web e SSH.
- **Aula 44:** Armazenamento de Bloco (EBS): Tipos de volume e IOPS.
- **Aula 45: Lab:** Criando, anexando e formatando um disco EBS extra no Linux.
- **Aula 46:** Armazenamento de Objetos (S3): Conceito de Buckets.
- **Aula 47:** S3 Features: Classes de armazenamento (Tiering) e Custos.
- **Aula 48: Lab:** Hospedagem de Site Estático no S3 (Bucket Policy).
- **Aula 49:** Endereçamento Público: Elastic IP (EIP) vs IP Dinâmico.
- **Aula 50:** Automação: User Data (Scripts de inicialização automática).
- **Aula 51: Lab Sprint II:** Provisionar instância já com site instalado via script.
- **Aula 52:** Monitoramento Básico: Métricas do CloudWatch (CPU, Disco) .
- **Aula 53:** Troubleshooting: Diagnóstico de falhas de conexão (Ping/Telnet).
- **Aula 54:** Análise de Logs: Verificando /var/log/syslog e logs do Nginx.
- **Aula 55:** Planejamento da Migração: Desenhando a arquitetura da Startup na nuvem.
- **Aula 56: Sprint Review II:** Demonstração da VPC e Instância na nuvem.
- **Aula 57:** Revisão Prática de IaaS e Redes.
- **Aula 58: Avaliação Somativa 2 (Prática):** Desafio de Infraestrutura .
- **Aula 59:** Correção da Avaliação e Feedback Individual.
- **Aula 60:** Fechamento do 2º Bimestre.

3º BIMESTRE (30 Aulas)

- **Aula 61:** Banco de Dados: IaaS (DB na VM) vs PaaS (Gerenciado).
- **Aula 62:** Bancos Relacionais (RDS): Conceitos e setup de MySQL/Postgres .
- **Aula 63:** Bancos NoSQL: Introdução ao DynamoDB.
- **Aula 64: Lab:** Conectando Aplicação EC2 ao RDS (Security Groups cruzados).
- **Aula 65:** Alta Disponibilidade: Multi-AZ e Redundância.
- **Aula 66:** Escalabilidade: Vertical (Scale Up) vs Horizontal (Scale Out).
- **Aula 67:** Load Balancer (ELB): Distribuindo tráfego entre instâncias.
- **Aula 68:** Componentes ELB: Target Groups e Listeners.
- **Aula 69:** Health Checks: Como o ELB sabe quem está "vivo".
- **Aula 70:** Auto Scaling Groups (ASG): O que são Launch Templates.
- **Aula 71:** Políticas de Escalonamento: Escalar por % de CPU ou Rede.
- **Aula 72:** Lab: Configuração de Load Balancer + Auto Scaling.
- **Aula 73:** Lab: Teste de Stress (Gerar carga para ver novas VMs surgindo).
- **Aula 74:** Introdução aos Containers: O problema da compatibilidade.
- **Aula 75:** Docker vs Máquinas Virtuais: Arquitetura.
- **Aula 76:** Lab: Instalação do Docker e comandos básicos (run, ps).
- **Aula 77:** Imagens Docker: Docker Hub e Versionamento (Tags).
- **Aula 78:** Dockerfile: Criando imagens personalizadas (FROM, RUN).
- **Aula 79:** Lab: Containerizando a aplicação da Startup.
- **Aula 80:** Persistência em Docker: Volumes e Bind Mounts.
- **Aula 81:** Redes no Docker: Bridge e comunicação entre containers.
- **Aula 82:** Orquestração Local: Docker Compose.

UFG UNIVERSIDADE FEDERAL DE GOIÁS

- **Aula 83:** Containers na Nuvem: ECR (Registry) e upload de imagens.
- **Aula 84:** Introdução Teórica: Kubernetes (K8s) e ECS.
- **Aula 85:** Desacoplamento: Filas (SQS) e Notificações (SNS).
- **Aula 86:** Performance: CDNs (CloudFront) e Cache.
- **Aula 87:** Sprint Review III: Apresentação da arquitetura elástica/container.
- **Aula 88:** Revisão de Escalabilidade e Docker.
- **Aula 89:** Avaliação Somativa 3 (Teórico-Prática): Cenários de arquitetura .
- **Aula 90:** Feedback e Fechamento do 3º Bimestre.

4º BIMESTRE (30 Aulas)

- **Aula 91:** Identidade e Acesso: O serviço IAM.
- **Aula 92:** IAM: Usuários, Grupos e Políticas (JSON) .
- **Aula 93:** IAM Roles: Permissões para serviços (EC2 acessando S3).
- **Aula 94: Lab:** Configurando uma Role de segurança na prática.
- **Aula 95:** Computação Serverless: O que é FaaS (Lambda/Functions).
- **Aula 96:** Serverless: Gatilhos (Triggers) e Eventos.
- **Aula 97: Lab:** Criando função Lambda para processamento simples.
- **Aula 98:** DevOps: Conceitos de CI/CD (Integração Contínua).
- **Aula 99:** Infraestrutura como Código (IaC): Terraform e CloudFormation.
- **Aula 100: Lab:** Leitura e execução de script IaC básico.
- **Aula 101:** FinOps: Gerenciamento de Custos na Nuvem.
- **Aula 102:** Ferramentas: Calculadoras (TCO) e Budgets.
- **Aula 103:** Modelo de Responsabilidade Compartilhada e Compliance.
- **Aula 104:** Auditoria e Logs: CloudTrail.
- **Aula 105: Início da Sprint Final:** Planejamento da entrega.
- **Aula 106:** Refatoração: Melhorando a segurança do projeto (HTTPS/Encryption).
- **Aula 107:** Documentação Técnica: Desenhando a topologia final (Draw.io).
- **Aula 108:** Documentação de Usuário: Guia de instalação/deploy.
- **Aula 109:** Testes Finais de integração na infraestrutura.
- **Aula 110:** O Pitch: Como "vender" o projeto tecnicamente.
- **Aula 111:** Estruturação da Apresentação: Storytelling do problema/solução.
- **Aula 112 e 113:** Pré-Banca: Apresentação de ensaio (Grupo A e Grupo B).
- **Aula 114:** Feedback dos ensaios e ajustes finais.
- **Aula 115:** Congelamento do ambiente (ninguém mexe mais no código).
- **Aula 116 e 117: APRESENTAÇÃO FINAL:** Banca Avaliadora .
- **Aula 118:** Análise Crítica: Discussão sobre desafios e lições aprendidas .
- **Aula 119:** Orientação de Carreira: Certificações (Cloud Practitioner) e Mercado.
- **Aula 120:** Fechamento de Notas e Encerramento do Ano Letivo.

REFERÊNCIAS

ESCOLA DO FUTURO

Bibliografia Básica:

- SILVA, E. **Computação em Nuvem: Conceitos, Tecnologias e Tendências.** Editora Erica, 2018.
- GABRIEL, F. **Dominando a AWS: Do Zero à Certificação.** Casa do Código.
- TURATI, A. **Descomplicando o Docker.** Brasil, 2019.
- VERAS, M. **Virtualização: Componente Central do Datacenter.** Brasport.
- DOCUMENTAÇÃO OFICIAL: AWS Documentation (aws.amazon.com/documentation), Microsoft Learn (learn.microsoft.com).

Bibliografia Complementar:

- KIM, Gene; BEHR, Kevin; SPAFFORD, George. **O Projeto Fênix: Um romance sobre TI, DevOps e a ajuda ao seu negócio.** Alta Books.
- MATOS, A. **Segurança em Nuvem: Guia Prático.** Novatec.
- MAGALHÃES, I. **Engenharia de Software na Nuvem.** Editora Santos.
- TAURION, Cezar. **Cloud Computing: Computação em Nuvem.** Brasport.
- RIGBY, Darrell; ELK, Sarah; BEREZ, Steve. **Ágil do Jeito Certo: transformação sem caos.** Editora Benvirá, 2020 .

UFG UNIVERSIDADE FEDERAL DE GOIÁS