

PÓS-GRADUAÇÃO EAD

CURSO DE ESPECIALIZAÇÃO EM

SEGURANÇA CIBERNÉTICA

Defesa, auditoria e gestão da segurança da informação em
ambientes corporativos e institucionais.





APRESENTAÇÃO DO CURSO

O Curso de Especialização em Segurança Cibernética tem como objetivo capacitar profissionais para atuar em defesa, auditoria e gestão da segurança da informação em ambientes corporativos e institucionais, formando especialistas preparados para lidar com as ameaças digitais modernas.

360h

CARGA HORÁRIA

13

DISCIPLINAS

EAD

MODALIDADE

MÓDULO 1

FUNDAMENTOS PARA SEGURANÇA CIBERNÉTICA

180h

01 SEGURANÇA DA INFORMAÇÃO — INTRODUÇÃO, NORMAS E PADRÕES

30h

PROGRAMA

Visão Geral da Segurança da Informação: Leis, normas e padrões de segurança da informação; Proteção da Informação; Papéis e Responsabilidades; Classificação da Informação; Políticas e Procedimentos. Normas e Padronização. Principais Normas de Segurança; Certificação de Segurança da Informação; NBR ISO/IEC 27001:2006; Processo de Certificação; Processo de Implantação; Objetivos de Controles; Controles.

BIBLIOGRAFIA

1. Information Security Policies, Procedures and Standards — Guidelines for Effective Information Security Management. Thomas R. Peltier — Auerbach.
2. A Norma ABNT NBR ISO/IEC 27001:2006. Autores: Roberto M. Lautert, Tulio A. de Souza. Orientador: Anderson O. da Silva — DI/CCE PUC-Rio.
3. ABNT NBR ISO/IEC 27001:2006 — Tecnologia da informação — Técnicas de segurança.
4. Sistemas de gestão de segurança da informação — Requisitos, ABNT.
5. ABNT NBR ISO/IEC 17799:2005 — Tecnologia da informação — Técnicas de segurança.
6. Código de prática para a gestão da segurança da informação, ABNT.



PROGRAMA

Terminologia e protocolos das redes. Redes locais. O modelo OSI. Meios de comunicação. O modelo TCP/IP: Camada de aplicação, transporte, rede e inter rede. Ativos: Repetidor, switch, roteadores. Programação de roteadores. Tecnologias de redes LAN e padrões de redes. Conceitos de cabeamento estruturado. Norma EIA/TIA. Acessórios para redes de cabos UTP e equipamentos. Configuração básica de roteadores, configuração da interface fast ethernet, configuração da interface serial, configuração de roteamento estático, configuração de roteamento estático com default, configuração com os protocolos de roteamento dinâmico: RIP, RIPv2, OSPF, EIGRP. Configuração de vlan em switch, configuração de tecnologias de interface WAN: ppp, hdlc e frame relay, configuração de NAT, SSH, Telnet, DHCP local, DHCP remoto e access-list em roteadores.

BIBLIOGRAFIA

1. COMER, D. Interligação em redes com TCP/IP. Campus, 2015.
2. TANENBAUM, A. Redes de computadores. Pearson, 2011.
3. FARREL, A. A internet e seus protocolos: Uma análise comparativa. Campus, 2005.
4. TORRES, G. Redes de computadores: Curso completo. Axel Books, 2001.
5. CARVALHO, T.; et. al. Arquitetura de redes de computadores OSI e TCP/IP. Makron, 1994.

03 CONCEITOS DE LINUX

PROGRAMA

Arquitetura do Sistema. Instalação e manutenção de pacotes Linux. Comandos GNU e Unix. Devices, Linux Filesystems, Hierarquia Padrão dos Filesystem. Shell, Scripting e Gerenciamento de Dados. Interfaces e Desktops. Tarefas administrativas. Serviços Essenciais do sistema. Fundamentos de Rede. Segurança.

BIBLIOGRAFIA

1. WARD, B. Como o Linux funciona: o que todo super usuário deveria saber. Novatec, 2015.
2. NEGUS, C.; BRESNAHAN, C. Linux: A bíblia. Alta Books, 2014.
3. SILBERSCHATZ, A.; GALVIN, P.; GAGNE, G. Fundamentos de sistemas operacionais: Princípios básicos. LTC, 2013.
4. FILHO, J. Descobrindo o Linux: Entenda o sistema operacional GNU/Linux. Novatec, 2012.
5. YAGHMOUR, K. Construindo sistemas Linux embarcados. Alta Books, 2009.

PROGRAMA

Introdução: tendências, arquiteturas, ataques, serviços, ferramentas, modelos e mecanismos de segurança e defesa de ataques em redes de computadores; Criptografia: técnicas clássicas, hash, assinaturas digitais e protocolos. VPN: segurança TCP/IP, WEB, protocolos de autenticação. Segurança lógica. Introdução aos firewalls: princípios e projetos de firewall.

BIBLIOGRAFIA

1. STALLINGS, William. Criptografia e segurança de redes: princípios e práticas. 6. ed. São Paulo, SP: Pearson Prentice Hall, 2008. xvii, 492 p. ISBN 9788576051190.
2. MORAES, Alexandre F. Segurança em Redes — Fundamentos. 1. ed. São Paulo: Erica, 2010. ISBN 9788536503257.
3. COMER, Douglas E. Redes de computadores e Internet: abrange transmissão de dados, ligações inter-redes, web e aplicações. 4. ed. Porto Alegre: Bookman, 2007.
4. COMER, D. Interligação em redes com TCP/IP. Campus, 2015.
5. TANENBAUM, A. Redes de computadores. Pearson, 2011.

05 **DIREITO DIGITAL****PROGRAMA**

Introdução à regulamentação da internet. Marco Civil da Internet e a proteção geral de dados. Teoria geral dos contratos aplicada ao marketing digital. Comércio eletrônico e direitos do consumidor. Direitos autorais e direitos conexos aos de autor. Proteção legal de marcas e de outros sinais distintivos. Responsabilidade civil na internet. Direitos de personalidade e novas tecnologias.

BIBLIOGRAFIA

1. DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). “DIREITO & INTERNET III: MARCO CIVIL DA INTERNET — LEI Nº 12.965/2014”. São Paulo: Quartier Latin, 2015. t. I e II.
2. SOUZA, Carlos Affonso; LEMOS, Ronaldo. “MARCO CIVIL DA INTERNET: CONSTRUÇÃO E APLICAÇÃO”. Juiz de Fora: Editar, 2016. LEI Nº 12.965/2014. MARCO CIVIL DA INTERNET.
3. ROVER, Aires José (org.). Direito e Informática. SP: Manole, 2004. ROVER, Aires José (org.). Direito, Sociedade e Informática: limites e perspectivas da vida digital. Florianópolis: Fundação Boiteux, 2000.
4. PECK, Patrícia. Direito Digital. 6ª ed. 2016. Saraiva.

PROGRAMA

Estudo das técnicas e conceitos para respostas a Incidentes de segurança. Conhecimento sobre requisitos de criação, funcionamento e atividades de um Computer Security Incident Response Team (CSIRT); criar e gerenciar uma equipe de resposta a incidentes de segurança; Técnicas e ferramentas de tratamento de incidentes; Conhecimento de estudos de casos e simulações de incidentes.

BIBLIOGRAFIA

1. COMER, Douglas E. Interligação de redes com TCP/IP. Rio de Janeiro: Campus, 2006.
2. LAWRIE, B.; WILLIAM, S. Segurança de Computadores: Princípios e Práticas. Elsevier Academic, 3 de agosto de 2017.
3. MCCARTHY, N. K. Resposta a Incidentes de Segurança em Computadores – Planos para Proteção de Informação em Risco. Bookman, 2013.

07 GERENCIAMENTO DE IDENTIDADE E ACESSO

PROGRAMA

Gerenciamento de Identidades e de Acesso; Conceitos básicos; Federação de identidades; Tipos de federações; Tecnologias.

BIBLIOGRAFIA

1. SHARMAN, Raj; SMITH, Sanjukta Das; GUPTA, Manis. Digital Identity and Access Management: Technologies and Frameworks. IGI Global, 2011.
2. BENANTAR, Messaoud. Access Control Systems: Security, Identity Management and Trust Models. Springer, 2010.
3. DOS SANTOS, Alfredo Luiz. Gerenciamento de Identidades, 2007.

08 FIREWALLS, IDS E IPS

30h

PROGRAMA

Tipos de firewall; topologias e tecnologias de firewall; implementação de firewall; Proxies; Filtros de pacotes e NAT; Serviços na DMZ; Filtros avançados; Implantação de firewalls com software livre (Iptables/netfilter) e soluções proprietárias; sistemas de detecção de intrusos (IDS); sistemas de prevenção de intrusos (IPS); sistemas de detecção de intrusos em hosts (HIDS); Implementação de IDS/IPS com ferramentas livres e solução proprietárias.

BIBLIOGRAFIA

1. LARRIEU, C. Sistemas de detecção de intrusão (IDS). Disponível em: CCM — Comunidade Online.
2. MEHRA, P. A brief study and comparison of Snort and Bro Open Source Network Intrusion Detection Systems. International Journal of Advanced Research in Computer and Communication Engineering, v. 1, n. 6, p. 383-386, 2012.
3. BROWN, D. J.; SUCKOW, B.; WANG, T. A Survey of Intrusion Detection Systems. Department of Computer Science, University of California, San Diego, 2002.
4. ROUSE, Margaret. Firewall. 2014. From Secure Web gateways, from evaluation to sealed deal.
5. MORAES, Alexandre Fernandes de. Firewalls — Segurança no Controle de Acesso. Ed. Érica, 2015.

09 PENTEST — TESTE DE INTRUSÃO

30h

PROGRAMA

Introdução à segurança. Teste de invasão. Ética hacker. Levantamento de informações. Google hacking. Varreduras ativas, passivas, furtivas de rede, enumeração e ataques com engenharia social. Ignorando proteções. Atacando o sistema. Ataques envolvendo técnicas de força bruta. Trojans, backdoors, vírus e worms, vulnerabilidade em aplicações WEB. Sniffing, atacando através da rede, wireless hacking, Metasploit Framework.

BIBLIOGRAFIA

1. WEIDMAN, G. Testes de Invasão. Novatec, 1ª edição, 10 de outubro de 2014.
2. BROAD, J.; BINDNER, A. Hacking com Kali Linux: Técnicas práticas para testes de invasão. Novatec Editora, 1ª edição, 20 de junho de 2017.
3. MORENO, D. Introdução ao Pentest. Novatec, 2015.

PROGRAMA	Introdução a investigação forense. Forense em sistemas operacionais Windows e Linux. Sleuth kit – TCP. Forense em memória RAM. Forense em Linux. Forense em tráfego de rede. Análise de Mallware. Esteganografia. Forense em e-mails. Ferramentas forenses.
BIBLIOGRAFIA	1. ALTHEIDE, Core; CARVEY, Harlan. Digital Forensics with Open Source Tools. Editora Syngress, 2011. 2. MELO, Sandro. Computação Forense com Software Livre. Rio de Janeiro: Alta Books, 2009. 1ª edição. 3. FARMER, Dan; VENEMA, Wietse. Perícia Forense Computacional: Teoria e Prática Aplicada. Prentice Hall, 2007. 4. SHINDER, D. L. Scene of the Cybercrime: Computer Forensics Handbook. Syngress, 2002.

11 SEGURANÇA EM SERVIDORES LINUX

PROGRAMA	Hardening: Configurações de Segurança Pós Instalação. Trabalhando com ACLs de File System e Atributos Extendidos. Criptografia de Discos. OpenSSL e GPG (GNU Privacy Guard). Isolamento de Serviços. Utilização do SYSLOG-NG. HIDS (Host Intrusion Detection System). IDS / IPS. Processo de Auditoria. SELinux. Segurança utilizando Firewalls. VPN.
BIBLIOGRAFIA	1. WARD, B. Como o Linux funciona: o que todo superusuário deveria saber. Novatec, 2015. 2. NEGUS, C.; BRESNAHAN, C. Linux: A bíblia. Alta Books, 2014. 3. SILBERSCHATZ, A.; GALVIN, P.; GAGNE, G. Fundamentos de sistemas operacionais: Princípios básicos. LTC, 2013. 4. FILHO, J. Descobrimo o Linux: Entenda o sistema operacional GNU/Linux. Novatec, 2012. 5. YAGHMOUR, K. Construindo sistemas Linux embarcados. Alta Books, 2009.

PROGRAMA

Auditoria de redes sem fio. Ataques a redes sem fio. Tráfego 802.11: conceitos, análise e captura. Metodologias de auditoria. Ferramentas de auditoria. Mapeamento de auditorias externas com o auxílio de GPS. Ameaças constantes: redes rogue e ataques DoS contra redes WLAN; Como auditar redes WEP. Como tornar redes WEP seguras. Dynamic WEP (DWEAP). Como auditar redes WPA. TKIP. Identificando redes WPA-PSK. Tornando redes WPA-PSK seguras. PEAP + WPA. Sistemas de Detecção de Intrusos (IDS) em redes WLAN; Modelos de implantação. Métodos de detecção. Como implantar uma WLAN segura. Arquitetura de autenticação. Free Radius. Configurando um access point baseado em OpenWrt. Configurando o cliente sem fio. Medidas de proteção do lado do cliente.

BIBLIOGRAFIA

1. MORAES, A. F. Redes Sem Fio — Instalação, Configuração e Segurança. Editora Érica, 2010.
2. NELSON, R. O. M. Segurança em Redes sem Fio. Novatec, 4ª edição, Nova Edição, 8 de dezembro de 2014.
3. MORENO, D. Pentest em Redes sem Fio. Novatec, 21 de março de 2016.

13 **SEGURANÇA DE APLICAÇÕES WEB — TESTE DE INVASÃO****PROGRAMA**

Arquitetura e tecnologias de aplicações web. Criptografia: cifras simétricas, cifras assimétricas, funções de hash criptográficas, MACs, assinaturas digitais, certificados digitais e SSL/TLS. Tipos de pentest e metodologia para teste de invasão. Injeção de SQL com acesso à plataforma subjacente, especificidades dos SGBDs e injeção de SQL às cegas. Injeção em LDAP, XML, SMTP e injeção de comandos. Transporte de credenciais por canais inseguros. Enumeração de usuários. Política de senhas fortes não implementadas pela aplicação. Falhas na programação ou projeto do mecanismo de autenticação. Mecanismos de recuperação de senhas vulneráveis. Condições de corrida no mecanismo de autenticação. Testes sobre o gerenciamento de sessões. Cross-Site Scripting (XSS) e CSRF. Teste dos mecanismos de autorização. Testes dos mecanismos criptográficos. Teste completo e relatórios.

BIBLIOGRAFIA

1. FERREIRA, R. Segurança em aplicações Web. Casa do Código, 10 de fevereiro de 2017.
2. WOLKERS, E. R. Segurança da Informação em Aplicações Web com Grails. Ciência Moderna, 1ª edição, 9 de setembro de 2015.
3. MORENO, D. Pentest em aplicações web. Novatec, 2017.

DOCENTES DO CURSO

13 DISCIPLINAS

DISCIPLINA	CH	TITULAÇÃO	DOCENTE RESPONSÁVEL	VÍNCULO
Segurança da Informação — Introdução, Normas e Padrões	30	MSc.	Luiz Gustavo Barros lattes.cnpq.br/9922522465810292	UEPG
Redes de Computadores	20	Dr.	Kleber Kendy Horikawa Nabas lattes.cnpq.br/7801062264058012	UTFPR
Conceitos de Linux	20	Dr.	Kleber Kendy Horikawa Nabas lattes.cnpq.br/7801062264058012	UTFPR
Segurança em redes	30	Dr.	Joilson Alves Junior lattes.cnpq.br/3062753386560903	UTFPR
Direito Digital	30	Esp.	Renata Milani Caldas Coelho lattes.cnpq.br/1506029662333796	Autônomo
Resposta a Incidentes de Segurança	20	Esp.	Maurício Barfknecht lattes.cnpq.br/3518350176865466	Autônomo
Gerenciamento de Identidade e Acesso	30	Esp.	Maurício Barfknecht lattes.cnpq.br/3518350176865466	Autônomo
Firewalls, IDS e IPS	30	Dr.	Kleber Kendy Horikawa Nabas lattes.cnpq.br/7801062264058012	UTFPR
Pentest — Teste de Intrusão	30	Dr.	Joilson Alves Junior lattes.cnpq.br/3062753386560903	UTFPR
Análise Forense	30	Esp.	Marcio Corcovado lattes.cnpq.br/4522157219119759	Autônomo
Segurança em Servidores Linux	30	Dr.	Joilson Alves Junior lattes.cnpq.br/3062753386560903	UTFPR
Segurança em Redes Sem Fio	30	Esp.	Henrique Fernando de Oliveira Rodrigues lattes.cnpq.br/4522157219119759	Autônomo
Segurança de Aplicações WEB — Teste de Invasão	30	MSc.	Rui Pimentel Leite lattes.cnpq.br/2481929003589822	UTFPR



UTFPR / DIRPPG-CT

ENDEREÇO	Av. Sete de Setembro 3165, 80230-901
TELEFONE	(41) 3310-4934
E-MAIL	dirppg-ct@utfpr.edu.br
SITE	especialização.ct.utfpr.edu.br