

FASUL EDUCACIONAL **(Fasul Educacional EaD)**

PÓS-GRADUAÇÃO

SEGURANÇA DA INFORMAÇÃO

CONTEÚDO PROGRAMÁTICO

SEGURANÇA DA INFORMAÇÃO

DISCIPLINA:
TECNOLOGIAS DIGITAIS PARA SEGURANÇA CIBERNÉTICA
CONTEÚDO PROGRAMÁTICO
AULA 1 TECNOLOGIA E SEGURANÇA O BIT, A INFORMAÇÃO ELEMENTAR NIBBLE, BYTE, WORD... SISTEMAS DE NUMERAÇÃO CONVERSÃO DA REALIDADE PARA INFORMAÇÃO DIGITAL
AULA 2 SISTEMA BINÁRIO REPRESENTAÇÃO DE NÚMEROS EM MÁQUINAS COMPUTACIONAIS CARACTERÍSTICAS DA INFORMAÇÃO SEGURA INTRODUÇÃO À CRIPTOGRAFIA CRYPTOGRAFIA SIMÉTRICA E ASSIMÉTRICA
AULA 3 CICLO DE VIDA DA INFORMAÇÃO E SEGURANÇA GARANTIA DE AUTENTICIDADE E INTEGRIDADE HASH, CRIPTOGRAFIA E ASSINATURA ELETRÔNICA PROCESSO DE ASSINATURA ELETRÔNICA CERTIFICADOS DIGITAIS
AULA 4 COMUNICAÇÃO DE DADOS COMUNICAÇÃO POR PACOTES DE DADOS CAMADAS CAMADAS DO MODELO OSI UMA TRANSMISSÃO DE DADOS
AULA 5 CONCEITOS RUDIMENTARES DE TELECOMUNICAÇÕES MEIO METÁLICO TRANSMISSÃO ÓPTICA RADIOPROPAGAÇÃO A CORRETA ESCOLHA DO MEIO
AULA 6 COMUTAÇÃO DE PACOTES E COMUNICAÇÃO ENTRE REDES PROTOCOLO IP UDP E TCP ATIVOS DE REDE IPSEC E SEGURANÇA EM TCP/IP

DISCIPLINA:
COMPUTAÇÃO EM NUVEM
RESUMO
Nesta disciplina veremos os conceitos e as terminologias de computação em nuvem, as diferentes tecnologias envolvidas em data centers na nuvem, a história da evolução dos data

centers, abordando os modelos de nuvem Pública, Privada e Híbrida e suas ofertas de serviço como IaaS, PaaS, SaaS, DaaS e a forma como eles se integram no cenário atual.

CONTEÚDO PROGRAMÁTICO

AULA 1

SURGIMENTO

EXEMPLOS

QUEM DEVE UTILIZAR E PARA QUÊ

TIPOS DE NUVENS E SERVIÇOS BÁSICOS

AULA 2

O RETORNO DO INVESTIMENTO NO DESENVOLVIMENTO INTERNO

COMPUTAÇÃO EM NUVEM É TERCEIRIZAÇÃO?

COMPRA DE ESPAÇO EXTERNO E GESTÃO INTERNA

CONTRATOS DE GARANTIA DE NÍVEL DE SERVIÇO

AULA 3

AMAZON: A VISÃO DE UMA PLATAFORMA DE SUCESSO

A NUVEM E A INTERNET DAS COISAS

VANTAGENS DO USO DA COMPUTAÇÃO EM NUVEM

DESVANTAGENS DO USO DA COMPUTAÇÃO EM NUVEM

AULA 4

COMO MIGRAR PARA A NUVEM

ATIVIDADES DE AUDITORIA

GESTÃO DO AMBIENTE QUE UTILIZA COMPUTAÇÃO EM NUVEM

FORMAÇÃO DE PROFISSIONAIS

AULA 5

O BIG DATA E A COMPUTAÇÃO EM NUVEM

COMPARATIVO: COMPUTAÇÃO EM NUVEM E OUTSOURCING

INTELIGÊNCIA ARTIFICIAL E COMPUTAÇÃO EM NUVEM

PERSPECTIVAS FUTURAS PARA A COMPUTAÇÃO EM NUVEM

AULA 6

SEGURANÇA DA INFORMAÇÃO

COMPARATIVO COMPUTAÇÃO EM NUVEM E OUTSOURCING

PRIVACIDADE DA INFORMAÇÃO

INTEGRIDADE DA INFORMAÇÃO

BIBLIOGRAFIAS

- MOIA, V. H. G. Um estudo sobre a segurança e privacidade no armazenamento de dados em nuvens. 2016. Disponível em: http://repositorio.unicamp.br/bitstream/REPOSIP/304987/1/Moia_VitorHugoGalhardo_M.pdf.
- VIEIRA, E. Como calcular o ROI em projetos de computação em nuvem. 2017. Disponível em: <http://blog.cbcloud.com.br/roi-em-projetos-de-computacao-emnuvem/>.
- WINTER, J. Sistemas cyber-físicos: a nova revolução. 2016. Disponível em: <https://www.eaware.com.br/sistemas-ciber-fisicos-a-nova-revolucao/>.

DISCIPLINA:

PROJETO ESTRUTURADO E GERÊNCIA DE REDES

RESUMO

Para a implantação de um projeto de redes de computadores em uma organização faz-se

necessário não apenas ter conhecimentos específicos de redes de computadores, mas também conceitos de gerencia de projetos. Pois, por meio desses conhecimentos é possível entender as necessidades dos clientes e a melhor forma de aderir cada uma das etapas de um projeto as topologias e infraestrutura de rede exigidas durante o processo de criação e implantação.

CONTEÚDO PROGRAMÁTICO

AULA 1

PROJETO
GESTÃO DE PROJETOS
CICLO DE VIDA DE PROJETOS
ETAPAS DE ELABORAÇÃO DE PROJETOS

AULA 2

METODOLOGIA TOP-DOWN
REQUISITOS DO CLIENTE
METAS DO CLIENTE
PARÂMETROS AVALIADOS NO PROJETO DE REDES

AULA 3

TRÁFEGO DE REDE
TOPOLOGIA DE REDE LÓGICA
ENDEREÇAMENTO DE REDE LÓGICA
SEGURANÇA E GERENCIAMENTO DE REDE LÓGICA

AULA 4

DOCUMENTAÇÃO DE PROJETO DE REDE FÍSICA
MAPA DE REDE
AVALIAÇÃO DE INFRAESTRUTURA
DOCUMENTAÇÃO DO PROJETO

AULA 5

ÁREAS DE GERENCIAMENTO
SISTEMA DE GERÊNCIA
ARQUITETURA DE GERÊNCIA
MODELOS

AULA 6

ELEMENTOS DE ZABBIX
SEGURANÇA DA INFORMAÇÃO
FIREWALL
IPTABLES

BIBLIOGRAFIAS

- MAXIMIANO, A. C. A. Administração de projetos: como transformar ideias em resultados. 3. ed. 2 reimp. São Paulo: Atlas, 2009.
- PROJECT MANAGEMENT INSTITUTE. Um guia do conjunto de conhecimentos em gerenciamento de projetos: Guia PMBOK®. 3. ed. Pensilvânia: Four Campus, 2012.
- RABECHINI JUNIOR, R. O gerente de projetos na empresa. São Paulo: Atlas, 2011.

DISCIPLINA:

SEGURANÇA DA INFORMAÇÃO

RESUMO

O que é segurança da informação? O conceito de segurança em si já comporta vários

significados. No idioma inglês, por exemplo, isso é diferenciado: o termo security refere-se à proteção contra ameaças intencionais, enquanto que seu sinônimo reliability indica a confiabilidade, a tolerância às falhas. Já o termo safety designa a proteção ao ambiente e aos seres vivos, incluindo-se aí a proteção à saúde e à vida. A segurança da informação é a parte da ciência da informação que tem por objetivo proteger os dados, as informações e os conhecimentos de modo a preservar o valor destes para os processos, produtos e serviços das pessoas e organizações.

CONTEÚDO PROGRAMÁTICO

AULA 1

SEGURANÇA NO CICLO DA VIDA DE INFORMAÇÃO
SEGURANÇA DA INFORMAÇÃO SUPOSTA POR TIC
SEGURANÇA DA INFORMAÇÃO CONVENCIONAL
SEGURANÇA DA TIC NA OPERAÇÃO DOS NEGÓCIOS

AULA 2

GESTÃO DE RISCOS
OS PROCESSOS DA GESTÃO DE RISCOS
TRATAMENTO DOS RISCOS
GESTÃO DA CONTINUIDADE DOS NEGÓCIOS

AULA 3

ÁREAS DE CONTROLE
CLASSIFICAÇÃO DA INFORMAÇÃO
PADRÕES DE CLASSIFICAÇÃO DA INFORMAÇÃO
PROCESSO DE CLASSIFICAÇÃO

AULA 4

CRİPTOGRAFIA SIMÉTRICA
CRİPTOGRAFIA ASSIMÉTRICA
ASSINATURA DIGITAL
INFRAESTRUTURA DE CHAVES PÚBLICAS

AULA 5

MONITORAMENTO DE TRÁFEGO
REDES PRIVADAS
MALWARE
INVASÃO DE PRIVACIDADE

AULA 6

GOVERNANÇA DA SEGURANÇA DA INFORMAÇÃO
COMPORTAMENTO ORGANIZACIONAL
CONSCIENTIZAÇÃO, TREINAMENTO E EDUCAÇÃO
PRINCÍPIOS ÉTICOS

BIBLIOGRAFIAS

- BEAL, A. Segurança da Informação: Princípios e Melhores Práticas para a Proteção dos Ativos de Informação nas Organizações. SÃO PAULO: ATLAS, 2008.
- FONTES, E. Segurança da Informação. 1. ED. SÃO PAULO: SARAIVA, 2001.
- KIM, D. Fundamentos de Segurança de Sistemas de Informação. 1. ED. RIO DE JANEIRO: LTC, 2014.

DISCIPLINA:

SEGURANÇA EM SISTEMAS DE INFORMAÇÃO

RESUMO

Na era moderna, os ciclos de produção e consumo presentes em nossa economia estão cada vez mais velozes, a inovação tem sido muito presente e está vinculada ao sucesso, a qualidade dos produtos criados, o consumismo acelerado, o ritmo cada vez mais rápido, todo esse cenário torna as informações um ativo muito valioso. A disputa, e toda essa competição nesse novo contexto, estão muito dependentes do compartilhamento de informações entre os mais diversos atores, como fornecedores, produtores, parceiros, clientes, colaboradores, entre outros. Dentro desse aspecto, com todo esse mar de informações sendo criado diariamente por essas entidades, hoje não é mais possível estar participando dessa disputa por inovações e armazenar as informações geradas em cofres, armários, gavetas e trancá-las com chaves e segredos, desenvolver a acessibilidade e a disponibilidade de tudo isso é a maneira encontrada para se manter no páreo, quando falamos de instituições públicas, o governo torna o processo mais complexo. Existe uma série de princípios a serem respeitados, nossas legislações, proteção de dados, princípios de segurança e defesa nacional, as informações são toda a base para a operação e funcionamento das organizações, empresas, órgãos públicos, governo e demais entidades.

CONTEÚDO PROGRAMÁTICO

AULA 1

HISTÓRIA E CONCEITOS

INTRODUÇÃO À SEGURANÇA DA INFORMAÇÃO

ISO 15408

FAMÍLIA ISO 27000

ISO 31000

AULA 2

FRAMEWORKS DE GESTÃO E APOIO À SEGURANÇA DA INFORMAÇÃO

INTRODUÇÃO À CRIPTOGRAFIA

HASH

CHAVE SIMÉTRICA E ASSIMÉTRICA

ASSINATURA E CERTIFICAÇÃO DIGITAL

AULA 3

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

SEGURANÇA DA INFRAESTRUTURA

SEGURANÇA DE REDES

SEGURANÇA DE SOFTWARE

SEGURANÇA DE DADOS

AULA 4

ATAQUES À SEGURANÇA

TÉCNICAS DE MITIGAÇÃO E CONTRAMEDIDAS DE SEGURANÇA

CONTROLE DE ACESSO, AUTORIZAÇÃO E CONTABILIZAÇÃO

IMPLEMENTAÇÃO DO AUTHENTICATION, AUTHORIZATION AND ACCOUNTING (AAA)

INTRODUÇÃO À PROCEDIMENTOS DE AUDITORIA

AULA 5

BYOD E SANDBOX

SEGMENTAÇÃO DE REDE

SEGURANÇA DE NUVEM PRIVADA, PÚBLICA E MISTA

SEGURANÇA EM FOG CLOUD (IOT)

SEGMENTAÇÃO DE REDE PARA IOT, AUTENTICAÇÃO, REGISTRO E AUTORIZAÇÃO

AULA 6

PROXY
IDS/IPS
CONTROLE DE CONTEÚDO
PROTEÇÃO ANTIMALWARE
FIREWALL E FIREWALL DE NOVA GERAÇÃO

BIBLIOGRAFIAS

- ALVES, D. Internet das Coisas (IoT): segurança e privacidade de dados pessoais. Rio de Janeiro: Alta Books, 2021.
- BAARS, H. Foundations of Information Security: based on ISO 27001 and 27002. Rio de Janeiro: Brasport, 2018.
- FRAGA, B. Técnicas de invasão: aprenda as técnicas usadas por hackers em invasões reais. São Paulo: Labrador, 2019.

DISCIPLINA:

DESAFIOS ESTRATÉGICOS PARA A SEGURANÇA E DEFESA CIBERNÉTICA

RESUMO

O surgimento dos primeiros computadores, sua evolução e o advento da internet foram, e ainda são, facilitadores da criação e do consumo exponencial da informação de uma maneira cada vez mais imediata. As novas tecnologias possibilitam que a expressão dos pensamentos, bem como das ideias das pessoas, floresçam em tempo real, criando assim um ciclo que envolve a produção e o consumo do que podemos considerar como informações cibernéticas (Cordeiro Viana e Silva; Bandeira, 2016).

CONTEÚDO PROGRAMÁTICO

AULA 1

A CIBERNÉTICA
O ESPAÇO CIBERNÉTICO
CIBERCULTURA
CIBERCRIMES

AULA 2

SEGURANÇA CIBERNÉTICA
PRIVACIDADE CIBERNÉTICA
MANUTENÇÃO DA INTEGRIDADE DE DADOS
A GESTÃO DA SEGURANÇA, PRIVACIDADE E INTEGRIDADE DE DADOS NO ESPAÇO CIBERNÉTICO

AULA 3

COMPROMETIMENTO DA INTERNET
GOVERNANÇA
GOVERNANÇA NAS CORPORAÇÕES
RESILIÊNCIA, DISSUAÇÃO E DEFESA: A CIBERSEGURANÇA NAS CORPORAÇÕES

AULA 4

POLÍTICA DE DEFESA CIBERNÉTICA BRASILEIRA
PARCERIAS INTERNACIONAIS
DOCTRINA MILITAR DE DEFESA CIBERNÉTICA (DMDC)
ESTRATÉGIA PARA GOVERNANÇA E IMPLEMENTAÇÃO DA POLÍTICA DE DEFESA CIBERNÉTICA NO BRASIL

AULA 5

INTELIGÊNCIA CIBERNÉTICA, SEGURANÇA CIBERNÉTICA E CIBERGUERRA
SITUAÇÃO DO BRASIL NO TOCANTE À SEGURANÇA CIBERNÉTICA

O SISTEMA NACIONAL DE SEGURANÇA E DEFESA CIBERNÉTICA
QUESTÕES CRÍTICAS COM RELAÇÃO À SEGURANÇA CIBERNÉTICA

AULA 6

DEFESA AMPLIADA CONTRA RAMSOMWARES

FALHAS DE SEGURANÇA NAS ESTRUTURAS DE PLATAFORMAS DE COMPUTAÇÃO EM NUVEM

PERSPECTIVAS DE SEGURANÇA NA INTERNET DAS COISAS (IOT)

PORTA ABERTA DOS APPS E RISCOS DA MOBILIDADE TOTAL

BIBLIOGRAFIAS

- CORDEIRO VIANA E SILVA, C.; BANDEIRA, K. P. Defesa cibernética no Brasil. Revista de Análise Internacional, v. 1, n. ago/dez, p. 13-27, 2016.
- FERREIRA NETO, F. B. et al. Projetos estratégicos de defesa e seus reflexos na formação do comandante de fração. In: CONGRESSO ACADÊMICO SOBRE DEFESA NACIONAL, 14. 2017, Resende. Artigos e Palestras, 2017, p. 1-13.
- SOUZA JUNIOR, A. F. de; ERMES STREIT, R. Segurança cibernética: política brasileira e a experiência internacional. Revista do Serviço Público, v. 68, n. 1, p. 107, 2017. Disponível em: <https://revista.enap.gov.br/index.php/RSP/article/view/864>.

DISCIPLINA:

LEI GERAL DE PROTEÇÃO DE DADOS

RESUMO

A gestão eletrônica de documentos (GED) é uma evolução natural da gestão documental convencional, que tem como base o papel. A gestão de documentos convencional é um processo caro, lento e sujeito a erros, que exige muito espaço físico e muito tempo para gerenciamento e recuperação de documentos. O GED substitui o gerenciamento manual de documentos pelo gerenciamento digital, o que traz inúmeras vantagens. Com o GED, documentos podem ser facilmente digitalizados, indexados e armazenados em um sistema eletrônico centralizado. Isso permite que documentos sejam recuperados rapidamente por meio de pesquisas por palavras-chave e evita a perda ou destruição de documentos físicos. Além disso, a gestão eletrônica de documentos também melhora a segurança dos documentos, uma vez que é possível definir níveis de acesso aos documentos, criptografá-los e protegê-los contra alterações não autorizadas. O GED também permite a criação de trilhas de auditoria que registram todas as ações realizadas em relação a um documento.

CONTEÚDO PROGRAMÁTICO

AULA 1

A LGPD NA PERSPECTIVA CONSTITUCIONAL: OS DIREITOS FUNDAMENTAIS

A LGPD E A RELAÇÃO COM OUTROS DIPLOMAS LEGAIS

ÂMBITO DE APLICAÇÃO DA LGPD

OS FUNDAMENTOS DA LGPD

AULA 2

CONCEITOS FUNDAMENTAIS

HIPÓTESES LEGAIS E GERAIS DE TRATAMENTO DE DADOS PESSOAIS

CONSENTIMENTO DO TITULAR

LEGÍTIMO INTERESSE DO CONTROLADOR

AULA 3

TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS

TRATAMENTO DE DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES

TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

COMPARTILHAMENTO DE DADOS PELO PODER PÚBLICO

AULA 4

DIREITOS DO TITULAR DE DADOS PESSOAIS

CICLO DE VIDA DOS DADOS PESSOAIS

AGENTES DE TRATAMENTO DE DADOS: CONTROLADOR E OPERADOR

ENCARREGADO DOS DADOS (DPO)

AULA 5

SANÇÕES ADMINISTRATIVAS

ÓRGÃOS DE FISCALIZAÇÃO E REGULAÇÃO NACIONAL

ÓRGÃOS ESTADUAIS DE FISCALIZAÇÃO E REGULAÇÃO

O PAPEL DO CONTROLE EXTERNO NA FISCALIZAÇÃO DA LGPD

AULA 6

BOAS PRÁTICAS E GOVERNANÇA

PREMISSAS FUNDAMENTAIS DE GOVERNANÇA EM PRIVACIDADE À LUZ DA LGPD

ELEMENTOS MANDATÓRIOS MÍNIMOS DO PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

O PROGRAMA DE “GOVERNANÇA EM PRIVACIDADE”: COMO ESTRUTURÁ-LO?

BIBLIOGRAFIAS

- AMORA, J. Relação entre compliance e LGPD. Risco Legal, S.d. Disponível em: <https://vgriscolegal.com.br/blog/relacao-entre-lgpd-e-o-compliance/>.
- ANPD – Autoridade Nacional de Proteção de Dados. Tratamento de dados pessoais pelo Poder Público – Guia orientativo. Brasília: ANPD, 2022.
- BARROS, L. Gestão eletrônica de documentos: o que é e como funciona a GED? Tangerino, 2022. Disponível em: <https://tangerino.com.br/blog/gestaoeletronica-de-documentos/#Como-funciona-a-Gestão-Eletrônica-deDocumentos?>.

DISCIPLINA:

CRIOPTOGRAFIA E CRYPTOANÁLISE

CONTEÚDO PROGRAMÁTICO

AULA 1

TIPOS DE MALWARE

AMEAÇAS AO E-MAIL

MECANISMOS DE ATAQUE

TIPOS DE ATAQUE

COMPONENTES DA SEGURANÇA

AULA 2

ORIGEM HISTÓRICA

MODELO OSI E CRIPTOGRAFIA

CRIOPTOGRAFIA SIMÉTRICA

CRIOPTOGRAFIA ASSIMÉTRICA

OS ALGORITMOS DE CRIPTOGRAFIA

AULA 3

CRIOPTOGRAFIA DE BLOCO E DE FLUXO

ESTEGANOGRAFIA

INTEGRIDADE DOS DADOS

FUNÇÕES DE HASH

OS ALGORITMOS DE HASH

AULA 4

O HASHING E A INTEGRIDADE DOS DADOS
O HASH PARA A SEGURANÇA DE SENHAS
ASSINATURA DIGITAL
OPERAÇÃO COM ASSINATURA DIGITAL
ALGORITMOS DE ASSINATURAS DIGITAIS

AULA 5

CERTIFICADO DIGITAL
AUTORIDADE CERTIFICADORA
CERTIFICADO DIGITAL
CADEIA DE CERTIFICADOS
TIPOS DE CERTIFICADOS E CHAVES PÚBLICAS

AULA 6

MÉTODOS DE AUTENTICAÇÃO DE USUÁRIOS
AUTENTICAÇÃO COM DISPOSITIVOS FÍSICOS
AUTENTICAÇÃO COM BIOMETRIA
A SEGURANÇA DOS DADOS
PROTEÇÃO DOS PACOTES IP

DISCIPLINA:
ETHICAL HACKER

RESUMO

Em informática, um hacker é uma pessoa que se dedica, de forma entusiasmada, a programar, conhecer e alterar dispositivos programas, redes de computador. Para um hacker é um dever de natureza ética compartilhar suas competências e seus conhecimentos. Por exemplo: elaborando um software gratuito e facilitando o acesso à informação e aos recursos de computação sempre que o seja possível (Soares, 2014). Graças a seus conhecimentos, realizam feitos memoráveis, com a criação dos softwares livres, e feitos façanhosos, por exemplo: a quebra de barreiras que aparentemente deveriam proteger e ou limitar o acesso a certos dados e informações.

CONTEÚDO PROGRAMÁTICO

AULA 1

PROCURA-SE O HACKER
MEDO DE HACKERS?
TIPOS DE HACKERS
PROTEJA O SEU COMPUTADOR

AULA 2

HACKER ÉTICO VERSUS AUDITOR DE SEGURANÇA
POR DENTRO DA MENTE DE UM HACKER
O MUNDO REAL
ESTRATÉGIA DE ATAQUE

AULA 3

PLANEJAMENTO PARA OS TESTES: PARTE 2
PORTAS
SENHAS
CONHECENDO O METASPLOIT

AULA 4

ESSENTIAL NETTOOLS - PARTE 1

ESSENTIAL NETTOOLS - PARTE 2

ESTEGANOGRAFIA - PARTE 1

ESTEGANOGRAFIA - PARTE 2

AULA 5

AIRCRAK-NG

REAVR

PIXIEWPS E WIFITE

WIRESHARK

AULA 6

WASH E FERN WIFI CRACKER

BULLY E REAVR

WIFITE OU WIFITE2?

GOOGLE HACKING

BIBLIOGRAFIAS

- ROMÃO, S. da C. Segurança de informação um estudo de caso descritivo com as principais defesas e ameaças em uma empresa de tecnologia na cidade de Fortaleza. Projeto de pesquisa de Trabalho de Conclusão de Curso (Bacharelado em Administração) – Centro De Ensino Superior Do Ceará, Fortaleza, 2013.
- SOARES, A. E. T. Cultura Hacker: os novos sujeitos do comum (s). Revista InterLegere, n. 14, 2014.
- MAGGIO, V. de P. R. JusBrasil. 2012. Disponível em: <https://vicentemaggio.jusbrasil.com.br/artigos/121942478/novo-crime-invasaode-dispositivo-informatico-cp-art-154-a/>.

DISCIPLINA:

CRIMES CIBERNÉTICOS

RESUMO

Esta disciplina tem por escopo estudar o Direito Penal Informático, introduzindo brevemente as noções que permeiam o Direito Penal, a criminalidade cibernética e a dificuldade de tipificação das condutas, desembocando, finalmente, em uma análise da realidade brasileira acerca da legislação que pretende combater os cibercrimes. Assim entenderemos como e porque o Direito Penal passou a se preocupar com algumas condutas adotadas no ambiente digital, como se deu o processo de tipificação e quais foram as efetivamente previstas em nosso direito pátrio.

CONTEÚDO PROGRAMÁTICO

AULA 1

DADOS SOBRE CRIMES INFORMÁTICOS

TIPIFICAÇÃO CRIMINAL: A TEORIA “TCC” (TÉCNICA, COMPORTAMENTO E CRIME)

CONDUTAS INFORMÁTICAS QUE PODEM SER CONSIDERADAS CRIMES (PARTE 1)

CONDUTAS INFORMÁTICAS QUE PODEM SER CONSIDERADAS CRIMES (PARTE 2)

AULA 2

TUTELA AOS BENS JURÍDICOS

CONCEITO JURÍDICO DE CRIME INFORMÁTICO

CLASSIFICAÇÃO DOS CRIMES INFORMÁTICOS

SUJEITO ATIVO, COMPETÊNCIA E LUGAR

AULA 3

A CONSTRUÇÃO DA LEGISLAÇÃO BRASILEIRA

CRIMES INFORMÁTICOS COMETIDOS POR FUNCIONÁRIOS PÚBLICOS - LEI N.

9.983/2000

CRIMES INFORMÁTICOS PUROS E A LEI CAROLINA DIECKMANN (LEI N. Nº 12.737/2012)

INVASÃO DE DISPOSITIVO INFORMÁTICO: ART. 154-A DO CÓDIGO PENAL

AULA 4

FALSIFICAÇÃO DE DOCUMENTO PARTICULAR

CRIME DE DANO

CRIME DE PEDOFILIA

CRIMES CONTRA A HONRA

AULA 5

CRIMES DE FALSA IDENTIDADE

FRAUDE BANCÁRIA – FURTO QUALIFICADO

FRAUDE BANCÁRIA – ESTELIONATO

CRIME ECONÔMICOS E A LAVAGEM DE DINHEIRO

AULA 6

CASOS CONCRETOS: CRIMES PRÓPRIOS

CASOS CONCRETOS: CRIMES IMPRÓPRIOS

PERSPECTIVAS FUTURAS

CONCLUSÕES

BIBLIOGRAFIAS

- _____. Lei n. 12.965, de 23 de abril de 2014. Diário Oficial da União, Brasília, DF, 24 abr. 2014.
- JESUS, D. de; MILAGRE, J. A. Manual de crimes informáticos. São Paulo: Saraiva, 2016.
- JUSTINIANO, N. F. Terminologia e tecnologia: um estudo de termos de crimes cibernéticos. Dissertação (Mestrado em Linguística) – UNB, Brasília, 2017.

DISCIPLINA:

SEGURANÇA DE REDES DE COMPUTADORES

CONTEÚDO PROGRAMÁTICO

AULA 1

CLIENTES E SERVIDORES

ELEMENTOS DE UMA REDE

A ABRANGÊNCIA DAS REDES

REDES CONFIÁVEIS

AMEAÇAS E MEDIDAS DE SEGURANÇA

AULA 2

O PROCESSO DE COMUNICAÇÃO

MODELO OSI

A CAMADA DE TRANSPORTE

A CAMADA DE REDE

CAMADA DE ENLACE E CAMADA FÍSICA

AULA 3

A REDE WI-FI

A SEGURANÇA DA REDE WI-FI

AS MENSAGENS ELETRÔNICAS

PROTOCOLOS DE E-MAIL

HTTP E HTTPS

AULA 4

AS REDES PRIVADAS
A REDE WAN E AS VPNS
O IPSEC
A OPERAÇÃO DO IPSEC
FERRAMENTAS DE MONITORAÇÃO

AULA 5

MÉTODOS DE ATAQUES
ATAQUES DE RECONHECIMENTO ESTRUTURADOS
OS ATAQUES DE ACESSO
MITIGANDO OS ATAQUES DE ACESSO
ATAQUES DE NEGAÇÃO DE SERVIÇO

AULA 6

DETECÇÃO DE INTRUSÃO
PREVENÇÃO DE INTRUSÃO
OS FIREWALLS
A EVOLUÇÃO DO FIREWALL
A DEEP WEB

DISCIPLINA:

MARCO CIVIL DA INTERNET

CONTEÚDO PROGRAMÁTICO

AULA 1

A FACE OCULTA DA INTERNET
OS RISCOS DA TECNOLOGIA DA INFORMAÇÃO
A ERA DA VIGILÂNCIA DIGITAL
REGULAMENTAÇÃO DA TECNOLOGIA DA INFORMAÇÃO

AULA 2

A REGULAMENTAÇÃO DA INTERNET NO BRASIL E O MARCO CIVIL DA INTERNET
A NEUTRALIDADE DA REDE
A INIMPUTABILIDADE DA REDE
A PRIVACIDADE NA REDE

AULA 3

A REGULAMENTAÇÃO DA INTERNET NO BRASIL E O MARCO CIVIL DA INTERNET
A NEUTRALIDADE DA REDE
A INIMPUTABILIDADE DA REDE
A PRIVACIDADE NA REDE

AULA 4

FUNDAMENTO CONSTITUCIONAL DA PRIVACIDADE
PROTEÇÃO DA PRIVACIDADE NO MARCO CIVIL DA INTERNET
CONFLITO ENTRE O DIREITO À PRIVACIDADE E O DIREITO À INFORMAÇÃO
DIREITO AO ESQUECIMENTO

AULA 5

FUNDAMENTOS DA LIBERDADE DE EXPRESSÃO
A FIGURA DO “PROVEDOR”
RESPONSABILIZAÇÃO DOS PROVEDORES

REMOÇÃO DE CONTEÚDO DA INTERNET

AULA 6

IDENTIFICAÇÃO DO RESPONSÁVEL PELO ATO ILÍCITO

A QUESTÃO DO ÔNUS DA PROVA NA INTERNET

PROBLEMAS DE JURISDIÇÃO NA INTERNET

CRIMES DIGITAIS NA INTERNET