Universidade de Brasília

ANEXO I

CURRÍCULO DE HABILITAÇÃO - PÓS-GRADUAÇÃO

Código: PC069-2023
Nome: PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO
Unidade Responsável: PROGRAMA DE PÓS-GRADUAÇÃO PROFISSIONAL EM ENGENHARIA ELÉTRICA- 11.01.01.11.03.18
Tipo do Curso: Especialização
Modalidade Educação: A Distância
Polos: BRASÍLIA - DF
Método de Avaliação: CONCEITO
Carga Horária: 375
Carga Horária Prática: 0
Número do Vagas: 120
Grande Área: Engenharias
Área: Engenharia Elétrica
Tipo do Trabalho deConclusão: ARTIGO CIENTÍFICO
Banca Examinadora: Sim
Financiamento: Termo de Execução Descentralizada (TED)
Período do Curso: 18/03/2024 a 31/12/2026
Público Alvo: Servidores que atuam nos mais diversos órgãos do SISP como agentes demelhoria da privacidade e segurança da informação naqueles órgãos

Justificativa e Objetivo: O país demanda soluções inovadoras que possam enfrentar o desafio demanter os sistemas de informação e sua infraestrutura crítica segura. Isso porque, os incidentes de segurança da informação têm acontecido de forma sistêmica em diversos setores da economia, seja na área pública quanto na área privada. O risco cibernético foi considerado nos anos 2022 e 2023, a classe de risco mais crítica dentro das organizações, à frente de capital humano, e incerteza macroeconômica e geopolítica. Essa temática tem tido uma grande relevância e demanda nos últimos anos. Parte disso é devido a intensificação dos ataques cibernéticos que afetam o setor público, privado e todas as organizações, pessoas e sistemas de todo o globo. Tudo está sujeito ariscos cibernéticos. Órgãos de todas as esferas da república, a infraestruturacrítica de nosso país, além de empresas privadas de todos os setores têm sido alvo de hackers. Não obstante, a proteção de dados pessoais passou a ser um direito fundamental o que exige um novo olhar sobre como os dispositivos eletrônicos tratam informações pessoais. Soluções inovadoras para esse problema que está disseminado é cada vez mais imperativo, o que necessitade esforços conjuntos da academia, Governo e Indústria. O Programa de Pós-Graduação Profissional em Engenharia Elétrica da Universidade de Brasília se apropriou dessa oportunidade desde que sua gestão passou a ser autônoma do programa acadêmico, já que, atualmente, possui uma área de concentração única em Segurança Cibernética com linhas de pesquisa que, em sua maioria,permitem-nos caracterizar o nosso programa como Engenharia Elétrica. Apesar de, em um primeiro momento, um leigo entender que a Segurança Cibernética possa ser uma temática estritamente tecnológica, deve-se ressaltar que a solução desse desafio ultrapassa essas fronteiras. Para enfrentar os desafios da temática é necessário desenvolver disciplinas que estão relacionadas à Segurança de Sistemas, à

Segurança de Infraestrutura, e a Segurança de Plataformas, contudo, há também necessidade de se estudar as metodologias e técnicas para ataque e defesa, bem como os aspectos humanos, organizacionais e regulatórios dessa temática. O curso de Especialização em Privacidade e Segurança da Informação, objeto da presente proposta, é curso de Pós-Graduação Latu Sensu que será ministrado pela Universidade de Brasília(UnB) para servidores do Poder Executivo, em quatro turmas, iniciando a partirde 2024, com um ingresso de 30 alunos no primeiro semestre de 2024; e turmas subsequentes iniciando nos anos de 2025, 2026 e 2027. O objetivo final será contribuir para a melhoria da Segurança Cibernética dentro do Poder Executivo. As turmas terão duração de 18 meses, onde 12 meses serão destinadas para cursar disciplinas, e os 6 meses finais para a elaboração do artigo final. O curso será desenvolvido em regime de mútua cooperação entre o Ministério da Gestão e da Inovação em Serviços Públicos, por meio de descentralização de recursos, realizados por meio de um TED, com duração de 5 anos.

Local do Curso: As aulas ocorrerão na modalidade de ensino à distância, com encontro ssíncronos em plataforma virtual de aprendizagem, nas segundas, terças e quintas no período noturno, das 19h às 22h40min. Provas das disciplinas serão realizadas presencialmente, na sede de nosso programa (Universidade de Brasília); Defesa do trabalho de conclusão de curso, no formato de artigo científico, de forma presencial, na sede de nosso programa (Universidade de Brasília).

GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Ementa: ABNT ISO 27001. Gestão de Riscos de Segurança da Informação. Política nacional de segurança da informação(PNSI). Visão geral dos normativos do GSI. Frameworks de Segurança de Gestão de Segurança da Informação(Série 27.000; NIST; CIS Controls). Framework de privacidade e segurança da informação da SGD (partesegurança).

Conteúdo Programático: Unidade 1: Introdução à Segurança da Informação Conceitos fundamentais de segurança da informação.Importância da segurança da informação nas organizações e na sociedade. Panorama atual das ameaças àsegurança da informação. Unidade 2: ABNT ISO 27001 - Sistemas de Gestão de Segurança da Informação Visãogeral da ABNT ISO 27001. Estrutura da norma e seus requisitos. Processo de certificação e auditoria.Implementação de um Sistema de Gestão de Segurança da Informação (SGSI) de acordo com a ISO 27001.Unidade 3: Gestão de Riscos de Segurança da Informação Princípios da gestão de riscos. Metodologias eframeworks para a avaliação de riscos. Identificação, análise, avaliação e tratamento de riscos de segurança dainformação. Relação entre a ISO 27001 e a gestão de riscos. Unidade 4: Política Nacional de Segurança daInformação (PNSI) Contexto e importância da PNSI no Brasil. Objetivos e princípios da PNSI. Legislaçãorelacionada à PNSI. Implementação e conformidade com a PNSI. Unidade 5: Normativos do GSI (Gestão deSegurança da Informação) Visão geral dos principais normativos do Governo Brasileiro relacionados à segurançada informação. ABNT NBR ISO/IEC 27001:2013 como referência. A relação entre os normativos do GSI e a ISO27001. Unidade 6: Frameworks de Segurança da Informação Série ISO/IEC 27000 e ISO/IEC 27002. NIST(National Institute of Standards and Technology) e suas diretrizes de segurança. CIS Controls (Center forInternet Security) e suas práticas. Comparação e seleção de frameworks de acordo com as necessidadesorganizacionais. Unidade 7: Framework de Privacidade e Segurança da Informação da SGD (Secretaria deGoverno Digital) - Parte Segurança Visão geral do framework de privacidade e segurança da informação da SGD.Aspectos relacionados à segurança da informação, proteção de dados e privacidade. Implementação de controlese práticas de acordo com o framework da SGD. Unidade 8: Estudos de Caso e Exemplos Práticos Análise de casosreais de implementação da ISO 27001. Exemplos de gestão de riscos de segurança da informação. Casos deaplicação dos frameworks de segurança. Exercícios práticos e discussões em grupo. Unidade 9: Avaliação eExame Final Preparação para a avaliação final. Revisão dos principais tópicos. Exame final ou projeto práticorelacionado à gestão de segurança da informação.

Método de ensino-aprendizagem: Os alunos serão avaliados, em cada disciplina, levando em conta sua participação em sala de aula e ematividades como provas, simulações, estudos de caso, oficinas, dinâmicas, seminários, pesquisas de campo,visitas técnicas, projetos de intervenção, exposição dialogada, perguntas orientadoras, entre outras queestimulem o pensamento reflexivo e crítico. Serão atribuídas menções (SR, II, MI, MM, MS ou SS) em todas asdisciplinas do curso e no trabalho de conclusão do curso (TCC), sendo aprovados os alunos que obtiverem, emcada disciplina e no TCC, menção igual ou superior a MM e frequência mínima de 75% em cada disciplina. Seráconcedido ao aluno que obtiver aprovação nas disciplinas e no artigo um Certificado de Especialização emPrivacidade e Segurança da Informação.

Bibliografia: ABNT NBR ISO/IEC 27001:2022 "Segurança da informação, segurança cibernética e proteção à privacidade –Sistemas de gestão de segurança da informação - Requisitos". Rio de Janeiro: ABNT, 2022. BRASIL. Ministério daGestão e da Inovação. Secretaria de Governo Digital. Diretoria de Privacidade e Segurança da

Informação. Guiado Framework de Privacidade e Segurança da Informação – versão 1.1.2. Brasília-DF: SGD, 2023.UNIVERSIDADE DE BRISTOL. CyBOK - The Cyber Security Body of Knowledge. 2021.

Docente: Rafael Rabelo Nunes.

GESTÃO DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Ementa: ABNT NBR ISO 27701. Lei Geral de Proteção de Dados. Principais frameworks de mercado e outras legislações dereferência. Visão geral dos guias da ANPD. Framework de Privacidade e Segurança da Informação da SGD (parteprivacidade). Privacy by Design.

Conteúdo Programático: **Unidade 1: Introdução à Privacidade e Proteção de Dados** - Conceitos fundamentais de privacidade eproteção de dados. - Importância da privacidade de dados nas organizações. - Contextualização da LGPD e suarelevância. **Unidade 2: ABNT NBR ISO 27701 - Sistema de Gestão de Privacidade de Dados (SGPD)** - Visãogeral da ABNT NBR ISO 27701. - Estrutura da norma e seus requisitos. - Processo de implementação de umSGPD. - Relação entre ISO 27701 e ISO 27001. **Unidade 3: Lei Geral de Proteção de Dados (LGPD)** - Detalhes da LGPD, incluindo princípios, direitos do titular, obrigações do controlador e do operador. - Impacto daLGPD nas organizações. - Exigências de conformidade e penalidades. **Unidade 4: Principais Frameworks deMercado e Legislações de Referência** - Série ISO/IEC 27000 e ISO/IEC 27002 com foco em privacidade. -GDPR (Regulamento Geral de Proteção de Dados da União Europeia). - Outras legislações e regulamentações deproteção de dados ao redor do mundo. - Comparação entre LGPD e GDPR. **Unidade 5: Guia da ANPD eOrientações Regulatórias** - Visão geral dos guias e orientações emitidos pela ANPD. - Interpretação e aplicaçãodas orientações da ANPD. - Boas práticas e diretrizes para conformidade com a LGPD. **Unidade 6: Frameworkde Privacidade e Segurança da Informação da SGD (Parte Privacidade)** - Detalhamento do framework de privacidade da SGD. - Aspectos relacionados à privacidade de dados e sua integração com segurança dainformação. - Implementação de controles e práticas de acordo com o framework da SGD. **Unidade 7: Privacyby Design** - Conceito de "Privacy by Design" (Privacidade desde a concepção) e sua importância. - Integraçãode princípios de privacidade em projetos e sistemas. - Desenvolvimento e implementação de sistemas e serviçoscom foco na privacidade. **Unidade 8: Estudos de Caso e Exemplos Práticos** - Análise de casos reais deconformidade com a LGPD e ISO 27701. - Exemplos de implementação de Privacy by Design. - Discussões emgrupo e exercícios práticos. **Unidade 9: Avaliação e Exame Final** - Preparação para a avaliação final. -Revisão dos principais tópicos. - Exame final ou projeto prático relacionado à privacidade e proteção de dados.

Método de ensino-aprendizagem: Os alunos serão avaliados, em cada disciplina, levando em conta sua participação em sala de aula e ematividades como provas, simulações, estudos de caso, oficinas, dinâmicas, seminários, pesquisas de campo,visitas técnicas, projetos de intervenção, exposição dialogada, perguntas orientadoras, entre outras queestimulem o pensamento reflexivo e crítico. Serão atribuídas menções (SR, II, MI, MM, MS ou SS) em todas asdisciplinas do curso e no trabalho de conclusão do curso (TCC), sendo aprovados os alunos que obtiverem, emcada disciplina e no TCC, menção igual ou superior a MM e frequência mínima de 75% em cada disciplina. Seráconcedido ao aluno que obtiver aprovação nas disciplinas e no artigo um Certificado de Especialização emPrivacidade e Segurança da Informação.

Bibliografia básica: ABNT NBR ISO/IEC 27701:2019 "Técnicas de segurança – Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBRISO/IEC 27702 para a Gestão da Privacidade da Informação – Requisitos e Diretrizes". Rio de Janeiro: ABNT,2019. UNIVERSIDADE DE BRISTOL. CyBOK - The Cyber Security Body of Knowledge. 2021. BRASIL. Ministério daGestão e da Inovação. Secretaria de Governo Digital. Diretoria de Privacidade e Segurança da Informação. Guiado Framework de Privacidade e Segurança da Informação – versão 1.1.2. Brasília-DF: SGD, 2023.

Docente: Edna Dias Canedo.

METODOLOGIA CIENTÍFICA

Ementa: Conceitos de Ciência e Pesquisa. O Conhecimento Científico. Teorias e Validação. Método Científico. MetodologiaGeral da Pesquisa. Problema. Tipos de Pesquisa. Pesquisa Bibliográfica. Pesquisa Experimental e Não-Experimental.

Conteúdo Programático: **Unidade 1: Introdução à Ciência e Pesquisa** - Definição de Ciência e sua importância. - O papel da pesquisana construção do conhecimento. - Distinção entre conhecimento empírico e conhecimento científico. **Unidade2: O Conhecimento Científico** - Características do conhecimento científico. - Diferenças entre opinião, crença eevidência científica. - Paradigmas e revoluções científicas. **Unidade 3: Teorias e Validação** - Definição efunção das teorias na pesquisa científica. - Processo de formulação e teste de hipóteses. - Validade econfiabilidade na pesquisa. **Unidade 4: Método Científico** - Passos do método científico: observação,formulação de hipóteses, experimentação, análise de dados e conclusões. - Limitações do método científico. -Abordagens qualitativas e quantitativas na pesquisa. **Unidade 5: Metodologia Geral da Pesquisa** - Aimportância da metodologia na pesquisa científica. - Planejamento de pesquisa: escolha do tema, definição deobjetivos e questões de pesquisa. - Etapas da pesquisa: coleta, análise e interpretação de dados. **Unidade 6:Problema de Pesquisa** - Definição e importância do problema de pesquisa. - Formulação de um problema depesquisa claro e relevante. - Relação entre o problema de pesquisa, os objetivos e as hipóteses. **Unidade 7:Tipos de Pesquisa** - Pesquisa exploratória, descritiva e explicativa. - Pesquisa transversal e longitudinal. -Pesquisa de campo, de laboratório e documental. **Unidade 8: Pesquisa Bibliográfica** - O papel da pesquisabibliográfica na pesquisa científica. - Métodos de busca e seleção de fontes bibliográficas. - Organização e citaçãode referências bibliográficas. **Unidade 9: Pesquisa Experimental e Não-Experimental** - Princípios da pesquisaexperimental. - Variáveis independentes e dependentes. - Desenhos de pesquisa não-experimentais: estudo decaso, pesquisa de campo, pesquisa correlacional, etc. **Unidade 10: Coleta e Análise de Dados** - Métodos decoleta de dados: questionários, entrevistas, observações, etc. - Técnicas de amostragem. - Análise qualitativa equantitativa de dados. **Unidade 11: Ética na Pesquisa** - Princípios éticos na pesquisa científica. - Consentimento informado e proteção de participantes. - Plágio, falsificação e má conduta científica. **Unidade12: Apresentação e Comunicação de Resultados** - Estrutura de um relatório de pesquisa. - Apresentação deresultados de forma clara e objetiva. - Publicação e divulgação científica. **Unidade 13: Trabalho Final dePesquisa** - Elaboração de um projeto de pesquisa ou trabalho final. - Apoio e orientação ao longo do processode pesquisa. - Apresentação e defesa do trabalho final.

Método de ensino-aprendizagem: Os alunos serão avaliados, em cada disciplina, levando em conta sua participação em sala de aula e ematividades como provas, simulações, estudos de caso, oficinas, dinâmicas, seminários, pesquisas de campo,visitas técnicas, projetos de intervenção, exposição dialogada, perguntas orientadoras, entre outras queestimulem o pensamento reflexivo e crítico. Serão atribuídas menções (SR, II, MI, MM, MS ou SS) em todas asdisciplinas do curso e no trabalho de conclusão do curso (TCC), sendo aprovados os alunos que obtiverem, emcada disciplina e no TCC, menção igual ou superior a MM e frequência mínima de 75% em cada disciplina. Seráconcedido ao aluno que obtiver aprovação nas disciplinas e no artigo um Certificado de Especialização emPrivacidade e Segurança da Informação.

Bibliografia: WAZLAWICK, R. S. - Metodologia de Pesquisa para Ciência da Computação. 3ª ed. Rio de Janeiro:Elsevier/Campus, 2020 (livro-texto). ROSA, C. A. P. – História da Ciência – A Ciência Moderna. Vol. II-Tomo I, 2ªed. Fundação

Alexandre Gusmão, 2012. BOOTH, W. C.; COLOMB, G. G.; WILLIAMS, J. M. A Arte da pesquisa,edição padrão. São Paulo: Martins Fontes, 2019.

Docente: William Ferreira Giozza.

DIREITO DIGITAL E PRIVACIDADE

Ementa: Overview de tópicos relacionados na Constituição Federal; Código de Defesa do Consumidor (art. 43); Lei daPropriedade Industrial (art. 195); Código Civil (art. 20); Lei de Acesso à Informação; Lei Carolina Dickman;Marco Civil da Internet; Convenção de Budapeste; Lei Geral de Proteção de Dados Pessoais (LGPD). Histórico(GDPR e outras normas internacionais, e o surgimento no Brasil). Princípios e principais conceitos. Escopo deaplicação. Bases legais. Tratamento de Dados Pessoais no Poder Público. Direitos do titular de dados.Transferência internacional de dados.

Conteúdo Programático: **Unidade 1: Introdução aos Fundamentos Legais** - Visão geral dos principais dispositivos legais relacionadosà privacidade e proteção de dados. - Importância da legislação na sociedade e nos negócios. **Unidade 2:Constituição Federal** - Análise dos tópicos relevantes da Constituição Federal relacionados à privacidade eproteção de dados. - Direitos fundamentais e garantias individuais. **Unidade 3: Código de Defesa doConsumidor (Art. 43)** - O direito à privacidade e a proteção do consumidor. - Regras e responsabilidades dasempresas em relação aos dados dos consumidores. **Unidade 4: Lei da Propriedade Industrial (Art. 195)** -Aspectos da proteção de propriedade intelectual relacionados à privacidade. - Patentes, marcas registradas esegredos comerciais. **Unidade 5: Código Civil (Art. 20)** - Direito à imagem e sua relação com a privacidade. - Responsabilidade civil por violação de privacidade. **Unidade 6: Lei de Acesso à Informação** - Acesso àinformação pública e suas implicações na privacidade. - Transparência governamental e proteção de dados.**Unidade 7: Lei Carolina Dickman** - Análise da Lei Carolina Dickman e sua importância para a proteção daprivacidade de crianças e adolescentes na internet. **Unidade 8: Marco Civil da Internet** - Princípios ediretrizes do Marco Civil da Internet. - Implicações para a privacidade e a proteção de dados pessoais online.**Unidade 9: Convenção de Budapeste** - Visão geral da Convenção de Budapeste sobre Cibercrime. - Implicações para a proteção de dados e a cooperação internacional. **Unidade 10: Lei Geral de Proteção deDados Pessoais (LGPD) - Histórico** - Evolução da LGPD no contexto internacional. - Comparação com o GDPR eoutras normas internacionais. **Unidade 11: Princípios e Conceitos da LGPD** - Princípios fundamentais daLGPD. - Conceitos-chave, como dados pessoais, titular, controlador e operador. **Unidade 12: Escopo deAplicação da LGPD** - Quem está sujeito à LGPD. - Definição de tratamento de dados pessoais. **Unidade 13:Bases Legais para o Tratamento de Dados Pessoais** - Consentimento e outras bases legais para o tratamentode dados. - Tratamento de dados sensíveis. **Unidade 14: Tratamento de Dados Pessoais no Poder Público** -Regras específicas para o tratamento de dados pessoais pelo setor público. - Transparência e accountability nogoverno. **Unidade 15: Direitos do Titular de Dados** - Direitos dos indivíduos em relação aos seus dadospessoais. - Como exercer esses direitos. **Unidade 16: Transferência Internacional de Dados** - Regras para atransferência de dados pessoais para o exterior. - Mecanismos de transferência de dados adequados.

Método de ensino-aprendizagem: Os alunos serão avaliados, em cada disciplina, levando em conta sua participação em sala de aula e ematividades como provas, simulações, estudos de caso, oficinas, dinâmicas, seminários, pesquisas de campo,visitas técnicas, projetos de intervenção, exposição dialogada, perguntas orientadoras, entre outras queestimulem o pensamento reflexivo e crítico. Serão atribuídas menções (SR, II, MI, MM, MS ou SS) em todas asdisciplinas do curso e no trabalho de conclusão do curso (TCC), sendo aprovados os alunos que obtiverem, emcada disciplina e no TCC, menção igual ou superior a MM e frequência mínima de 75% em cada disciplina. Será concedido ao aluno que obtiver aprovação nas

disciplinas e no artigo um Certificado de Especialização emPrivacidade e Segurança da Informação.

Bibliografia: Cyber Security Body of Knowledge (CyBOK). Versão 1.1, 2021. UNIVERSIDADE DE BRISTOL. Capítulo 5 - Privacy& Online Rights, Knowledge Are. p. 171-198. BRASIL. Guia de Boas Práticas Lei Geral de Proteção de Dados(LGPD). Agosto de 2020. DONEDA, Danilo. Da Privacidade à Proteção de Dados Pessoais.Thomson Reuters,Revista dos Tribunais; 2ª ed. 7 de out. 2019.

Docente: Virgínia de Melo Dantas Trinks.

OPERAÇÕES DE SEGURANÇA

Ementa: Fundamentos de segurança da informação; principais ameaças; gestão de identidade e acesso; criptografia;segurança em redes; sistemas de detecção e prevenção; monitoramento de redes e sistemas; SOC; backup erecuperação; Security by Design.

Conteúdo Programático: **Unidade 1: Introdução aos Fundamentos de Segurança da Informação** - Conceitos básicos de segurança dainformação. - Importância da segurança da informação nas organizações. - A evolução das ameaças cibernéticas.**Unidade 2: Principais Ameaças à Segurança da Informação** - Tipos de ameaças cibernéticas, como malware,phishing, ransomware e ataques de engenharia social. - Táticas, técnicas e procedimentos (TTPs) utilizados porinvasores. - Estudos de casos de incidentes de segurança. **Unidade 3: Gestão de Identidade e Acesso** -Autenticação e autorização. - Controle de acesso baseado em funções (RBAC). - Single Sign-On (SSO) egerenciamento de identidade. - Autenticação multifator (MFA). **Unidade 4: Criptografia** - Princípios dacriptografia. - Criptografia simétrica e assimétrica. - Uso de criptografia para proteger dados em trânsito e emrepouso. - Protocolos criptográficos comuns. **Unidade 5: Segurança em Redes** - Conceitos de segurança derede. - Firewalls, IDS (Sistemas de Detecção de Intrusão) e IPS (Sistemas de Prevenção de Intrusão). - VirtualPrivate Networks (VPNs) e segurança de Wi-Fi. - Proteção contra ataques de rede, como DDoS. **Unidade 6:Sistemas de Detecção e Prevenção** - Funcionamento de sistemas de detecção de intrusão (IDS) e sistemas deprevenção de intrusão (IPS). - Monitoramento em tempo real e análise de tráfego. - Configuração e políticas deIDS/IPS. **Unidade 7: Monitoramento de Redes e Sistemas** - A importância do monitoramento contínuo. -Ferramentas de monitoramento de rede e sistemas. - Análise de logs e alertas de segurança. - Resposta aincidentes. **Unidade 8: Centro de Operações de Segurança (SOC)** - Funções e responsabilidades de um SOC.- Processos de triagem, investigação e resposta a incidentes. - Desenvolvimento de políticas e procedimentos doSOC. **Unidade 9: Backup e Recuperação** - Estratégias de backup e recuperação de dados. - Políticas deretenção de dados. - Testes de recuperação de desastres. **Unidade 10: Security by Design** - Princípios doSecurity by Design. - Integração da segurança desde o início do ciclo de desenvolvimento de software. -Considerações de segurança em arquitetura de sistemas. **Unidade 11: Tendências e Desafios em Segurança daInformação** - Exploração das tendências emergentes em segurança da informação. - Desafios futuros eevolução das ameaças cibernéticas. - O papel da conformidade regulatória. **Unidade 12: Aplicações Práticas eEstudos de Caso** - Estudos de casos reais de incidentes de segurança. - Exercícios práticos de configuração desegurança. - Projetos práticos de implementação de medidas de segurança.

Método de ensino-aprendizagem: Os alunos serão avaliados, em cada disciplina, levando em conta sua participação em sala de aula e ematividades como provas, simulações, estudos de caso, oficinas, dinâmicas, seminários, pesquisas de campo,visitas técnicas, projetos de intervenção, exposição dialogada, perguntas orientadoras, entre outras queestimulem o pensamento reflexivo e crítico. Serão atribuídas menções (SR, II, MI, MM, MS ou SS) em todas asdisciplinas do curso e no trabalho de conclusão do curso (TCC), sendo aprovados os alunos que obtiverem, emcada disciplina e no TCC, menção igual ou superior a MM e frequência mínima de 75% em cada disciplina. Seráconcedido ao aluno que obtiver aprovação nas disciplinas e no artigo um Certificado de Especialização emPrivacidade e Segurança da Informação.

Bibliografia: KUROSE, J. and K. Ross. Computer Networking: A Top-Down Approach. Pearson, USA, 8ª ed., p. 800, 2022.BEHROUZ, Forouzan. TCP/IP Protocol Suite.

McGraw-hill Forouzan Networking USA, 4ª ed., p.1024, 2017.ZIMMERMAN, C. Ten Strategies of a World-Class Cybersecurity Operations Center. MITRE Editora, p.346, 2014.

Docente: Georges Daniel Amvame Nze.

FUNDAMENTOS DE GESTÃO DE INCIDENTES CIBERNÉTICOS

Ementa: Compreensão do ambiente de ameaças atual e dos processos de gestão incidentes. Código de ética de um CSIRT.Ferramentas e tecnologias de segurança usadas por um CSIRT. Identificação de informações críticas. Detecção eanálise de incidentes. Processo de triagem. Identificação dos passos básicos da resposta. Ataques envolvendoDNS e uso de DNS no processo de tratamento de incidentes. Busca de informações de contato. Coordenação daresposta a incidentes e disseminação de informações. Tratamento de ataques comuns envolvendo e-mails ecódigos maliciosos. Cooperação com as polícias e os operadores da justiça.

Conteúdo Programático: **Unidade 1: Introdução à Gestão de Incidentes de Segurança** - Conceitos fundamentais de segurança dainformação. - Compreensão do ambiente de ameaças atual. - Importância da gestão de incidentes. **Unidade 2:Código de Ética de um CSIRT** - Ética e responsabilidade na atuação de um CSIRT. - Princípios éticos ediretrizes de conduta. - Respeito à privacidade e à confidencialidade. **Unidade 3: Ferramentas e Tecnologias deSegurança para CSIRTs** - Ferramentas e recursos utilizados em um CSIRT. - Monitoramento de segurança. -Softwares de detecção de ameaças. - Automação e orquestração de incidentes. **Unidade 4: Identificação deInformações Críticas** - Identificação e classificação de ativos críticos. - Proteção de informações sensíveis. -Políticas de retenção de dados. **Unidade 5: Detecção e Análise de Incidentes** - Métodos e técnicas dedetecção de incidentes. - Análise de padrões e indicadores de comprometimento. - Investigação forense digital.**Unidade 6: Processo de Triagem de Incidentes** - Triagem de incidentes: classificação e priorização. - Criaçãode categorias de incidentes. - Documentação e registro de incidentes. **Unidade 7: Passos Básicos da Respostaa Incidentes** - Procedimentos iniciais de resposta. - Isolamento de sistemas comprometidos. - Contenção deincidentes. - Notificação de partes interessadas. **Unidade 8: Ataques envolvendo DNS e Uso de DNS noTratamento de Incidentes** - Ataques DNS comuns. - Uso do DNS para detecção e resposta a incidentes. -Proteção do DNS contra abusos. **Unidade 9: Busca de Informações de Contato** - Localização e contato compartes afetadas. - Comunicação com outras equipes de segurança. - Coleta de informações relevantes.**Unidade 10: Coordenação da Resposta a Incidentes e Disseminação de Informações** - Coordenação interna eexterna. - Compartilhamento de informações com outros CSIRTs e organizações. - Comunicação eficaz duranteum incidente. **Unidade 11: Tratamento de Ataques Comuns envolvendo E-mails e Códigos Maliciosos** -Análise de e-mails de phishing. - Mitigação de ataques de malware. - Prevenção e resposta a ransomware.**Unidade 12: Cooperação com as Polícias e os Operadores da Justiça** - Papel de um CSIRT na investigação decrimes cibernéticos. - Cooperação com autoridades legais. - Preparação para procedimentos judiciais. **Unidade13: Exercícios Práticos e Estudos de Caso** - Simulações de incidentes de segurança. - Análise de estudos decaso reais. - Aplicação prática dos conceitos aprendidos. **Unidade 14: Avaliação e Melhoria Contínua** -Avaliação do desempenho do CSIRT. - Implementação de melhorias no processo de resposta a incidentes. -Aperfeiçoamento de políticas e procedimentos.

Método de ensino-aprendizagem: Os alunos serão avaliados, em cada disciplina, levando em conta sua participação em sala de aula e ematividades como provas, simulações, estudos de caso, oficinas, dinâmicas, seminários, pesquisas de campo,visitas técnicas, projetos de intervenção, exposição dialogada, perguntas orientadoras, entre outras queestimulem o pensamento reflexivo e crítico. Serão atribuídas menções (SR, II, MI, MM, MS ou SS) em todas asdisciplinas do curso e no trabalho de conclusão do curso (TCC), sendo aprovados os alunos que obtiverem, emcada disciplina e no TCC, menção igual ou superior a MM e frequência mínima de

75% em cada disciplina. Seráconcedido ao aluno que obtiver aprovação nas disciplinas e no artigo um Certificado de Especialização emPrivacidade e Segurança da Informação.

Bibliografia: Cyber Security Body of Knowledge (CyBOK). Version 1.1, 2021 UNIVERSIDADE DE BRISTOL. Capítulo 8 -Security Operations & Incident Management, p. 251-286. BRASIL. Ministério da Gestão e da Inovação. Secretariade Governo Digital. Diretoria de Privacidade e Segurança da Informação. Guia de Resposta a Incidentes deSegurança – versão 3.0 Brasília-DF: SGD, 2023. PEMBLE, M. W. A.; GOUCHER, Wendy F. The CIOś Guide toInformation Security Incident Managment. Boca Raton, FL: CRC Press Editora, p. 266, 2019.

Docente: Éder Souza Gualberto.

DESENVOLVIMENTO SEGURO

Ementa: Conceitos de segurança da informação; tecnologias e processos da segurança de redes; política de segurança dossistemas de informação; projetos de laboratório de segurança. Processo de desenvolvimento seguro; Ecossistema OWASP; Coleta de requisitos de segurança; Princípios de design seguro; Modelagem de ameaças; STRIDE;DREAD; DevSecOps; SAST; DAST; Segurança em APIs.

Conteúdo Programático: **Unidade 1: Introdução aos Conceitos de Segurança da Informação** - Conceitos básicos de segurança dainformação. - Objetivos e princípios da segurança da informação. - Importância da segurança da informação nasorganizações. **Unidade 2: Tecnologias e Processos de Segurança de Redes** - Mecanismos de segurança derede, como firewalls, IDS/IPS e VPNs. - Protocolos e práticas seguras de comunicação. - Segurança em redessem fio e redes móveis. **Unidade 3: Política de Segurança dos Sistemas de Informação** - Desenvolvimento eimplementação de políticas de segurança. - Gestão de riscos e conformidade regulatória. - Monitoramento eauditoria de políticas de segurança. **Unidade 4: Projetos de Laboratório de Segurança** - Criação econfiguração de laboratórios de segurança. - Simulações de ameaças e ataques em ambientes controlados. -Práticas seguras de testes em laboratório. **Unidade 5: Processo de Desenvolvimento Seguro** - Princípios dodesenvolvimento seguro de software. - Integração da segurança no ciclo de vida do desenvolvimento. - Avaliaçãode riscos de segurança em desenvolvimento de software. **Unidade 6: Ecossistema OWASP (Open WebApplication Security Project)** - Visão geral do OWASP. - Top 10 de ameaças em aplicações web. - Ferramentase recursos do OWASP. **Unidade 7: Coleta de Requisitos de Segurança** - Identificação e documentação derequisitos de segurança. - Compreensão das necessidades do cliente em relação à segurança. - Priorização derequisitos de segurança. **Unidade 8: Princípios de Design Seguro** - Design de sistemas e aplicações com focona segurança. - Práticas de arquitetura segura. - Modelagem de ameaças e cenários de ataque. **Unidade 9:Modelagem de Ameaças e Métodos de Avaliação** - Metodologias de modelagem de ameaças. - STRIDE(Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege). - DREAD(Damage, Reproducibility, Exploitability, Affected Users, Discoverability). **Unidade 10: DevSecOps** -Integração da segurança no ciclo de vida DevOps. - Práticas de DevSecOps. - Automação de testes de segurança.**Unidade 11: Segurança Estática (SAST) e Dinâmica (DAST) de Aplicações** - Análise estática de código fonte.- Análise dinâmica de segurança de aplicações. - Ferramentas e técnicas SAST e DAST. **Unidade 12: Segurançaem APIs** - Riscos de segurança em APIs. - Autenticação e autorização em APIs. - Proteção contra ataques emAPIs. **Unidade 13: Estudos de Caso e Exemplos Práticos** - Análise de casos reais de vulnerabilidades eataques de segurança. - Exercícios práticos de modelagem de ameaças. - Desenvolvimento seguro de aplicações.**Unidade 14: Avaliação e Melhoria Contínua** - Avaliação do desempenho em segurança da informação. -Implementação de melhorias em processos e práticas de segurança. - Atualização de políticas e diretrizes desegurança.

Método de ensino-aprendizagem: Os alunos serão avaliados, em cada disciplina, levando em conta sua participação em sala de aula e ematividades como provas, simulações, estudos de caso, oficinas, dinâmicas, seminários, pesquisas de campo,visitas técnicas, projetos de intervenção, exposição dialogada, perguntas orientadoras, entre outras queestimulem o pensamento reflexivo e crítico. Serão atribuídas menções (SR, II, MI, MM, MS ou SS) em todas asdisciplinas do curso e no trabalho de conclusão do curso (TCC), sendo aprovados os alunos que obtiverem, emcada disciplina e no TCC, menção igual ou superior a MM e frequência mínima de

75% em cada disciplina. Seráconcedido ao aluno que obtiver aprovação nas disciplinas e no artigo um Certificado de Especialização emPrivacidade e Segurança da Informação.

Bibliografia: PRESSMAN, Roger S.; MAXIM, Bruce R. Engenharia de software-9. McGraw Hill Brasil, 2021. ATTWOOD, Sam;WILLIAMS, Ashley. Exploring the UK Cyber Skills Gap through a mapping of active job listings to the CyberSecurity Body of Knowledge (CyBOK). In: Proceedings of the 27th International Conference on Evaluation andAssessment in Software Engineering, p. 273-278, 2023. CABRAL, Carlos; CAPRINO, Willian. Trilhas em segurançada informação: caminhos e ideias para a proteção de dados. Brasport Editora, 1ª ed. p. 411, 2015.

Docente: Fábio Lúcio Lopes de Mendonça.

SEGURANÇA EM NUVEM

Ementa: Fundamentos de nuvem. Principais ataques e problemas de segurança em nuvem. Segurança de dados nanuvem. Segurança de infraestrutura em cloud. Ferramentas e técnicas para configurações seguras de nuvempública como AWS, Azure e GCP. Protocolos de autenticação e autorização em nuvem. Projeção e implementaçãode planos de continuidade de negócios e recuperação de desastres em nuvem. Auditoria de segurança na nuvem.Testes de penetração em nuvem.

Conteúdo Programático: **Unidade 1: Introdução aos Fundamentos de Nuvem** - Conceitos básicos de computação em nuvem. -Modelos de serviço (IaaS, PaaS, SaaS) e modelos de implantação (pública, privada, híbrida). - Vantagens edesafios da computação em nuvem. **Unidade 2: Principais Ataques e Problemas de Segurança em Nuvem** -Ameaças comuns à segurança em nuvem. - Ataques de negação de serviço (DDoS) em ambientes de nuvem. -Vazamento de dados e ameaças internas. **Unidade 3: Segurança de Dados na Nuvem** - Proteção de dadosem repouso e em trânsito. - Criptografia de dados na nuvem. - Gerenciamento de chaves de criptografia.**Unidade 4: Segurança de Infraestrutura em Cloud** - Gerenciamento de identidade e acesso (IAM). -Configuração segura de servidores e redes em nuvem. - Monitoramento e detecção de ameaças em tempo real.**Unidade 5: Ferramentas e Técnicas para Configurações Seguras em Nuvem Pública** - Configuração seguraem AWS, Azure e GCP. - Uso de templates de infraestrutura como código (IaC). - Avaliação de configuraçõescomuns e melhores práticas. **Unidade 6: Protocolos de Autenticação e Autorização em Nuvem** - OAuth,OpenID Connect e SAML. - Gerenciamento de identidade federada. - Single Sign-On (SSO) em ambientes denuvem. **Unidade 7: Continuidade de Negócios e Recuperação de Desastres em Nuvem** - Planos decontinuidade de negócios na nuvem. - Backups e replicação de dados. - Recuperação de desastres em ambientesde nuvem. **Unidade 8: Auditoria de Segurança na Nuvem** - Necessidades de auditoria e conformidade nanuvem. - Ferramentas de monitoramento de segurança. - Geração e análise de registros de auditoria. **Unidade9: Testes de Penetração em Nuvem** - Metodologias e abordagens para testes de penetração. - Avaliação devulnerabilidades em ambientes de nuvem. - Relatórios e mitigação de descobertas de segurança. **Unidade 10:Estudos de Caso e Exercícios Práticos** - Análise de casos reais de incidentes de segurança em nuvem. -Exercícios práticos de configuração segura em nuvem. - Simulações de incidentes e respostas. **Unidade 11:Avaliação e Melhoria Contínua** - Avaliação da postura de segurança em nuvem. - Implementação de melhoriase ajustes. - Acompanhamento de ameaças emergentes em nuvem.

Método de ensino-aprendizagem: Os alunos serão avaliados, em cada disciplina, levando em conta sua participação em sala de aula e ematividades como provas, simulações, estudos de caso, oficinas, dinâmicas, seminários, pesquisas de campo,visitas técnicas, projetos de intervenção, exposição dialogada, perguntas orientadoras, entre outras queestimulem o pensamento reflexivo e crítico. Serão atribuídas menções (SR, II, MI, MM, MS ou SS) em todas asdisciplinas do curso e no trabalho de conclusão do curso (TCC), sendo aprovados os alunos que obtiverem, emcada disciplina e no TCC, menção igual ou superior a MM e frequência mínima de 75% em cada disciplina. Seráconcedido ao aluno que obtiver aprovação nas disciplinas e no artigo um Certificado de Especialização emPrivacidade e Segurança da Informação.

Bibliografia: Cyber Security Body of Knowledge (CyBOK). Version 1.1, 2021. UNIVERSIDADE DE BRISTOL. Capítulo 8 -Security Operations & Incident Management; Capítulo 11 - Operating Systems and Virtualisation; Capítulo 14 - Authentication, Authorisation & Accountability; Capítulo 19 - Network Security.

BRASIL. Instrução Normativa Nº5, de 30 de agosto de 2021 do Gabinete de Segurança Institucional, Brasília, DF. Edição 165, Seção 1, p. 2.VACCA, Jhon R. Cloud Computing Security: Foundations and Challenges; 1ª Ed. p. 520, 2016. DOIhttps://doi.org/10.1201/9781315372112; ISBN 9781315372112.

Docente: Robson de Oliveira Albuquerque.

SEGURANÇA OFENSIVA

Ementa: Introdução a testes de intrusão e análise de vulnerabilidades. Reconhecimento. Enumeração. Exploração deinfraestrutura. Exploração de aplicações web. Escalação de privilégios e movimentação lateral. Engenharia social.Evasão de defesa. Exploração de redes sem fio. Exploração em Active Directory. Metodologias de testes deintrusão.

Conteúdo Programático: **Unidade 1: Introdução a Testes de Intrusão e Análise de Vulnerabilidades** - Conceitos fundamentais detestes de intrusão e análise de vulnerabilidades. - Objetivos e benefícios dos testes de intrusão. - Abordagens detestes de segurança. **Unidade 2: Reconhecimento** - Fases do reconhecimento. - Coleta de informações sobrealvos. - Ferramentas e técnicas de reconhecimento. **Unidade 3: Enumeração** - Enumeração de serviços esistemas. - Identificação de pontos de entrada potenciais. - Técnicas de enumeração em redes e sistemas.**Unidade 4: Exploração de Infraestrutura** - Identificação e exploração de vulnerabilidades em sistemasoperacionais. - Ataques a serviços de rede. - Utilização de exploits. **Unidade 5: Exploração de AplicaçõesWeb** - Identificação de vulnerabilidades em aplicações web. - Injeções de SQL, Cross-Site Scripting (XSS),Cross-Site Request Forgery (CSRF), entre outros. - Ferramentas de análise de segurança para aplicações web.**Unidade 6: Escalação de Privilégios e Movimentação Lateral** - Escalação de privilégios em sistemas e redes.
- Movimentação lateral na infraestrutura. - Aumento do acesso e persistência. **Unidade 7: Engenharia Social**- Técnicas de engenharia social. - Phishing, pretexting, tailgating, entre outros. - Prevenção e conscientização.**Unidade 8: Evasão de Defesa** - Evitando a detecção por sistemas de segurança. - Ofuscação de malware. -Técnicas de evasão de antivírus e IDS/IPS. **Unidade 9: Exploração de Redes Sem Fio** - Vulnerabilidades emredes Wi-Fi. - Ataques de força bruta em redes sem fio. - Uso de ferramentas para testar a segurança em redesWi-Fi. **Unidade 10: Exploração em Active Directory** - Segurança e ataques a infraestruturas baseadas emActive Directory. - Exploração de vulnerabilidades em serviços AD. - Escalação de privilégios no ambiente AD.**Unidade 11: Metodologias de Testes de Intrusão** - Frameworks e metodologias de testes de intrusão, comoOWASP Testing Guide e Penetration Testing Execution Standard (PTES). - Planejamento de testes de intrusão. -Relatórios e documentação de resultados. **Unidade 12: Ética e Conformidade em Testes de Intrusão** -Códigos de ética e conduta em testes de intrusão. - Conformidade regulatória e legal. - Responsabilidades dotestador de intrusão. **Unidade 13: Exercícios Práticos e Estudos de Caso** - Simulações de testes de intrusãoem ambientes controlados. - Análise de estudos de caso de testes de intrusão reais. - Aplicação prática dosconceitos aprendidos. **Unidade 14: Avaliação e Melhoria Contínua** - Avaliação do desempenho de segurançaapós os testes de intrusão. - Implementação de melhorias e mitigação de vulnerabilidades. - Acompanhamentode ameaças e atualização de medidas de segurança.

Método de ensino-aprendizagem: Os alunos serão avaliados, em cada disciplina, levando em conta sua participação em sala de aula e ematividades como provas, simulações, estudos de caso, oficinas, dinâmicas, seminários, pesquisas de campo,visitas técnicas, projetos de intervenção, exposição dialogada, perguntas orientadoras, entre outras queestimulem o pensamento reflexivo e crítico. Serão atribuídas menções (SR, II, MI, MM, MS ou SS) em todas asdisciplinas do curso e no trabalho de conclusão do curso (TCC), sendo aprovados os alunos que obtiverem, emcada disciplina e no TCC, menção igual ou superior a MM e frequência mínima de 75% em cada disciplina. Seráconcedido ao aluno que obtiver aprovação nas disciplinas e no artigo um Certificado de Especialização emPrivacidade e Segurança

da Informação.

Bibliografia: WYLIE, Phillip L.; CRAWLEY, Kim. The Pentester Blueprint: Starting a career as an ethical hacker. John Wiley &Sons Editora, p. 192, 2020. ERICKSON, Karnel. Hacking. Francesco Cammardella, 2019. MESSIER, Ric. CEH v10Certified Ethical Hacker Study Guide. John Wiley & Sons Editora, p. 592, 2019.

Docente: João José Costa Gondim

TÓPICOS AVANÇADOS EM GESTÃO DE INCIDENTES CIBERNÉTICOS

Ementa: Revisão do ciclo de vida do tratamento de incidentes. Ameaças avançadas persistentes (APTs). Revisão dastécnicas e categorias de análise de malware e de artefatos. Causas fundamentais das vulnerabilidades.Tratamento de vulnerabilidades. Análise, coordenação e resposta a major events e incidentes complexos.Desenvolvimento de publicações e comunicações eficazes.

Conteúdo Programático: Módulo 1: Revisão do ciclo de vida do tratamento de incidentes Introdução ao ciclo de vida de tratamento deincidentes Fases do ciclo de vida: Detecção, Avaliação, Resposta e Recuperação Papéis e responsabilidadesdurante cada fase Melhores práticas e metodologias Módulo 2: Ameaças Avançadas Persistentes (APTs) Definiçãoe características das APTs Histórico e evolução das APTs Casos de estudo de ataques APT notáveis Estratégias dedetecção e mitigação de APTs Módulo 3: Revisão das técnicas e categorias de análise de malware e de artefatosIntrodução à análise de malware Categorias de malware: Vírus, Trojans, Worms, Ransomware, etc. Técnicas deanálise estática e dinâmica Ferramentas e recursos para análise de malware Módulo 4: Causas fundamentais dasvulnerabilidades Compreendendo as causas subjacentes de vulnerabilidades Erros de programação comunsVulnerabilidades de configuração Exploração de vulnerabilidades por atacantes Módulo 5: Tratamento devulnerabilidades Avaliação de risco e priorização de vulnerabilidades Estratégias de mitigação e correção Gestãode patches e atualizações de segurança Testes de penetração para verificar correções Módulo 6: Análise,coordenação e resposta a major events e incidentes complexos Identificação de eventos e incidentes complexosCoordenação de resposta com várias partes interessadas Utilização de equipes de resposta a incidentes (CSIRTs)Exercícios de simulação de incidentes Módulo 7: Desenvolvimento de publicações e comunicações eficazesComunicação interna e externa durante incidentes Elaboração de relatórios pós-incidentes Comunicação com aalta administração e partes interessadas Gerenciamento de relações públicas em incidentes de segurançaAvaliação Final: Exame teórico abrangendo os tópicos do curso Estudo de caso prático envolvendo um incidentesimulado Apresentação de um plano de resposta a incidentes.

Método de ensino-aprendizagem: Os alunos serão avaliados, em cada disciplina, levando em conta sua participação em sala de aula e ematividades como provas, simulações, estudos de caso, oficinas, dinâmicas, seminários, pesquisas de campo,visitas técnicas, projetos de intervenção, exposição dialogada, perguntas orientadoras, entre outras queestimulem o pensamento reflexivo e crítico. Serão atribuídas menções (SR, II, MI, MM, MS ou SS) em todas asdisciplinas do curso e no trabalho de conclusão do curso (TCC), sendo aprovados os alunos que obtiverem, emcada disciplina e no TCC, menção igual ou superior a MM e frequência mínima de 75% em cada disciplina. Seráconcedido ao aluno que obtiver aprovação nas disciplinas e no artigo um Certificado de Especialização emPrivacidade e Segurança da Informação.

Bibliografia: The Cyber Security Body of Knowledge (CyBOK). Versão 1.1, 2021. UNIVERSIDADE DE BRISTOL. Capítulo 6 -Malware & Attack Technologies, p. 2021-2021. BRASIL. Ministério da Gestão e da Inovação. Secretaria deGoverno Digital. Diretoria de Privacidade e Segurança da Informação. Guia de Gerenciamento de Vulnerabilidadese Modelo de Política de Gerenciamento de Vulnerabilidades: versão 2.0 Brasília-DF: SGD, 2023. BRASIL.Ministério da Gestão e da Inovação. Secretaria de Governo Digital. Diretoria de Privacidade e Segurança daInformação. Guia de Resposta a Incidentes de Segurança – versão 3.0 Brasília-DF: SGD.

Docente: João José Costa Gondim.

ELABORAÇÃO DE ARTIGOS CIENTÍFICOS

Ementa: Instrumentalizar o(a) aluno(a) para realizar uma ciência básica e relatar seus resultados em um artigo científico;apresentar as principais seções de um artigo científico e o que deve ser relatado em cada uma delas; apresentaros principais aspectos da escrita científica; apresentar as bases de uma pesquisa bibliográfica.

Conteúdo programático: Módulo 1: Introdução à Pesquisa Científica Definição e importância da pesquisa científica O papel da pesquisa naprodução do conhecimento Diferenças entre pesquisa básica e aplicada Módulo 2: Etapas do Processo dePesquisa Formulação de uma pergunta de pesquisa Revisão da literatura: identificação de lacunas e revisãobibliográfica Coleta de dados: métodos qualitativos e quantitativos Análise e interpretação de dados Módulo 3:Estrutura e Conteúdo de um Artigo Científico Introdução: apresentação do problema de pesquisa e justificativaRevisão da literatura: síntese das pesquisas anteriores Metodologia: descrição dos métodos de pesquisaResultados: apresentação dos principais achados Discussão: interpretação dos resultados e implicaçõesConclusão: sumário das descobertas e possíveis direções futuras Módulo 4: Escrita Científica Efetiva Estilo deescrita científica Uso adequado de citações e referências bibliográficas Evitar plágio e má conduta acadêmicaEstratégias para clareza e concisão na escrita Módulo 5: Apresentação Gráfica de Dados e Tabelas Escolha ecriação de gráficos apropriados Design de tabelas eficazes Interpretação de gráficos e tabelas Módulo 6: PesquisaBibliográfica e Gerenciamento de Referências Identificação de fontes de pesquisa confiáveis Utilização de basesde dados acadêmicas Ferramentas de gerenciamento de referências (e.g., EndNote, Zotero) Técnicas de buscaeficazes Módulo 7: Ética na Pesquisa Científica Princípios éticos na pesquisa Consentimento informado e éticacom seres humanos e animais Prevenção de fraudes e má conduta científica Responsabilidade autoral ecolaboração Módulo 8: Preparação e Submissão de Artigos Científicos Preparação do manuscrito para submissãoEscolha da revista e adequação ao estilo da revista Processo de revisão por pares Gerenciamento de revisões erespostas aos revisores Avaliação Final: Os alunos serão avaliados por meio da elaboração de um artigo científicoem um formato adequado, seguindo todas as diretrizes apresentadas durante o curso.

Método de ensino-aprendizagem: Os alunos serão avaliados, em cada disciplina, levando em conta sua participação em sala de aula e ematividades como provas, simulações, estudos de caso, oficinas, dinâmicas, seminários, pesquisas de campo,visitas técnicas, projetos de intervenção, exposição dialogada, perguntas orientadoras, entre outras queestimulem o pensamento reflexivo e crítico. Serão atribuídas menções (SR, II, MI, MM, MS ou SS) em todas asdisciplinas do curso e no trabalho de conclusão do curso (TCC), sendo aprovados os alunos que obtiverem, emcada disciplina e no TCC, menção igual ou superior a MM e frequência mínima de 75% em cada disciplina. Seráconcedido ao aluno que obtiver aprovação nas disciplinas e no artigo um Certificado de Especialização emPrivacidade e Segurança da Informação.

Bibliografia: BRASIL. Advocacia Geral da União. Casa Civil. Controlaria Geral da União. Guia de Boas Práticas - Lei Geral deProteção de Dados Pessoais, consolidado no âmbito do Comitê Central de Governança de Dados. SCHUSTER, E.;LEVKOWITZ, H. A. I. M.; OLIVEIRA JUNIOR, O. N. Writing Scientific Papers in English Successfully: Your Complete
Roadmap. 1ª ed. São Carlos, Compacta Gráfica e Editora, p. 194, 2014. The Cyber Security Body of Knowledge(CyBOK). Versão 1.1, 2021. UNIVERSIDADE DE BRISTOL. Capítulo 9, seção 9.1.3 - Conceptual Models, p. 296-300.

Docente: Demétrio Antonio da Silva Filho.

INTELIGÊNCIA DE AMEAÇAS CIBERNÉTICAS

Ementa: Fundamentos de inteligência e contrainteligência. Introdução à inteligência de ameaças cibernéticas. Ciclos devida de inteligência de ameaças. Modelos de inteligência de ameaças cibernéticas (Cyber Kill Chain; MITREATT&CK. Diamond model; 5W3H). Protocolos para compartilhamento de inteligência de ameaças cibernéticas. Segurança de operações (OPSEC). Inteligência de vulnerabilidades. Ferramentas para inteligência de ameaças cibernéticas.

Conteúdo Programático: Módulo 1: Introdução à Inteligência e Contrainteligência Definição de inteligência e contrainteligência Importânciada inteligência na segurança cibernética Papel da contrainteligência na proteção contra ameaças Módulo 2:Inteligência de Ameaças Cibernéticas Conceitos básicos de inteligência de ameaças cibernéticas A importância daprevisão e detecção precoce de ameaças A relação entre inteligência de ameaças e segurança cibernética Módulo3: Ciclos de Vida de Inteligência de Ameaças Coleta de dados e informações Análise de informações Produção deinteligência Distribuição de inteligência Utilização de inteligência na tomada de decisões Módulo 4: Modelos deInteligência de Ameaças Cibernéticas Cyber Kill Chain: um modelo de estágios de um ataque cibernético MITREATT&CK: Matriz de Táticas e Técnicas de Ataque Diamond Model: análise de ator, infraestrutura, alvo e impacto5W3H: análise de Quem, O quê, Onde, Quando, Por quê, Como, Quanto Módulo 5: Protocolos paraCompartilhamento de Inteligência de Ameaças Cibernéticas STIX/TAXII: Padrões para compartilhamentoestruturado de ameaças ISACs (Information Sharing and Analysis Centers) Plataformas de compartilhamento deinformações de segurança Módulo 6: Segurança de Operações (OPSEC) Conceitos de OPSEC na cibersegurançaIdentificação de informações sensíveis Implementação de medidas para proteger informações críticas OPSEC emcomunicações e operações cibernéticas Módulo 7: Inteligência de Vulnerabilidades Identificação e avaliação devulnerabilidades em sistemas Classificação de vulnerabilidades Utilização de inteligência para priorizar correçõesAmeaças baseadas em vulnerabilidades conhecidas Módulo 8: Ferramentas para Inteligência de AmeaçasCibernéticas Visão geral de ferramentas de análise de ameaças Plataformas de análise de segurança Ferramentasde coleta de informações e indicadores de comprometimento (IOCs) Avaliação Final: Os alunos deverão realizarum projeto prático que envolve a aplicação dos conceitos e técnicas aprendidos durante o curso para identificar,analisar e responder a uma ameaça cibernética simulada.

Método de ensino-aprendizagem: Os alunos serão avaliados, em cada disciplina, levando em conta sua participação em sala de aula e ematividades como provas, simulações, estudos de caso, oficinas, dinâmicas, seminários, pesquisas de campo,visitas técnicas, projetos de intervenção, exposição dialogada, perguntas orientadoras, entre outras queestimulem o pensamento reflexivo e crítico. Serão atribuídas menções (SR, II, MI, MM, MS ou SS) em todas asdisciplinas do curso e no trabalho de conclusão do curso (TCC), sendo aprovados os alunos que obtiverem, emcada disciplina e no TCC, menção igual ou superior a MM e frequência mínima de 75% em cada disciplina. Seráconcedido ao aluno que obtiver aprovação nas disciplinas e no artigo um Certificado de Especialização emPrivacidade e Segurança da Informação.

Bibliografia: The Cyber Security Body of Knowledge (CyBOK). Versão 1.1, 2021. UNIVERSIDADE DE BRISTOL.Capítulo 6 -Malware & Attack Technologies; Capítulo 7 - Adversarial Behaviours; Capítulo 9 - Forensics. Capítulo 19 -Network Security. BRASIL. Decreto Nº 10.222. de 5 de fevereiro de 2020. Aprova a Estratégia Nacional deSegurança Cibernética. Brasília, DF. Edição 26, Seção 1, página 6. The Threat Intelligence Handbook: MovingToward a Security Intelligence Program, Second

Edition; Edited: Zane Pokorny. Cyberedge Press. ISBN: 978-1-948939-06-5.

Docente: Robson de Oliveira Albuquerque.

TÓPICOS AVANÇADOS EM SEGURANÇA DA INFORMAÇÃO

Ementa: Seminários integrados com palestras diversas sobre pesquisas recentes sobre segurança da informação,envolvendo arquiteturas de segurança da informação, estratégias de segurança da informação, governança egestão de riscos de segurança da informação, o novo framework CSF do NIST, cultura de segurança dainformação, segurança em cadeias de suprimento, privacidade diferencial, arquiteturas zero-trust, segurança deredes 5G, entre outros.

Conteúdo Progrmático: Módulo 1: Introdução e Visão Geral da Segurança da Informação Boas-vindas e apresentação do programa deseminários Visão geral dos desafios atuais em segurança da informação Tendências e avanços recentes emcibersegurança Módulo 2: Arquiteturas de Segurança da Informação Abordagens arquiteturais para protegersistemas e dados Modelos de segurança em camadas Arquiteturas de microssegmentação Aplicações emambientes de nuvem Módulo 3: Estratégias de Segurança da Informação Desenvolvimento de estratégias desegurança alinhadas aos objetivos de negócios Abordagens proativas vs. reativas em segurança Estratégias paraproteção de dados e prevenção de ameaças Módulo 4: Governança e Gestão de Riscos em Segurança daInformação Estruturas de governança em segurança da informação Identificação, avaliação e tratamento deriscos Frameworks de gestão de riscos em segurança Boas práticas em conformidade regulatória Módulo 5: ONovo Framework CSF do NIST Introdução ao Cybersecurity Framework (CSF) do NIST Componentes e princípiosdo CSF Aplicação prática do CSF em ambientes organizacionais Módulo 6: Cultura de Segurança da InformaçãoFomentando uma cultura de segurança nas organizações Treinamento e conscientização em segurançaAbordagens para envolvimento dos funcionários Módulo 7: Segurança em Cadeias de Suprimento (Supply Chain)Avaliação de riscos em cadeias de suprimento Estratégias de mitigação de ameaças Monitoramento e auditoria deparceiros e fornecedores Módulo 8: Privacidade Diferencial (Differential Privacy) Conceitos fundamentais deprivacidade diferencial Aplicações em análise de dados sensíveis Desafios e considerações éticas Módulo 9:Arquiteturas Zero Trust Princípios do modelo Zero Trust Implementação de políticas de confiança mínima Casosde uso e benefícios Módulo 10: Segurança de Redes 5G Desafios de segurança em redes 5G Abordagens paraproteção de redes 5G Implicações da segurança para IoT e comunicações móveis Módulo 11: Apresentações dePesquisas Recentes Alunos ou pesquisadores convidados apresentarão suas pesquisas recentes em segurança dainformação Módulo 12: Discussões e Encerramento Discussões e reflexões finais sobre os tópicos abordados nosseminários Oportunidades futuras em pesquisa e prática em segurança da informação Avaliação Final: Avaliaçãobaseada na participação ativa nos seminários, discussões e apresentações.

Método de ensino-aprendizagem: Os alunos serão avaliados, em cada disciplina, levando em conta sua participação em sala de aula e ematividades como provas, simulações, estudos de caso, oficinas, dinâmicas, seminários, pesquisas de campo,visitas técnicas, projetos de intervenção, exposição dialogada, perguntas orientadoras, entre outras queestimulem o pensamento reflexivo e crítico. Serão atribuídas menções (SR, II, MI, MM, MS ou SS) em todas asdisciplinas do curso e no trabalho de conclusão do curso (TCC), sendo aprovados os alunos que obtiverem, emcada disciplina e no TCC, menção igual ou superior a MM e frequência mínima de 75% em cada disciplina. Seráconcedido ao aluno que obtiver aprovação nas disciplinas e no artigo um Certificado de Especialização emPrivacidade e Segurança da Informação.

Bibliografia: The Cyber Security Body of Knowledge (CyBOK). Versão 1.1, 2021. UNIVERSIDADE DE BRISTOL. Capítulo 2 -Risk Management and Governance; Capítulo 4 - Human Factors. HAYDEN, L. People-Centric Security:Transforming your Enterprise

Security Culture. Nova Iorque: McGrawHills, 1ª ed., p. 416, 2015. SULLIVAN, J.Building a Corporate Culture of Security: Strategies for Strenghening Organizationsl Resilience. São Paulo:Butterworth-Heinemann, 1ª ed.,p. 298, 2016.

Docente: Joao Souza Neto.

TÓPICOS AVANÇADOS EM PRIVACIDADE

Ementa: Seminários integrados com palestras diversas sobre pesquisas recentes sobre privacidade e produção de artigos.

Conteúdo Programático: Módulo 1: Introdução e Visão Geral Boas-vindas e apresentação do programa de seminários Visão geral dosdesafios atuais em privacidade de dados Importância da pesquisa em privacidade Módulo 2: Tendências emPrivacidade Discussão das tendências atuais em proteção de dados pessoais Leis de privacidade eregulamentações globais Implicações da privacidade na tecnologia Módulo 3: Privacidade na Era Digital Proteçãode dados em ambientes digitais Privacidade em mídias sociais e plataformas online Rastreamento de dados eprivacidade do usuário Módulo 4: Privacidade e Ética Ética na coleta e uso de dados pessoais Desafios éticos empesquisa e prática em privacidade Casos de estudo e dilemas éticos Módulo 5: Privacidade na Saúde e na Ciênciade Dados Privacidade em pesquisa médica e de saúde Privacidade diferencial e proteção de dados em pesquisascientíficas Desafios na anonimização de dados Módulo 6: Privacidade e Segurança da Informação Integração de
privacidade em estratégias de segurança Proteção de dados em sistemas de informações Incidentes de violaçãode privacidade e resposta a incidentes Módulo 7: Pesquisas Recentes em Privacidade Apresentações depesquisadores convidados sobre suas pesquisas recentes em privacidade de dados Módulo 8: Produção de ArtigosCientíficos Estrutura e elementos essenciais de um artigo acadêmico Escolha de periódicos e conferências parapublicação Práticas de escrita acadêmica e revisão por pares Módulo 9: Metodologia de Pesquisa Metodologias depesquisa aplicáveis à privacidade Coleta de dados, análise e interpretação Considerações estatísticas empesquisas sobre privacidade Módulo 10: Apresentação de Artigos em Seminários Alunos ou pesquisadoresconvidados apresentarão seus artigos acadêmicos em andamento ou publicados Discussões e feedbackconstrutivo Módulo 11: Discussões e Encerramento Discussões finais sobre os tópicos abordados nos semináriosReflexões sobre o estado atual da pesquisa em privacidade Avaliação Final: Avaliação baseada na participaçãoativa nos seminários, apresentações de artigos e discussões.

Método de ensino-aprendizagem: Os alunos serão avaliados, em cada disciplina, levando em conta sua participação em sala de aula e ematividades como provas, simulações, estudos de caso, oficinas, dinâmicas, seminários, pesquisas de campo,visitas técnicas, projetos de intervenção, exposição dialogada, perguntas orientadoras, entre outras queestimulem o pensamento reflexivo e crítico. Serão atribuídas menções (SR, II, MI, MM, MS ou SS) em todas asdisciplinas do curso e no trabalho de conclusão do curso (TCC), sendo aprovados os alunos que obtiverem, emcada disciplina e no TCC, menção igual ou superior a MM e frequência mínima de 75% em cada disciplina. Seráconcedido ao aluno que obtiver aprovação nas disciplinas e no artigo um Certificado de Especialização emPrivacidade e Segurança da Informação.

Bibliografia: ABNT NBR ISO/IEC 27701:2019 "Técnicas de segurança – Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBRISO/IEC 27702 para a gestão da privacidade da informação – Requisitos e Diretrizes". Rio de Janeiro: ABNT,2019. UNIVERSIDADE DE BRISTOL. CyBOK - The Cyber Security Body of Knowledge. 2021. BRASIL. Ministério daGestão e da Inovação. Secretaria de Governo Digital. Diretoria de Privacidade e Segurança da Informação. Guiado Framework de Privacidade e Segurança da Informação – versão 1.1.2. Brasília-DF: SGD, 2023.

Docente: Daniel Chaves Cafe

ELABORAÇÃO DE PRÉ-PROJETO DE PESQUISA

Ementa: Elaboração de pré-projeto de pesquisa a partir de um tema de interesse do discente.

Conteúdo Programático: Módulo 1: Introdução à Pesquisa Científica Definição de pesquisa científica Importância da pesquisa no contextoacadêmico e profissional Elementos essenciais de um projeto de pesquisa Módulo 2: Escolha do Tema eFormulação do Problema Identificação de áreas de interesse Refinamento do foco da pesquisa Formulação clara eespecífica do problema de pesquisa Módulo 3: Revisão da Literatura Métodos de busca de literatura relevanteOrganização e análise de artigos e trabalhos relacionados Identificação de lacunas na literatura Módulo 4:Definição de Objetivos e Hipóteses Estabelecimento de objetivos de pesquisa Formulação de hipóteses ouquestões de pesquisa Alinhamento dos objetivos com o problema identificado Módulo 5: Metodologia de PesquisaSeleção de métodos de pesquisa (quantitativos, qualitativos, mistos) Escolha de técnicas de coleta de dadosDescrição detalhada dos procedimentos de pesquisa Módulo 6: Coleta e Análise de Dados (Se Aplicável)Planejamento da coleta de dados Processo de coleta de dados Métodos de análise de dados e interpretaçãoMódulo 7: Estrutura e Elementos de um Pré-Projeto Capa e elementos pré-textuais Introdução Revisão daliteratura Metodologia Referências Módulo 8: Apresentação do Pré-Projeto Preparação para a apresentaçãoComunicação eficaz do projeto de pesquisa Feedback e revisão após a apresentação Módulo 9: Revisão eAperfeiçoamento Avaliação crítica do pré-projeto Revisão da redação e formatação Incorporação de feedback deprofessores e colegas Módulo 10: Entrega do Pré-Projeto Final Preparação e submissão do pré-projeto finalCumprimento de prazos e requisitos de apresentação Avaliação Final: Avaliação baseada na qualidade do pré-projeto final e na apresentação.

Método de ensino-aprendizagem: Os alunos serão avaliados, em cada disciplina, levando em conta sua participação em sala de aula e ematividades como provas, simulações, estudos de caso, oficinas, dinâmicas, seminários, pesquisas de campo,visitas técnicas, projetos de intervenção, exposição dialogada, perguntas orientadoras, entre outras queestimulem o pensamento reflexivo e crítico. Serão atribuídas menções (SR, II, MI, MM, MS ou SS) em todas asdisciplinas do curso e no trabalho de conclusão do curso (TCC), sendo aprovados os alunos que obtiverem, emcada disciplina e no TCC, menção igual ou superior a MM e frequência mínima de 75% em cada disciplina. Seráconcedido ao aluno que obtiver aprovação nas disciplinas e no artigo um Certificado de Especialização emPrivacidade e Segurança da Informação.

Bibliografia: BOOTH, W. C.; COLOMB, G. G.; WILLIAMS, J. M. A Arte da pesquisa, edição padrão. São Paulo: Martins Fontes,p. 368, 2019. COOPER, D. R.; SCHINDLER, P. S. Schindler. Métodos de pesquisa em Administração.12ª.ed. SãoPaulo: McGraw Hill Brasil, 2016. PERDIGÃO, D. M.; HERLINGER, M.; WHITE, O. M. Teoria e prática da pesquisaaplicada. Rio de Janeiro - RJ: Elsevier Brasil, p. 504, 2011.

Docnete: Luiz Antonio Ribeiro Junior.

ORIENTAÇÃO PARA ELABORAÇÃO DE ARTIGO CIENTÍFICO

Ementa: Orientação para elaboração de artigo científico.

Conteúdo Programático: Módulo 1: Introdução à Escrita Científica Definição de artigo científico Importância da comunicação científicaElementos essenciais de um artigo Módulo 2: Escolha do Tema e Formulação do Problema de PesquisaIdentificação de um tópico relevante Refinamento do problema de pesquisa Definição de objetivos claros Módulo3: Revisão da Literatura Métodos para buscar literatura relevante Análise e organização de artigos relacionadosIdentificação de lacunas na pesquisa existente Módulo 4: Estrutura do Artigo Científico Título, resumo e palavras-chave Introdução: apresentação do problema e justificativa Revisão da literatura: síntese de pesquisas anterioresMetodologia: descrição dos métodos de pesquisa Resultados: apresentação dos principais achados Discussão:interpretação dos resultados e implicações Conclusão: resumo das descobertas e direções futuras Módulo 5:Escrevendo de Forma Clara e Concisa Estilo de escrita científica Uso adequado de citações e referênciasbibliográficas Evitar plágio e má conduta acadêmica Dicas para clareza e concisão na escrita Módulo 6:Metodologia de Pesquisa Descrição detalhada dos métodos utilizados Coleta de dados e procedimentos Análise dedados e ferramentas estatísticas Ética na pesquisa e consentimento informado Módulo 7: Formatação e Normasde Publicação Normas de formatação (ABNT, APA, IEEE, entre outras) Elementos pré-textuais, textuais e pós-textuais Preparação do manuscrito para submissão Módulo 8: Revisão e Feedback Processo de revisão e ediçãoFeedback de orientadores e colegas Revisão gramatical e ortográfica Módulo 9: Preparação para Submissão eApresentação Escolha da revista ou conferência apropriada Preparação da carta de apresentação Apresentaçãoem conferências e defesa do artigo Módulo 10: Publicação e Pós-Publicação Processo de revisão por paresEstratégias para aumentar a visibilidade do artigo Responsabilidades após a publicação Avaliação Final: Avaliaçãobaseada na qualidade do artigo científico elaborado durante o curso e na apresentação do mesmo.

Método de ensino-aprendizagem: Os alunos serão avaliados, em cada disciplina, levando em conta sua participação em sala de aula e ematividades como provas, simulações, estudos de caso, oficinas, dinâmicas, seminários, pesquisas de campo,visitas técnicas, projetos de intervenção, exposição dialogada, perguntas orientadoras, entre outras queestimulem o pensamento reflexivo e crítico. Serão atribuídas menções (SR, II, MI, MM, MS ou SS) em todas asdisciplinas do curso e no trabalho de conclusão do curso (TCC), sendo aprovados os alunos que obtiverem, emcada disciplina e no TCC, menção igual ou superior a MM e frequência mínima de 75% em cada disciplina. Seráconcedido ao aluno que obtiver aprovação nas disciplinas e no artigo um Certificado de Especialização emPrivacidade e Segurança da Informação.

Bibliografia: BRASIL. Advocacia Geral da União. Casa Civil. Controlaria Geral da União. Guia de Boas Práticas - Lei Geral deProteção de Dados Pessoais, consolidado no âmbito do Comitê Central de Governança de Dados. SCHUSTER, E.;LEVKOWITZ, H. A. I. M.; OLIVEIRA JUNIOR, O. N. Writing Scientific Papers in English Successfully: Your CompleteRoadmap. 1ª ed. São Carlos, Compacta Gráfica e Editora, p. 194, 2014. The Cyber Security Body of Knowledge(CyBOK). Versão 1.1, 2021. UNIVERSIDADE DE BRISTOL. Capítulo 9, seção 9.1.3 - Conceptual Models, p. 296-300.

Docente: Rafael Rabelo Nunes.

Documento assinado eletronicamente por **Rafael Rabelo Nunes**, **Professor(a) de Magistério Superior do Departamento de Administração da FACE**, em 17/01/2025, às 17:03, conforme horário oficial de Brasília, com fundamento na Instrução da Reitoria 0003/2016 da Universidade de Brasília.

Documento assinado eletronicamente por **Georges Daniel Amvame Nze**, **Coordenador(a) do Programa de Pós-Graduação Profissional em Engenharia Elétrica - PPEE**, em 20/01/2025, às 10:21, conforme horário oficial de Brasília, com fundamento na Instrução da Reitoria 0003/2016 da Universidade de Brasília.

A autenticidade deste documento pode ser conferida no site http://sei.unb.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **12260531** e o código CRC **E7BFD2B7**.

Referência: Processo nº 23106.003633/2025-53 SEI nº 12260531