



PROJETO PEDAGÓGICO DO CURSO

**Programa de Pós-Graduação Profissional
em Engenharia Elétrica**

Mestrado Profissionalizante – *Stricto Sensu*

21 de março de 2023



Márcia Abraão Moura

Reitora

Rafael Rabelo Nunes

Coordenador

Georges Daniel Amvame Nze

Coordenador Substituto

Docentes permanentes

Alexandre Solon Nery

Carlos André de Melo

Daniel Chaves Café

Demétrio Antônio da Silva Filho

Edna Dias Canedo

Fábio Lúcio Lopes de Mendonça

Fabiana Freitas Mendes

Flávio Elias Gomes de Deus

Geraldo Pereira Rocha Filho

João José Costa Gondim

Luiz Antônio Ribeiro Júnior

Rafael Timóteo de Sousa Júnior

Ugo Silva Dias

Vinícius Pereira Gonçalves

William Ferreira Giozza

Docentes colaboradores

Daniel Alves da Silva

Éder Souza Gualberto

João Paulo Javidi da Costa

Robson de Oliveira Albuquerque

Apoio técnico

Abner Braga Amorim de Almeida

Cristiana Rosa da Costa Castro

Tayná Gabriela Araújo Albuquerque



Sumário

1. Apresentação	4
2. Contextualização.....	5
2.1 A Universidade de Brasília (UnB)	5
2.2 O Programa de Pós-Graduação Profissional em Engenharia Elétrica (PPEE)	6
3. Legislação	8
4. Justificativa.....	8
5. Missão.....	9
6. Objetivos	10
7. Linhas de pesquisa	11
8. Parceria de projetos	12
9. Infraestrutura.....	18
10. Ensino à distância	19
11. Docentes	23
12. Internacionalização	31
13. Critérios de seleção	31
14. Matriz curricular.....	36
14.1 Ementário das disciplinas com bibliografias básicas e complementares.....	38
12.2 Estudos orientados	49
12.3 Estágio de docência.....	50
15. Sistema de avaliação	50
16. Sistema de obtenção e aproveitamento de créditos	51
17. Produções.....	51
18. Comissão examinadora.....	52
19. Conclusão e duração do curso.....	53
20. Diplomação	53
21. Egressos	53



1. Apresentação

A evolução tecnológica das sociedades está ligada ao aprimoramento do conhecimento humano. Os Programas de Pós-Graduação *Stricto Sensu* exercem papel fundamental na interconexão entre ciência, inovação e transformação social. Nesse contexto, pesquisas acadêmicas têm impacto no empreendedorismo, na economia e na tecnologia, sempre tangenciados por aspectos de sustentabilidade.

Nesse sentido, a discussão sobre o Projeto Pedagógico do Curso (PPC) do Programa de Pós-Graduação Profissional em Engenharia Elétrica (PPEE) da Universidade de Brasília (UnB) constitui um momento importante no Departamento de Engenharia Elétrica. O debate sobre o assunto foi fomentado pelos professores permanentes, colaboradores e representantes do corpo discente do PPEE na 20ª reunião ordinária do Colegiado. Isso demonstra a relevância da participação de todos na construção do projeto, cujo lugar de ocupação é a ética, o cotidiano profissional e a excelência na formação. Contudo, as discussões estabelecidas na reunião do Programa estão longe de esgotar o assunto, que precisará ser revisado considerando as constantes e pertinentes necessidades de mudanças e adequações.

Nessa perspectiva, o PPC está direcionado em atender aos princípios básicos da segurança cibernética, associado aos avanços tecnológicos do cotidiano com excelência na formação. Trata-se de uma ação com propósitos claros, compromissos definidos em coletivo e com ética. Nesse sentido, deve-se considerar o PPC como um processo permanente de reflexão e discussão do ensino-aprendizagem na pós-graduação, além da busca pela formação humana, tendo como prioridade a excelência por meio de pesquisas inovadoras.

Assim, as bases teóricas, princípios norteadores, objetivos, estratégias e tudo mais que se encontra nesse documento, devem manter uma permanente inter-relação evolução. O PPC está alicerçado nos avanços tecnológicos, como resultado da estrutura curricular e qualidade do corpo docente e discente do PPEE.

Do ponto de vista formal, a integralização créditos se faz com base no regime de oferta de componentes curriculares, junto com a defesa de dissertação, associado ao número mínimo de 20 créditos.

O PPEE disponibilizará vagas de maneira semestral, com quantidade variada, obedecendo os critérios de credenciamento, recredenciamento e número de orientandos por docente.



O planejamento do programa é semestral com matrícula por componente curricular, o que traz flexibilidade para permitir escolha de disciplinas, com as quais os discentes podem direcionar seus interesses de pesquisa.

2. Contextualização

2.1 A Universidade de Brasília (UnB)

A Fundação Universidade de Brasília (UnB) foi criada pela Lei n. 3998, de 15 de dezembro de 1961 e regulamentada pelo Decreto nº 500, de 15 de janeiro de 1962, iniciando suas atividades acadêmicas em 21 de abril de 1962, no Campus Darcy Ribeiro, situado na Asa Norte, Plano Piloto, em Brasília, Distrito Federal, às margens do Lago Paranoá. Com bases mais flexíveis, a UnB foi criada com a perspectiva de renovar o ensino superior no país.

Com o propósito de ampliar sua abrangência territorial, descentralizar suas atividades acadêmicas e apoiar o desenvolvimento na região, a partir de 2006, a UnB se tornou uma universidade *multicampi*, inaugurando inicialmente o Campus da Faculdade UnB Planaltina e, posteriormente, os *campus* das Faculdades da Ceilândia (FUP) e do Gama (FGA). Atualmente, considerando os seus quatro *campus*, a UnB atende, aproximadamente, 45 mil alunos distribuídos entre os seus diferentes cursos de graduação e pós-graduação.

A Universidade de Brasília está constituída por 53 departamentos, distribuídos entre os seus quatro *campus* (Darcy Ribeiro, Planaltina, Ceilândia e Gama) e entre as suas 14 faculdades e 12 institutos. Possui também 12 centros de pesquisa especializados, 4 centros de ensino e pesquisa, 1 hospital universitário e 2 hospitais veterinários, 1 fazenda com mais de 4.000 hectares (Reserva Ecológica e Experimental Fazenda Água Limpa), entre outros.

Atualmente, a UnB oferece 139 cursos de graduação, dos quais 30 são noturnos e 9 são à distância, além de 155 cursos de pós-graduação, sendo 87 de Mestrado e 68 de Doutorado. A Universidade também se destaca sendo o maior centro de ensino e de pesquisa da região Centro-Oeste, com 706 grupos de pesquisa científica e tecnológica cadastrados na base do Diretório dos Grupos de Pesquisa no Brasil do Conselho Nacional de Desenvolvimento Científico e Tecnológico do Ministério da Ciência e Tecnologia (CNPq-MCT).

No Campus Darcy Ribeiro está localizada a Faculdade de Tecnologia, que foi criada em 1967 e que hoje compreende 5 importantes departamentos da UnB: Departamento de Engenharia Civil e Ambiental, Departamento de Engenharia Elétrica, Departamento de Engenharia Florestal, Departamento de Engenharia Mecânica e Departamento de Engenharia da Produção. O Departamento de



Engenharia Elétrica é o responsável pelos cursos de graduação em Engenharia Elétrica, Engenharia Mecatrônica e Engenharia de Redes e Engenharia da Computação, como também pelo Programa de Pós-Graduação Profissional em Engenharia Elétrica.

2.2 O Programa de Pós-Graduação Profissional em Engenharia Elétrica (PPEE)

O Mestrado Profissional em Engenharia Elétrica, em que pese ter seu registro e coordenação próprios junto à CAPES, no âmbito da UnB, era um programa gerido como parte do Programa de Pós-Graduação em Engenharia Elétrica – PPGEE (Acadêmico), obedecendo ao Regulamento Interno do PPGEE e a uma resolução específica de 12 de fevereiro de 2013 que estabelece normas complementares para o funcionamento do curso de Mestrado Profissional no Programa de Pós-Graduação em Engenharia Elétrica (PPGEE) da Universidade de Brasília. Tal resolução específica é amparada no Art. 3, § 2º do Regulamento Interno do PPGEE e foi aprovada pelo Colegiado do PPGEE em sua XI reunião, realizada em 14 de dezembro de 2012.

Desde a sua criação, o Mestrado Profissional em Engenharia Elétrica foi ofertado na forma de turmas específicas, com ingresso de alunos regulado por edital vinculado à turma. Por tal razão, o programa passou por períodos intermediários em que esteve sem turma em andamento, portanto, sem alunos. Em tais períodos, a produtividade mensurada pela avaliação CAPES esteve em baixa, contrastando com os períodos alternados de boa produtividade. Tal situação foi objeto de crítica apresentada em cada resultado de avaliação da CAPES.

Conseqüentemente à publicação dos resultados da Avaliação Quadrienal 2013-2016, o Departamento de Engenharia Elétrica da UnB recebeu em 27/10/2018 a visita do Coordenador da Área de Engenharias IV da CAPES, Professor Murilo A. Romero, EESC/USP. Nessa ocasião, o Coordenador das Engenharias IV esteve reunido com os coordenadores dos dois programas acadêmicos (Programa de Pós-Graduação em Engenharia Elétrica – PPGEE e Programa de Pós-Graduação em Sistemas Eletrônicos e de Automação – PGEA) e o coordenador do Programa Profissional em Engenharia Elétrica (PPEE), assim como a coordenadora do Programa em Engenharia Biomédica da FGA. No que se refere ao programa profissional PPEE, após discussão dos resultados da avaliação quadrienal, o Coordenador das Engenharias IV apresentou considerações importantes para o futuro do PPEE, especificamente:

- Que o PPEE deveria evoluir para ter uma gestão própria independente do programa acadêmico, considerando ainda as novas definições da CAPES quanto aos programas profissionais que devem objetivar ser completos, no sentido de ter mestrado e doutorado



profissionais, além da possibilidade de uma avaliação quadrienal baseada em critérios próprios e específicos dos programas profissionais;

- Que a oferta de turmas do PPEE deveria passar a ser regular, não impedindo a criação de turmas específicas sob demanda;
- Que o PPEE deve objetivar ser um programa completo, no sentido da inclusão de um conjunto abrangente de áreas da engenharia elétrica, sem lacunas de áreas importantes;
- Que o PPEE deveria buscar um foco temático que fosse o seu diferenciador, tanto com relação aos programas acadêmicos de Engenharias IV da UnB quanto com relação a outros programas profissionais de Engenharias IV brasileiros, sugerindo-se um direcionamento em função das duas últimas ofertas de turmas nos domínios da segurança cibernética, segurança da informação e forense em engenharia elétrica e tecnologias da informação.

Buscando atender tais requisitos, fez-se necessário escolher uma área focal para o programa e estabelecer o regulamento para que o PPEE passasse a ter sua gestão própria no âmbito da UnB. Tal se fez a partir de deliberações do Colegiado do PPGE, primeiramente com a instituição, pelo ato nº 002/2017, de uma comissão voltada à reformulação do mestrado profissional (processo SEI 23106.070955/2017-06), o que levou à proposição de um regulamento específico do programa profissional. Em seguida, tal proposição de regulamento foi aprovada pelo Colegiado do PPGE, em sua reunião de 18/05/2018.

O novo regulamento do PPEE parte assim de um regulamento existente e aprovado em todas as instâncias cabíveis na UnB (conforme resolução CEPE 080/2017), com a retirada das determinações específicas de programas acadêmicos e a integração das determinações mais próprias aos programas profissionais. O novo regulamento do PPEE estabelece um foco na área de concentração em Segurança Cibernética, considerada como o diferencial do PPEE com relação ao programa acadêmico de origem e com relação a outros programas profissionais de engenharia elétrica no Brasil. Por outro lado, tal área de concentração embasa uma estratégia de criar linhas de pesquisa que se enquadrem dentro da segurança cibernética e que cubram os diversos domínios da engenharia elétrica, tangenciando também, outras áreas do conhecimento.

A aprovação da primeira versão do regulamento pela Faculdade de Tecnologia, em 30/03/2020, e pelo Decanato de Pós-Graduação, em 04/12/2020, buscava atender às diretrizes da CAPE, assim como passar a gerir o Programa de Pós-Graduação Profissional em Engenharia Elétrica de maneira independente, com seu próprio Colegiado e Coordenação, bem como com uma oferta regular de vagas, a partir do período 2018/2.



3. Legislação

No âmbito da Universidade de Brasília, o PPEE está estruturado segundo a legislação vigente e as normas internas da UnB, as quais estabelecem que:

- O funcionamento e coordenação cabe, no plano executivo, ao Decanato de Pós-Graduação (DPG);
- No plano deliberativo, ao Conselho de Ensino, Pesquisa e Extensão (CEPE), diretamente ou por meio da Câmara de Pesquisa e Pós-Graduação (CPP), nos termos do Art. 77 do Regimento Geral da UnB;
- A coordenação didática e científica cabe ao Conselho dos Cursos de Pós-Graduação da Faculdade de Tecnologia (CCPG/FT), na forma em que dispõe o Regimento Geral da UnB; e
- A coordenação das atividades será exercida pelo Colegiado do Programa e pela Comissão de Pós-Graduação (CPG/PPEE).

4. Justificativa

A localização da Universidade de Brasília no planalto central, próximo aos poderes da administração pública e setores da inteligência, favorecem o acesso a diversos órgãos que corroboram a utilização de seguranças cibernéticas em seus contextos específicos. E, com apoio de instituições parceiras, o PPG tem produzido elevada quantidade de artigos científicos relacionados de alto impacto nacional e internacional.

A proximidade do centro político-administrativo do país, com várias instituições e organizações governamentais e não-governamentais com atuação nacional e internacional favorece o acesso e participação de pesquisadores, alunos e egressos no processo de decisão de políticas públicas e estratégias que contribuem para o desenvolvimento de aplicativos e sistemas em todo o país. A centralidade da localização espacial do Programa contribui também para atender discentes de várias regiões do Brasil.

O PPEE almeja somar esforços na busca de fortalecimento dos sistemas eletrônicos contra-ataques cibernéticos como também, a necessidade da formação de mestres no ramo da segurança cibernética tornar-se cada vez mais evidente, considerando os graves problemas relacionados à temática existente nos dias atuais, bem como a necessidade de mestres nas instituições de ensino e de pesquisa, nas autarquias e nas atividades específicas da Segurança Cibernética, seja no setor público ou privado.

O PPEE é voltado para pesquisas e discussões mais profundas para atender às reais necessidades do Brasil em termos de produção e melhoria de problemas.



5. Missão

O Programa de Pós-Graduação Profissional em Engenharia Elétrica da Universidade de Brasília tem a missão de formar recursos humanos com excelência técnica e científica em Segurança Cibernética e o desenvolvimento de tecnologias, sempre respeitando os métodos científicos e ética profissional.

A atuação do PPEE é alicerçada em pilares de desenvolvimento socioeconômico para contribuir com o desenvolvimento a partir de resultados de pesquisas científicas. Para isso, a atuação do corpo docente e discente do Programa é baseada na interdisciplinaridade, pluralidade de ideias e no amplo diálogo para solução de problemas tecnológicos encontrados em nível local, regional e nacional.

Como resultado de sua atuação, pesquisas realizadas no âmbito do PPEE têm contribuído com o fortalecimento do desenvolvimento tecnológico, nesse contexto, o PPEE é o único programa que oferece curso de mestrado profissional em Engenharia Elétrica com foco em Segurança Cibernética no Brasil.

O Programa de Pós-Graduação Profissional em Engenharia Elétrica (PPEE) da Universidade de Brasília (UnB) tem objetivos e missão definidos em seu regulamento, os quais encontram-se explicitados da seguinte forma:

Art. 2º O Programa de Pós-Graduação Profissional em Engenharia Elétrica (PPEE) da Universidade de Brasília (UnB) tem a missão de prover a capacitação de pessoal, pesquisa e a prática profissional avançada e transformadora de conhecimentos científicos, tecnologias, procedimentos e processos aplicados, por meio do método científico, habilitando o profissional para atuar em atividades técnico-científicas e de inovação, mediante:

I - O oferecimento de cursos de pós-graduação stricto sensu – Mestrado Profissional em Engenharia Elétrica e lato sensu – Especialização

II - Desenvolvimento de projetos de pesquisa e inovação;

III - Promoção de atividades de extensão tecnológica

Tal missão e objetivos são vinculados, no presente período de avaliação, ao foco específico de atuação no domínio da segurança cibernética, o que define uma vocação do PPEE para atuar em qualquer das áreas profissionais da engenharia elétrica, sem recobrimento com o programa acadêmico coirmão, mas voltado para atender às necessidades relevantes da sociedade, da atualidade e que requerem abordagens sempre mais avançadas.

Por outro lado, esse foco na segurança cibernética permite atender às necessidades prementes de todo o país, mas que encontra na região do Distrito



Federal uma série de instituições para as quais a formação de profissionais e a pesquisa aplicada são de enorme interesse, valendo citar o Gabinete de Segurança Institucional da Presidência da República (GSI/PR), os Ministérios da Justiça e Segurança Pública (MJSP), da Economia (ME), da Defesa (MD) e das Comunicações (MC), a Controladoria Geral da União (CGU), o Tribunal de Contas da União (TCU), assim como os respectivos órgãos vinculados, como a Agência Brasileira de Inteligência (ABIN), o Departamento de Polícia Federal (DPF), o Departamento de Polícia Rodoviária Federal (PRF), o Conselho Administrativo de Defesa Econômica (CADE), o Departamento Nacional de Auditoria do SUS (DENASUS), a Advocacia Geral da União (AGU), a Agência Nacional de Telecomunicações (ANATEL) e as três forças armadas, Aeronáutica, Marinha e Exército (neste, o Comando de Defesa Cibernética - CDCIber).

6. Objetivos

Entendemos que, atualmente, a pós-graduação no Brasil se tornou um caminho necessário para o desenvolvimento de capacitação nos setores da pesquisa científica, avanços tecnológicos e dos recursos humanos, para o incremento de novos profissionais no ensino superior, empreendedorismo e na prestação de serviços à sociedade, com maior qualificação de conhecimentos em áreas específicas.

Desse modo, o PPEE tem seu objetivo focado na formação de excelência de professores, pesquisadores e profissionais em nível de pós-graduação nos âmbitos local, regional, nacional e internacional, em tópicos de engenharia elétrica, com ênfase em segurança cibernética. Para tanto, o Programa busca oferecer aos alunos experiências teóricas, de campo e de laboratório para contribuir com a atuação em instituições públicas e privadas de pesquisa e ensino, organizações não-governamentais e empresas do setor de inteligência. Adicionalmente, o Programa tem desenvolvido esforços para ampliar a visão empreendedora dos alunos para atuar, em nível nacional e internacional, em empresas e organizações não-governamentais.

Especificamente, o PPEE visa formar profissionais da área de inteligência e pesquisadores, qualificados e com elevado nível de excelência, com capacidade criadora e de inovação, capazes de contribuir com avanços científicos, tecnológicos e sociais na área de Segurança Cibernética.

Busca também por aprimorar e consolidar a competência científica para conduzir pesquisas originais e independentes em áreas específicas capacitando profissionais para: (i) adquirir independência no exercício da pesquisa; (ii) inovar no desenvolvimento da pesquisa e da produção de conhecimento; (iii) atuar



como pesquisadores e/ou docentes na área pública, iniciativa privada e organizações não-governamentais; (iv) exercer papel de liderança, especialmente em instituições de ensino superior, sociedades científicas e grupos de pesquisa.

7. Linhas de pesquisa

Considerando esse foco de atuação na segurança cibernética, o regulamento do programa, visando articulação, aderência e atualização, é bastante específico com relação a uma única área de concentração, com linhas de pesquisa fortemente vinculadas e complementares.

Detalham-se, assim, em termos de interesses em propriedades clássicas da segurança cibernética (disponibilidade, integridade e confidencialidade), bem como em tecnologias e processos para a construção de medidas de segurança preventivas, de monitoração, de controle, de mitigação e de recuperação contra ataques cibernéticos:

- Segurança de Infraestrutura, de Plataformas, de Software e de Sistemas

Abrange segurança de hardware; segurança de rede; criptografia; sistemas operacionais e virtualização; sistemas distribuídos; autenticação, autorização e auditoria; segurança em sistemas distribuídos; segurança de software; segurança na web e mobile; segurança no ciclo de desenvolvimento.

- Segurança e Inteligência Cibernética

Abrange os softwares maliciosos e as tecnologias utilizadas para ataques; o estudo de comportamento de adversários; inteligência cibernética; forense computacional; segurança de operações; incidentes de segurança; OSINT (Inteligência de Fontes Abertas).

- Aspectos Humanos, Organizacionais, Legais e Regulatórios em Segurança Cibernética

Abrange a gestão de riscos; a governança de tecnologia da informação; os aspectos humanos em segurança cibernética; privacidade; aspectos legais e regulatórios em segurança cibernética.

- Ciência e engenharia de dados, e concepção e desenvolvimento de materiais estratégicos e críticos para segurança cibernética



Abrange os materiais concebidos computacionalmente para aplicações críticas, constituindo os componentes de hardware computacional e de redes, de dispositivos de internet das coisas, de elementos sensores e atuadores em processos industriais e sistemas críticos, como os de produção de energia nuclear, limpeza de água, detecção de surtos epidemiológicos, defesa agropecuária, sistemas veiculares e de transporte, superfícies para aplicação em telecomunicações e assuntos similares, onde a segurança dos materiais semicondutores seja aspecto relevante, em diversas escalas, especialmente a dos nano-materiais. Também abrange a engenharia de dados e da inteligência artificial para efeito de utilização na tomada de decisão em segurança e inteligência cibernética, com a criação de processos e ferramentas de software para monitoração de ameaças e análise de risco, contramedidas de prevenção, detecção, contenção, reparação, resposta passiva e ativa.

8. Parceria de projetos

O PPEE possui ainda diversos projetos em andamento em parceria com o Laboratório de Tecnologias da Tomada de Decisão (LATITUDE/UnB), dentro os quais, destacamos o projeto da 1ª turma específica com a Agência Brasileira de Inteligência, na qual, tem por objetivo alavancar a pesquisa aplicada a transferência de tecnologia, bem como capacitar profissionais do setor de inteligência do país.

Essa estrutura vem atraindo alunos das instituições citadas e gerando os respectivos processos de transferências de tecnologias e de conhecimento. Por outro lado, a maior parte dos trabalhos do mestrado são vinculados aos temas de projetos existentes, incluindo os projetos com apoio das agências de fomento CNPq - Conselho Nacional de Desenvolvimento Científico e Tecnológico, Outorga 312180/2019-5 PQ-2, Outorga BRICS 2017-591 LargEWiN e Outorga 465741/2014-2 INCT em Cibersegurança, CAPES - Coordenação de Aperfeiçoamento de Pessoal de Nível Superior, Outorga 23038.007604/2014-69 FORTE e Outorga 88887.144009/2017-00 PROBRAL, e FAP-DF - Fundação de Apoio à Pesquisa do Distrito Federal (Outorga 0193.001366/2016 UIoT e Outorga 0193.001365/2016 SSDDC). Também cabe citar a vinculação com projetos apoiados pelo Ministério da Economia, Outorga 005/2016 DIPLA e Outorga 083/2016 ENAP, pela Secretaria de Segurança Institucional da Presidência da República, Outorga ABIN 002/2017, pelo Conselho Administrativo de Defesa Econômica, Outorga CADE 08700.000047/2019-14, e pela Advocacia Geral da União, Outorga AGU 697.935/2019.

O PPEE tem um total de vinte e sete projetos de pesquisa, atualmente, em andamento, distribuídos e conduzidos pelos membros permanentes do



Programa. Na tabela a seguir, os projetos estão relacionados às linhas de pesquisas.

Incentiva-se a participação de discentes em projetos de pesquisas de docentes, de forma a ampliar o envolvimento dos alunos nas publicações dos professores do Programa

Atualmente, o PPEE tem um total de 42 (quarenta e dois) projetos de pesquisa em andamento distribuídos e conduzidos pelos membros permanentes do Programa. Na tabela a seguir, os projetos estão relacionados às linhas de pesquisas.

Tabela 1 - Projetos de pesquisa por linha de pesquisa

Projeto de pesquisa	Linha de pesquisa
(ABIN) Análise de malware e engenharia de dados	Segurança e Inteligência Cibernética
(AGU) Pesquisa Aplicada e Inovação em Processos e Tecnologias do Tratamento da Documentação, Informação, inteligência e conhecimento nos Domínios da Atividade da Advocacia Geral da União	Aspectos Humanos, Organizacionais, Legais e Regulatórios em Segurança Cibernética
Algoritmos de Consenso em Sistemas de Gestão de Saúde baseados em Blockchain.	Ciência e engenharia de dados, e concepção e desenvolvimento de materiais estratégicos e críticos para segurança cibernética
Aplicação de métodos multicritérios para apoio à decisão	Aspectos humanos, organizacionais, legais e regulatórios em segurança cibernética
Aspectos Organizacionais e Regulatórios sobre Segurança Cibernética	Aspectos humanos, organizacionais, legais e regulatórios em segurança cibernética
Atualização e Implementação dos Instrumentos de Gestão de Documentos do Ministério da Saúde.	Segurança de infraestrutura, de plataformas, de software e de sistemas



(CADE) Pesquisa aplicada com fundamento no estudo de necessidades, análise informacional, concepção, prototipação e experimentação com vistas à inovação tecnológica e de processos no domínio da Defesa Econômica para o Conselho Administrativo de Defesa	Aspectos humanos, organizacionais, legais e regulatórios em segurança cibernética
(CAPES) Projeto e desenvolvimento de redes sem fio em larga-escala coletoras de energia	Segurança de infraestrutura, de plataformas, de software e de sistemas
(CEPESC) Pesquisa Aplicada ao Desenvolvimento de Sistemas de Softwares Seguros.	Segurança e inteligência cibernética
Desenvolvimento e Estudo de Novos Nanomateriais para Aplicações em Produção de Energia Limpa	Ciência e engenharia de dados, e concepção e desenvolvimento de materiais estratégicos e críticos para segurança cibernética
(DIPLA/MP) Pesquisa Aplicada em Planejamento Estratégico, Gestão de Riscos Corporativos e Gestão da Informação Corporativa no âmbito das competências da Diretoria de Planejamento e Gestão do Ministério do Planejamento, Orçamento e Gestão.	Segurança de infraestrutura, de plataformas, de software e de sistemas
(DPF) Propostas de frameworks para coleta de evidências forenses	Segurança e inteligência cibernética
(DPF) Uso de técnicas de inteligência artificial para processamento de evidências	Segurança de infraestrutura, de plataformas, de software e de sistemas
(DTIC) Proposta de avaliação e melhoria da governança de tecnologia da informação e comunicação da diretoria de tecnologia da informação e comunicação da secretaria	Aspectos humanos, organizacionais, legais e regulatórios em segurança cibernética



executiva do ministério da justiça e segurança pública	
(ENAP escola) Integração de tecnologias e métodos aplicados a prática de escola virtual da administração pública federal	Aspectos humanos, organizacionais, legais e regulatórios em segurança cibernética
(ENAP Governamental) Produção de dados e conhecimento estratégico na tomada de decisão na gestão governamental	Segurança e inteligência cibernética
Explorando Inteligência Computacional e Segurança da Informação em IoT e Imagens de Tomografia Computadorizada	Ciência e engenharia de dados, e concepção e desenvolvimento de materiais estratégicos e críticos para segurança cibernética
(FAP/DF) Forense de sistemas operacionais e bancos de dados	Ciência e engenharia de dados, e concepção e desenvolvimento de materiais estratégicos e críticos para segurança cibernética
(FAP/DF) Secure software defined data center (SSDDC): Disponibilização de ambiente de nuvem computacional segura	Segurança e inteligência cibernética
(FAP/DF) Universal Internet of Things (UIoT): Middleware sensível ao contexto para gerenciamento e controle de dispositivos e serviços em ambientes de IoT	Ciência e engenharia de dados, e concepção e desenvolvimento de materiais estratégicos e críticos para segurança cibernética
Fatores humanos na segurança cibernética	Aspectos humanos, organizacionais, legais e regulatórios em segurança cibernética
Instituto Nacional de Ciência e Tecnologia em Segurança Cibernética - Núcleo 6	Segurança de infraestrutura, de plataformas, de software e de sistemas
Mestrado Profissional em Engenharia Elétrica, na área de concentração: Segurança Cibernética, linha de pesquisa Ciência e Engenharia de	Ciência e engenharia de dados, e concepção e desenvolvimento de



Dados – 1ª Turma para Profissionais do Setor de Justiça e Segurança Pública	materiais estratégicos e críticos para segurança cibernética
(MJSP) Pesquisa aplicada com inovação científica para o desenvolvimento formativo e tecnológico da Secretaria Nacional do Consumidor (SENACON) do Ministério da Justiça e Segurança Pública (MJSP) por meio de técnicas de Inteligência Artificial	Segurança e inteligência cibernética
(MTIC) Apoio a projeto estratégico de comunicações digitais em DF de interesse da academia, forças armadas e sociedade civil	Segurança de infraestrutura, de plataformas, de software e de sistemas
Observatório da Segurança Cibernética	Aspectos humanos, organizacionais, legais e regulatórios em segurança cibernética
Pesquisa aplicada à integração de Inovações Tecnológicas à arquitetura de sistemas de informação de serviços e benefícios socioassistenciais do trabalho social com pessoas e famílias do SUAS	Ciência e engenharia de dados, e concepção e desenvolvimento de materiais estratégicos e críticos para segurança cibernética
(PF) Pesquisa Aplicada de Inovações Tecnológicas no domínio da Perícia Criminal Federal.	Aspectos humanos, organizacionais, legais e regulatórios em segurança cibernética
(PGFN) Pesquisas e inovação tecnológica aplicadas às temáticas da informação e das comunicações no domínio da Procuradoria Geral da Fazenda Nacional	Ciência e engenharia de dados, e concepção e desenvolvimento de materiais estratégicos e críticos para segurança cibernética
(PPEE) Segurança de redes e criptografia	Segurança de infraestrutura, de plataformas, de software e de sistemas
Projeto AMORIS – Aplicativo Móvel e Central de Comando e Controle sobre Rede IoT para Suporte a Ações de	Ciência e engenharia de dados, e concepção e desenvolvimento de



Solidariedade no Combate ao COVID-19 e outros Surtos	materiais estratégicos e críticos para segurança cibernética
Projeto e Desenvolvimento de Redes sem Fio de Larga-Escala Coletoras de Energia	Segurança de infraestrutura, de plataformas, de software e de sistemas
Proposta de Avaliação e Melhoria da Governança de Tecnologia da Informação e Comunicação (TIC) da Diretoria de Tecnologia da Informação e Comunicação (DTIC) da Secretaria Executiva (SE), do Ministério da Justiça e Segurança Pública (MJSP).	Aspectos humanos, organizacionais, legais e regulatórios em segurança cibernética
(P4SEC) EAGER USBRCCR COLLABORATIVE Securing Networks in the Programmable Data Plane Era	Segurança e inteligência cibernética
Requisitos de Software	Segurança de infraestrutura, de plataformas, de software e de sistemas
(SDDC) Secure Software Defined Data Center - SSDDC: Disponibilização de Ambiente de Nuvem Computacional Segura	Segurança de infraestrutura, de plataformas, de software e de sistemas
(SDN) Projeto de Pesquisa Avaliação do Desempenho de Controladores de Software Defined Networks	Segurança de infraestrutura, de plataformas, de software e de sistemas
Segurança em Sistemas Embarcados e Microcontroladores	Ciência e engenharia de dados, e concepção e desenvolvimento de materiais estratégicos e críticos para segurança cibernética
Segurança na camada física pelas futuras redes de comunicação sem fio.	Ciência e engenharia de dados, e concepção e desenvolvimento de materiais estratégicos e críticos para segurança cibernética



Serviços Cientes dos Espaços Urbanos via Federated Learning em Sistemas de Transporte Inteligente	Ciência e engenharia de dados, e concepção e desenvolvimento de materiais estratégicos e críticos para segurança cibernética
SISTeR City – Sistemas Inteligentes Seguros e em Tempo Real para Cidades Inteligentes (Secure near-real-time intelligent computing systems for Smart Cities)	Ciência e engenharia de dados, e concepção e desenvolvimento de materiais estratégicos e críticos para segurança cibernética
1ª Turma Específica ABIN/PPEE	Segurança e inteligência cibernética

A participação de pesquisadores colaboradores no programa e as parcerias com empresas privadas têm possibilitado aos discentes e docentes o acesso a dados e campos experimentais para a implementação de trabalhos de pesquisa dos docentes e discentes do programa. A participação direta e o acesso a dados de levantamento de campo possibilitam maior aprendizado e fixação de conteúdos teóricos, além de dar mais robustez aos resultados e pesquisas no âmbito do Programa. As empresas e instituições parceiras têm disponibilizado também o acesso a bases de dados extremamente relevantes para as pesquisas.

9. Infraestrutura

O PPEE da Universidade de Brasília está inserido administrativamente e estruturalmente no Departamento de Engenharia Elétrica da Faculdade de Tecnologia. Em parcerias institucionais e privadas, o PPEE conta com apoio do Laboratório de Tomada de Decisões Latitude.

Para atender ao conjunto de atividades vinculadas aos seus objetivos, o PPEE conta com a infraestrutura laboratorial para o ensino de graduação e pós-graduação do Departamento de Engenharia Elétrica da UnB. Assim, estão disponíveis laboratórios voltados para atender às disciplinas básicas, laboratórios com atividades integradas de ensino e pesquisa e laboratórios que atendem somente a atividades de pesquisa. Tais laboratórios estão associados a grupos de pesquisa específicos, cada um desses grupos tendo um professor coordenador. Vários laboratórios são compartilhados por mais de um grupo de pesquisa, ou grupos de mais de um Programa de Pós-Graduação. Cada laboratório possui infraestrutura própria e está associado a projetos de pesquisa específicos das áreas. A quase totalidade desses laboratórios permite atividades que integram alunos de graduação e de pós-graduação, sendo um elemento importante da integração entre os dois níveis de formação.



Como auxílio à produção intelectual discente, a Biblioteca Central da UnB (BCE) possui acervo com 563.069 volumes e 7.902 títulos de periódicos, dos quais 37.145 volumes e mais de 2.143 títulos de periódicos são na área de ciências exatas e engenharia. Além de ser ligada à rede mundial de computadores, a BCE possui sistema de catalogação e indexação disponível para consultas online. A Biblioteca disponibiliza o Repositório Institucional da UnB (RIUnB), para a divulgação da produção científica realizada na Universidade. Possui também uma Biblioteca Digital de Monografias, onde se encontram acervos de textos de teses, dissertações e monografias produzidas na UnB, incluindo as que vêm sendo produzidas no PPEE.

Ressalta-se também um conjunto de laboratórios do Departamento de Engenharia Elétrica, assim como as salas de aula, salas de estudo, salas de docentes e áreas administrativas, que são atendidos por rede local de computadores sem fio e filiar. Em três diferentes pontos de presença dessa rede há roteadores com conexão de 1Gbps à Rede da UnB (RedUnB), e desta, por intermédio da Rede Metropolitana Giga Candanga, cuja conexão de 10Gbps é realizada pela Rede Nacional de Ensino e Pesquisa (RNP). Por intermédio dessa rede, e utilizando, aproximadamente, uma centena de computadores e quiosques de acesso à Internet, o discente possui acesso à informação científica e técnica acessível por sistemas de recuperação, tanto no próprio Departamento, quanto na Base de Dissertações e Teses da Biblioteca Central da UnB e no portal de periódicos da CAPES.

Todas as salas de aula são equipadas com computador e equipamento multimídia, com acesso à Internet por rede com fio e sem fio. No entanto, enquanto perdurar a pandemia do COVID-19, tecnologias de EAD estão sendo utilizadas no apoio à totalidade das turmas/disciplinas, de forma síncrona e/ou assíncrona remotamente. Para tanto, são utilizados os ambientes da Microsoft Teams e Moodle (Aprender3) da UnB com apoio do Centro de Ensino à Distância - CEAD/UnB, assim como o Moodle do Laboratório de Redes - LabRedes (www.campusvirtual.unb.br). Os laboratórios continuam em pleno funcionamento durante o período da pandemia COVID-19 para prestar suporte aos docentes e técnico-administrativos, bem como aos discentes, que estão trabalhando em caráter de teletrabalho.

10. Ensino à distância

O PPEE tem dedicado esforços especiais para ampliar as oportunidades para inovação na formação de alunos no curso de Mestrado Profissional. Destacam-se a disponibilização e o acesso a estações experimentais e instituições e empresas parceiras do programa, o uso de videoconferências e da plataforma



EAD (Ensino a distância) Moodle e Teams em apoio a aulas presenciais, defesas de dissertações e apresentações temáticas, acesso a base de dados, treinamento no uso de plataformas de processamento de dados e oferta de Tópicos especiais por convidados nacionais e internacionais.

O uso de recursos audiovisuais em sala de aula (datashow e aparelhos de TV de alta resolução), quadros inteligentes, recursos para videoconferência e plataforma EAD Moodle, têm complementado as aulas presenciais com a participação especial de professores convidados de outras localidades e países. Os recursos de videoconferência ampliaram a participação de membros de bancas com maior qualificação e adequação para cada tópico de pesquisa, com menor gasto financeiro e maior benefício aos resultados das pesquisas no programa.

O Programa, regularmente, não oferece aula para o curso de Mestrado Profissional na modalidade à distância, entretanto, várias disciplinas do programa atualmente são apoiadas com o uso de ferramentas da plataforma Moodle de Ensino a Distância (EAD). A experiência indica que o apoio das disciplinas em ferramentas EAD tem complementado e amplificado o conteúdo das aulas presenciais. Atualmente, a Universidade de Brasília está reforçando as estratégias de EAD a partir da oferta de treinamentos e capacitação de professores e técnicos para o uso dessas ferramentas de ensino.

Em 2020 e 2021, as instâncias superiores da Universidade de Brasília, em consonância com a Política Nacional de Educação, diante de uma situação excepcional imposta pela pandemia da Covid-19, autorizaram os programas de pós-graduação a oferecer o ensino à distância. Com isso, várias disciplinas do Programa que puderam ser adaptadas e que não incluíam carga horária de atividades laboratoriais inerentes à área de atuação, foram ofertadas na modalidade de Ensino a distância. Esta é uma situação excepcional e, com o fim da pandemia, deverão ser retomadas na forma presencial.

Entretanto, tivemos várias lições e experiências aprendidas durante a pandemia e que vêm sendo mantidas total ou parcialmente, dependendo das normas e regulamentos que estiverem vigentes no futuro. Por exemplo, tivemos sucesso na realização das bancas de defesa de dissertação, com a participação de membros externos com mais efetividade, facilidade e baixo custo. Tais experiências poderão ser mantidas se não houver objeção normativa ou legal. Outra experiência positiva e com sucesso foi a realização de Colóquios e Seminários temáticos online, com a participação de pesquisadores e docentes de instituições de ensino e pesquisa no exterior e fora de Brasília, com ampla participação de docentes e discentes.



Com isso, no âmbito do PPEE, a discussão sobre a modalidade de ensino à distância é constante. Resultados indicam que algumas disciplinas podem ser ofertadas parcial ou totalmente via EAD, àquelas que requerem atividades em laboratórios seguem mantidas na modalidade de ensino presencial. Outras atividades de defesas de dissertações, reuniões e eventos científicos, quando convém, se beneficiam das ferramentas EAD.

De forma geral, a Universidade de Brasília tem a Secretaria de Tecnologia e Informação (STI) para apoiar as atividades acadêmicas, de extensão e pesquisa de graduação e pós-graduação dos centros, institutos, departamentos e laboratórios. Isso inclui, para alunos, professores e servidores, o acesso à internet de alta velocidade em todos os campi da Universidade, webmail, serviços de armazenamento e backup de dados, acesso à internet com ou sem fio (wireless), webpages, sistema de ensino à distância, videoconferência, antivírus, aplicativos de escritório, licenças corporativas de software privados e acesso a sites corporativos relacionados a fins científicos e acadêmicos.

A Biblioteca Central da Universidade de Brasília (BCE) também disponibiliza várias salas de informática para o uso dos alunos da graduação e pós-graduação, usando a plataforma “Aprender” (Moodle), em que vários professores do PPEE utilizam como apoio para aulas presenciais e/ou para oferta de disciplinas on-line. O acesso à internet no Campus Darcy Ribeiro, onde o PPEE está localizado, disponibiliza internet 24/7 (tempo integral) aos discentes, docentes e servidores, tanto dentro quanto fora das salas de aula.

Ela também é responsável pelo provimento de informações às atividades de Ensino, Pesquisa e Extensão da Universidade. O acervo da BCE busca atender às demandas dos discentes, docentes e comunidade acadêmica com excelência no atendimento às necessidades de informações dos usuários.

A BCE-UnB está conectada na internet e dispõe de uma série de serviços à comunidade acadêmica e, com destaque a alunos da pós-graduação, os treinamentos em normas da ABNT, editor de referências bibliográficas Mendley e em pesquisa em base de dados, reservas de salas para estudo individual ou grupo, laboratórios de acesso digital, cabines de áudio e vídeo, sala de videoconferências, sala de exposições.

Atualmente, a BCE conta com um acervo de mais de 250 mil títulos de livros e 10 mil títulos de periódicos, incluindo mais de 2400 livros e 600 mil artigos na área de meio ambiente, natureza e conservação, 1300 livros e 150 mil artigos em tópicos de silvicultura, tecnologia de madeira e floresta. Anualmente, dentro do Plano Diretor Institucional (PDI), a BCE faz levantamento de demandas dos docentes de graduação e pós-graduação para aquisição de novos livros



(nacionais e internacionais) e materiais acadêmicos de responsabilidade da Biblioteca, que são utilizados tanto em ensino de graduação como em pós-graduação.

Além disso, a BCE disponibiliza o acesso a várias bases de dados, com destaque ao Portal de Periódicos da Capes, BASE- Bielefed Academic Search Engine, BDPA – Base de Dados de Pesquisa Agropecuária (Embrapa), coleção digitalizada retrospectiva de periódicos JSTOR, BDTD – Biblioteca Digital de Teses e Dissertações do IBICT, base de dados PROQUEST, BRAPCI – Base de Dados Referencial de Artigos de Periódicos Plano Pedagógico do Curso – PPG-Ciências Florestais - UnB em Ciência da Informação, Pubmed, SciELO – Scientific Electronic Library Online, SIDRA – Sistema IBGE de Recuperação Automática, Portal de Periódicos da Capes, PROQUEST, SciVal e serviços de comutação bibliográfica (COMUT, IBICT, Bireme).

Adicionalmente, no âmbito da Faculdade de Tecnologia, o PPEE dispõe de uma ampla estrutura de informática, incluindo acesso à internet e a computadores. Destacamos aqui os computadores e softwares da Unidade de Laboratórios de Ensino de Graduação (Uleg/FT), disponíveis para atividades acadêmicas da pós-graduação no novo prédio da Faculdade de Tecnologia (FT) da UnB, com mais de 2400 m² ocupados com nove laboratórios, duas salas de informática, uma de projetos, uma de tutoria e um espaço para inovação. Para as aulas que necessitam de computadores, estão disponíveis 6 (seis) salas de aula do ULEG (Unidade de Laboratórios Ensino da Graduação) da Faculdade de Tecnologia para os alunos da pós-graduação, equipadas com uma média de 30 (trinta) computadores de mesa (desktops), com licenças corporativas de softwares da Microsoft Office, ArcGIS 10.6, Inventário Florestal, Autocad e vários outros softwares de acesso livre de processamento de dados estatísticos.

Além da estrutura para atividades acadêmicas, a Faculdade de Tecnologia está equipada com WorkStations e softwares para modelagem e processamento de alta performance, exigidas para trabalhos e pesquisas específicas. A partir de 2020, a Universidade de Brasília passou a oferecer a todos os seus docentes e discentes (graduação e pós-graduação) o acesso ao pacote Office 365, com espaço de 1Tb no Onedrive para cada usuário. Em destaque, neste pacote é oferecido o editor de texto Word, planilha Excel e o MS-Teams para videoconferência, que tem sido usado como ferramenta principal para o ensino à distância, defesas de dissertações e teses, exames de qualificação, reunião de colegiados e outras videoconferências de eventos técnicos e científicos.

De forma mais específica, o PPEE dispõe de uma webpage (<https://ppee.unb.br/>) atualizada para apoiar a transparência, o acesso à informação e a gestão do Programa. A webpage do Programa foi atualizada, com as ferramentas mais



modernas de internet, hospedada num provedor de internet da Faculdade de Tecnologia. A nova Ferramenta possibilita acesso e atualização mais rápidos, com ferramentas interativas para diversos recursos online.

11. Docentes

O Programa de Pós-Graduação Profissional em Engenharia Elétrica (PPEE), segue, para credenciamento, recredenciamento e descredenciamento de orientadores e coorientadores de Mestrado Profissional, os critérios estabelecidos na Resolução da Direção da Faculdade de Tecnologia N° 003/2022, da Faculdade de Tecnologia da Universidade de Brasília.

O quadro de docentes permanentes é constituído por professores doutores que constituem vínculo de servidores com a Universidade de Brasília, conforme:

Tabela 2 – Docentes permanentes

Nome do docente	Nível	Temáticas de estudo	Linhas de pesquisa atuante
Alexandre Solon Nery, Dr.	<i>Professor Adjunto</i>	Computação de Alto Desempenho Máquinas Reconfiguráveis Aprendizado de Máquina MLOPs Big Data	Ciência e engenharia de dados, e concepção e desenvolvimento de materiais estratégicos e críticos para segurança cibernética.
Carlos André de Melo Alves, Dr.	<i>Professor Adjunto</i>	Gestão de Riscos de Segurança da Informação Frameworks de Gestão de Riscos e de Segurança da Informação	Aspectos humanos, organizacionais, legais e regulatórios em Segurança Cibernética.



		Gestão de Segurança da Informação no Setor Público	
Daniel Chaves Café, Dr.	<i>Professor Adjunto</i>	Desenvolvimento de Sistemas Embarcados Segurança de Sistemas Operacionais Embarcados Segurança de Nanossatélites Segurança de Estações Terrestres Satelitais	Ciência e engenharia de dados, e concepção e desenvolvimento de materiais estratégicos e críticos para segurança cibernética.
Demétrio Antônio da Silva Filho, Dr.	<i>Professor Associado</i>	Uso de Aprendizagem de Máquina na Solução de Problemas de Segurança Cibernética e Afins	Ciência e engenharia de dados, e concepção e desenvolvimento de materiais estratégicos e críticos para segurança cibernética
Edna Dias Canedo, Dra.	<i>Professora Associada</i>	Engenharia de Software Engenharia de Requisitos Privacidade e Segurança de Dados Mineração de Dados em	Segurança de Infraestrutura, de Plataformas, de Software e de Sistemas Aspectos humanos, organizacionais, legais e regulatórios em Segurança Cibernética



		Repositórios de Software	
Fabiana Freitas Mendes, Dra.	<i>Professora Adjunta</i>	Aspectos humanos em Cybersecurity Engenharia de Software Qualidade de Software Modelos e normas de qualidade de software	Aspectos humanos, organizacionais, legais e regulatórios em Segurança Cibernética
Flávio Elias Gomes de Deus, Dr.	<i>Professor Associado</i>	Segurança da Informação Forense computacional, entre outros tópicos correlatos	Segurança e Inteligência Cibernética.
Georges Daniel Amvame Nze, Dr.	<i>Professor Associado</i>	Segurança Cibernética Segurança em SDN Open Source Intelligence (OSINT) Segurança em IoT	Segurança de Infraestrutura, de Plataformas, de Software e de Sistemas Segurança e Inteligência Cibernética Ciência e engenharia de dados, e concepção e desenvolvimento de materiais estratégicos



		Segurança em Containerização Ferramentas de Cibersegurança	e críticos para segurança cibernética
Geraldo Pereira Rocha Filho, Dr	<i>Professor Adjunto</i>	Sistemas ciberfísicos para cidades inteligentes Segurança em redes móveis e redes veiculares Ciência de dados, computação móvel e embarcada Criptomoedas e mecanismos de consenso distribuído	Ciência e engenharia de dados, e concepção e desenvolvimento de materiais estratégicos e críticos para segurança cibernética
João José Costa Gondim, Dr.	<i>Professor Adjunto</i>	Segurança Cibernética Segurança de redes Big Data Open Source Intelligence (OSINT) Cyber Threat Intelligence Segurança em IoT DevSecOps	Segurança e Inteligência Cibernética Segurança de Infraestrutura, de Plataformas, de Software e de Sistemas



		Ataques Cibernéticos	
Luiz Antônio Ribeiro Júnior, Dr.	<i>Professor Adjunto</i>	Modelagem e Simulação de Processos Optoeletrônicos em Semicondutores Orgânicos Uso da Dinâmica Molecular Reativa para o Estudo das Propriedades Físico-Químicas de Novas Nanoestruturas Uso da Teoria do Funcional de Densidade para o Estudo da Estrutura Eletrônica	Ciência e engenharia de dados, e concepção e desenvolvimento de materiais estratégicos e críticos para segurança cibernética
Rafael Rabelo Nunes, Dr.	<i>Professor Adjunto</i>	Gestão de Riscos de Segurança da Informação Gestão da Segurança da Informação Frameworks de Segurança da Informação Métodos e Modelos de Decisão em Segurança da Informação	Aspectos humanos, organizacionais, legais e regulatórios em Segurança Cibernética.



Rafael Timóteo de Sousa Júnior, PhD	<i>Professor Associado</i>	Segurança Cibernética Open Source Intelligence (OSINT) Segurança de Redes: análise de vulnerabilidades, detecção de intrusão, medidas de proteção Inteligência artificial aplicada em segurança Segurança da Inteligência artificial Medidas de segurança distribuídas – aplicações em IoT, SDN, 5G/6G Forense computacional: aquisição, preservação, análise de anomalias, visualização	Segurança e Inteligência Cibernética Segurança de Infraestrutura, de Plataformas, de Software e de Sistemas
Ugo Silva Dias, Dr.	<i>Professor Adjunto</i>	Segurança em Redes Móveis e Redes Veiculares Redes de celulares 6G	Ciência e engenharia de dados, e concepção e desenvolvimento de materiais estratégicos e críticos para segurança cibernética.



		Segurança na camada física	
		Antenas em fluídos	
Vinícius Pereira Gonçalves, Dr.	<i>Professor Adjunto</i>	Internet das Coisas (IoT) Segurança Cibernética Interação Humano-Computador (IHC) Ciência de Dados Aprendizado de Máquina	Ciência e engenharia de dados, e concepção e desenvolvimento de materiais estratégicos e críticos para segurança cibernética.
William Ferreira Giozza, PhD	<i>Professor Associado</i>	Avaliação de desempenho de redes e sistemas de computadores Infraestruturas críticas de redes de computadores Redes ópticas IoT e Nanonetworks	Ciência e engenharia de dados, e concepção e desenvolvimento de materiais estratégicos e críticos para segurança cibernética

O PPEE conta ainda com professores colaboradores, que são de instituições parceiras e exercem contribuições para com o programa.

Tabela 3 – Docentes colaboradores



Nome do docente	Temáticas de estudo	Linhas de pesquisa atuante
Daniel Alves da Silva, Dr.	Engenharia de Software Business Architecture Internet das Coisa (IoT) Segurança Cibernética	Segurança e Inteligência Cibernética
Éder Souza Gualberto, Dr.	Aprendizado de Máquina de Processamento de Linguagem Natural Segurança da Informação Redes de Computadores	Ciência e engenharia de dados, e concepção e desenvolvimento de materiais estratégicos e críticos para segurança cibernética Segurança e Inteligência cibernética Aspectos humanos, organizacionais, legais e regulatórios em Segurança Cibernética
Fábio Lúcio Lopes de Mendonça, Dr.	Redes de computadores (infra estrutura e segurança) Redes lot(implementações e segurança) Administração e gerência de redes	Ciência e engenharia de dados, e concepção e desenvolvimento de materiais estratégicos e críticos para segurança cibernética
João Paulo Javidi da Costa, PhD	Veículos autônomos Processamento de sinais de arranjo de sensores Comunicações sem fio Sistemas de Navegação por Satélite	Segurança de Infraestrutura, de Plataformas, de Software e de Sistemas



	Ciência forense digital	
Robson de Oliveira Albuquerque, Dr.	Segurança Cibernética	Segurança de Infraestrutura, de Plataformas, de Software e de Sistemas
	Segurança de redes	
	Big Data	
	Open Source Intelligence (OSINT)	Segurança e inteligência cibernética
	Cyber Threat Intelligence	Ciência e engenharia de dados, e concepção e desenvolvimento de materiais estratégicos e críticos para segurança cibernética
	Segurança em IoT	
	DevSecOps	
	Ataques Cibernéticos	

O PPEE exige que os docentes permanentes, quando tiverem vagas disponíveis e obedecendo às normas internas do programa, ofereçam-nas no edital de seleção subsequente, garantindo assim fluxo constante na relação ingresso/egresso.

O PPEE, de acordo com a resolução CEPE 044/2020 da Universidade de Brasília, deixará sempre 10% das vagas ofertadas reservadas para negros, 01 vaga para indígena e 01 vaga para quilombolas.

Os casos omissos serão discutidos no colegiado do PPEE e deliberados por maioria simples.

12. Internacionalização

Intensifica o processo em andamento de internacionalização do programa com maior intercâmbio científico e acadêmico com instituições e grupos de pesquisas estrangeiros, realização de eventos científicos (seminários e colóquios) internacionais (via web conferência), com a participação de pesquisadores de instituições nacionais e internacionais.

13. Critérios de seleção

O PPEE decidiu em colegiado que disponibilizará vagas semestralmente com quantidade variada, obedecendo aos critérios de credenciamento,



recredenciamento e número de orientandos por docente segundo critérios CAPES de 8 (oito) orientandos por docente permanente e 3 (três) por docente colaborador. Logo, serão ofertadas vagas para o mestrado profissional com a realização de processo seletivo, para que o ingresso aconteça sempre no semestre subsequente.

De acordo com resolução CEPE 044/2020 da Universidade de Brasília, 20% das vagas devem ser reservadas para negros, 01 vaga para indígena e 01 vaga para quilombolas. Todavia, caso elas não sejam preenchidas, poderão ser ocupadas pela ampla concorrência. Poderão inscrever-se candidatos residentes no Brasil ou no exterior.

Poderão inscrever-se no processo seletivo para o curso de mestrado profissional do PPEE candidatos graduados ou em fase de conclusão de curso de graduação, desde que possam concluir o seu curso até o primeiro dia do período letivo, de acordo com o calendário acadêmico aprovado pelo CEPE da UnB, em instituições reconhecidas pelo Ministério da Educação ou equivalente. O processo de seleção será composto pelas seguintes etapas:

Avaliação do histórico escolar: consistirá em uma análise e pontuação dos documentos comprobatórios apresentados pelo candidato. De caráter classificatório, serão avaliados com base nas disciplinas cursadas na graduação e, quando aplicável, disciplinas cursadas com aproveitamento em curso de pós-graduação stricto sensu. A nota do histórico escolar é calculada por meio da soma ponderada do índice de Rendimento Acadêmico (IRA), ou equivalente, tendo como fator de ponderação a avaliação da universidade de origem. Para os candidatos oriundos da Universidade de Brasília, o IRA do histórico de graduação será utilizado como instrumento de avaliação (tabela 4). Na ausência do IRA ou para as universidades que usam outros conceitos e outros critérios de índice de rendimento, caberá à comissão de seleção calcular um IRA equivalente para o histórico escolar proveniente de cada instituição. O tempo de permanência no curso será considerado no processo de avaliação. Reduz-se até 0,2 ponto no IRA para cada semestre que exceda o tempo esperado para titulação no curso até o limite de 0,6 ponto. O histórico escolar de pós-graduação, caso o candidato o apresente, também será utilizado, desde que dele constem pelo menos três notas de disciplinas de pós-graduação concluídas. Assim, será atribuído um IRA para cada histórico escolar apresentado, sendo que o cálculo de nota relativa à avaliação do histórico escolar será a média ponderada dos IRAs.

Avaliação do currículo: Serão atribuídos pontos ao Curriculum Vitae de acordo com a tabela a seguir:



Tabela 4 - Tabela de pontuação - Nota do Curriculum Vitae (NCV)

Item	Pontuação	Limite Máximo
Monitoria em nível de graduação*	0,1 ponto/semestre	0,5 ponto
Atividade de iniciação científica concluída*	Até 1,0 ponto por atividade	2,0 pontos
Atividades extracurriculares (*), (***)	Até 0,25 ponto/semestre	0,5 ponto
Livro publicado*	Até 1,5 pontos/livro	
Artigo completo publicado ou aceito em periódico indexado*	Até 1,5 pontos/artigo	
Capítulo de livro publicado	Até 1,0 ponto/capítulo	2,0 pontos
Artigo completo publicado em congresso internacional*	Até 0,5 ponto/artigo	2,0 pontos
Artigo completo publicado em congresso nacional*	Até 0,25 ponto/artigo	2,0 pontos
Resumo publicado em congresso nacional ou internacional*	Até 0,1 ponto/artigo	0,5 ponto
Patentes, registro de Software, registros de ideias, anotações de responsabilidade técnica concedidas*	Até 1,5 ponto/patente	3,0 pontos
Atividade profissional em nível de 3º grau em instituições e/ou empresas	Até 0,25 ponto/ano	2,0 pontos
Experiência didática em nível universitário*	Até 0,25 ponto/disciplina	2,0 pontos



Participação em banca de trabalho final ou de conclusão de curso de graduação e/ou pós-graduação*	Até 0,10 ponto/participação	10,5 ponto
Orientação e/ou Co orientação de projeto de iniciação científica, trabalho final ou de conclusão de curso de graduação e/ou pós-graduação*	Até 0,25 ponto/orientação	2,0 pontos
Estágios em nível de 3º grau em instituições e/ou empresas*	Até 0,5 ponto/ano	1,0 ponto
Disciplina cursada e aprovada em programa de pós-graduação stricto sensu*	Até 0,5 ponto/disciplina	2,0 pontos
Curso de especialização (pós-graduação lato sensu concluído*	Até 1,0 ponto/curso	2,0 pontos

(*) Atividade concluída na área de Engenharia Elétrica ou em área afim.

(**) Para ser considerado na pontuação, o candidato deverá apresentar documento comprobatório do seu nível de compreensão em língua inglesa, compatível com atividade de pós-graduação, incluindo o diploma de curso de inglês e/ou teste de proficiência para leitura e/ou comprovante de moradia em país de língua inglesa por um período mínimo de seis meses. O aluno poderá apresentar também documento comprobatório do seu nível de compreensão de textos nos idiomas francês, alemão, espanhol ou outra língua estrangeira julgada, pela comissão de seleção, compatível com a atividade a ser desenvolvida pelo candidato.

(***) atividades desenvolvidas no âmbito da Universidade ou Faculdade de caráter representativo, político, esportivo etc., além de premiações ou competições oficiais de caráter tecnológico como Minibaja, Guerra de robôs, Aerodesign, Fórmula SAE, organização de eventos científicos (congressos, simpósios, mostras científicas) e outras atividades julgadas pertinentes pela comissão de seleção. Todos os pontos da tabela serão somados. A nota do NCV para cada candidato pode ser calculada pela fórmula $(1) NCV = 4 + \text{somatório dos pontos atribuídos}$. A NCV não pode ser superior a 10 pontos. Os candidatos cuja pontuação NCV excedam esse limite serão beneficiados em caso de empate na nota final com relação a outro candidato.

Avaliação de Pré-projeto de trabalho de Mestrado Profissional: De caráter eliminatório e classificatório, sendo a nota mínima para aprovação igual a seis. A avaliação será feita pelos professores ofertantes das vagas, que neste momento, terão seus nomes resguardados em sigilo. Cada professor deverá



atribuir uma nota ao pré-projeto, de acordo com a tabela a seguir, com os respectivos pesos:

Tabela 5 - Pontuação dos itens de avaliação do Pré-projeto de pesquisa.

Item	Ponto
Contextualização e atualidade do tema; e relevância da bibliografia	Até 3,5
Viabilidade do projeto	Até 1,5
Conteúdo da proposta em relação à linha e ao tema de pesquisa escolhido pelo candidato	Até 5,0

A nota final da avaliação do Pré-projeto de dissertação será a média aritmética das notas atribuídas por cada professor. O Pré-projeto deve ser composto dos seguintes itens: introdução, justificativa, objetivos, metodologia, plano de trabalho, cronograma e referências bibliográficas. O documento deverá possuir no máximo 6 páginas. Na folha de rosto do projeto, deverá ser indicado o nome do candidato, o título do projeto e a linha de pesquisa escolhida e o tema. No documento deverá ser detalhado o número de disciplinas a serem cursadas por semestre e o número de horas semanais que serão dedicadas ao curso de pós-graduação, bem como possíveis disciplinas já cursadas ao nível de pós-graduação no Programa de Pós-Graduação em Engenharia Elétrica (PPGEE), ou em outro(s) Programa(s) de pós-graduação. O candidato deverá especificar e justificar sua candidatura para o regime de tempo integral ou parcial. Se o candidato estiver empregado e desejar ser admitido como tempo integral, anexar declaração do empregador que o libere para o curso de pós-graduação. No caso de candidato com opção para regime de tempo parcial, que tenha especificado horários de trabalho e de cursos conflitantes, deverá anexar declaração do empregador que o libere nos períodos dedicados à pós-graduação.

Prova de Compreensão e Interpretação de Texto em Língua Estrangeira (Inglês): A prova terá a duração de duas horas e será realizada na sede do Programa, na data e horário descritos no cronograma deste edital. A prova escrita consistirá em tradução e/ou interpretação de texto em inglês na área de conhecimento do curso. A resposta do candidato deverá ser elaborada em Língua Portuguesa. No caso de candidatos estrangeiros, deverá ser elaborada em Língua Inglesa. Será permitido o uso de dicionário impresso. De caráter



eliminatório, sendo a nota mínima para aprovação igual a seis, os candidatos deverão ler um texto retirado de periódico internacional de divulgação científica ou artigo técnico de tema amplo, que aborda temáticas relacionadas à área de concentração do mestrado profissional. A avaliação será feita pela comissão de seleção. Cada membro da comissão de seleção deverá atribuir uma nota para a resposta do candidato. A nota final da Prova de Compreensão e Interpretação de Texto em Língua Estrangeira (Inglês) será a média aritmética das notas atribuídas por cada membro da comissão de seleção. Considerando que a prova não se qualifica como documento comprobatório, o Programa não emitirá declaração para candidatos que sejam aprovados.

Serão dispensados desta prova: candidatos estrangeiros que tenham nacionalidade em países nos quais o inglês é a língua materna; candidatos que apresentem documento comprobatório de proficiência em língua inglesa no ato da inscrição. Os tipos de documentos comprobatórios aceitos incluem: documento comprovando aprovação em Prova de Interpretação e/ou Compreensão de Texto em Língua Estrangeira (Inglês) em processo seletivo anterior em nível de pós-graduação (mestrado de doutorado) na Universidade de Brasília; certificados de conclusão em curso de idiomas (inglês) em instituições públicas ou privadas que totalizam, no mínimo, 60 horas em nível intermediário ou avançado; TOEFL iBT (≥ 72 pontos); TOEFL ITP (≥ 300 pontos); TOEIC - Test of English for International Communication com Listening Comprehension and Reading Comprehension (≥ 594 pontos); IELTS ($\geq 5,0$ pontos); ETAPP – Test of English for Academic and Professional Purposes ($\geq B2$); Cambridge – Certificate Of Proficiency in English (B2).

14. Matriz curricular

Os objetivos principais do PPEE incluem a formação acadêmica de alunos no curso de Mestrado Profissional em Engenharia Elétrica para atuar em nível de excelência como docentes, pesquisadores e profissionais qualificados em áreas temáticas relacionadas à segurança cibernética e tecnologia. Para a formação dos alunos, é necessário a conclusão de 20 créditos (300 horas/aulas) em disciplinas.

As disciplinas são ofertadas semestralmente adequando-se às demandas, conceitos e temáticas atuais. Estas disciplinas podem ser oferecidas de diferentes departamentos da UnB (Departamento de Ciência da Computação, Departamento de Física e Faculdade de Economia, Administração, Contabilidade e Ciência da Informação) e com participação de pesquisadores colaboradores (nacionais e internacionais) de instituições parceiras.



O currículo do PPEE contém 21 (vinte e uma) disciplinas da Área de Concentração, sendo, Metodologia de Pesquisa Científica 1 (código PPEE2004), de 30h/a, Metodologia de Pesquisa Científica 2 (código PPEE2005), de 30 h/a e Segurança Cibernética (código PPEE3353), de 60h/a fortemente recomendadas que os alunos as cursem.

As disciplinas do Domínio Conexo podem ser ofertadas pelo Programa e por diversos departamentos e institutos da Universidade de Brasília e estão disponíveis semestralmente aos alunos interessados nas diferentes temáticas das linhas de pesquisa do programa. As disciplinas do Tronco Comum, da Área de Concentração e do Domínio Conexo, estão regulamentadas pela Secretaria de Atendimento Acadêmico (SAA). Mais detalhes das disciplinas ofertadas pelo Programa estão apresentados a seguir.

Tabela 6 – Disciplinas fortemente recomendáveis

Código	Nomenclatura	Carga horária
PPEE2004	Metodologia de Pesquisa Científica 1	30h/a
PPEE2005	Metodologia de Pesquisa Científica 2	30h/a
PPEE3353	Segurança Cibernética	60h/a

Tabela 7 - Disciplinas da Área de Concentração

Código	Nomenclatura	Carga horária
PPEE2006	Aplicações de Ciências de Dados em Segurança Cibernética	60h/a
PPEE2007	Estágio de Docência em Engenharia 1	30h/a
PPEE1996	Estudo Orientado 1	30h/a
PPEE1997	Estudo Orientado 2	30h/a
PPEE3357	Estudo Orientado 3	60h/a
PPEE2008	Fatores Humanos em Segurança Cibernética	60h/a
PPEE2009	Gestão de Riscos Corporativos	60h/a



PPEE2010	Inteligência Cibernética	60h/a
PPEE2011	Privacidade e Segurança Cibernética	60h/a
PPEE2012	Segurança de Redes 1	60h/a
PPEE2018	Segurança em Sistemas Distribuídos	60h/a
PPEE2013	Segurança em Internet das Coisas	60h/a
PPEE2014	Segurança no Desenvolvimento de Software	60h/a
PPEE3363	Tópicos em Segurança Cibernética 1	60h/a
PPEE3364	Tópicos em Segurança Cibernética 2	60h/a
PPEE2015	Tópicos em Segurança Cibernética 3	60h/a
PPEE2016	Tópicos em Segurança Cibernética 4	30h/a
PPEE2017	Tópicos em Segurança Cibernética 5	30h/a

14.1 Ementário das disciplinas com bibliografias básicas e complementares

METODOLOGIA DE PESQUISA CIENTÍFICA 1

Professor(es) ofertante(s): Fabiana Freitas Mendes, Daniel Alves da Silva e/ou William Ferreira Giozza.

Carga horária: 30h/a.

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

Bibliografia básica: 1. WAZLAWICK, R. S. **Metodologia de Pesquisa para Ciência da Computação**. 3ª Edição. Rio de Janeiro: Elsevier/Campus, 2020 (livro-texto); 2. ROSA, C. A. P. **História da Ciência – Da Antiguidade ao Renascimento Científico**. Vol. I, 2ª Edição. Fundação Alexandre Gusmão, 2012 (ROSA, C. A. P. **História da Ciência – Da Antiguidade ao Renascimento Científico**. 2ª. ed. [S. l.]: Fundação Alexandre Gusmão, 2012. Disponível em: <www.funag.gov.br>. 3. ROSA, C. A. P. **História da Ciência –**



A Ciência Moderna. 2ª. ed. Tomo I: Fundação Alexandre Gusmão, 2012. v. 2. Disponível em: <www.funag.gov.br>.

Bibliografia complementar: 1. ROSA, C. A. P. **História da Ciência – O Pensamento Científico e a Ciência do Sec. XIX.** 2ª. ed. Tomo II: Fundação Alexandre Gusmão, 2012. v. 2. Disponível em: <www.funag.gov.br>. 2. ROSA, C. A. P. **História da Ciência – A Ciência e o Triunfo do Pensamento Científico no Mundo Contemporâneo.** 2ª. ed. [S. l.]: Fundação Alexandre Gusmão, 2012. v. 3. Disponível em: <www.funag.gov.br>. 3. LAKATOS, E. M.; MARCONI, M. A. **Fundamentos de Metodologia Científica.** 6ª ed. São Paulo: Atlas, 2006. 315 p. 4. BARBETTA, P. A *et al.* **Estatística para Cursos de Engenharia e Informática.** 2ª. ed. São Paulo: Atlas, 2008. 4. Artigos e relatórios disponibilizados via plataforma Aprender. 5. Artigos e relatórios disponibilizados via plataforma Aprender 3.

METODOLOGIA DE PESQUISA CIENTÍFICA 2

Professor(es) ofertante(s): Demétrio Antônio da Silva Filho, Daniel Alves da Silva e/ou Fabiana Freitas Mendes.

Carga horária: 30h/a.

Ementa: Conceitos de Ciência e Pesquisa. O Conhecimento Científico. Método Científico. Regras. Básicas da Escrita Científica. Pesquisa Bibliográfica. Elementos de uma Apresentação Científica.

Bibliografia básica: 1. SCHUSTER, E. *et al.* **Writing scientific papers in English successfully: your complete roadmap.** 1ª ed. [S. l.]: São Carlos, Compacta Gráfica e Editora, 2014. 2. LAKATOS, E. M.; MARCONI, M. A. **Fundamentos de Metodologia Científica.** 6ª ed. São Paulo: Atlas, 2006. 315 p. 3. ROSA, C. A. P. **História da Ciência – A Ciência Moderna.** 2ª. ed. Tomo I: Fundação Alexandre Gusmão, 2012. v. 2. Disponível em: <www.funag.gov.br>.

Bibliografia complementar: 1. ROSA, C. A. P. **História da Ciência – O Pensamento Científico e a Ciência do Sec. XIX.** 2ª. ed. Tomo II: Fundação Alexandre Gusmão, 2012. v. 2. Disponível em: <www.funag.gov.br>. 2. ROSA, C. A. P. **História da Ciência – A Ciência e o Triunfo do Pensamento Científico no Mundo Contemporâneo.** 2ª. ed. [S. l.]: Fundação Alexandre Gusmão, 2012. v. 3. Disponível em: <www.funag.gov.br>. 3. BARBETTA, P. A *et al.* **Estatística para Cursos de Engenharia e Informática.** 2ª. ed. São Paulo: Atlas, 2008. 4. Artigos e relatórios disponibilizados via plataforma Aprender.

SEGURANÇA CIBERNÉTICA 1



Professor(es) ofertante(s): Rafael Rabelo Nunes, Robson de Oliveira Albuquerque e/ou Daniel Alves da Silva.

Carga horária: 60h/a.

Ementa: Princípios e conceitos de segurança cibernética. Modelos de controle de acesso. Criptografia e seus algoritmos. Questões de implementação e usabilidade. Segurança física. Segurança de sistemas operacionais. Software maliciosos. Segurança de redes. Segurança na camada de enlace. Segurança na camada de rede. Segurança na camada de transporte. Segurança em DNS. VPNs. Segurança em redes sem fio. Segurança na Web. Segurança em Internet das Coisas. Segurança em aplicações distribuídas. Modelos de gestão de riscos e de gestão da segurança. Engenharia Social. Direito digital. Forense computacional.

Bibliografia básica: 1. GOODRICH, M. **Introdução à Segurança de computadores.** São Paulo: Bookman, 2013. ISBN 9780321512949. 2. STALLINGS, William. **Criptografia e Segurança de Redes.** 6ª Edição. São Paulo: Pearson, 2015. ISBN 9788543005898. 3. FONTES, E. **Segurança da Informação: O usuário faz a diferença.** São Paulo: Saraiva, 2006. ISBN 9788502122185.

Bibliografia complementar: 1. GALVÃO, M. **Fundamentos em Segurança da Informação.** São Paulo: Pearson, 2015. ISBN 9788543009452. 2. PINHEIRO, P. **Direito Digital.** 6ª Edição. São Paulo: Saraiva, 2016. 3. TERADA, R. **Segurança de Dados.** São Paulo: Blucher, 2008. ISBN 9788521215400. 4. NAKAMURA, E. T.; GEUS, P. L. **Segurança de Redes em Ambientes Cooperativos.** São Paulo: Novatec, 2010. 5. ABNT NBR ISO/IEC 27001:2013. **Tecnologia da Informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Requisitos,** 2013.

APLICAÇÕES DE CIÊNCIAS DE DADOS EM SEGURANÇA CIBERNÉTICA

Professor(es) ofertante(s): Alexandre, Eder Souza Gualberto, Geraldo e Vinícius.

Carga horária: 60h/a.

Ementa: Aprendizado supervisionado e não supervisionado. Redução de dimensionalidade. Engenharia de features. Processamento de linguagem natural. Redes neurais artificiais. Tópicos emergentes de Ciência de Dados aplicadas à Segurança Cibernética.

Bibliografia básica: 1. ALPAYDIN, E. **Introduction to Machine Learning.** [S. l.]: MIT Press, 2020. 2. JURAFSKY, D; MARTIN, J. **Speech and Language Processing.** [S. l.]: Prentice Hall, 2008. 3. CHARU, Aggarwal. **Neural Networks and Deep Learning.** [S. l.]: Springer, 2018.



Bibliografia complementar: 1. BISHOP, C. M. **Pattern Recognition and Machine Learning**. [S. l.]: Springer, 2006. 2. BIRD, Steven *et al.* **Natural Language Processing with Python**. O'Reilly Media: [s. n.], 2009. 3. MÜLLER, A. **Introduction to Machine Learning with Python: A Guide for Data Scientists**. O'Reilly Media: [s. n.], 2016. 4. VANDERPLAS, Jake. **Python Data Science Handbook**. O'Reilly Media: [s. n.], 2016. 5. MANNING, Christopher D.; RAGHAVAN, Prabhakar; SCHÜTZE, Hinrich. **Introduction to Information Retrieval**. Cambridge University Press: [s. n.], 2008. 6. VANDERPLAS, J. **Whirlwind Tour of Python**. O'Reilly Media.: [s. n.], 2016.

ESTÁGIO DE DOCÊNCIA EM ENGENHARIA 1

Professor(es) ofertante(s): Fábio Lúcio Lopes de Mendonça, William Ferreira Giozza e/ou Rafael Timóteo de Sousa Júnior. (pegar a mesma ementa do PPGEE)

Carga horária: 30h/a

Ementa: Iniciativa de formação docente orientada à qualificação dos discentes para o ensino, a orientação e a pesquisa, por meio de integração supervisionada como graduação

Bibliografia completa da disciplina em que o estágio de docência será realizado e demais referências pertinentes aos objetivos de aprendizagem.

ESTUDO ORIENTADO 1

Professor(es) ofertante(s): Todos os professores credenciados no PPEE.

Carga horária: 30h/a

Ementa: Levantamento bibliográfico voltado ao tema da dissertação. Leitura e resenha de artigos. Fundamentos metodológicos sobre elaboração de dissertações. Orientação científica. Supervisão e apoio do orientador para a elaboração do plano de trabalho do aluno.

Bibliografias: A critério do professor e dependentes dos tópicos propostos para estudo.

ESTUDO ORIENTADO 2

Professor(es) ofertante(s): Todos os professores credenciados no PPEE.



Carga horária: 30h/a

Ementa: Levantamento bibliográfico voltado ao tema da dissertação. Leitura e resenha de artigos. Fundamentos metodológicos sobre elaboração de dissertações. Orientação científica. Supervisão e apoio do orientador para a elaboração do plano de trabalho do aluno.

Bibliografias: A critério do professor e dependentes dos tópicos propostos para estudo.

ESTUDO ORIENTADO 3

Professor(es) ofertante(s): Todos os professores credenciados no PPEE.

Carga horária: 60h/a

Ementa: Levantamento bibliográfico voltado ao tema da dissertação. Leitura e resenha de artigos. Fundamentos metodológicos sobre elaboração de dissertações. Orientação científica. Supervisão e apoio do orientador para a elaboração do plano de trabalho do aluno.

Bibliografias: A critério do professor e dependentes dos tópicos propostos para estudo.

FATORES HUMANOS EM SEGURANÇA CIBERNÉTICA

Professor(es) ofertante(s): Edna Dias Canedo e/ou Fabiana Freitas Mendes

Carga horária: 60h/a.

Ementa: Aspectos humanos em cybersecurity. Medição de fatores humanos. Usabilidade de soluções de cybersecurity. Erro humano. Percepção, educação e engajamento de profissionais de cybersecurity.

Bibliografia básica: 1. BASIN, D. **The cyber security body of knowledge: 4 Human Factors.** University of Bristol. Ch: [s. n.], 2021. Available at: www.cybok.org. 2. ESPINOSA, C. **The Smartest Person in the Room: The Root Cause and New Solution for Cybersecurity.** USA: Lioncrest Publishing: [s. n.], 2021. ISBN 978-1-544-51621-9.

Bibliografia complementar: 1. ANDRIESSEN, J *et al.* **Cybersecurity Awareness. Switzerland.** In: Springer International Publishing: [s. n.], 2022. ISBN 978-3-031-04227-0. 2. MITNICK, K. D.; SIMON, W. L. **The art of intrusion: the real stories behind the exploits of hackers, intruders, and deceivers.** John Wiley & Sons. In: [S. l.: s. n.], 2009. ISBN 978-0-470-50382-



9. 3.WATTERS, P *et al.* **Cognition, Behavior and Cybersecurity.** In: Lausanne: Frontiers Media SA: [s. n.], 2021. doi: 10.3389/978-2-88971-412-4.

GESTÃO DE RISCOS CORPORATIVOS

Professor(es) ofertante(s): Éder Souza Gualberto, Rafael Rabelo Nunes e/ou Carlos André de Melo Alves.

Carga horária: 60h/a.

Ementa: Risco (conceito e tipos). Introdução à Gestão de Riscos. Princípios de Gestão de Riscos. Estrutura de Gestão de Riscos. Técnicas para identificação, análise e avaliação de riscos. Modelos de gestão de riscos. Tópicos emergentes em Gestão de Riscos.

Bibliografia Básica: 1. BERNSTEIN, Peter L. **Desafio aos Deuses: A Fascinante História do Risco.** Rio de Janeiro: Elsevier, 2019. 2. Associação Brasileira de Normas Técnicas. **ABNT NBR ISO 31000: Gestão de Riscos - Diretrizes.** Rio de Janeiro, 2018. 3. Associação Brasileira de Normas Técnicas. **ABNT NBR ISO 31010: Gestão de Riscos – Técnicas para o processo de avaliação de riscos.** 2ª Edição. Rio de Janeiro, 2021.

Bibliografia Complementar: 1. BRASIL. Tribunal de Contas da União. **Referencial básico de Gestão de Riscos.** Brasília, 2018. 2. DAMODARAN, A. **Gestão Estratégica do Risco.** [S. l.]: Bookman, 2009. 3. PIRES, Claudio. **Gestão por processos na prática.** [S. l.: s. n.], 2019. 4. Committee of Sponsoring Organizations of the Treadway Commission. Enterprise Risk Management - Integrating with Strategy and Performance. Executive Summary. June, 2017. Disponível em: <<https://www.coso.org/Shared%20Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf>>

INTELIGÊNCIA CIBERNÉTICA

Professor(es) ofertante(s): Robson de Oliveira Albuquerque.

Carga horária: 60h/a.

Ementa: Fundamentos de Inteligência. Fundamentos de Contra-Inteligência. Disciplinas de Inteligência; Ciclos de Inteligência; Operation Security (OPSEC). Open source Intelligence (OSINT). Inteligência de Ameaças. Inteligência de Ameaças Cibernéticas (CTI). Modelos de Inteligência de ameaças cibernéticas.

Bibliografia básica: 1. JOHNSON, Loch K. **Handbook of Intelligence Studies.** 1ª ed. [S. l.: s. n.], 2006. ISBN - 9780415777834; 2. PRUNCKUN,



Hank. **Counterintelligence Theory and Practice (Security and Professional Intelligence Education Series Book 29)**. 2. ed. [S. l.: s. n.], 2019. 3. BAZZELL, Michael. **Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information**. 8th or 9th. ed. [S. l.: s. n.], [2022]. 4. **Open Source Intelligence Investigation: From Strategy to Implementation**. [S. l.]: Babak Akhgar, P. Saskia Bayerl, Erasmus University Rotterdam, Fraser Sampson, Springer International Publishing ISBN: 978-3319476704. 2018.

Bibliografia complementar: 1. TROIA, Vinny. **Hunting Cyber Criminals: A Hacker's Guide to Online Intelligence Gathering Tools and Techniques**. ISBN-13 - 978-1119540922. ed. [S. l.: s. n.], 2020. 2. PALACÍN, Valentina. **Intelligence and Data-Driven Threat Hunting: A hands-on guide to threat hunting with the ATT&CK™ Framework and open source tools**. [S. l.: s. n.], [2020]. 3. **The Threat Intelligence Handbook: Moving Toward a Security Intelligence Program**: Edited: Zane Pokorny;. 2ª ed. [S. l.: s. n.], [2022]. ISBN 978-1-948939-06-5.

PRIVACIDADE E SEGURANÇA CIBERNÉTICA

Professor(es) ofertante(s): Edna Dias Canedo, Fabio Lucio Lopes de Mendonca e/ou Daniel Alves da Silva.

Carga horária: 60h/a

Ementa: Requisitos de segurança e de privacidade; Ética em requisitos; Técnicas, métodos, metodologias, frameworks e ferramentas para a elicitación de requisitos de segurança e privacidade. Lei Geral de Proteção de Dados (LGPD) e General Data Protection Regulation (GDPR).

Bibliografia básica: 1. MACIEL, Rafael Fernandes. **Manual prático sobre a Lei Geral de Proteção de Dados Pessoais: Atualizado com a Medida Provisória nº 869/18**. 1ª ed. atual. [S. l.]: M Digital Education, 2019. v. 1. 2. BLOKDYK, Gerardus. **GDPR A Complete Guide - 2020 Edition. Practical Tools for Self-Assessment**. [S. l.]: 5STARCooks, 2019. 3. **Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines**. Standard, International Organization for Standardization. First edition. (2019) ISO/IEC 27701. Disponível em: <https://webstore.ansi.org/preview-pages/ISO/preview_ISO+IEC+27701-2019.pdf>

Bibliografia complementar: 1. WIEGERS, Karl; BEATTY, Joy. **Software Requirements (Developer Best Practices)**. 3. ed. [S. l.]: Microsoft, 2013. 2. BLOKDYK, Gerardus. **Security Requirements A Complete Guide - 2019 Edition**. [S. l.]: 5STARCooks, 2019. 3. BLOKDYK, Gerardus. **Privacy Requirements A Complete Guide - 2019 Edition**. [S. l.]: 5STARCooks,



2019. **4. REGULATION**, G. D. P. EU Data Protection Rules. European Commission. (2018). Disponível em: <https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en>. **5. PIPER**, D. L. A. Data protection laws of the world: Full handbook. DLA Piper Intelligence. 2019. 1–834. Disponível em <<https://www.dlapiperdataprotection.com/>> **6. PRESIDÊNCIA DA REPÚBLICA. Lei Geral de Proteção de Dados Pessoais (LGPD), Secretaria-Geral**, [S. l.], 2018. Disponível em <<https://www.pnm.adv.br/wp-content/uploads/2018/08/Brazilian-General-Data-Protection-Law.pdf>>.

SEGURANÇA DE REDES 1

Professor(es) ofertante(s): Georges Daniel Amvame Nze e/ou Rafael Timóteo de Sousa Júnior.

Carga horária: 60h/a

Ementa: Estudo, análise, implementação e configuração dos diversos Protocolos da Pilha TCP/IP; Aplicação de linguagem de programação Python e Script em BASH para automação de redes; Aplicação dos conceitos de Gerência e Segurança de Redes via criação de ambientes NOC e SOC; Estudo e análise de Ataques Cibernéticos via Topologias de Interconexão de Redes por Emulação de Rede.

Bibliografia básica: **1. KUROSE, J.; ROSS, K. Computer Networking: A Top-Down Approach.** 7. ed. [S. l.]: Pearson Education, 2017. **2. FOROUZAN, Behrouz A. TCP/IP Protocol Suite.** 4ª ed. [S. l.]: McGraw Hill, 2010. **3. DIOGENES, Yuri; OZKAYA, Erdal. Cybersecurity – Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team Tactics.** Packt Publishing USA: [s. n.], 2018.

Bibliografia complementar: **1. FALL, Kevin R.; STEVENS, W. R. TCP/IP Illustrated, Volume 1: The Protocols.** 2. ed. Addison-Wesley Professional Computing Series: [s. n.], 2011. **2. COMER, Douglas E. Internetworking with TCP/IP.** 6. ed. [S. l.]: Prentice-Hall, 2013. v. 1. **3. ERIBERTO, João. Análise de Tráfego em Redes TCP/IP: Utilize tcpdump na análise de tráfegos em qualquer sistema operacional".** [S. l.]: Novatec Editora Ltda, 2013. **4. M, Antonio, et al. (Equipe IPv6.br). Laboratório de IPv6: Aprenda na prática usando um emulador de rede.** [S. l.]: Novatec Editora Ltda, 2015. Disponível em: <<http://ipv6.br/livro-lab-ipv6-nicbr.pdf>>. **5. TUSHAR, Shantanu. Linux Shell Scripting Cookbook.** 2. ed. [S. l.]: Packt Publishing, 2013. **6. MEDHI, Deepankar. Network Routing: Algorithms, Protocols, and Architectures.** 1ª ed. [S. l.]: Morgan Kaufmann, 2007. **7. SETH, Sameer; VENKATESULU, M. Ajaykumar. TCP/IP Architecture, Design and Implementation in Linux".** 1ª ed. [S. l.]: Morgan Kaufmann, 2008.



SEGURANÇA EM SISTEMAS DISTRIBUÍDOS

Professor(es) ofertante(s): Rafael Timóteo de Sousa Júnior.

Carga horária: 60h/a

Ementa: Fundamentos e Conceitos. Metodologias de Desenvolvimento de Sistemas. Arquiteturas de Sistemas Distribuídos, Desenvolvimento de Sistemas Distribuídos.

Bibliografia básica: 1. COLOURIS, G. et al. **Distributed Systems: Concepts and Design**, 5th Edition. Pearson. 2. TANEBAUM, A.S. and STEEN, M.V. **Distributed Systems: Principles and Paradigms**, 2nd Edition. 3. KUROSE, J. F.; ROSS, K. W. **Redes de Computadores e a Internet – Uma Abordagem Top-down** - 3ª Ed. Pearson Education.

Bibliografia complementar: 1. The Gnutella protocol specification v 0.4, Document revision 1.2. Disponível em: <www.clip2.com>. 2. STOICA, I. et al. **Chord: a scalable peer-to-peer lookup service for Internet applications**, SIGCOMM 2001. 3. FOSTER, I. **The Grid: a new infrastructure for 21st century science**. Physics Today, 2002. 4. GHEMAWAT, S. and DEAN, J. **MapReduce: Simplified Data Processing on Large Clusters**. OSDI 2004. 5. FOSTER, I. et al. **On death, taxes and the convergence of peer-to-peer and grid computing**. IPTPS 2003. 6. SOUSA, JR, R. T.; ADNANE, A.; BIDAN, C.; MÉ, L. **Vulnerabilidades e Proteções do Protocolo de Roteamento Ad Hoc OLSR sob o Ponto de Vista da Confiança**. Revista IEEE América Latina, v. 7, p. 594-602, 2009. 7. HOLTZ, M. D.; DAVID, B. M.; SOUSA JR, R. T. **Building Scalable Distributed Intrusion Detection Systems Based on the MapReduce Framework**. Telecomunicações (Santa Rita do Sapucaí), v. 13, p. 22-31, 2011.

SEGURANÇA EM INTERNET DAS COISAS

Professor(es) ofertante(s): Daniel Chaves Café, Fábio Lúcio Lopes de Mendonça.

Carga horária: 60h/a.



Ementa: Internet das Coisas. Sistemas Operacionais Embarcados de Tempo Real. Comunicação entre processos. Proteção da memória. Conectividade.

Bibliografia básica: 1. ALMEIDA, Rodrigo M. A; MORAES, C. H. V; SERAPHIM, T. F. P. **Programação de Sistemas Embarcados**, Elsevier. [S. l.: s. n.], 2016. 2. OLIVEIRA, Rômulo Silva de. **Fundamentos dos Sistemas de Tempo Real**. [S. l.: s. n.], 2020. 3. ALMEIDA, Marcelo Barros de. **Implementando Sistemas Operacionais de Tempo Real em Microcontroladores**. ed. MSP430. [S. l.: s. n.], [2022].

Bibliografia complementar: 1. LI, Qing; YAO, Carolyn. **Real-Time Concepts for Embedded Systems**. [S. l.: s. n.], 2003. 2. WANG, Jiacun. **Real-Time Embedded Systems**, Wiley. [S. l.: s. n.], 2017. 3. COOLING, Jim. **Real-time Operating Systems: Book ½**. [S. l.: s. n.], [2022]. 4. WANG, K.C. **Embedded and Real-Time Operating Systems**. [S. l.: s. n.], 2017. 5. LAMIE, Edward L. Lamie. **Real-Time Embedded Multithreading Using ThreadX**. [S. l.: s. n.], 2016.

SEGURANÇA NO DESENVOLVIMENTO DE SOFTWARE

Professor(es) ofertante(s): Edna Dias Canedo.

Carga horária: 60h/a.

Ementa: Introdução ao ciclo de vida de desenvolvimento de software seguro (Secure SDLC ou SDL). Introdução ao OWASP e DevSecOps.

Bibliografia básica: 1. VIEGA, J; MACGRAW, G. R. **How to avoid security problems the right way, portable documents**. *In*: HOW to avoid security problems the right way, portable documents: Pearson Education. [S. l.: s. n.], 2001. 2. WYSOPAL, C.; NELSON, L; DUSTIN, E; DAI, Zovi. **Identifying software security flaws**: Pearson Education. *In*: HOW to avoid security problems the right way, portable documents: Pearson Education. [S. l.: s. n.], 2006. 3. WICHERS, D.; WILLIAMS, J. **Owasp top-10 2017. The Ten Most Critical Web Application Security Risks**. OWASP Foundation, 3, 4.

Bibliografia complementar: 1. AL-AHMAD, W. **Building secure software using xp**. *In* **Developing and Evaluating Security-Aware Software Systems**. *In*: IN Developing and Evaluating Security-Aware Software Systems: IGI Global. [S. l.: s. n.], 2013. p. 161-175. 2. MCGRAW, G. **IEEE Security & Privacy**. *In*: IEEE Security & Privacy. [S. l.: s. n.], 2004. p. 80-83. 3. AXELROD, C. W. **Engineering safe and secure software systems**: Artech House. [S. l.: s. n.], 2013. 4. ANDERSON, R. **A guide to building dependable distributed systems**: John Wiley & Sons. [S. l.: s. n.], 2020. 5. HSU, T. H. C. **Ensure continuous security, deployment, and delivery with DevSecOps**: Packt Publishing Ltd. [S. l.: s. n.], 2018.



TÓPICOS EM SEGURANÇA CIBERNÉTICA 1

Professor(es) ofertante(s): Fabio Lucio Lopes de Mendonça, Daniel Chaves Café, João José Costa Gondim e/ou Rafael Timóteo de Sousa Júnior.

Carga horária: 60h/a.

Ementa: Disciplina de ementa variável na área de concentração "Segurança Cibernética". Deve abordar em profundidade tópicos consolidados e emergentes de uma ou mais áreas de conhecimento da Segurança Cibernética.

Bibliografia básica: A critério do professor.

bibliografia complementar: A critério do professor.

TÓPICOS EM SEGURANÇA CIBERNÉTICA 2

Professor(es) ofertante(s): Fabio Lucio Lopes de Mendonça, Daniel Chaves Café, João José Costa Gondim e/ou Rafael Timóteo de Sousa Júnior.

Carga horária: 60h/a.

Ementa: Disciplina de ementa variável na área de concentração "Segurança Cibernética". Deve abordar em profundidade tópicos consolidados e emergentes de uma ou mais áreas de conhecimento da Segurança Cibernética.

Bibliografia básica: A critério do professor.

bibliografia complementar: A critério do professor.

TÓPICOS EM SEGURANÇA CIBERNÉTICA 3

Professor(es) ofertante(s): Fabio Lucio Lopes de Mendonça, Daniel Chaves Café, João José Costa Gondim e/ou Rafael Timóteo de Sousa Júnior.

Carga horária: 60h/a.

Ementa: Disciplina de ementa variável na área de concentração "Segurança Cibernética". Deve abordar em profundidade tópicos consolidados e emergentes de uma ou mais áreas de conhecimento da Segurança Cibernética.

Bibliografia básica: A critério do professor.

bibliografia complementar: A critério do professor.



TÓPICOS EM SEGURANÇA CIBERNÉTICA 4

Professor(es) ofertante(s): Daniel Chaves Café e/ou William Ferreira Giozza.

Carga horária: 30h/a.

Ementa: Disciplina de ementa variável na área de concentração "Segurança Cibernética". Deve abordar em profundidade tópicos consolidados e emergentes de uma ou mais áreas de conhecimento da Segurança Cibernética.

Bibliografia básica: A critério do professor.

bibliografia complementar: A critério do professor.

TÓPICOS EM SEGURANÇA CIBERNÉTICA 5

Professor(es) ofertante(s): Daniel Chaves Café e/ou William Ferreira Giozza.

Carga horária: 30h/a.

Ementa: Disciplina de ementa variável na área de concentração "Segurança Cibernética". Deve abordar em profundidade tópicos consolidados e emergentes de uma ou mais áreas de conhecimento da Segurança Cibernética.

Bibliografia básica: A critério do professor.

bibliografia complementar: A critério do professor.

12.2 Estudos orientados

As disciplinas Estudo Orientado 1 e 2, que inclui a preparação efetiva de um plano de trabalho contendo as atividades a serem desenvolvidas durante o curso, juntamente com o projeto de dissertação, é uma possibilidade para dedicação exclusiva a estudos particulares. Os (As) alunos(as) devem, preferencialmente, matricular-se nesta disciplina nos dois últimos semestres de sua vida acadêmica. Assim, a dissertação deve ser apresentada no período correto. Essas disciplinas são de 2 créditos cada e devem ser feitas sequencialmente em dois semestres letivos.

A disciplina Estudo Orientado 3, que inclui a preparação e entrega da versão preliminar da dissertação, também é uma oportunidade para o aluno conseguir tempo para estudos individuais e deve ser cursada, preferencialmente, no terceiro semestre acadêmico regular de cada aluno(a). Essa disciplina é de 4



créditos e deve ser feita em momento estratégico na carreira acadêmica do aluno.

12.3 Estágio de docência

O estágio de docência no âmbito do PPEE é implementado com a oferta da disciplina: Estágio de docência em Engenharia Elétrica 1 (código PPEE2007) de 2 créditos e 30hs/aula, disponível para todos os discentes. A matrícula nessa disciplina é optativa para os discentes.

O objetivo dessa oferta é possibilitar que os discentes tenham a oportunidade de desenvolver atividades de docência dedicadas a alunos de graduação em disciplinas de sua área de atuação, sempre sob a supervisão de professores do programa.

A prática de docência constitui disciplina do currículo, tendo caráter optativo para os alunos, visto que, até o momento, o programa não possui alunos bolsistas da CAPES.

15. Sistema de avaliação

Para lograr êxito e obter créditos cursados nas disciplinas no PPEE, os alunos serão submetidos ao sistema de avaliação adotado pela UnB, que estabelece os seguintes conceitos/equivalências numéricas:

Tabela 8 - Menções, equivalência numérica e situação

Menção	Equivalência numérica	Situação
SS	9,00 a 10,00	Aprovado
MS	7,00 a 8,90	Aprovado
MM	5,00 a 6,90	Aprovado
MI	3,00 a 4,90	Reprovado
II	0,10 a 2,90	Reprovado
SR	Sem aproveitamento	Reprovado



16. Sistema de obtenção e aproveitamento de créditos

A critério do PPEE e obedecidas as equivalências, os créditos cursados como aluno(a) especial ou em mestrados anteriores em outras instituições poderão ser aproveitados em um máximo de 8 (oito) créditos. Mesmo aproveitando créditos em disciplinas cursadas anteriormente, o(a) aluno(a) deverá cursar outras disciplinas (do tronco comum ou eletivas) para completar os créditos equivalentes do curso.

Aos discentes do PPEE é facultado o aproveitamento de até 8 (oito) créditos cursados há no máximo 10 (dez) anos antes da data da matrícula no programa, com aprovação em cursos de pós-graduação stricto sensu em instituições brasileiras ou estrangeiras, incluindo disciplinas cursadas por meio de acordo de cotutela.

Os (As) discentes do PPEE poderão cursar disciplinas de pós-graduação stricto sensu na modalidade aluno(a) especial em qualquer instituição de ensino superior e aproveitar crédito no Programa, não ultrapassando os 8 (oito) créditos máximos para aproveitamento, com a devida anuência de seus respectivos orientadores. Esta modalidade de aproveitamento de créditos tem o objetivo de fortalecer a formação do(a) discente na área de concentração e linha de pesquisa dos(as) discentes.

Em todos os casos de aproveitamento de disciplinas, é necessário a compatibilidade bibliográfica de pelo menos 70% de uma das disciplinas ofertadas pelo PPEE.

17. Produções

Os discentes regulares que ingressaram no PPEE a partir de 2018, ou seja, a partir do início da gestão autônoma do programa, já produziram efetivamente conteúdo relevante e aparecendo como autores principais e coautores de parte dessas publicações.

Instituiu-se no Art. 34, incisos I e II do Regulamento do Programa, que para obter o diploma de Mestre, o aluno deve comprovar publicações ou registro de pesquisa, desenvolvimento e inovações, tornando como obrigatório, além da produção de uma dissertação de qualidade, a publicação de trabalhos científicos ou registros devidamente emitidos por entidades públicas com as devidas atribuições de competências. O objetivo aqui instaurado é de incentivar os alunos a se manterem vinculados nos eixos da universidade pública (pesquisa, extensão e inovação), produzindo trabalhos acadêmicos de qualidade em coautoria com os respectivos orientadores, ou seja, o (a) mestrando(a) deve



submeter pelo menos um artigo em revista científica com Qualis CAPES mínimo A4, em tópicos relacionados ao seu trabalho de pesquisa.

Portanto, até o final do período letivo 2022/2, 35 (trinta e cinco) defesas de Trabalho de Conclusão (https://ppee.unb.br/?page_id=36) contribuíram para várias publicações em nível nacional e internacional, dentre as quais registram-se: 60 (sessenta) publicações em revistas, congressos e/ou periódicos científicos e 3 (três) Registros de Programa de Computador (BR512020000871-2; BR512020001758-4; BR512020001705-3).

Considerando ainda a parceria com o Laboratório de Tomada de Decisões (LATITUDE-www.latitude.unb.br), diversos discentes e docentes, conforme registrado na Plataforma, e tendo como missão a geração de projetos de PD&I, relatórios técnicos, registros de softwares, artigos científicos dentre outros previstos nos planos de trabalhos celebrados com diversas instituições públicas e privadas.

Dessa forma, o PPG mostra contínua dedicação de esforços para aumentar o volume de produtos nos diversos âmbitos de seus alcances, por meio de dissertações, projetos, desenvolvimentos e pesquisas.

18. Comissão examinadora

A dissertação de Mestrado é julgada por uma Comissão Examinadora constituída pelo professor orientador, este sem direito a julgamento, e composta por 2 (dois) outros membros titulares, sendo, pelo menos, um deles não vinculado ao PPEE, e por 1 (um) suplente.

Os membros da Comissão Examinadora, exceto o orientador, não poderão estar envolvidos com o projeto da dissertação.

A Comissão Examinadora, indicada pelo orientador, será analisada e escolhida pela Comissão de Pós-graduação do Programa (CPG/PPEE), observados os critérios de excelência na área de conhecimento do trabalho a ser avaliado e homologado.

Para participação em banca examinadora, o PPEE exige critérios mínimos conforme atos específicos.

A cada dissertação, a Comissão Examinadora atribuirá uma das seguintes menções: aprovação, aprovação com revisão de forma, reformulação ou reprovação. As decisões da Comissão Examinadora de Dissertação de Mestrado serão tomadas por unanimidade.



19. Conclusão e duração do curso

Para concluir o curso de Mestrado o aluno terá 24 meses e, em casos excepcionais, prorrogáveis por mais 6 meses, além de atender às condições mínimas exigidas pelo PPEE em Atos específicos.

20. Diplomação

A expedição do diploma de Mestre ficará condicionada à homologação, pelo Decanato de Pós-Graduação, de relatório elaborado pela Comissão Examinadora. O relatório de defesa deverá ser encaminhado ao Decanato de Pós-graduação (DPG) pelo Coordenador do PPEE, no prazo máximo de 15 (quinze) dias, a partir da data final estipulada pela banca examinadora.

O diploma será o único documento emitido para comprovação do título, ficando vedada, em qualquer instância, a emissão de declaração ou cópia do relatório de defesa, como comprovante de titulação. Em caso de redação em outros idiomas que não o português, um pedido circunstanciado deverá ser submetido para apreciação do PPEE.

21. Egressos

A formação pretendida e o perfil de egressos dos discentes do PPEE se coadunam com as características almeçadas da Universidade de Brasília, a qual se pauta na formação de mestres com excelência em formação e pesquisas, tecnologias de ponta, ética, responsabilidade social e desenvolvimento sustentável. Do mesmo modo, a grande área Engenharias IV da CAPES idealiza o impacto social dos conhecimentos obtidos em dissertações e outros produtos desenvolvidos

Em consonância com o perfil geral do egresso pretendido pela UnB e Capes, o PPEE tem diversos estudantes realizando estudos com inteligência artificial. Também, os mestres egressos de nosso Programa têm atuação direta em diversas instituições e autarquias públicas e privadas como no Ministério da Justiça e Segurança Pública, Agência Brasileira de Inteligência, Escola Nacional de Administração Pública, Exército Brasileiro, Caixa Econômica Federal, Banco do Brasil, Tribunal de Justiça do Distrito Federal e Territórios, Embratel, Supremo Tribunal Federal, Universidades Federais como a própria UnB e diversos Institutos Federais (IFs), em Universidades Privadas e outros órgãos do governo, entidades de classe, entre outras.

O PPEE busca formar profissionais para atuar como docentes, pesquisadores e profissionais qualificados, em nível de excelência e com capacidade criadora de



inovação, para contribuir com os avanços na ciência e tecnologia e para atuação nas diversas áreas da segurança cibernética, na administração pública e privada, não-governamental e sociedade civil ligados aos setores de inteligência e segurança.

De acordo com o levantamento mais recente, o perfil de atuação predominante dos egressos do PPEE desde 2018 é do setor público, incluindo instituições públicas (Senado Federal, Exército Brasileiro, Agência Brasileira de Inteligência e Banco do Brasil) e de instituições financeiras (Banco do Brasil, Caixa Econômica Federal e Banco de Brasília). Em menor proporção, os egressos estão atuando em organizações não-governamentais e em empresas privadas.

A partir dos objetivos do PPEE e da análise do perfil dos egressos, foram estabelecidas algumas diretrizes principais para a orientação da atuação do Programa e no fortalecimento de suas ações.

Como o PPEE visa formar profissionais na área de segurança cibernética, nos diversos domínios da Engenharia Elétrica, pelo fomento à compreensão, pesquisa e aplicação de técnicas e métodos de trabalho pertinentes aos sistemas de energia elétrica, eletrônica e automação, telecomunicações, redes de comunicação e sistemas de informação, que contribuam à proteção e resiliência desses sistemas; muitos ingressos que solicitam matrícula no PPEE são profissionais que atuam em órgãos do governo, como forças da lei, forças armadas, órgãos de controle e auditoria, os quais estão preocupados com o crescimento da insegurança, e buscam modelos de análise de evidências e localização de informações atinentes à segurança nacional e do cidadão.

Assim, em 2020, como resultado de avaliação final, 10 (dez) egressos obtiveram seus Diplomas de Mestre em Engenharia Elétrica na área de concentração de Segurança Cibernética após terem tido êxito em publicação de trabalhos científicos e apresentação individual da defesa de Trabalho de Conclusão de curso, de forma remota via plataforma Microsoft Teams. A título de exemplo, segue lista dos órgãos aos quais pertencem os egressos do PPEE: Caixa Econômica Federal; Tribunal de Justiça do Distrito Federal e Territórios (TJDFT); Banco do Brasil (Diretoria de Tecnologia); Gerência de Espectro, Órbita e Radiodifusão (ORER) da Superintendência de Outorga e Recursos à Prestação (SOR) da Agência Nacional de Telecomunicações (Anatel); Exército Brasileiro (Escola de Comunicações); Casa Civil (Presidência da república); Força Aérea Brasileira (FAB); CINDACTA-I (FAB) e Supremo Tribunal Federal (STF) dentre outros.



Outro destaque da atuação do PPEE é a formação de pós-doutorados que atuam em Universidades estrangeiras e no próprio PPEE como pesquisadores colaboradores.

Universidade de Brasília – UnB

Programa de Pós-Graduação Profissional em Engenharia Elétrica - PPEE

www.unb.br – www.ppee.unb.br

