PROGRAMA DE FORMAÇÃO EM CIBERSEGURANÇA PARA A AMÉRICA LATINA E O CARIBE

BID

COSEC UC3M COMPUTER SECURITY LAB

PROGRAMA DE FORMAÇÃO EM CIBERSEGURANÇA PARA A AMÉRICA LATINA E O CARIBE

Banco Interamericano de Desenvolvimento (BID)
Ariel Nowersztern
Santiago Paz
Darío Kagelmacher
Florencia Cabral Berenfus
Pablo Libedinsky

Computer Security Lab (COSEC)
Arturo Ribagorda
Juan Tapiador
José María de Fuentes
Lorena González

Códigos JEL: F52, I20, I23, I25, I28, J24, J44, J45, O15, O30

Palavras-chave: cibersegurança, educação superior

Banco Interamericano de Desenvolvimento
1300 New York Avenue, N.W.
Washington, D.C. 20577
www.iadb.org

O Setor de Instituições para o Desenvolvimento foi o responsável pela produção da publicação.

Provedores externos:

Coordenação da produção editorial: A&S Information Partners, LLC
Revisão editorial: Giovana Boselli
Diagramação: Gastón Cleiman

PROGRAMA DE FORMAÇÃO EM CIBERSEGURANÇA PARA A AMÉRICA LATINA E O CARIBE

BID

COSEC UC3M COMPUTER SECURITY LAB

Sumário

Tabela de figuras

Índice de tabelas

Prólogo

Vivemos em um mundo cada vez mais digitalizado, em que as tecnologias têm papel essencial na nossa qualidade de vida. As tecnologias digitais já são um elemento fundamental nos mais diversos setores, como as finanças, o governo, o transporte, a energia, a saúde ou a educação. E essa transformação foi ainda mais acelerada com o início da pandemia de COVID-19. Em 2020, testemunhamos como a tecnologia deixou de ser uma comodidade para transformar-se em uma ferramenta essencial.

Conforme nos lembram as notícias diariamente, a digitalização aumentou o nosso uso de plataformas on-line e, com isso, a probabilidade de sermos vítimas de ataques cibernéticos. Dado o enorme impacto que os incidentes de cibersegurança podem ter na vida dos cidadãos – nas finanças, na segurança, privacidade ou na manutenção dos serviços essenciais – preparar-se para enfrentar os riscos do espaço cibernético é uma responsabilidade conjunta de todos os atores do mundo digital. Para tanto, são necessários recursos humanos capazes de defender o ambiente digital. Contudo, as evidências mostram que um dos grandes desafios da cibersegurança é a escassez de profissionais capacitados. Estima-se que, em 2021, haverá 3,5 milhões de vagas nessa área, das quais 630.000 estarão na América Latina e no Caribe.

A formação de profissionais especializados em cibersegurança é fundamental. O Relatório Regional de Cibersegurança publicado pelo Banco Interamericano de Desenvolvimento (BID) e a Organização dos Estados Americanos (OEA), em meados de 2020, demonstrou que ainda existe muito espaço para o desenvolvimento de programas universitários na área de cibersegurança na América Latina e no Caribe. Se a formação de profissionais não for ampliada nos próximos anos, nossa região não apenas ficará sujeita a um número cada vez mais frequente de ataques cibernéticos, além da limitação da capacidade de desenvolvimento digital. Os riscos de ignorar esse fato são muito grandes.

O BID estabeleceu uma produtiva cooperação com a Universidad Carlos III de Madrid, uma das instituições espanholas pioneiras em cibersegurança e com notável trajetória acadêmica no assunto. O primeiro produto dessa

colaboração foi um curso on-line aberto e massivo (MOOC), lançado no início de 2020, voltado para a aprendizagem das ferramentas e aplicações práticas de cibersegurança.

As universidades e as instituições de ensino superior têm papel central no desenvolvimento de talentos humanos, especialmente nas áreas relacionadas com as tecnologias avançadas. O presente documento, produto de meses de elaboração e validação, oferece um programa de mestrado em cibersegurança de uso livre e gratuito, que indica o caminho para suprir a lacuna de ensino na América Latina e no Caribe. O programa é fruto do esforço compartilhado com 68 excelentes instituições acadêmicas da região, cuja estreita colaboração, agradecemos. Desde o começo do processo de elaboração, o programa foi avaliado e recebeu colaboração das instituições destinatárias, que indicaram suas necessidades e recomendações por meio de pesquisas e oficinas de discussão. Para essa e outras iniciativas de cibersegurança, o BID contou com o valioso apoio técnico e financeiro do governo da Espanha.

Em nossa instituição, estamos muito comprometidos com o fortalecimento do capital humano de cibersegurança na região. O presente documento se une a todos os demais esforços que o BID impulsionou nos últimos anos para se aproximar do conhecimento especializado e continuar oferecendo apoio técnico e financeiro aos países membros, com o objetivo de fortalecer o espaço cibernético da América Latina e do Caribe, e seguir estimulando o desenvolvimento digital nas nossas sociedades.

Miguel Porrúa

Coordenador do cluster de dados e governo digital
Divisão de inovação para atendimento ao cidadão
Banco Interamericano de Desenvolvimento

Introdução e visão metodológica

/10

O presente documento descreve um programa de formação em cibersegurança, em nível de mestrado, desenvolvido pela Universidade Carlos III de Madrid (UC3M) para a região da América Latina e o Caribe (ALC), no contexto de um contrato de apresentação de serviços subscrito pelo Banco Interamericano de Desenvolvimento (BID).

O desenvolvimento desse programa de cibersegurança atendeu às necessidades e preferências identificadas por distintas universidades latino-americanas. O programa visa ao desenvolvimento de um plano voltado para essa região, cujo objetivo é formar profissionais nessa área que satisfaçam as necessidades existentes. As contribuições dessas instituições foram coletadas pela UC3M e incorporadas ao programa de formação aqui apresentado. Assim, o desenho do programa se forma, principalmente, a partir da visão que surge das instituições consultadas, ainda que também da experiência docente da UC3M no assunto.

1. Metodologia de coleta de informação

Para obter a visão das instituições, foi elaborada uma pesquisa com o fim de estabelecer as bases para o desenvolvimento do programa de formação, com as seguintes questões:

- Em que idioma deveria ser ministrado o programa?
- Que modelo de aulas seria mais recomendado?
- Desconsiderando a resposta anterior e, supondo que se opte pelo modelo presencial, se cada hora-aula requer uma hora e meia de estudo individual, que carga horária presencial deveria ter o mestrado?
- Na sua opinião, atendendo às necessidades de formação do seu país, qual deveria ser a duração de um mestrado em cibersegurança?
- Que título deveriam receber os alunos que concluíssem um mestrado dessa natureza?
- Considera que o plano de estudos deveria contemplar a realização de um trabalho final (doravante, TF) obrigatório?
- Consideraria a possibilidade de que o TF fosse feito como projeto ou trabalho de pesquisa em uma empresa?
- Acredita que as necessidades do seu país recomendariam que o mestrado tivesse áreas de especialização, de modo que, além da formação generalista, os alunos pudessem escolher entre duas ou mais áreas de especialização?
- Considera oportuno que os alunos façam parte da formação em uma empresa? (Com opções de período de três ou seis meses)
- Qual deveria ser a porcentagem da carga horária do TF em relação à carga horária presencial total?
- Assinale a demanda das disciplinas em cibersegurança.

A fim de garantir a eficácia do instrumento, a pesquisa procurou ter foco no interesse da região em certas disciplinas, ainda que sem contemplar os conteúdos detalhados que deveriam ser abordados em cada uma. Esses pormenores teriam estendido substancialmente a pesquisa, sem contribuir com informação relevante para as disparidades que, sem dúvida, teriam manifestado as universidades pesquisadas.

A pesquisa foi acompanhada do devido documento com informações relativas ao tratamento de dados pessoais, a fim de que os entrevistados pudessem

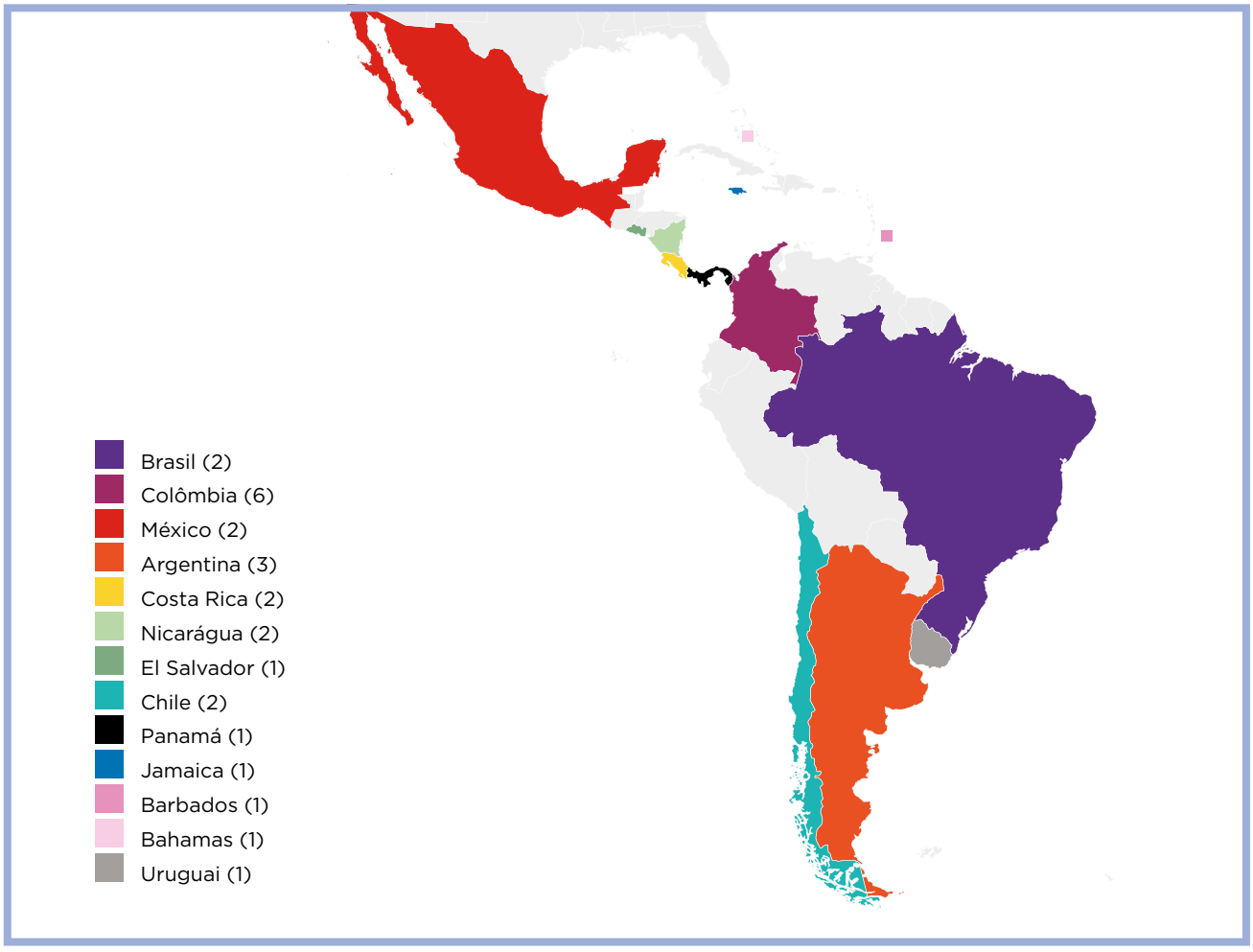
exercer osdireitos previstos na normativa legal europeia,[1] e sua adaptação ao marco constitucional espanhol[2] acerca da proteção e tratamento de seus dados.

1 Regulamento Geral (UE) 679/2018 de Proteção de Dados Pessoais.

2 Lei orgânica 3/2018 de proteção de dados pessoais e garantia dos direitos digitais.

A pesquisa foi enviada por e-mail a 105 universidades latino-americanas e caribenhas, com um lembrete posterior às que não tinham respondido. Depois disso, foram enviados outros dois e-mails, sendo o primeiro a sete professores de cibersegurança de universidades indicadas pela Associação Nacional de Universidades e Instituições de Educação Superior (ANUIES), do México, e o segundo a professores de cibersegurança de seis universidades da região objeto do estudo. Foram recebidas 31 respostas,

Figura 1. Países participantes e a quantidade de universidades que responderam à pesquisa.



dentre as quais uma foi descartada por estar incompleta, e cinco por procederem da mesma instituição acadêmica. Assim, foram consideradas válidas 25 respostas. A **figura 1** mostra os países que participaram da pesquisa e, entre parênteses, o número de instituições acadêmicas em cada um deles que a responderam.

2. Síntese das respostas e recomendações recebidas

A análise das respostas permitiu estabelecer as bases do programa. Na **figura 2**, são apresentados o idioma, o tipo de modelo de ensino, a duração do mestrado e o tipo de formação que os alunos deveriam ter, de acordo com as respostas recebidas.

No que se refere ao idioma, dada a diversidade de respostas, não se considera recomendar um deles, mas deixar a questão ao arbítrio de cada universidade. De acordo com a experiência dos autores, entretanto, um mestrado de caráter majoritariamente técnico como esse deveria ser ministrado em inglês ou, pelo menos, em modalidade bilíngue, sendo o inglês uma das línguas. Por exemplo, inglês e espanhol, inglês e português, etc.

A **figura 3** mostra se os pesquisados estão de acordo ou não com o estabelecimento de um TF, com sua realização em uma empresa, com a divisão

Figura 2. Número de respostas à pesquisa (I)

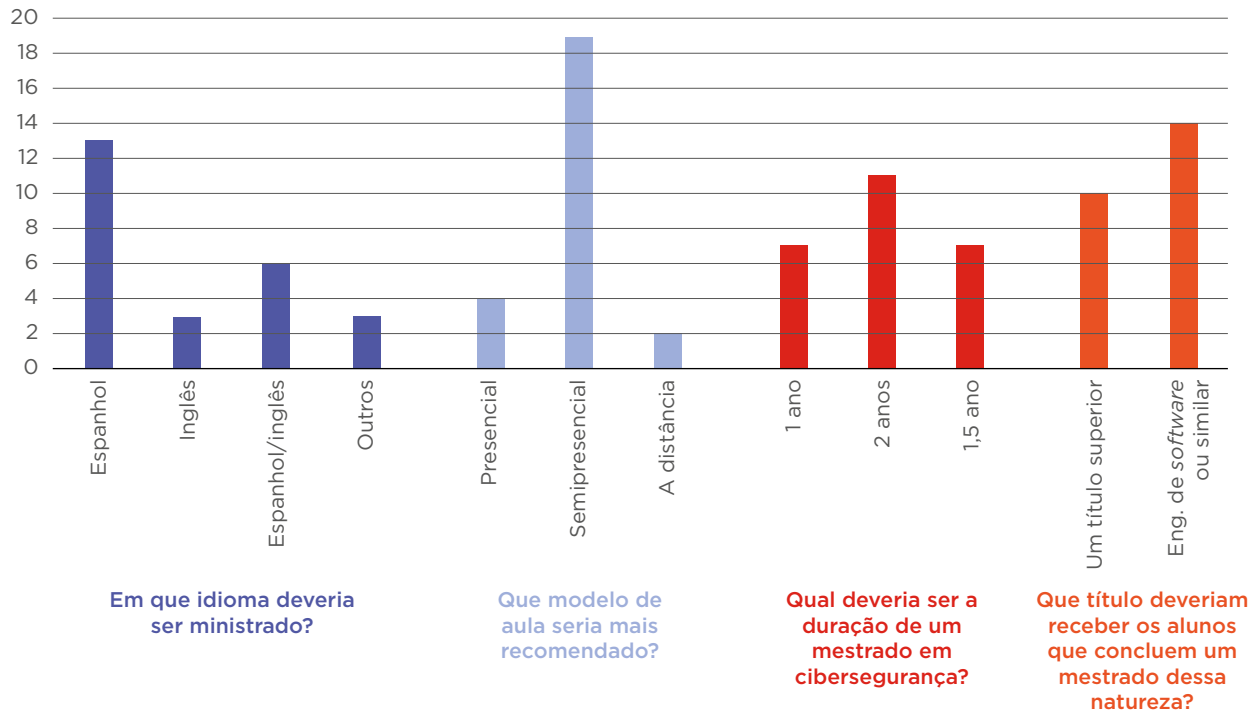
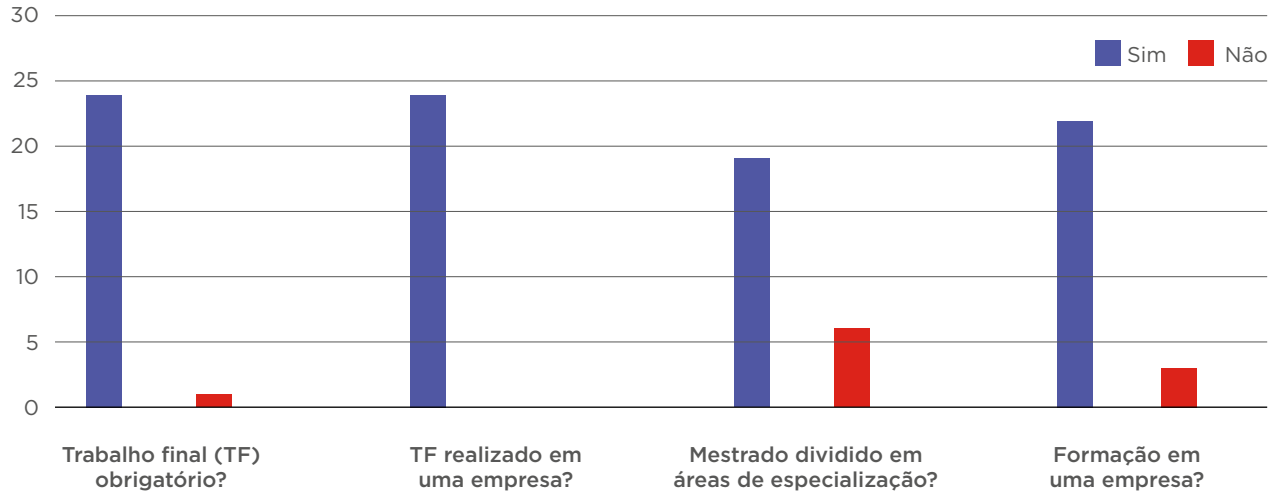


Figura 3. Número de respostas à pesquisa (II)



do mestrado em áreas de especialização e com a realização de parte da formação em uma empresa.

Como pode ser observado, a esmagadora maioria considera que o mestrado deveria incluir um TF, todos consideram que o TF deveria ser realizado em uma empresa e quase todos que os alunos deveriam concluir a formação em uma empresa (independentemente do TF). Por último, a maioria também é favorável a estabelecer áreas de especialização.

Com relação às disciplinas que poderiam compor o mestrado, a **tabela 1** apresenta a demanda esperada para as disciplinas propostas.

Tabela 1. Número de respostas sobre a demanda de disciplinas propostas

Disciplinas propostas	Alta demanda	Pouca demanda
Desenvolvimento de sist. seg./seg. DevOps	19	6
Análise de cibersegurança	18	6
Seg. em sist. industriais (inclusive IoT)	10	14
Seg. em sist. ciberfísicos	10	14
Segurança na computação em nuvem	22	3
Segurança em *big data*	19	6
Informática forense	17	7
Adm. e gestão da seg.	9	13
Seg. em redes (IDS, SIEM, etc.)	21	4
Comunicações seguras (protocolos)	16	9

Em relação à carga horária semanal de aula presencial, os pesquisados indicam majoritária preferência pela carga de 15 horas[3] semanais.

3 No documento, são feitas referências a horas-aula em vez de créditos, cuja duração em horas-aula presenciais e de trabalhos do aluno podem variar entre os países.

Igualmente, sugerem que haja um período de formação de três meses em uma empresa.

Portanto, atendendo aos resultados da pesquisa, o programa terá, entre outras, as seguintes características:

Tabela 2. Síntese das recomendações oferecidas pelas universidades da América Latina e o Caribe pesquisadas.

Característica	Sugestão
Duração	2 anos
Idioma	Dada a variedade das respostas, não é possível recomendar um idioma
Formato das aulas	Semipresencial
Carga horária	15 horas semanais
Formação anterior	Engenheiro de sistemas (bacharelado), de *software*, de computação e similares
Trabalho final (TF)	Sim, preferencialmente realizado em uma empresa
Orientação formativa	Formação generalista e especializada
Formação em empresas	Sim, por três meses
Disciplinas mais demandadas	• Desenvolvimento de sistemas seguros/ segurança DevOps • Análise em cibersegurança • Segurança na computação em nuvem • Segurança em *big data* • Informática forense • Segurança em redes (IDS, SIEM, etc.) • Comunicações seguras (protocolos)

3. Incorporação das recomendações ao desenho do programa e adaptações introduzidas

As recomendações recebidas foram levadas em consideração para a elaboração do programa. No entanto, durante a etapa final, foi necessário adaptar algumas das recomendações, tomando decisões diferentes, sintetizadas nos grupos descritos a seguir.

Devido ao fato de os pesquisados terem, majoritariamente, optado por permitir o acesso a

graduados sem formação específica em tecnologias da informação e das comunicações (TIC), bem como por estabelecer áreas de especialização, fazer estágio em empresas ou organismos públicos e elaborar um TF, pareceu oportuno, para fins de organização, agrupar as disciplinas em módulos conforme sua natureza. Assim, as disciplinas a serem cursadas pelos alunos sem conhecimentos específicos de TIC foram incorporadas a um módulo de nivelamento (módulo 0), as gerais de cibersegurança foram compreendidas em um módulo denominado generalista ou de cibersegurança geral (módulo 1), as disciplinas de especialização em um módulo com o mesmo nome (módulo 2), as optativas em um módulo de formação complementar (módulo 3) e, finalmente, o trabalho final e as práticas em empresas no designado TF/estágio (módulo 4).

a) Incorporação de disciplinas que não estavam entre as mais demandadas

Foi incorporada uma disciplina cuja demanda não tinha sido identificada como alta, mas cujo estudo foi considerado como imprescindível para o correto aproveitamento do mestrado. Trata-se de criptografia aplicada, disciplina que, em grande parte dos programas de pós-graduação em cibersegurança, se dedica, entre outros temas, a tratar das técnicas criptográficas (incluindo as funções *hash*, assinatura digital, etc.).

Do mesmo modo, optou-se por incorporar ao programa proposto outras disciplinas que, por experiência, também são convenientes, ainda que nesse caso, como formação optativa à margem das áreas de especialização. Essas, ao lado de outras indicadas como mais demandadas, estão no módulo 3, Formação complementar.

Assim, optou-se por incluir a disciplina Administração e gestão da segurança, no módulo 1 (portanto, como obrigatória), a fim de abranger alguns conteúdos demandados pelos pesquisados, como auditoria, bem como contemplar outros temas, por exemplo, os sistemas de gestão da segurança da informação (família ISO/IEC 27000, COBIT, marco do NIST), de importância crescente.

Também foram acrescentados Segurança em internet das coisas (IoT) e Segurança em sistemas ciberfísicos. Ambas as disciplinas estão adquirindo grande relevância pela dependência crescente dos sistemas de controle industriais (e, fundamentalmente, os que respaldam infraestruturas críticas) das tecnologias da informação (TI). Ou, de outro modo, da integração das TIs nas tecnologias operacionais (TO). Há cada vez mais demanda por especialistas dessa área, à medida que vai se desenvolvendo a Indústria 4.0 (em grande parte, graças à IoT).

Finalmente, optou-se também por incluir uma disciplina optativa sobre os aspectos legais da cibersegurança, haja vista a cada vez mais numerosa incorporação dessa disciplina a normas legais de todo tipo (códigos penais que contemplam o delito informático, leis de proteção de dados pessoais, de regulamentação do uso da internet e do comércio eletrônico, etc.) que não podem deixar de fazer parte de um projeto de formação em cibersegurança, ainda que como disciplina optativa.

Por outro lado, foi incorporada a disciplina Proteção de dados, por ser considerada imprescindível para a compreensão de muitos dos conceitos associados à cibersegurança, questão também mencionada por algum dos pesquisados.

b) Divisão de disciplinas

Por questões de metodologia de ensino e, especialmente, esperando alcançar um calendário equilibrado no conjunto das aulas ministradas, algumas das disciplinas propostas na pesquisa foram divididas em unidades de ensino menores. Concretamente, considerou-se oportuno dividir a disciplina Segurança em redes em Técnicas de ciberataque e Sistemas de ciberdefesa, e a disciplina Análise de cibersegurança se dividiria em Exploração de sistemas de *software*, Análise de *malware*, Ameaças persistentes avançadas e Segurança em dispositivos móveis. Além do já exposto, essa divisão visa estabelecer um tratamento mais direcionado dos conceitos, com o conseguinte aprofundamento no tema, o que redundará em maior nível de especialização dos alunos.

c) Caracterização de disciplinas e definição de disciplinas optativas

A fim de adequar a proposta de formação ao aluno, qualquer programa inclui uma quantidade de disciplinas com caráter optativo. Nesse sentido, a escolha foi incorporar como tais aquelas em relação às quais houve menor demanda (particularmente, Segurança em IoT e Segurança em sistemas ciberfísicos). Além disso e, tendo em vista o conjunto global desenhado, foram propostas outras disciplinas que podem ser de interesse, sempre observando o panorama atual da cibersegurança.

4. Refinamento da proposta inicial e oficina de apresentação de resultados

A proposta inicial foi levada ao BID, para que propusesse as recomendações que considerasse oportunas e que depois de discutidas serão incorporadas. Essa proposta assim enriquecida foi distribuída às universidades que participaram da pesquisa para receber seus comentários e reflexões que, incorporados à proposta, resultaram na versão final do programa. Para concluir, essa versão foi discutida em reuniões virtuais, para as quais foram convidadas diferentes universidades da região e, delas, resultou o programa definitivo.

Foram realizadas duas reuniões virtuais, entre outubro e dezembro de 2020, das quais participaram 54 universidades.

Programa

/18

1. Descrição do título

O programa de estudos deste mestrado pretende que os alunos adquiram conhecimentos científicos e tecnológicos avançados sobre cibersegurança, fundamentalmente em seus aspectos mais técnicos, sendo seu principal objetivo proporcionar habilidades, aptidões e conhecimentos teóricos e práticos na área, de maneira sólida, porém flexível, para facilitar sua adaptação a um ambiente que muda tão rapidamente como o atual.

Os dados básicos são os seguintes:

Título: mestre em cibersegurança
Idioma: a ser escolhido pela universidade
Duração: dois anos, divididos em quatro quadrimestres
Carga horária total: entre 1.480,5 e 1.699,5 horas

2. Justificativa do título

2.1 Justificativa do título proposto, argumentando seu interesse acadêmico, científico ou profissional

Em poucos anos, a segurança da informação e, mais concretamente, a cibersegurança, ganhou importância extraordinária em todos os setores sociais, públicos e privados, de todos os países e, inclusive, no âmbito pessoal dos habitantes de quase todos eles. Obviamente, isso aconteceu devido à dependência crítica das sociedades aos sistemas e redes de comunicação que, perante uma interrupção ou simples degradação do serviço que oferecem, colocariam setores essenciais desses países em situação calamitosa. Um exemplo disso pode ser extraído do Global Risks Report,[4] anualmente publicado pelo *World Economic Forum* (Fórum Econômico Mundial) que, ano após ano, situa os ciberataques como um dos riscos mais relevantes no que se refere à probabilidade de ocorrência e impacto. Assim, na décima quinta edição do Fórum, ocorrida em 2020, do total de trinta riscos estudados, os ciberataques aparecem como o sétimo risco de maior probabilidade de ocorrência e o oitavo quanto ao impacto que pode causar. Além disso, também figuram no relatório os riscos de roubo ou fraudes de dados e as interrupções das infraestruturas de informação, ambos muito vinculados aos ciberataques.

Por outro lado, o *Global Cibersecurity Index*,[5] bienalmente publicado pela União Internacional das Telecomunicações (UIT),[6] em sua edição de 2018 (última publicada até a publicação do presente documento), classificou os países que o compõem, quase 200, conforme seu nível de cibersegurança.[7] Essa classificação agrupa os países em três grandes blocos: países com alto, médio e baixo comprometimento com a cibersegurança.

O primeiro país da região da América Latina e o Caribe é o Uruguai, que figura na 55ª e última posição dentro do bloco de países com alto comprometimento. Para encontrar o país seguinte da região, deve-se retroceder à 14ª posição, já no bloco de comprometimento médio (que compreende 53 países), seguido de outros dez países da região. Por último, entre os países de baixo comprometimento, encontramos outros 13 países da região.

4 https://es.weforum.org/reports/the-global-risks-report-2020

5 https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

6 A UIT está constituída por mais de 190 países e 800 entidades privadas e públicas.

7 Para sua classificação, avalia cinco critérios, os quais denomina pilares, que são: legal (marco legal do tratamento de cibersegurança e ciberdelinquência), técnico (instituições técnicas e marco de tratamento de cibersegurança), organizacional (políticas de cooperação institucional, estratégias de cibersegurança nacionais), fomento de capacidades (investigação, formação, certificação profissional, agências públicas de fomento) e cooperação (marco de cooperação, redes de partilha de informação).

Porém, se quisermos destacar exclusivamente a região estudada, o relatório mais relevante por seu nível de detalhamento é o intitulado "Cibersegurança: riscos, progressos e o caminho a seguir na América Latina e o Caribe",[8] edição de 2020, do Banco Interamericano de Desenvolvimento (BID) e da Organização dos Estados Americanos (OEA). O relatório toma como base o "Modelo de maturidade da capacidade de cibersegurança para as nações (CMM)", desenvolvido pelo Centro Global de Capacitação de Segurança Cibernética (GCSCC, da sigla em inglês) da Universidade de Oxford.[9]

O CMM avalia a robustez da cibersegurança a partir de cinco pontos de vista (ou dimensões, na terminologia do modelo): política e estratégia de cibersegurança, cultura cibernética e social, educação, capacitação e habilidades em cibersegurança, marcos legais e regulatórios, além de padrões, organizações e tecnologias. Por sua vez, segmenta essas dimensões em fatores (por exemplo, a primeira dimensão é formada pelos fatores: estratégia nacional de cibersegurança, resposta a incidentes, proteção de infraestruturas críticas, etc.) e, finalmente, subdivide esses fatores em distintos componentes (aspectos, em seus próprios termos) que analisa para conferir pontuação de um a cinco a cada um deles, conforme seu nível de evolução (maturidade). Essas pontuações correspondem respectivamente a: inicial; formativa; consolidada; estratégica e dinâmica. Com essas ferramentas do modelo, o relatório obtém o nível de maturidade de cada um dos países da América Latina e o Caribe.

De acordo com os resultados, o relatório assinala:

> (...) embora a América Latina e o Caribe tenham melhorado suas capacidades de cibersegurança desde 2016, o nível médio de maturidade da região ainda está entre 1 e 2, segundo o Modelo de Maturidade da Capacidade de Cibersegurança para as Nações (no qual 1 significa etapa Inicial e 5 significa dinâmica ou avançada).

O estudo também constata uma grande disparidade de resultados entre os diferentes países da região. Assim, ao passo que a sub-região do Cone Sul apresenta o nível de maturidade mais elevado nas cinco dimensões (mantém-se entre 2 e 3), a sub-região do Caribe mostra o nível médio entre 1 e 2 nas citadas dimensões.

Em resumo, considendo-se o "*Global Cibersecurity Index*", da UIT, ou o relatório "Cibersegurança: riscos, progressos e caminhos a seguir na América Latina e o Caribe", edição de 2020, da OEA e do BID, o resultado é o mesmo e expõe a fragilidade global da região (certamente, com grandes diferenças entre países) no que se refere à cibersegurança.

De qualquer forma e, levando em consideração o fato de a segurança nunca ser absoluta, todos os países, em maior ou menor grau, apresentam fragilidades em seus sistemas de cibersegurança, como demonstram as estatísticas anuais do *Internet Crime Complaint Center*, do FBI, dos Estados Unidos que, em seu *Internet Crime Report* [10] (edição de 2019, última até a data do presente estudo), registra o total mundial de 467.361 denúncias, com perdas globais de 3,5 bilhões de dólares. E isso considerando o fato, geralmente aceito, de que os crimes cibernéticos são denunciados em menor medida que qualquer outro tipo de crime, seja pela escassa confiança em seu esclarecimento, seja pela perda de reputação que pressupõe o reconhecimento da incapacidade de as empresas evitarem esse tipo de ações criminosas.

8 Observatório para a Cibersegurança da ALC (com a participação do Banco Interamericano de Desenvolvimento [BID], Organização dos Estados Americanos [OEA] e do Centro Global de Capacidade em Segurança Cibernética da Universidade de Oxford), Cibersegurança: riscos, progressos e o caminho a seguir na América Latina e o Caribe, 2020. Veja https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe.

9 https://www.oxfordmartin.ox.ac.uk/cyber-security/.

10 https://pdf.ic3.gov/2019_IC3Report.pdf

Apesar da relutância em denunciar, em 2018, o presidente da União Europeia, em seu relatório anual sobre o Estado da União, assinalou que, em alguns países europeus, os cibercrimes somavam mais de 50% do total de crimes denunciados.[11]

Esse grande volume de cibercrimes ficou ainda mais evidente com a pandemia da COVID-19. O incremento do trabalho remoto, das reuniões on-line, do comércio eletrônico, da educação a distância, etc., vem propiciando grande aumento de ciberataques, alguns deles contra infraestruturas críticas tão importantes neste momento como, por exemplo, as sanitárias.

Sem sombra de dúvida, um facilitador dos cibercrimes é a carência mundial de especialistas em cibersegurança, pois a capacidade formadora das universidades, dos centros de capacitação profissional e das empresas nem sempre é suficiente para formar a quantidade de profissionais em cibersegurança demandada por empresas e organismos públicos. Assim, de acordo com o National Institute of Standard and Technology (NIST), entre setembro de 2017 e outubro de 2018, foram demandados 313.735 especialistas em cibersegurança.[12] Por sua vez, a consultoria Frost & Sullivan calculava em quase cinco milhões o número de profissionais em cibersegurança necessários em 2019, em todo o mundo, ao passo que estimava em quase 4,5 milhões os profissionais efetivamente existentes naquele momento, com defasagem, portanto, de meio milhão de profissionais.[13]

Nesse aspecto, a situação da América Latina e o Caribe (ALC) é ainda pior. Assim como ressaltou o CEO da Capabilia, depois de sua parceria com a Deloitte, "A América Latina é hoje, depois da Ásia, a região que mais tem vagas a serem preenchidas".[14]

Essa carência de formação na região se vê refletida no citado relatório de cibersegurança de 2020, da OEA e do BID que, no marco da dimensão "Educação, capacitação e habilidades em cibersegurança", do modelo CMM supramencionado, indica maturidade não superior à apresentada em outras dimensões.

De acordo com esse relatório, somente um terço dos países da região realizaram avanços nessa dimensão, obtendo níveis de maturidade médios (consolidados), embora, por exemplo, o Uruguai, alcance o nível estratégico. No entanto, segundo os professores Pablo Ruiz Tagle-Vial e Daniel Álvarez Valenzuela: "O presente relatório revela um escasso ou nulo avanço no nível de maturidade de dois terços dos países da América Latina e o Caribe, em matéria de educação, capacitação e desenvolvimento de habilidades de cibersegurança. Nesses países, a oferta de formação especializada em segurança digital é inexistente ou tem caráter incipiente e, usualmente, considera somente a dimensão técnica da cibersegurança".

Ao considerar-se os três fatores (sensibilização, marco para a educação e marco para a formação profissional) que conformam a terceira dimensão "Educação, capacitação e habilidades de segurança" do CMM, observamos que:

- no que se refere à sensibilização ou à conscientização, a ampla maioria se situa em níveis de formação ou estabelecidos (isto é, o segundo e terceiro níveis). Contudo, alguns países, como a Venezuela, ainda estão no nível inicial. No outro extremo se situa o Uruguai, que mostra um louvável indicador estratégico;

11 https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-factsheet-cybersecurity_es.pdf

12 New Data Show Demand for Cybersecurity Professionals Accelerating. NIST. https://www.nist.gov/news-events/news/2018/11/new-data-show-demand-cybersecurity-professionals-accelerating

13 The 2015 (ISC)2 Global Inform. Sec. Workforce Study. Frost & Sullivan

14 Martín Sola y el empleo en ciberseguridad: "América Latina es hoy, después de Asia, la zona que más vacantes tiene que llenar", janeiro de 2020. https://tecno.americaeconomia.com/articulos/martin-sola-y-el-empleo-en-ciberseguridad-america-latina-es-hoy-despues-de-asia-la-zona

- no que tange ao marco para a educação, nenhum dos países alcança níveis estratégicos ou dinâmicos. A ampla maioria se situa em níveis intermediários (de formação ou estabelecidos), embora haja cinco países ainda em fase inicial;

- finalmente, em relação ao marco para a formação profissional, o panorama é diferente do que vemos com os indicadores anteriores, embora igualmente suscetível de melhora. Nesse caso, a ampla maioria de países se situa no nível de formação, apesar de cinco deles estarem no nível estabelecido e, novamente, o Uruguai se posicionar no nível estratégico.

Tendo em vista os indicadores anteriores, a situação educativo-formativa em cibersegurança na ALC se beneficiará substancialmente de um título de mestrado que, adequadamente implantado nas Universidades participantes, permita a aquisição e consolidação de capacidades avançadas em todas as facetas da cibersegurança. O caráter acadêmico do título permitirá mitigar a carência de aproximação sistemática e rigorosa em relação a esse campo do conhecimento, oferecendo assim um plano estruturado que permita sólida capacitação. Além disso, é previsível que a implantação desse título sirva como catalizador para o surgimento de iniciativas acadêmicas em níveis inferiores (engenharias ou bacharelados) que facilitem a preparação para o acesso ao título proposto.

2.2 Modelo docente semipresencial: justificativa e características

Embora o secular modelo de ensino universitário presencial esteja solidamente assentado na sociedade e apresente vantagens inigualáveis, sobretudo no que se refere aos estudos tecnológicos, não é menos verdadeiro o fato de os cursos técnicos semipresenciais, que só exigem a presença do aluno durante as aulas práticas, estarem ganhando espaço rapidamente, principalmente nos estudos técnicos de pós-graduação, nos quais cada vez mais se inscrevem profissionais com título que desejam mudar ou aprofundar sua orientação no mundo do trabalho.

O modelo de aprendizagem semipresencial formulado para esse título conta com uma sólida base de informação, que combina de maneira natural com o conhecimento prático de habilidades, estratégias e ferramentas que habilitam para a resolução de novos problemas a antecipação de futuras ameaças de cibersegurança.

A semipresencialidade ou *b-learning* (do inglês, *blended learning*, também chamada de aprendizagem mista ou bimodal) permite reunir as vantagens do modelo tradicionalmente presencial com as derivadas do uso da tecnologia aplicada à aprendizagem (ou *e-learning*). De fato, habilita um nível de acompanhamento muito mais rico e individualizado, já que as plataformas on-line de ensino (como Moodle, Edx, Blackboard Collaborate, Hangouts Meet, etc.) oferecem inúmeros indicadores relacionados ao desempenho do aluno. Assim, é possível determinar se o plano previsto está sendo seguido, se há tentativa de realização de algum exercício e se está havendo melhora nas provas, entre muitos outros indicadores.

A modalidade semipresencial na qual se oferece este mestrado está plenamente justificada, levando em consideração uma série de fatores. Em primeiro lugar, vem das recomendações das instituições acadêmicas consultadas para a preparação desta proposta. Por outro lado, nos últimos tempos, tem-se evidenciado o aumento do número de alunos que optam pela modalidade não unicamente presencial, já que permite melhor conciliação com o contexto de trabalho e pessoal dos alunos.

Nesse sentido, a atual pandemia global da COVID-19 evidenciou a conveniência de optar por modalidades educacionais que não sejam dependentes de forma

exclusiva da presença física dos alunos e, nesse caso, possam se tornar totalmente a distância.

O último dos fatores a considerar é que a consecução das competências mencionadas neste documento é alcançável através do modelo de ensino semipresencial, no qual o uso de uma plataforma de ensino virtual e as aulas presenciais são meios complementares para desenvolver estratégias de ensino adequadas para a cibersegurança.

Deve-se destacar ainda que este âmbito de conhecimento exige, de forma regular, a aplicação prática dos conhecimentos teóricos adquiridos. Assim, é impossível dissociar as duas facetas da aprendizagem, já que o especialista em cibersegurança deve contar com a bagagem teórica e o conhecimento prático, de forma similar a outras disciplinas que demandam alto grau de experimentação.

Além disso, é importante considerar um marco de formação tanto para alunos quanto para professores. A semipresencialidade exige o uso de ferramentas e recursos de múltiplas naturezas, sendo necessário que os alunos estejam preparados para esse novo modelo, e os professores tenham os conhecimentos adequados para ministrar suas aulas dessa forma.

Em todo caso, deve ficar a critério de cada universidade a definição da modalidade de ensino, pois, por exemplo, pode ser que potenciais alunos de certas áreas de influência de uma universidade tenham infraestrutura de comunicação inadequada para o ensino semipresencial.

2.2.1 Recursos de ensino necessários

Com o fim de possibilitar essa modalidade de ensino, as instituições educacionais deverão contar com uma série de recursos e meios que garantam o ensino eficaz. Nesse sentido, além das próprias ferramentas on-line que permitam a difusão de materiais e a comunicação professor/aluno, serão necessários certos elementos de informação que permitam que o aluno siga adequadamente o plano de estudo. Entre esses elementos, estão:

- um site específico no qual sejam detalhados o funcionamento dessa modalidade de formação e os recursos e meios que estarão à disposição dos alunos;

- um cronograma semanal por disciplina, no qual se especifique não somente a tarefa a ser feita pelo aluno, mas também as horas de dedicação previstas e as atividades docentes (incluindo as avaliativas) que serão desenvolvidas.

Com relação aos meios técnicos que deverão ser habilitados para o modelo de ensino escolhido, deve-se destacar a necessidade de incorporar sistemas de videoconferência nas aulas. Isso permitirá que as aulas presenciais possam ser transmitidas ao vivo e que, além disso, sejam gravadas para ficar à disposição dos alunos ao longo do período letivo, facilitando, assim, o acompanhamento dessas aulas, especialmente para os alunos que tenham dificuldades singulares para assisti-las (nas disciplinas que não exijam presença em todas elas).

Além dos citados sistemas de videoconferência, será necessário contar com o equipamento mínimo para a gestão da transmissão e produção do vídeo, como uma cabine de controle e pessoal de supervisão dos meios de comunicação audiovisuais.

Para o máximo aproveitamento do modelo docente, é recomendável que a sala de aula conte com conectividade e equipamento informático que permita ao professor interagir com os alunos durante a aula, inclusive com aqueles alunos conectados remotamente. Para isso, recomenda-se contar com espaços de conversação interativos, como chat, fóruns de discussão ou redes sociais.

Finalmente, dado o nível altamente experimental desse mestrado, é necessário que os alunos disponham da infraestrutura adequada para concluir com sucesso a sua formação. Isso pode ser alcançado por duas vias:

- **alunos com equipamentos com recursos adequados.** Os equipamentos devem ter capacidade suficiente para executar múltiplas máquinas virtuais simultaneamente para, por exemplo, simular ataques;

- **organização com um sistema de gestão de usuários e máquinas virtuais.** O uso de serviços na nuvem é uma boa alternativa, em especial os conhecidos como sistemas de *cyber range* para o treinamento com ambientes já preparados. Alternativamente, pode-se optar pela aquisição de um número de servidores dimensionados ao número de alunos e pela compra de licenças de *software* de *hypervisor* (por exemplo, VMWare vSphere) para simular distintos ambientes de rede com múltiplos tipos de máquinas virtuais.

2.3 Perfil dos candidatos e resultados de aprendizagem

O aluno que queira cursar esse mestrado deve ter boa base de tecnologias da informação e das comunicações. Assim, o caráter principalmente prático do mestrado requer contar com um sólido conhecimento de programação, como o uso das linguagens C, Java ou Python; de sistemas operacionais, com conhecimento dos tipos de processadores, memórias e arquiteturas existentes; e de telecomunicações e redes, para conhecer o funcionamento das redes e dos principais protocolos de comunicação. Concretamente, a formação prévia é estabelecida no módulo 0 do curso, cuja função é proporcionar aos alunos que não tenham cursado disciplinas associadas às tecnologias das comunicações, uma boa base e o ponto de partida para aproveitar satisfatoriamente as aulas teóricas e práticas.

Por outro lado, a curiosidade e inquietação pela cibersegurança, bem como a criatividade, a capacidade de inovação, o pensamento crítico e o interesse pela aprendizagem contínua são qualidades muito valiosas para os potenciais alunos do mestrado.

No que diz respeito aos resultados de aprendizagem, esses devem ser avaliados de acordo com vários instrumentos. Por um lado, seria necessário contar com pesquisas de avaliação respondidas pelos alunos que, de forma introspectiva, permitiriam uma análise do nível de conhecimento adquirido após cursar certa disciplina. O instrumento também avaliaria a percepção dos alunos em relação à utilidade da disciplina em questão e do método de ensino. Do mesmo modo, deve-se coletar propostas dos alunos em relação à melhora da ementa de cada disciplina, em termos de ensino e de avaliação dos conhecimentos adquiridos.

Igualmente, deve-se coletar a opinião do corpo docente (professores e coordenadores) acerca do seu nível de satisfação com o desenvolvimento do curso, a porcentagem da ementa realmente desenvolvida, a adequação do ritmo de ensino para atingir essa porcentagem e outros indicadores do nível acadêmico percebido nos alunos, além de seu grau de comprometimento e seguimento das atividades acadêmicas propostas para a disciplina.

Em todo caso, os anteriores e qualquer outro instrumento de avaliação do processo de ensino-aprendizagem têm de estar alinhados com o estabelecido no programa de garantia interna da qualidade acadêmica da instituição que concederá o título.

3. Competências

As competências estabelecidas são o mínimo múltiplo comum das competências que figuram em uma amostra significativa de tipos de verificação, de mestrados similares ao que aqui nos ocupa, aprovados pela Agência Nacional de Avaliação da Qualidade de Credenciamento (ANECA, da sigla em espanhol) da Espanha, que é o organismo público responsável por aprovar os cursos com títulos oficiais no país.

As **competências básicas**, apresentadas na **tabela 3**, constituem uma série de habilidades, conhecimentos e atitudes adaptadas aos diferentes contextos. Assim, são aquelas que qualquer aluno deve adquirir para seu desenvolvimento profissional e sua adequada integração no ambiente de trabalho no qual se supõe que se desenvolverá profissionalmente.

As **competências gerais**, apresentadas na **tabela 4**, referem-se às habilidades, atributos, valores e qualidades que se espera que o aluno alcance. São gerais, posto que sua aquisição se produz a partir da aproximação à disciplina da cibersegurança de forma global, motivo pelo qual são "transversais" às tecnologias da informação, às telecomunicações e a outros campos do saber.

Tabela 3. Competências básicas

Código	Denominação
CB1	Dispor de conhecimentos que permitam desenvolver ou aplicar ideias de forma original, com frequência em contexto de investigação.
CB2	Aplicar os conhecimentos adquiridos e as capacidades desenvolvidas de resolução de problemas em contextos inovadores relativos à cibersegurança.
CB3	Emitir opiniões a partir de informação potencialmente incompleta, inexata ou limitada, que incluam reflexões sobre as responsabilidades sociais e éticas de sua atividade profissional.
CB4	Comunicar suas conclusões e argumentos subjacentes a públicos diversos, não necessariamente especialistas, com clareza e eficácia.
CB5	Incorporar as habilidades necessárias para um ciclo contínuo de aprendizagem, que pode ser, em grande medida, autogerido ou autônomo.
CB6	Dispor de capacidade de coordenação de equipes de trabalho, cuja interação se desenvolva, total ou parcialmente, através de meios de comunicação eletrônicos.

Tabela 4. Competências gerais

Código	Denominação
CG1	Compreender e aplicar métodos e técnicas de investigação de ciberataques a um sistema informático concreto.
CG2	Conceber, desenhar, implementar e manter um sistema global de ciberdefesa para um ambiente técnico definido.
CG3	Elaborar documentos, planos e projetos de trabalho, no âmbito da cibersegurança, que contem com rigor, clareza, concisão e simplicidade.
CG4	Conhecer a normativa técnica relativa à cibersegurança, suas implicações no design, na operação e na garantia de sistemas informáticos.
CG5	Desenvolver, implantar e manter um Sistema de Gestão da Segurança da Informação (SGSI).
CG6	Compreender o estado das ciberameaças no âmbito global em geral e no âmbito da América Latina e o Caribe (ALC), em particular, e expressar seu alcance empregando linguagem técnica clara e precisa.

Tabela 5. Competências específicas

Código	Denominação	Áreas de conhecimento de CCG
CE1	Analisar e detectar anomalias e assinaturas de ataques aos sistemas informáticos e redes de comunicações.	*Component Security, Organizational Security*
CE2	Analisar e detectar técnicas de ocultação de ataques a sistemas informáticos e redes de comunicações.	*Software Security*
CE3	Conhecer as tendências atuais em técnicas de ciberataque e as consequências reais que acarretam.	*Software Security, Societal Security*
CE4	Analisar sistemas para neles encontrar evidências de ataques, determinar seu impacto e adotar as medidas necessárias para manter a cadeia de custódia dessas evidências.	*Software Security*
CE5	Aplicar os serviços, mecanismos e protocolos de segurança oportunos para garantir a infraestrutura informática específica.	*Data Security*
CE6	Desenhar e avaliar arquiteturas de segurança de sistemas informáticos e redes de comunicação.	*Software Security, System Security*
CE7	Conhecer e aplicar os mecanismos criptográficos pertinentes para proteger os dados, tanto os armazenados em um dispositivo quanto aqueles em trânsito nas redes.	*Data Security*
CE8	Analisar e gerir os riscos da introdução de dispositivos pessoais em um ambiente corporativo e estabelecer as contramedidas adequadas para mitigá-los.	*Organizational Security*
CE9	Capacidade para aplicar as metodologias existentes em análises e gestão de riscos, transmitir os resultados obtidos e propor o tratamento de risco oportuno para um ambiente corporativo particular.	*Organizational Security*
CE10	Conhecer as ameaças próprias dos sistemas ciberfísicos, seus mecanismos específicos de proteção e ser capaz de antecipar-se às ameaças que possam surgir e responder a elas.	*Software Security, System Security*
CE11	Conhecer as ameaças derivadas do tratamento de megadados (big data) e aplicar medidas de proteção eficazes, preservando as necessidades próprias dos ambientes operacionais.	*Software Security, System Security*
CE12	Estabelecer o nível de segurança de um sistema baseado na computação na nuvem e aplicar medidas de proteção adequadas e eficazes.	*Software Security, System Security*
CE13	Conhecer os processos e técnicas de desenvolvimento de programas informáticos que incorporem as necessidades de cibersegurança desde o seu desenho até entrarem na fase de produção.	*Component Security*

As **competências específicas**, apresentadas na **tabela 5**, referem-se a habilidades concretas relativas a um determinado cargo de trabalho, sendo onde mais se evidenciam as especificidades da empresa ou organização. Além disso, para cada competência, foi identificada uma equivalência com as áreas de conhecimento estabelecidas no ACM *Cybersecurity Curricular Guidance (CCG)*.[15]

Perceba-se que, especialmente as competências básicas, poderiam ser adaptadas de acordo com as competências próprias da América Latina e, mais concretamente, dos países nos quais se desenvolva o mestrado.

4. Acesso e admissão de alunos

4.1 Requisitos de acesso e perfil de ingresso recomendado

Este mestrado está voltado a engenheiros e bacharéis de áreas do conhecimento relacionadas com as tecnologias da informação e das comunicações. No entanto, de acordo com as respostas da maioria dos pesquisados, deve ser aberto também para profissionais de outras áreas das ciências e engenharias que, contando com experiência no âmbito das TIC ou não, busquem um grau de especialização em cibersegurança. Nesse último caso, foram previstas disciplinas de nivelamento para proporcionar os conhecimentos tecnológicos básicos necessários.

Os candidatos que tiverem um título de alguma área do conhecimento diferente devem ser avaliados pelo Comitê de administração do mestrado, e as disciplinas cursadas por eles devem corresponder às evidências e resultados fidedignos de suas capacidades e, em última instância, o potencial de aproveitamento dos estudos do mestrado.

5. Plano de estudos

O presente programa de mestrado foi concebido para proporcionar aos alunos uma capacitação científico-tecnológica avançada na área de cibersegurança, abordando a disciplina a partir de uma perspectiva integral. Essa concepção se articula mediante a provisão de noções teóricas, que são acompanhadas das ferramentas técnicas adequadas para sua colocação em prática em um ambiente real. A formulação dos conteúdos incorpora as facetas de pesquisa e desenvolvimento, de maneira que os alunos possam não apenas se desenvolver profissionalmente nelas, mas também empregá-las como forma de atualização permanente.

As disciplinas foram propostas fundamentalmente com base nas opiniões recebidas dos pesquisados. Outros aspectos da formação, como o trabalho final ou o estágio em empresas, reuniram a aceitação unânime das universidades consultadas.

5.1 Descrição geral do plano de estudos e seu planejamento

O plano de estudos está organizado com atenção a uma dupla dimensão:

- **Estruturação temporal.** O mestrado adota a divisão por períodos acadêmicos quadrimestrais, que poderão ser implementados na faixa anual mais conveniente em função dos processos acadêmicos de admissão de alunos da instituição ofertante. Nesse sentido, o mestrado tem quatro quadrimestres que, habitualmente, são ministrados em dois cursos ou anos letivos.

15 Cybersecurity Curricular Guidance for Associate-Degree Programs. ACM. Janeiro de 2020. http://ccecc.acm.org/files/publications/Cyber2yr2020.pdf.

A duração mais comum de um quadrimestre é de 15 semanas, mais uma ou duas para a realização dos exames finais. Como a preferência dos pesquisados foi de 15 horas semanais (presenciais e a distância), o número total de horas é de 225 por quadrimestre. Considerando que, em média, cada hora-aula pressupõe para o aluno mais 1,5 hora de estudo (ou de realização de trabalhos), resulta em uma carga adicional semanal de 22,5 horas, totalizando 37,5 horas de dedicação ao mestrado, o que significa uma razoável carga de trabalho. Como será exposto mais adiante, essa carga semanal varia ligeiramente entre os quadrimestres.

- **Estruturação conceitual.** O mestrado se organiza em módulos, que agrupam uma ou mais disciplinas relacionadas com uma faceta da cibersegurança. Assim, o programa está dividido em quatro módulos principais e um de nivelamento.

  A seguir, cada um dos cinco módulos será apresentado, incluindo a dedicação necessária de tempo para cada um. Embora os dois primeiros módulos, isto é, os módulos 0 e 1, sejam compostos por disciplinas obrigatórias (o módulo 0 sendo apenas para alunos com carências de formação em TIC), o módulo 2 se estrutura em duas áreas de especialização diferentes, podendo o aluno escolher uma de ambas conforme seus interesses profissionais. Por sua vez, o módulo 3 está integralmente constituído por disciplinas optativas que podem ser escolhidas livremente pelos alunos, independentemente da área de especialização seguida no módulo anterior. Se a universidade considerar oportuno, alunos de uma especialização podem escolher como optativas as disciplinas da outra especialização.

  Finalmente, o módulo 4 se relaciona com a realização do trabalho final e com as práticas em empresas, que servirão como ponto de entrada no ambiente de trabalho.

  Uma consideração importante é que a **cibersegurança não** é uma disciplina **completamente teórica** e, portanto, **todas as disciplinas devem ter uma parte prática considerável** para complementar a teoria e, assim, permitir que os alunos dominem e utilizem as ferramentas habituais no mundo da cibersegurança. Além disso, é importante considerar que todas as práticas realizadas no mestrado e, especialmente, aquelas nas quais possa ser colocado em risco um sistema, deverão ser realizadas em ambientes virtuais.

Módulo 0. Nivelamento

Devido ao fato de inúmeros pesquisados terem indicado suas preferências por abrir o acesso ao mestrado a qualquer candidato com nível superior, independentemente da natureza de seu título (técnica, científica ou outra), considera-se como ponto indispensável dotar os alunos de um módulo de nivelamento (módulo 0) que lhes proporcione os conhecimentos mínimos das TIC, sem os quais lhes seria impossível aproveitar satisfatoriamente o restante do mestrado.

Com tal propósito, o módulo se estrutura nos três pontos abaixo descritos, considerados o mínimo indispensável para o objetivo proposto:

A) arquitetura de sistemas informáticos;
B) fundamentos de redes de comunicações;
C) técnicas de programação.

Dado que se considerou impossível que um aluno sem formação prévia nessas disciplinas seja capaz de formar-se nelas em menos de um quadrimestre, propõe-se investir em cada uma delas entre 60 e 70 horas de aula.

Módulo 1. Cibersegurança geral

Neste módulo, são proporcionados ao aluno conhecimentos nas disciplinas de cibersegurança consideradas básicas para sua formação, seja qual for a especialidade posteriormente escolhida. Sendo assim, as disciplinas serão obrigatórias.

- **A)** Sistemas de ciberdefesa
- **B)** Técnicas de ciberataque
- **C)** Comunicações seguras
- **D)** Criptografia aplicada
- **E)** Exploração de sistemas de *software*
- **F)** Administração e gestão da segurança

Para cada uma delas, considerou-se razoável dedicar entre 32 e 36 horas-aula.

Módulo 2. Especialização em cibersegurança

Este módulo tem duas possíveis áreas de especialização, de maneira que o aluno deverá escolher o que mais se aproximar de suas preferências.

Assim como no módulo anterior, entende-se que seja razoável dedicar entre 32 e 36 horas-aula para cada disciplina.

2.1 Engenharia de sistemas seguros

Os alunos que escolherem essa área de especialização se formarão em aspectos relacionados com a especificação, design e desenvolvimento, implantação e manutenção de sistemas seguros. As disciplinas a cursar serão:

- **A)** Desenvolvimento de sistemas seguros e segurança DevOps
- **B)** Análise e gestão de riscos em cibersegurança
- **C)** Segurança no tratamento de megadados (*big data*)
- **D)** Segurança na computação na nuvem

2.2 Análise de cibersegurança

Nesta área de especialização, os alunos serão treinados na análise de dados de cibersegurança, cursando para isso as seguintes disciplinas:

- **A)** Análise de *malware*
- **B)** Ameaças persistentes avançadas
- **C)** Informática forense
- **D)** Segurança em dispositivos móveis

Módulo 3. Formação complementar

Este módulo visa complementar a formação recebida pelos alunos em outras disciplinas que, específicas ou não, possam ser de interesse tanto para aqueles que tenham seguido a área de especialização de análise de cibersegurança como para os que tenham optado pela engenharia de sistemas seguros. Para isso, são propostas as seguintes disciplinas, entre as quais o aluno terá que escolher três:

- **A)** Segurança em IoT
- **B)** Segurança em sistemas ciberfísicos
- **C)** Marco legal da cibersegurança
- **D)** Cibercrimes, ciberterrorismo e ciberguerra
- **E)** Autenticação e controle de acesso
- **F)** Técnicas de exfiltração de dados
- **G)** Inteligência artificial para cibersegurança
- **H)** Ciberinteligência

Estima-se que para cada uma dessas disciplinas seja preciso dedicar 23-25 horas-aula.

Parece razoável permitir que, em vez de escolher uma ou várias das anteriores, o aluno escolha uma ou várias disciplinas da área de especialização que não escolheu, ainda que isso implique cursar mais horas totais do que as previstas para obter o título de mestre.

Além disso, ficam estabelecidas um total de **oito palestras de caráter obrigatório**, que serão ministradas no último quadrimestre, quando é possível ter mais aproveitamento pelo fato de já se haver adquirido o conhecimento das disciplinas do mestrado.

Pretende-se que essas palestras sejam ministradas por pessoas de fora, por exemplo, funcionários de empresas de cibersegurança, funcionários públicos especialistas em cibersegurança ou integrantes das forças e quadros de segurança nacionais, que exponham os alunos ao mundo profissional e ofereçam-lhes diferentes pontos de vistas sobre alguns dos desafios existentes em seu país. Assim, as palestras não devem estar associadas a disciplinas concretas, mas, sim, permitir que os palestrantes exponham suas experiências profissionais em distintos ambientes empresariais e públicos nos quais a cibersegurança desempenhe papel relevante.

A experiência demonstra que o tempo razoável para cada palestra seja de 1h30min, o que totaliza 12 horas.

Módulo 4. Trabalho final e estágio

Este módulo, de caráter obrigatório, corresponde à realização do trabalho final (TF) e de prática (estágio) em uma empresa do setor de cibersegurança ou de qualquer outro que tenha um departamento de cibersegurança. O TF pode ser feito dentro da empresa em que o aluno fez o estágio, bem como considerando as atividades que ali sejam realizadas. Além disso, o estágio será supervisado de maneira conjunta por docentes e profissionais da empresa.

Considerando os módulos estabelecidos, o mestrado terá duração de dois anos. O **planejamento** é exibido na **tabela 6**. Note-se que é importante que todos os alunos disponham dos conhecimentos indicados no módulo 0, mas cada universidade poderá disponibilizar esse módulo no período que considerar oportuno, por exemplo, aberto durante alguns meses por ano para a formação de futuros alunos do mestrado.

Tabela 6. Planejamento temporal do mestrado

Ano 1	
1º quadrimestre	2º quadrimestre
Módulo 0	Módulo 1
Ano 2	
1º quadrimestre	2º quadrimestre
Módulo 2 Módulo 3	Módulo 4 Palestras

5.2 Atividades de formação, disciplinas a serem ministradas, descrição do objetivo e conteúdo

5.2.1 Conteúdo das disciplinas a serem ministradas

Módulo 0. Nivelamento

Como indicado anteriormente, este módulo está composto por disciplinas **obrigatórias** para os **alunos** que **não** tiverem as **competências iniciais** necessárias.

A) Arquitetura de sistemas informáticos

Compreender como funcionam os computadores é essencial para, posteriormente, ser capaz de detectar possíveis problemas. Nesta disciplina, são introduzidos os princípios do design de computadores, para que os alunos conheçam os conceitos básicos sobre os tipos de arquiteturas existentes e o impacto que podem ter no rendimento.

Do mesmo modo, serão descritos os principais tipos de memória e processadores. O conteúdo desta disciplina é o seguinte:

1) Fundamentos do design de computadores
   - 1.1. Estrutura básica de um computador
   - 1.2. Rendimento
   - 1.3. Tipos de arquiteturas
2) Sistema de memória
   - 2.1. Memória cache
   - 2.2. Memória principal
   - 2.3. Memória virtual
3) Funcionamento dos processadores
   - 3.1. Processadores ILP
   - 3.2. Multiprocessadores
4) Linguagem *assembly*

B) Fundamentos de redes de comunicações

Compreender a estrutura e o funcionamento dos computadores é um pré-requisito para estudar as medidas de proteção. Nesta disciplina, são apresentados, inicialmente, os modelos básicos utilizados nas redes de computadores, para, posteriormente, aprofundar os distintos níveis que os compõem. Assim, será possível compreender o que ocorre em um computador do momento em que uma mensagem é criada até ser recebida pelo destinatário. O conteúdo desta disciplina é o seguinte:

1) Introdução às redes de computadores
   - 1.1. Modelo de camadas OSI (*Open System Interconnection*)
   - 1.2. Modelo de referência TCP/IP (internet)
2) Técnicas de transmissão
3) Nível físico
4) Nível de link
   - 4.1. Direcionamento
   - 4.2. Tecnologias e dispositivos
5) Nível de rede
   - 5.1. Protocolo IP
6) Nível de transporte
   - 6.1. Protocolo TCP
   - 6.2. Protocolo UCP
7) Nível de aplicação
   - 7.1. Protocolos associados à transferência e compartilhamento de arquivo
   - 7.2. Protocolos associados ao correio eletrônico
   - 7.3. Protocolos associados à navegação *web*

C) Técnicas de programação

Compreender o desenvolvimento de programas é necessário para identificar os ataques aos mesmos ou erros gerados. Nesta disciplina, serão estudadas diferentes técnicas de programação, como é desenvolvido um programa e quais são as ferramentas necessárias. Será feita uma introdução às bases da programação em linguagens de nível alto e baixo. O conteúdo da disciplina será o seguinte:

1) Tipos de técnicas de programação
   - 1.1. Programação estruturada
   - 1.2. Programação modular
   - 1.3. Programação orientada a objetos
   - 1.4. Programação concorrente
   - 1.5. Programação funcional
   - 1.6. Programação lógica
2) Desenvolvimento de programas
   - 2.1. Compilação
   - 2.2. Ferramentas de desenvolvimento

3) Linguagens de programação

3.1. C
3.2. Java
3.3. Python

Módulo 1. Cibersegurança geral

Este módulo trata dos fundamentos técnicos da cibersegurança que respaldam qualquer posterior especialização nessa área. Para isso, são incluídas as seguintes disciplinas **obrigatórias**:

A) Sistemas de ciberdefesa

Compreender os diferentes lugares nos quais é possível realizar ataques é um requisito necessário para mitigá-los, detectá-los ou preveni-los. Nesta disciplina, além de introduzir o conceito da ciberdefesa, serão apresentados diversos mecanismos utilizados na área, como os *firewalls*, os sistemas de detecção de intrusões (IDS) e os sistemas de gestão de eventos e segurança da informação. O conteúdo da disciplina é o seguinte:

1) Introdução aos sistemas de ciberdefesa

2) Sensores locais: auditoria e análise de eventos

2.1. Gestão de usuários e acessos
2.2. Análise de registros (*logs*) de segurança

3) *Firewalls* e segmentação de redes

3.1. Fundamentos de filtragem de tráfego
3.2. Tipos de *firewalls*
3.3. Segmentação de redes

4) Sistemas de detecção e prevenção de ataques

4.1. Detecção de assinaturas de ataque
4.2. Detecção de anomalias
4.3. Resposta automática a tentativas de intrusão

5) Sistemas de gestão de eventos e informação de segurança (SIEM)

5.1. Conceitos e arquiteturas de SIEM
5.2. Regras de agregação e correlação
5.3. Arquiteturas distribuídas de sensores de detecção
5.4. Estratégias de sensorização de redes

B) Técnicas de ciberataque

Compreender os procedimentos pelos quais podem ser perpetrados os ciberataques é uma parte essencial da cibersegurança. A disciplina visa fazer com que os alunos se familiarizem com os fundamentos e as possibilidades de realização dos ciberataques. Por isso, são ensinadas diferentes técnicas utilizadas para atacar os sistemas, começando pela fase de reconhecimento até conseguir controlar um sistema ou provocar fugas de dados e eliminar os rastros que podem ser deixados. O conteúdo da disciplina é o seguinte:

1) Introdução às técnicas de ciberataque

1.1. Conceitos e definições
1.2. Tipos de ciberataques
1.3. Fases típicas de uma intrusão

2) Aquisição de informação do objetivo e análise de vulnerabilidades

2.1. Técnicas de reconhecimento: fontes abertas
2.2. Enumeração de redes e escaneamento de serviços
2.3. Identificação e análise de vulnerabilidades

3) Exploração

3.1. Exploração de sistemas de autenticação e exploração de *software*
3.2. Consumo de recursos e DoS
3.3. Engenharia social, malware e técnicas de evasão

4) Persistência

4.1. Eliminação de evidências
4.2. Escalação de privilégios
4.3. Estabelecimento de canais de acesso alternativos
4.4. Ocultamento de presença

C) Comunicações seguras

Compreender os protocolos de comunicação e os aspectos de segurança de cada um deles é fundamental para proporcionar segurança às comunicações. Nesta disciplina, são expostos os protocolos seguros utilizados nas redes de comunicação e tudo o que significa sua segurança, dos contragolpes que podem ser usados para mitigar os ataques até as medidas de defesa que podem ser estabelecidas. Abaixo o conteúdo é apresentado de forma detalhada:

1) Princípios de segurança de redes de comunicações

1.1. Definições e conceitos: serviços de segurança vs. mecanismos de segurança
1.2. Ataques mais comuns às redes de comunicações
1.3. Contramedidas e custos da segurança

2) Segurança no nível físico e de links. Ataques e defesas

2.1. Redes ethernet: ataques e defesas
2.2. Os protocolos PPP e EAP. Autenticação, Autorização e Auditoria (AAA)
2.3. Segurança em redes sem fio

3) Segurança no nível de rede

3.1. Segurança em IPv4 e IPv6
3.2. Protocolos auxiliares (ICMP, DHCP), ataques e defesas
3.3. Protocolos de encaminhamento, ataques e defesas
3.4. IPsec

4) Segurança no nível de transporte

4.1. TLS/SSL
4.2. Redes privadas virtuais (VPN)

5) Segurança no nível de aplicação

5.1. Segurança em DNS
5.2. Segurança em aplicativos de automação de escritório: navegação *web* e correio eletrônico
5.3. Segurança em outros aplicativos: controle e execução remota, transferência e compartilhamento de arquivos

D) Criptografia aplicada

Compreender as principais medidas para proporcionar segurança aos dados mediante o uso da criptografia é um requisito imprescindível na proteção de sistemas e redes. Nesta disciplina, serão definidos os principais tipos e algoritmos criptográficos existentes, bem como algoritmos para assegurar a procedência dos dados, considerando a autenticação e a assinatura digital. Além disso, a proteção dos dados também requer saber se eles foram modificados e até que ponto e, por isso, deve-se introduzir o conceito e uso de funções de resumo. O conteúdo é o seguinte:

1) Introdução

1.1. Introdução à proteção da informação: definições e dimensões da segurança da informação

1.2. Classificação dos sistemas de criptografia (simétricos ou assimétricos)

2) Criptografia

2.1. Cifra de bloco e de fluxo
2.2. Algoritmos de cifra: simétricos e assimétricos
2.3. Gestão de chaves criptográficas
2.4. Criptografia com curvas elípticas
2.5. Outros mecanismos de criptografia
2.6. Implementações e livrarias criptográficas

3) Autenticação de mensagens e entidades

3.1. Funções *hash* criptográficas e códigos de autenticação de mensagens (MAC)
3.2. Assinatura digital e padrões
3.3. Certificados digitais e infraestruturas de chaves públicas (PKI)

E) Exploração de sistemas de *software*

Compreender as principais vulnerabilidades dos sistemas facilita sua exploração. Nesta disciplina, são apresentadas as principais vulnerabilidades e contramedidas estabelecidas em três níveis: de *software*, de rede e *web*. Assim, para cada um deles, serão expostas algumas das vulnerabilidades técnicas mais conhecidas, bem como os mecanismos para preveni-las. Finalmente, na última parte, será abordada a importância dos repositórios de vulnerabilidade e as linguagens de intercâmbio de vulnerabilidades e ataques. De maneira mais detalhada, abaixo os temas tratados serão:

1) Introdução

1.1. Vulnerabilidades em componentes de *software*
1.2. Mecanismos de exploração
1.3. Ferramentas e laboratório de análise e síntese

2) Exploração de vulnerabilidades no *software*

2.1. Violações de memória
2.2. Condições de carreira
2.3. Confusão de privilégios
2.4. Exploração da interface de usuário

3) Exploração de sistemas *web*

3.1. Vulnerabilidades no canal
3.2. Vulnerabilidades no servidor
3.3. Vulnerabilidades no navegador

4) Informação sobre vulnerabilidades e formas de exploração

4.1. Repositórios
4.2. Linguagens e padrões de representação e intercâmbio

F) Direção e gestão da segurança

Compreender os procedimentos e normas relacionados com a gestão da segurança da informação é um requisito necessário, dado que atualmente, a segurança baseada exclusivamente em considerações técnicas é inconcebível. A disciplina permite conhecer as normas e marcos de gestão referentes aos sistemas da informação, aprofundando nos aspectos de formação e conscientização, planos de continuidade, etc. Além disso, também contempla a auditoria da segurança, que permite aos alunos fazerem o controle e a análise sistemática dos sistemas. Igualmente, seria possível considerar neste tema a estratégia nacional de cibersegurança, caso exista, que usualmente, nos países que a têm, é o marco de gestão no âmbito estatal da cibersegurança. O conteúdo da disciplina é:

1) Introdução

1.1. Normalização, avaliação, certificação, credenciamento instituições e processos
1.2. Marco legal

2) Direção e planejamento

2.1. Planos de segurança
2.2. Formação e conscientização
2.3. Classificação da informação
2.4. Planos de continuidade do negócio
2.5. Centros de resposta a incidentes (CERT, CSIRT) e de operações de segurança (SOC)

3) Gestão da segurança

3.1. COBIT (*Control Objectives for Information and Related Technology*, da sigla em inglês)
3.2. *NIST Cybersecurity Framework & SP 800 Series*
3.3. Família de normas ISO/IEC 27000

4) Auditoria da segurança

4.1. Marcos e padrões
4.2. Auditoria de dados pessoais
4.3. Evidências e sua análise
4.4. O relatório de auditoria

5) Estratégia nacional de cibersegurança

Módulo 2. Especialização em cibersegurança

Este módulo (que, na verdade, engloba dois) visa especializar o aluno em uma das duas áreas principais da cibersegurança. Para isso, foram estabelecidas duas áreas de especialização: engenharia de sistemas seguros e análise em cibersegurança. O aluno deve escolher o caminho que considerar mais alinhado com seus interesses.

2.1 Engenharia de sistemas seguros

A) Desenvolvimento de sistemas seguros e segurança DevOps

Compreender como desenvolver um sistema adequadamente, considerando a segurança em todo o processo, pode ser complexo e entediante, mas é fundamental para buscar minimizar o número de possíveis ataques. Para isso, nesta disciplina, são tratados os principais modelos, arquiteturas e mecanismos para o design seguro de *software*. Além disso, um termo que tem atraído os especialistas é DevOps (*Development Operations*), associado com metodologias ágeis de desenvolvimento de código e de grande uso na atualidade. Contudo, a disciplina não traz tanta ênfase em DevOps como metodologia ou paradigma de desenvolvimento de *software*, mas nos aspectos de segurança vinculados. Os temas propostos são:

1) Conceitos de engenharia de sistemas seguros

1.1. Propriedades de segurança
1.2. Princípios de design para a segurança
1.3. Arquiteturas de *software*

2) Requisitos de *software* seguro

2.1. Decomposição de políticas
2.2. Tipos de requisitos

3) Design de *software* seguro

3.1. Processos de design
3.2. Considerações de design
3.3. Segurança da arquitetura
3.4. Tecnologias

4) Segurança na implementação

4.1. Segurança das linguagens de programação
4.2. Bases de dados de vulnerabilidades
4.3. Práticas e controles defensivos
4.4. Código fonte e versões
4.5. Ambientes de desenvolvimento

4.6. Revisão e análise de código
4.7. Técnicas antimanipulação de código

5) Testes

5.1. Estratégias, planos e casos de teste
5.2. Tipos de testes
5.3. Avaliação de impacto e ações corretivas
5.4. Gestão do ciclo de vida dos dados de teste

6) Segurança em DevOps (DEVSecOps)

6.1. Conceito
6.2. Integração de cibersegurança em cada fase do processo

B) Análise e gestão de riscos em cibersegurança

Compreender os riscos que rondam um sistema, identificá-los e analisá-los para, então, decidir se é preciso aceitá-los, mitigá-los ou rechaçá-los e concluir com o tratamento adequado dos riscos mitigados é um processo conhecido como gestão de riscos. Nesta disciplina, descreve-se o processo para realizar uma análise de riscos em uma organização, identificando todos os ativos, avaliando-os e determinando os riscos associados, concluindo com a escolha do tratamento adequado daqueles não mantidos nem rechaçados.

Para tanto, serão apresentadas distintas metodologias de análise e gestão de riscos e demonstrados aplicativos em vários ambientes, como a internet das coisas ou os dispositivos móveis. O conteúdo desta disciplina é o seguinte:

1) Introdução e conceitos gerais de análise de riscos

1.1 Conceitos: ativos, ameaças, vulnerabilidades, salvaguardas
1.2 Análise qualitativa e quantitativa
1.3 Análise estática e dinâmica

2) Metodologias de análise e gestão de riscos

2.1 ISACA (COSO), CRAMM, EBIOS, PCI-DSS, NIST SP-800, etc.
2.2 ISO-27005. MAGERIT

3) Análise de riscos em ambientes atuais e futuros de aplicativos

3.1 Computação na nuvem
3.2 *Big Data* – inteligência artificial
3.3 Internet das coisas (IoT)

C) Ambientes móveis (*wireless, smartphones*, etc.), segurança no tratamento de megadados (*big data*)

Compreender como realizar a gestão de grandes quantidades de dados (*big data*) está se tornando uma prática habitual em inúmeras empresas e instituições. No mundo da cibersegurança, os megadados oferecem uma dupla vertente. Por um lado, o emprego de grandes volumes de dados se tornou uma ferramenta valiosa para identificar e enfrentar os ataques em tempo real. Por outro, as empresas têm usado os megadados de forma crescente para seus processos de negócios. Por isso, nesta disciplina, após uma introdução à ligação entre megadados e cibersegurança, são apresentados mecanismos para gerir e visualizar de forma segura esses megadados. Dentro da gestão de dados, há ênfase na análise de logs e sistemas de gestão de eventos e informação de segurança que, embora apresentados em outra disciplina de caráter obrigatório, são essenciais nesse âmbito. Além disso, introduz-se a relevância da privacidade na área, além das técnicas que podem ser utilizadas para protegê-la e os aspectos legais envolvidos no âmbito do processamento em massa de dados. O programa desta disciplina é o seguinte:

1) Introdução à cibersegurança em *big data*

1.1. Conceitos básicos
1.2. Desafios

1.3. Fontes de dados
1.4. Aplicativos de cibersegurança e *big data*

2) Análise de dados de cibersegurança

2.1. Principais técnicas de análise de dados
2.2. Como analisar dados de forma segura
2.3. Técnicas de visualização
2.4. Quadros de comando

3) Armazenamento seguro de dados

3.1. Bases de dados focados em segurança
3.2. Gestão e administração segura de bases de dados

4) Preservação da privacidade

4.1. Os problemas da privacidade
4.2. Técnicas de proteção da privacidade
4.3. Aspectos legais em *big data*

D) Segurança na computação na nuvem

Compreender as capacidades da nuvem para facilitar a capacidade de cômputo e armazenamento é fundamental para o uso e a gestão de muitos sistemas. Nesse cenário, aparecem novos desafios de segurança que devem ser enfrentados. Esta disciplina abrange os fundamentos da computação na nuvem e suas repercussões no âmbito da cibersegurança, identificando-se os riscos e ameaças existentes, bem como as técnicas de proteção das infraestruturas de computação na nuvem e capacidades de gestão de incidentes nesse ambiente. O conteúdo da disciplina é o seguinte:

1) Fundamentos da computação na nuvem

1.1. Definição
1.2. Sistemas e modelos de computação na nuvem
1.3. Desafios de segurança

2) Riscos e ameaças específicos

2.1. Externalização e provedores de serviços geridos
2.2. Compartilhamento de infraestruturas
2.3. Rastreamento da informação

3) Técnicas de segurança

3.1. Contêineres (*dockers*)
3.2. Virtualização
3.3. Balanceadores de carga

2.2 Análise de cibersegurança

A) Análise de *malware*

Compreender a quantidade de programas malignos (*malware*) e sua tendência em quantidade e variedade é necessário para saber enfrentá-los. Nesta disciplina, são contemplados os diferentes tipos de *malware* existentes, expondo seus comportamentos e as técnicas disponíveis para analisá-los, tanto básicas quanto avançadas que, embora requeiram conhecimentos técnicos superiores, são indispensáveis para identificar alguns tipos de características. O conteúdo desta disciplina é:

1) Introdução

1.1 Conceitos básicos e evolução
1.2 Técnicas de análise de *malware*

2) Técnicas básicas de análise

2.1 Análise estática básica
2.2 Análise dinâmica básica

3) Técnicas avançadas de análise

3.1 Desmontagem x86
3.2 Depuradores e IDA Pro
3.3 A API do Windows

4) Comportamentos e técnicas de evasão

4.1 Carregadores
4.2 Portas traseiras
4.3 Espiões
4.4 Persistência
4.5 Execução encoberta
4.6 Codificação
4.7 Antidesmontagem
4.8 Antidepuração
4.9 Antivirtualização
4.10 *Packers*

B) Ameaças persistentes avançadas

Compreender o que são e como funcionam as inúmeras ameaças que se caracterizam por estarem desenhadas para se perpetuarem nos equipamentos que infectam e são denominadas ameaças persistentes avançadas (*Advanced Persistent Threat, APT*) é necessário para ter uma visão holística das ameaças atuais. As APTs apareceram pela primeira vez em 2010 e, desde então, muitas delas têm sido identificadas, a maioria afetando equipamentos de alto nível crítico, como os que respaldam as infraestruturas críticas. São caracterizadas por utilizar um conjunto muito amplo de técnicas para realizar ataques e por sua sigilosidade e persistência, que dificultam muito sua identificação. Nesta disciplina, serão partilhados conhecimentos sobre as características das APTs, os principais mecanismos que utilizam e suas famílias mais conhecidas. O conteúdo é o seguinte:

1) Introdução

1.1. Caracterização das APTs
1.2. Comparação com outros programas malignos

2) Estratégias de comando e controle

2.1. Arquiteturas
2.2. Sigilo
2.3. Anonimato
2.4. Resiliência

3) Técnicas de evasão e persistência

3.1. Ocultamento de atividade e *rootkits*
3.2. Persistência sem uso de disco (*data-only*)
3.3. Ataques de mimetização

4) Panorama atual

4.1. Casos de estudo
4.2. Principais atores e capacidades
4.3. Tendências

C) Informática forense

Compreender quando ocorreu algum tipo de ataque ou incidente de segurança pode ser necessário para identificar sua procedência, além de ser o momento de aplicar a denominada informática forense. Nesta disciplina, o aluno aprenderá as bases da análise forense, tanto em sistemas quanto em dispositivos móveis, conhecendo os diferentes tipos de ferramentas de análise forense e os procedimentos e as políticas que devem ser aplicados. O conteúdo desta disciplina é o seguinte:

1) Introdução à análise forense

1.1. Conceitos básicos
1.2. Casos de exemplo
1.3. Conceitos técnicos fundamentais

2) Laboratório de análise forense

2.1. Políticas e procedimentos
2.2. Garantia da qualidade
2.3. Ferramentas
2.4. Evidências: obtenção, análise e custódia
2.5. Relatório forense

3) Ferramentas de análise forense

3.1. Análise forense de sistemas de arquivos
3.2. Análise forense de memória
3.3. Análise forense em redes de computadores
3.4. Internet e correio eletrônico
3.5. Análise forense em dispositivos móveis
3.6. Ferramentas e técnicas antiforenses

D) Segurança em dispositivos móveis

Compreender como proteger os dispositivos móveis é imprescindível, dado o uso cada vez maior desses aparelhos. Nessa disciplina, são apresentadas as bases das comunicações celulares, com vistas à sua segurança, por exemplo, introduzindo os problemas da segurança em WiFi. Sequencialmente, são descritos diferentes aspectos sobre a segurança nos sistemas operacionais Android e iOS, por serem os dois mais utilizados em dispositivos móveis. Finalmente, são apresentadas as novidades no que se refere às ameaças sofridas por esse tipo de dispositivo. O conteúdo desta disciplina engloba o seguinte:

1) Comunicações móveis

1.1. Introdução às comunicações móveis
1.2. Segurança em comunicações sem fio

2) Segurança em Android

2.1. Arquitetura Android
2.2. Modelo de segurança
2.3. Tipos de aplicativos Android
2.4. OWASP *Mobile Security Testing*
2.5. Engenharia reversa

3) Segurança em iOS

3.1. Arquitetura iOS
3.2. Modelo de segurança
3.3. Auditoria de aplicativos iOS

4) Aplicativos móveis maliciosos

4.1. Técnicas de análise: estáticas e dinâmicas
4.2. Engenharia reversa
4.3. Tendências

Módulo 3. Formação complementar

Para que os alunos continuem sua formação em cibersegurança e, ao mesmo tempo, possam ampliar seu conhecimento em outras disciplinas especializadas, porém mais horizontais, terão de escolher três disciplinas optativas, entre as seguintes:

A) Segurança na Internet das coisas (IoT)

Compreender os dispositivos que nos rodeiam e a capacidade de conexão de que dispõem para se conectarem entre si e à internet para compartilhar informações revela inúmeros problemas de segurança. Esses dispositivos e os meios por meio dos quais se interconectam recebem o nome de Internet das coisas (IoT) e estão expostos a diferentes ataques e vulnerabilidades. Nesta disciplina, são apresentados os dispositivos IoT, a segurança nas diversas arquiteturas e os protocolos, além dos aspectos de segurança associados a dispositivos concretos, como os dispositivos médicos, as câmeras de vigilância ou os dispositivos domésticos inteligentes. O conteúdo desta disciplina é o seguinte:

1) Introdução à Internet das coisas (IoT)

1.1 Definição de IoT
1.2 Dispositivos IoT e evolução

2) Arquiteturas e protocolos utilizados em IoT

2.1 Descrição
2.2 Problemas de segurança
2.3 Medidas de proteção

3) Segurança em dispositivos IoT

3.1 Tendências
3.2 Dispositivos médicos
3.3 Câmeras de vigilância
3.4 Dispositivos domésticos inteligentes
3.5 Outros

B) Segurança em sistemas ciberfísicos

Compreender os riscos e ameaças dos sistemas ciberfísicos, aqueles cujo design e funcionamento se baseiam na interação de sistemas mecânicos e tecnologias de comunicação, possibilita seu adequado monitoramento e controle, seja de forma física ou remota. São exemplos desse tipo de sistemas as plataformas embarcadas em robôs, sensores e atuadores e, inclusive, combinações desses elementos podem ser os veículos ou os sistemas industriais. Nesta disciplina, faz-se uma introdução a esses sistemas ciberfísicos para, posteriormente, introduzir as arquiteturas de referência desses sistemas e, finalmente, definir as ameaças concretas às quais eles estão expostos. O conteúdo desta disciplina é o seguinte:

1) Introdução aos sistemas ciberfísicos

1.1 Definição
1.2 Principais sistemas ciberfísicos e aplicativos

2) Arquiteturas de referência nos sistemas ciberfísicos

2.1 Sistemas industriais
2.2 Sistemas embarcados

3) Ameaças específicas

3.1 Riscos e ataques
3.2 Contramedidas
3.3 Tendências

C) Marco legal da cibersegurança

Compreender os aspectos legais da cibersegurança contribui para que se possa ter uma visão global, não exclusivamente técnica, desta disciplina. Além disso, esses aspectos técnicos estão intimamente vinculados às previsões legais dos países. Assim, o conhecimento dos aspectos legais da proteção de dados pessoais é de grande utilidade no desenvolvimento de programas, no conhecimento da validade legal da assinatura digital (ou eletrônica e suas distintas modalidades) e necessário na hora de planejar defesas contra ciberataques ou infrações penais como, por exemplo, delitos informáticos, para alguns sistemas de resposta a incidentes. Também caberia aqui tratar da regulamentação legal (nos países que a contemplam) da segurança dos sistemas e redes.

O conteúdo desta disciplina é o seguinte:

1) Normativa legal sobre proteção de dados pessoais
2) O crime informático e a Convenção de Budapeste sobre cibercrime
3) Aspectos legais da assinatura digital
4) A regulamentação legal da segurança em redes e sistemas de informação
5) Lei de proteção de infraestruturas críticas

D) Cibercrimes, ciberterrorismo e ciberguerra

Compreender os diferentes tipos de ameaças existentes em suas múltiplas formas e com base nos objetivos ajuda a compreender suas origens. Esta disciplina é uma introdução às ciberameaças, em que se identificam os tipos de ciberataques como os citados, para, a seguir, falar de suas características e o *modus operandi* de cada um, exemplificando com casos reais. Seus temas são:

1) Introdução, definições e conceitos básicos

   1.1. Origens
   1.2. Ciberataques
   1.3. Economia submersa
   1.4. Tendências
   1.5. Impacto econômico, financeiro e social dos ciberataques
   1.6. Identificação e perfilamento de cibercriminosos

2) Ciberataques e ciberativismo

   2.1. Tipos de ciberataques
   2.2. Cibercrimes
   2.3. Ciberespionagem
   2.4. Análise de casos práticos
   2.5. Aspectos legais

3) Ciberterrorismo e ciberoperações contra infraestruturas críticas

   3.1. Infraestruturas críticas: interconexão e vulnerabilidades
   3.2. Sistemas de controle industrial
   3.3. Outras infraestruturas críticas
   3.4. Análise de casos práticos

4) Ciberguerra

   4.1. Ciberarmamento: instrumentos lógicos, físicos e psicológicos
   4.2. Ciberdoutrina (Manual de Tallinn)
   4.3. Estratégias de desinformação
   4.4. Análise de casos práticos

E) Autenticação e controle de acesso

Compreender como os usuários e os sistemas controlam os acessos é o que se conhece como controle de acesso e tem vital importância em todos os sistemas. Igualmente, para gerir o acesso, os usuários ou as entidades têm de, em primeiro lugar, autenticar-se. Nesta disciplina, são apresentados os modelos e mecanismos de autenticação e controle de acesso, tanto no nível da rede quanto do usuário, assim como suas tecnologias e aplicações. O conteúdo desta disciplina é o seguinte:

1) Autenticação

   1.1. Fundamentos das técnicas de autenticação
   1.2. Senhas
   1.3. Desafio-resposta
   1.4. Biometria
   1.5. Autenticação multifatorial
   1.6. Usabilidade
   1.7. Sistemas de identidade federada
   1.8. Confiança digital

2) Controle de acesso discricionário

   2.1. A matriz de controle de acesso
   2.2. Transições e estados seguros
   2.3. Políticas de segurança

3) Controle de acesso obrigatório

   3.1. Fundamentos
   3.2. Confidencialidade: Bell-LaPadula
   3.3. Integridade: Biba
   3.4. Modelos híbridos: a muralha da China e Clark-Wilson
   3.5. Controle de acesso baseado em funções (RBAC)

4) Mecanismos de controle de acesso

   4.1. Listas de controle de acesso
   4.2. Capacidades
   4.3. Implementação em sistemas operacionais

F) Técnicas de exfiltração de dados

Compreender as técnicas utilizadas para exfiltrar dados sensíveis, como os dados pessoais, ajuda a conhecer um dos objetivos, cada vez mais

habitual, dos atacantes. Assim, os vazamentos de informação (*data leaks*), sejam por erro, omissão ou intencionalidade, constituem um dos eventos de segurança mais críticos nos ambientes corporativos modernos. Por isso, são abordados nesta disciplina tanto as técnicas para perpetrar o roubo de dados quanto os mecanismos para sua detecção. O conteúdo desta disciplina é o seguinte:

1) Introdução

1.1. Armazenamento e replicação
1.2. Tendências
1.3. Aspectos legais

2) Sistemas de proteção

2.1. Técnicas de marcação
2.2. Ferramentas de monitoramento
2.3. Sistemas de prevenção e soluções DLP (*data leakage prevention*)

3) Técnicas de exfiltração

3.1. Esteganografia clássica
3.2. Esteganografia moderna
3.3. Uso de meios não convencionais
3.4. Canais laterais
3.5. Detecção, esteganálise e caracterização matemática

G) Inteligência artificial para cibersegurança

Compreender as técnicas e os algoritmos de Inteligência Artificial (IA) mais usados em cibersegurança, bem como sua aplicação nesse contexto é fundamental. A IA está sendo utilizada em inúmeras áreas e também pode ser aplicada em cibersegurança. Nesta disciplina, são apresentadas as áreas da cibersegurança nas quais a IA tem aplicação, bem como os algoritmos e as ferramentas mais apropriadas em cada caso. O foco está na detecção de ciberataques e na autenticação de usuários, por seu crescente interesse. O conteúdo desta disciplina é o seguinte:

1) Introdução

1.1. Definição de inteligência artificial
1.2. Algoritmos de inteligência artificial
1.3. Usos da inteligência artificial em cibersegurança
1.4. Engenharia de características (*feature engineering*)
1.5. Explicabilidade (*explainability*)

2) Uso da inteligência artificial para a detecção de ataques

2.1. Padrões
2.2. Algoritmos
2.3. Ferramentas

3) Uso da inteligência artificial para autenticação

3.1. Padrões
3.2. Algoritmos
3.3. Ferramentas

H) Ciberinteligência

Compreender as técnicas e ferramentas mais utilizadas em ciberinteligência. Existe uma grande quantidade de recursos dos quais é possível obter informação, mas é necessário aprender a adquiri-la e analisá-la. Para isso, nesta disciplina, após uma introdução à ciberinteligência, são definidos e identificados os tipos mais comuns, que são: inteligência de fontes humanas, de fontes abertas, de fontes privadas e de sinais. Adicionalmente, são apresentadas as ferramentas mais utilizadas em cada caso e possíveis usos. O conteúdo desta disciplina é o seguinte:

1) Introdução

1.1. História da ciberinteligência
1.2. Usos da ciberinteligência
1.3. Usos da inteligência artificial em cibersegurança

2) Inteligência de fontes humanas (HUMINT)

2.1. Definição
2.2. Ferramentas
2.3. Casos de uso

3) Inteligência de fontes abertas (OSINT)

3.1. Definição
3.2. Ferramentas
3.3. Casos de uso

4) Inteligência de fontes privadas (PRIVINT)

4.1. Definição
4.2. Ferramentas
4.3. Casos de uso

5) Inteligência de sinais (SIGINT)

5.1. Definição
5.2. Ferramentas
5.3. Casos de uso

i) Palestras

Neste módulo, estão formuladas oito palestras a serem ministradas no último quadrimestre do segundo ano, cada uma com duração entre uma hora e uma hora e meia. Os palestrantes devem ser especialistas em diferentes áreas da cibersegurança e apresentar aos alunos o seu conhecimento concreto sobre um tema, partindo de sua experiência profissional. Com isso, pretende-se estabelecer vínculos entre a academia e a indústria, para que os alunos conheçam problemáticas e situações reais com as quais se depararão em seu trabalho. Abaixo, propõe-se uma lista meramente sugestiva de possíveis temáticas:

- Como criar um APT a partir do zero
- Controle e mitigação de riscos nas infraestruturas críticas
- Auditoria de segurança de um sistema
- A perseguição do delito informático
- Experiências de um CISO
- O funcionamento de um CERT ou CSIRT
- Gestão e organização da cibersegurança no Estado (organismos competentes, missões, estrutura, etc.)
- A mente de um *hacker*
- O direito na cibersegurança
- Sistemas de formação em cibersegurança
- Segurança física em ambientes informáticos
- Análise de *malware* avançado
- Sistemas de proteção de dados em uma organização
- Criptomoedas: uma faca de dois gumes
- O perigo dos *data brokers*
- A avaliação de um produto para sua certificação com a norma ISO/IEC 15 408
- Questões éticas relacionadas à cibersegurança

Módulo 4. Trabalho final e estágio

O TF é um projeto acadêmico cuja carga horária é de 240 horas de dedicação. O objetivo é demonstrar a aquisição de uma ou, preferencialmente, várias das competências adquiridas ao longo do mestrado. Para isso, pode-se elaborar um projeto acadêmico associado à cibersegurança e alinhado com algumas das disciplinas ministradas. Também será necessário fazer um estágio de três meses em empresas ou departamentos de cibersegurança. O aluno deverá redigir um documento que descreva o projeto realizado.

O TF deverá ser defendido oralmente perante uma banca avaliadora, cuja composição e organização será definida pela instituição que oferece o mestrado. Os integrantes deverão, em todos os casos, ser

especialistas acadêmicos na área de cibersegurança, devendo haver também algum integrante de instituição acadêmica de fora. Também pode fazer parte da banca algum representante do setor industrial de reconhecido prestígio, assegurando-se sempre que a maioria dos integrantes esteja vinculada a uma instituição acadêmica. Com o fim de qualificar homogeneamente os trabalhos, propõe-se o uso de uma matriz de avaliação, na qual sejam designados valores a diferentes critérios, tanto de conteúdo quanto de apresentação. A **tabela 7** mostra um exemplo de possível matriz de avaliação, em que os critérios concretos sobre os valores da matriz devem ser estabelecidos pela instituição. Finalmente, para auxiliar na difusão do mestrado e valorizar os trabalhos, recomenda-se a publicação dos TFs de forma aberta, preferencialmente por meio do repositório institucional de cada Universidade.

Além do TF, o módulo é concluído com um período de prática de três meses em empresas (estágio). Esse período deverá ser independente daquele utilizado para a elaboração do TF e constituirá o ponto de entrada do aluno no âmbito de trabalho da cibersegurança. Ao longo do período, o aluno contará com um docente encarregado de sua supervisão e com um profissional na instituição receptora que atuará como seu mentor. O estágio estará respaldado por um plano acordado entre as instituições participantes, no qual serão descritas as tarefas a serem realizadas e os indicadores de rendimento a serem utilizados. O crédito pela realização acontecerá após a apresentação de um relatório positivo de conclusão do período, devendo ser necessariamente referendado por ambas as instituições. Caso o aluno esteja trabalhando e já tenha iniciado sua carreira profissional, propõem-se as seguintes alternativas:

- que o estágio seja substituído pela realização de um TF de maior complexidade e extensão, o que deverá ser avaliado pelo diretor da instituição;
- se o aluno já realiza atividades relacionadas à cibersegurança na empresa na qual trabalha, estas poderão ser validadas pelo estágio. Ficará sob responsabilidade do docente encarregado da supervisão do trabalho a avaliação e aprovação dessa situação.

5.2.2 Disciplinas e competências

Na **tabela 8**, apresenta-se um resumo das disciplinas e atividades a serem realizadas em cada um dos módulos, além das competências atribuídas em

Tabela 7. Matriz de avaliação de TF

		Muito bom (4)	Bom (3)	Regular (2)	Ruim (1)
Exposição do tema	Organização e estrutura				
	Formulação do problema				
	Estado da questão				
Contribuição	Dificuldade e contribuição técnica				
Apresentação	Exposição oral				
NOTA FINAL					

Tabela 8. Competências por disciplinas e atividades

	Básicas						Gerais						Específicas												
	1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6	7	8	9	10	11	12	13
M0																									
a	x		x	x	x	x																			
b	x		x	x	x	x																			
c	x		x	x	x	x																			
M1																									
a	x	x	x	x	x	x	x	x	x	x				x			x	x	x						
b		x	x	x	x	x		x	x	x		x		x			x								
c	x	x	x	x	x	x	x	x	x	x			x	x			x								
d	x	x	x	x	x	x	x		x	x			x		x										
e	x	x	x	x	x	x	x		x	x		x	x		x					x					
f		x	x	x	x	x			x	x	x	x					x								
M2																									
2.1																									
a		x	x	x	x	x		x	x	x							x	x							x
b		x	x	x	x	x		x	x	x	x						x			x	x				
c	x	x	x	x	x	x	x	x	x	x							x						x		
d	x	x	x	x	x	x	x	x	x	x		x					x	x						x	
2.2																									
a	x	x	x	x	x	x	x		x	x			x		x				x						
b	x	x	x	x	x	x	x		x	x			x	x	x										
c	x	x	x	x	x	x	x	x	x	x						x									
d	x	x	x	x	x	x	x	x	x	x				x				x							
M3																									
a	x	x	x	x	x	x	x	x	x	x							x			x					
b	x	x	x	x	x	x	x	x	x	x							x	x				x			
c			x	x	x					x							x	x			x				
d	x	x	x	x	x	x	x		x	x					x										
e	x	x	x	x	x	x	x	x	x	x							x								
f	x	x	x	x	x	x		x	x			x		x	x				x	x					
g	x	x	x	x	x		x	x					x										x		
h	x	x	x	x	x							x			x										
Sm	x	x	x		x	x	x	x	x	x	x	x			x	x	x	x	x						
M4	x	x	x	x	x	x	x	x	x	x	x					x	x	x	x	x					

Tabela 9. Atribuição horária

Tipo de disciplina	Horas-aula (mín./máx.)	Horas de trabalho do aluno/ on-line (mín./máx.)
Obrigatórias	32-36	48-54
Optativas	23-25	34,5-37,5
TF	---	250-300
Estágio	---	250-300
Palestras	8-12	---

cada caso. Note-se que, no módulo de nivelamento (módulo 0), são adquiridas apenas as competências básicas, já que sua função é servir como ponto de partida para os alunos de disciplinas alheias às tecnologias da informação e das comunicações.

5.2.3 Resumo do conteúdo do curso e atribuição horária

Na **tabela 9**, definem-se os tipos de disciplina, obrigatórias ou optativas, considerando que o aluno deve escolher um bloco de disciplinas do módulo 2 (M2), e o número de horas presenciais e de trabalho atribuídas ao aluno. No módulo 4 (M4), deve-se considerar que o estágio foi estabelecido como trabalho de meio período (4 horas) durante três meses.

Considerando o fato de o mestrado ser de caráter semipresencial, o número de horas de trabalho do aluno é significativamente superior ao de aulas presenciais. Na **tabela 9**, mostra-se um intervalo de horas-aula e horas de trabalho do aluno. Posteriormente, cada instituição deverá ajustar a distribuição de acordo com seus critérios organizativos. Assim, cumprindo as seis disciplinas obrigatórias correspondentes ao módulo 1, as 4 obrigatórias da especialização escolhida no módulo 2, as 3 optativas do módulo 3, o TF, o estágio e as conferências, o número total de horas do mestrado seria de 1480,5 no menor caso e, de 1699,5, no máximo.

5.5 Metodologias de ensino

Dado o caráter semipresencial do mestrado, uma parte requererá a presença do aluno, e a outra poderá ser cursada a distância. A seguir estão expostas as atividades que compõem a metodologia, algumas de caráter presencial (P) e outras que podem ser realizadas tanto presencialmente como a distância (O).

Dentro da metodologia de ensino, considera-se:

- (P) aulas expositivas com apoio de meios informáticos e audiovisuais, nas quais são desenvolvidos os conceitos principais da disciplina e proporcionada a bibliografia para complementar a aprendizagem dos alunos;
- (P/O) discussão presencial ou a distância de textos recomendados pelo professor: artigos de imprensa, relatórios, manuais e/ou artigos acadêmicos, seja para discussão, seja para

ampliar e consolidar os conhecimentos da disciplina;
- (P/O) resolução de casos práticos, problemas, etc. formulados pelo professor de maneira individual ou em grupo;
- (P) exposição e discussão, com moderação do professor, de temas relacionados com o conteúdo da disciplina, bem como de casos práticos;
- (P/O) elaboração de trabalhos teórico-práticos e relatórios de maneira individual ou em grupo.

Cada professor pode escolher as atividades metodológicas que mais se adequem à sua disciplina. Recomenda-se, no entanto, que, no final de cada curso se faça uma reunião na qual professores e alunos reflitam sobre as forças e fragilidades das metodologias utilizadas, com o fim de aperfeiçoar futuras edições.

5.6 Sistemas de avaliação

No âmbito do sistema de avaliação, são contempladas as seguintes necessidades:

- participação em aula, inclusive naquelas ministradas a distância e nos fóruns on-line habilitados;
- trabalhos individuais ou em grupo realizados durante o curso;
- questionários, conjunto de problemas ou desafios práticos realizados durante o curso;
- exame final.

Cada professor terá de escolher uma ou mais formas de avaliação adequadas à sua disciplina. No entanto, devido ao fato de o mestrado ser de caráter semipresencial e o estágio ser um aspecto relevante, é recomendável que, caso se opte por ter um exame final, a nota atribuída a este seja uma porcentagem complementar ao restante das notas. Por exemplo, uma possível distribuição da avaliação pode ser feita com base no seguinte critério:

- atividades presenciais e práticas: 30%;
- exames parciais, trabalhos e outro tipo de atividades: 30%;
- exame final: 40%.

5.7 Plano de lançamento do mestrado

A difusão dos objetivos, conteúdos, corpo docente, etc. do mestrado deve ser estabelecida com suficiente antecipação ao início do curso acadêmico correspondente.

O meio mais eficiente costuma ser na forma de palestras (mais longas que as palestras do curso), ministradas pelo diretor ou subdiretor do mestrado aos alunos do último curso de cada um dos títulos próximos à temática da cibersegurança. Em tais palestras, seriam expostos a importância da cibersegurança no presente e no futuro, os ataques e os atacantes, o investimento empresarial e a demanda de profissionais dessa área, concluindo com os objetivos e a apresentação do programa do mestrado, além dos recursos informáticos (servidores e redes) à disposição dos alunos. Tudo isso com a ajuda de tabelas e gráficos (e, talvez, de vídeos, por exemplo, do YouTube).

Se a universidade tiver uma associação de ex-alunos ou serviço de orientação para o mercado de trabalho, costuma ser útil comunicar por e-mail os inscritos nesses serviços.

Igualmente, é interessante enviar e-mails a empresas que precisam de profissionais da cibersegurança, bem como a desenvolvedoras de *software*, informando-lhes a respeito do mestrado, pois, com frequência, elas preferem oferecer a formação aos seus funcionários de confiança, concedendo-lhes bolsa total ou parcial, antes de recorrer ao mercado de trabalho.

Por último, é imprescindível anunciar o mestrado no site da universidade, apresentando seus objetivos, o programa acadêmico, o corpo docente, a porcentagem de graduados trabalhando no setor (obviamente, a partir da segunda edição) e os recursos de ensino. E, melhor ainda, se o diretor do mestrado gravar um vídeo curto (de três ou quatro minutos, no máximo) tratando dos aspectos acima mencionados.

Anexo

Anexo

Lista de universidades que contribuíram para o desenvolvimento do programa

Na tabela a seguir, estão as instituições que contribuíram para o desenvolvimento do programa, tendo respondido a pesquisa ou participado de reuniões de feedback.

Universidade
Centro Universitário de Mineiros (UNIFIMES)
Escuela Superior Politécnica del Litoral (ESPOL)
Instituto de Computação, Universidade Estadual de Campinas (UNICAMP)
Instituto Federal Baiano (IFBAIANO)
Instituto Federal de Alagoas (IFAL)
Instituto Federal de Brasília (IFB)
Instituto Federal de Ceará (IFCE)
Instituto Federal de Educação, Ciência e Tecnologia Sul-rio-grandense (IFSUL)
Instituto Federal de Mato Grosso (IFMT)
Instituto Federal de Minas Gerais (IFMG)
Instituto Federal de Rondônia (IFRO)
Instituto Federal de Santa Catarina (IFSC)
Instituto Federal de São Paulo (IFSP)
Instituto Federal de Sergipe (IFS)
Instituto Federal do Acre (IFAC)
Instituto Federal do Amazonas (IFAM)
Instituto Federal do Maranhão (IFMA)
Instituto Federal do Pará (IFPA)
Instituto Federal do Piauí (IFPI)
Instituto Federal do Sul de Minas Gerais (IFSULDEMINAS)
Instituto Federal do Tocantins (IFTO)
Instituto Federal do Triângulo Mineiro (IFTM)
Instituto Tecnológico de Buenos Aires (ITBA)

Instituto Tecnológico de Costa Rica
Pontificia Universidad Javeriana
Tecnológico de Monterrey
The University of the West Indies (UWI)
Universidad Nacional Autónoma de Nicaragua (UNAN), campus de Managua
Universidad Austral
Universidad Cenfotec
Universidad de Buenos Aires (UBA)
Universidad de Chile
Universidad de Costa Rica
Universidad de la República Oriental del Uruguay
Universidad de la Sabana (UNISABANA)
Universidad de los Andes (UNIANDES)
Universidad de Talca (UTalca)
Universidad del Rosario (URosario)
Universidad del Valle (UNIVALLE)
Universidad EAFIT
Universidade Federal do Ceará (UFC)
Universidad Francisco Gavidia (UFG)
Universidad Iberoamericana IBERO (UIA)
Universidad Industrial de Santander (UIS)
Universidad Latina de Costa Rica
Universidad Latinoamericana de Ciencia y Tecnología (ULACIT)
Universidad Mayor de San Simón (UMSS)
Universidad Nacional Autónoma de México (UNAM)
Universidad Nacional Autónoma de Nicaragua (UNAN)
Universidad Nacional de Caaguazú (UNCA)
Universidad Nacional de La Plata (UNLP)
Universidad Nacional del Rosario (UNR)
Universidad Pontificia Bolivariana (UPB) – campus de Bucaramanga

Universidad Técnica Federico Santa María (USM)
Universidad Tecnológica de Panamá (UTP)
Universidad Tecnológica del Uruguay (UTEC)
Universidade de São Paulo (USP)
Universidade do Vale do Itajaí (UNIVALI)
Universidade Estadual da Região Tocantina do Maranhão (UEMASUL)
Universidade Federal de Mato Grosso (UFMT)
Universidade Federal do Pará (UFPA)
Universidade Federal do Paraná (UFPR)
Universidade Federal do Sul e Sudeste do Pará (UNIFESSPA)
Universidade Federal Fluminense (UFF)
Universidade Nilton Lins
University of Bahamas (UB)
University of the West Indies (UWI) – campus de Cave Hill


BID