**PLANO DE ENSINO**

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **DISCIPLINA** | CYBERSECURITY GOVERNANCE AND REGULATION | | | | | | | | |
| **DOCENTE** | LUCA BELLI | | | | | | | | |
| **CÓDIGO** | GRDDIRELE379/ GRDDIRELE366 | **SEMESTRE** | 2025.1 | **PERÍODO** | 6º/10º | **NATUREZA** | ELETIVA | **CARGA HORÁRIA** | 25/30h |

| | | |
|---|---|---|
| **EMENTA** | | The proposed Course aims at analyzing the concepts and dimensions necessary to understand the global cybersecurity governance, the economic and political interests that determine its evolution and that influence cybersecurity regulations. The course will explore a selection of cybersecurity issues from different national and regional perspectives. The course will feature several guest lectures from international specialist part of the CyberBRICS project and of the CTS-FGV Visiting Professors Programme. |
| **OBJETIVOS** | | Being able to understand the cybersecurity dynamics, players, and regulatory elements of the various of cybersecurity layers:<br>• data protection<br>• protection of critical infrastructure<br>• cyber-threats and cybercrimes |
| **METODOLOGIA** | | The proposed methodology is tripartite. Throughout the first part of the course, general theoretical concepts will be explored. Throughout the second part, a selection of national and international cybersecurity approaches will be explored. In the third module, the course will be essentially based on a participatory methodology, as the students will be required to deliver presentations on cybersecurity issues of their choice.<br>IMPORTANT: student participation will increase throughout the course, with part of the student grades depending on participation, especially during participatory seminars, and the successful completion of a presentation during the last part of the course. Students will be required to attend at least 75% of the classes, as prescribed by Brazilian law. |
| | **x** | Interpretar/aplicar as normas (princípios e regras) do sistema jurídico nacional, observando a experiência estrangeira comparada, quando couber, articulando o conhecimento teórico com a resolução de problemas. |
| | | Demonstrar competência na leitura, compreensão e elaboração de textos, atos e documentos jurídicos, de caráter negocial, processual ou normativo, bem como a devida utilização das normas técnico-jurídicas. |
| | | Demonstrar capacidade para comunicar-se com precisão. |
| | | Dominar instrumentos da metodologia jurídica, sendo capaz de compreender e aplicar conceitos, estruturas e racionalidades fundamentais ao exercício do Direito. |
| | | Adquirir capacidade para desenvolver técnicas de raciocínio e de argumentação jurídicos com objetivo de propor soluções e decidir questões no âmbito do Direito. |
| | | Desenvolver a cultura do diálogo e o uso de meios consensuais de solução de conflitos. |
| | | Compreender a hermenêutica e os métodos interpretativos, com a necessária capacidade de pesquisa e de utilização da legislação, da jurisprudência, da doutrina e de outras fontes do Direito. |
| | | Ter competências para atuar em diferentes instâncias extrajudiciais, administrativas ou judiciais, com a devida utilização de processos, atos e procedimentos. |
| | | Utilizar corretamente a terminologia e as categorias jurídicas. |
| | | Aceitar a diversidade e o pluralismo cultural. |
| | **x** | Compreender o impacto da inteligência artificial e das novas tecnologias na área jurídica. |
| | **x** | Possuir o domínio de tecnologias e métodos para permanente compreensão e aplicação do Direito. |
| | | Desenvolver a capacidade de trabalhar em grupos formados por profissionais do Direito ou de caráter interdisciplinar. |
| | | Apreender conceitos deontológico-profissionais e desenvolver perspectivas transversais sobre direitos humanos. |
| | **X** | Compreender a estrutura da Internet e a natureza dos vários instrumentos de regulação desse meio e dos atores ou stakeholders que influenciam a elaboração de tais instrumentos. Particularmente o curso visará permitir:<br><br>• A análise e a compreensão da estrutura técnica da Internet e dos principais atores econômicos e políticos que influenciaram a evolução da Internet;<br>• A análise e a compreensão do valor normativo da arquitetura (hardware e software) à base da Internet;<br>• A análise e a compreensão dos principais mecanismos de governança da Internet, ao nível nacional e internacional;<br>• Análise e compreensão das diferentes formas de regulação de Internet, do papel do estado e das entidades privadas no âmbito da regulação das redes eletrônicas e das plataformas que compõem a Internet. |

**CONTEÚDO PROGRAMÁTICO**

| AULA | TEMA |
|---|---|
| 1 | Presentation of the course, its relevance and objectives, and the methodology to be adopted. |
| 2 | The evolution of digital technology and its modalities of regulation |
| 3 | The concept of Cybersecurity and its layers |

| | | |
|---|---|---|
| 4 | | Data Security and Cybersecurity of Telecoms Infrastructure in Brazil |
| 5 | | The EU Approach to Cybersecurity and Security by Design |
| 6 | | Participatory seminar |
| 7 | | Cybercrime: from the Budapest Convention to the UN Convention |
| 8 | | **Cyber power** |
| 9 | | **Cyber defense** |
| 10 | | AI meets Cybersecurity |
| 11 | | A Cybersecurity Approach to Quantum Computing |
| 12 | | Participatory seminar |
| 13 | | Student Presentations |
| 14 | | Student Presentations |
| 15 | | Student Presentations |
| **TRILHA** | | Advocacia Empresarial |
| | | Carreiras Públicas |
| | | Regulação |
| | | Justiça e Sociedade |
| | **X** | Tecnologias |
| **CRITÉRIOS DE AVALIAÇÃO** | | The final grade will be based on the combined result of student participation to debates during class, student oral presentation, and written take-home exam.<br>The evaluation of the written exam (mid-term) will correspond to 30% (three out of ten points of the final grade). The written exam must be in English language.<br>The evaluation of the oral presentation (final exam) will correspond to 30% (three out of ten points of the final grade).<br>The remaining 40% (four out of ten points of the final grade), to reach 100% of the final grade (ten points), will depend on the student's effective participation in the debates held in the classroom. |
| **BIBLIOGRAFIA BÁSICA** | | VEALE, MICHAEL. & BROWN, IAN. (2020). Cybersecurity. Internet Policy Review, 9(4). https://doi.org/10.14763/2020.4.1533<br>BELLI, LUCA (2021). (Ed.) CyberBRICS: Cybersecurity regulations in BRICS countries. Springer. https://cyberbrics.info/cyberbrics-cybersecurity-regulations-in-the-brics-countries-full-ebook/<br>LEE A. BYGRAVE. Security by Design: Aspirations and Realities in a Regulatory Context. Oslo Law Review. Volume 8, No. 3-2021, p. 126–177. https://www.duo.uio.no/bitstream/handle/10852/94342/olr.8.3.2.pdf?sequence=1&isAllowed=y |
| **BIBLIOGRAFIA COMPLEMENTAR** | | ITU. (2014) Understanding cybercrime: Phenomena, challenges and legal response Geneva: ITU Telecommunication Development Bureau. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_E.pdf<br>ITU-T. (2008, April 18). X.1205: Overview of cybersecurity. https://www.itu.int/rec/T-REC-X.1205-200804-I<br>BELLI, L. (2021). Cybersecurity convergence in the BRICS countries. CyberBRICS. https://cyberbrics.info/cybersecurity-convergence-in-the-brics-countries/<br>KOSSEFF, J. (2020). Cybersecurity law (Second). Wiley. https://doi.org/10.1002/9781119517436<br>Global Cyber Security Capacity Centre. (2016). Cybersecurity Capacity Maturity Model for Nations (CMM) Revised Edition. Global Cyber Security Capacity Centre, University of Oxford. https://doi.org/10.2139/ssrn.3657116<br>MAURER, T., HOHMANN, M., SKIERKA, I., & MORGUS, R. (2015). National CSIRTs and Their Role in Computer Security Incident Response [Policy Paper]. New America; Global Public Policy Institute. http://newamerica.org/cybersecurity-initiative/policy-papers/national-csirts-and-their-role-in-computer-security-incident-response/ |