



PROJETO PEDAGÓGICO DE CURSO
Pós-Graduação *Lato Sensu*
Data Protection Officer - DPO

Sumário

1.	Nome do Curso e Área do Conhecimento.....	3
2.	Características Técnicas do Curso	3
3.	Público-alvo	3
4.	Critérios de Seleção.....	4
5.	Justificativa do Curso.....	4
6.	Objetivos do Curso	5
7.	Competências e Habilidades do Egresso.....	6
8.	Metodologia de Ensino e Aprendizagem	6
9.	Estágio Não Obrigatório	9
10.	Matriz Curricular	10
11.	Carga Horária.....	11
12.	Conteúdo programático	11
13.	Infraestrutura Física e Pedagógica	28

1. Nome do Curso e Área do Conhecimento

Nome do Curso: Data Protection Officer - DPO

Área de Avaliação (CAPES): CIÊNCIA DA COMPUTAÇÃO

Grande Área (CAPES): 10000003 CIÊNCIAS EXATAS E DA TERRA

Área do Conhecimento (CAPES): 10300007 CIÊNCIA DA COMPUTAÇÃO

Classificação OCDE: Computação e Tecnologias da Informação e Comunicação (TIC)

2. Características Técnicas do Curso

Modalidade: Educação a Distância

Número máximo de vagas por Polo/Unidade: 1000 alunos

Período de Oferecimento: O curso possui entrada intermitente, respeitadas as datas de início e de fim cadastradas na oferta, bem como observado o período indicado para a sua integralização.

Limitações legais

Resolução CNE/CES Nº 1, de 06 de abril de 2018, que estabelece normas para o funcionamento de cursos de pós-graduação lato sensu.

O candidato deverá ser graduado com diploma devidamente registrado segundo as normas estabelecidas pelo MEC.

3. Público-alvo

O público alvo do curso de pós-graduação em *Data Protection Officer* são cientistas da computação, analistas de sistemas, programadores, engenheiros da computação, tecnólogos da área de tecnologia da

informação, e demais profissionais da área de tecnologia da informação e de segurança da informação ligados direta ou indiretamente ao manejo de informações sensíveis, bem como operadores do direito e demais profissionais ligados ao uso de dados de usuários através de meios eletrônicos.

4. Critérios de Seleção

O ingresso na pós-graduação será realizado por meio de inscrição no portal da Instituição e entrega dos documentos solicitados. Em seguida, analisados pela área competente.

5. Justificativa do Curso

A economia mundial tem migrado seu principal eixo da manufatura e exploração de riquezas para a obtenção e tratamento de informações, no que alguns acadêmicos já veem como uma nova era, que substituí a industrial, a era da informação. Na esteira dessas mudanças, a comunidade internacional bem como seus países tem investido em acordos e legislações que tratam especificamente de como as informações e dados de pessoas e empresas são utilizados nesse novo modelo econômico. Assim como na GDPR na Europa, a LGPD no Brasil estabeleceu os limites e criou os mecanismos necessários para que se legislasse de forma objetiva sobre esses dados. Promulgada em 2018 e já em ação desde 2020, a Lei Geral de Proteção de Dados estabelece como o dados dos usuários devem ser tratados e quais as responsabilidades técnicas e legais das organizações detentoras desses dados. Surge assim a necessidade da imagem do Data Protection Officer, que na lei brasileira surge como encarregado, e é o responsável pelo tratamento e processo através do qual os dados serão obtidos e armazenados, bem como a disponibilização desses dados e sua finalidade para o proprietário, além de se responsabilizar junto às autoridades pelas questões relacionadas ao uso dessas informações.

Assim, justifica a implantação desse curso à necessidade de formação de profissionais com o perfil técnico e acadêmico necessário para o atendimento dessas demandas tão específicas e tão urgentes.

6. Objetivos do Curso

6.1. Objetivo Geral

- O curso tem por objetivo geral a formação de profissionais para atuação como DPO e Encarregado de dados para atuar junto às equipes de segurança, análise e mineração de dados, de acordo com as determinações da LGPD.

6.2. Objetivos Específicos

São objetivos específicos do curso de especialização em Data Protection Officer, desenvolver o aluno para:

- Comunicar e atender os titulares dos dados, de acordo com as suas necessidades;
- Analisar processos e fluxogramas para análises de uso consciente dos dados dos titulares bem como definir suas destinações;
- Mapear e inventariar produtos e processos que coletam dados dos usuários, bem como vincular tais dados de forma efetiva e segura com seus titulares;
- Treinar e orientar funcionários e contratados da entidade sobre práticas estabelecidas em relação ao tratamento de dados pessoais;
- Executar demais tarefas e atribuições determinadas na LGPD ou em normativas complementares;

7. Competências e Habilidades do Egresso

Competências

Atuar em empresas, instituições e governos a fim de atender as demandas dos titulares dos dados com responsabilidade e de acordo com a lei, conforme estabelecido na Lei Geral de Proteção de Dados, monitorando e protegendo dados para garantir que eles estejam de acordo com as regras e com as boas práticas determinadas pela lei.

Habilidades

- Analisar fluxos de dados a partir do olhar de segurança e titularidade dos dados.
- Atender e responder solicitações de titulares sobre disponibilidade e utilização dos dados, bem como identificar a criticidade de dados e a maneira como são transferidos, armazenados e utilizados
- Desenvolver treinamentos e manuais sobre utilização, disponibilização e armazenamento adequado dos dados bem como sua relação com os titulares e;
- Utilizar ferramentas e métodos para análise e inventário de dados.

8. Metodologia de Ensino e Aprendizagem

O desenvolvimento das disciplinas do curso se dará no ambiente virtual, onde o aluno cumprirá 40 horas por disciplina.

Estas 40 horas são compostas pelo estudo dos diversos insumos pedagógicos disponibilizados, como:

- ✓ materiais de leitura;
- ✓ videoaulas;

- ✓ slides;
- ✓ podcasts;
- ✓ indicações de leituras extras como artigos e capítulos de livros.

Como parte do modelo acadêmico, também contabilizamos:

- ✓ a interação com os tutores para esclarecimentos de dúvidas pedagógicas (via Fórum);
- ✓ a realização da avaliação disciplinar pelo aluno.

Vale ressaltar que cada aluno é único e tem seu próprio tempo para aprendizagem. Alguns conseguem assimilar o conteúdo com mais agilidade, outros precisam retomar as leituras e videoaulas para tornar sua aprendizagem efetiva.

O tempo gasto pelo aluno para o entendimento de cada disciplina depende também da sua familiaridade com o tema, ou seja, o conhecimento prévio que o aluno tem em relação a temática abordada.

No ambiente virtual, o aluno encontrará o conteúdo das disciplinas, organizados em temas/webaulas.

Para cada um deles, o aluno realizará um conjunto de atividades baseadas em leitura de textos de fundamentação teórica e acesso a recursos audiovisuais.

Um tutor apoiará as atividades realizadas no ambiente virtual, atendendo o aluno nas suas dúvidas por meio de ferramentas de comunicação.

O aluno, ao iniciar os seus estudos, terá um encontro presencial para acolhida/ambientação; esse encontro terá como objetivos:

- ✓ Integrar o aluno ao curso de Pós-Graduação.
- ✓ Dialogar e esclarecer as dúvidas sobre a proposta pedagógica do curso e as regras acadêmicas.
- ✓ Apresentar ao aluno o Ambiente Virtual de Aprendizagem (o primeiro acesso; o envio de documentos; os serviços de secretaria e financeiro; a disciplina Ambientação; a tutoria online; o boletim

acadêmico; as disciplinas e seus conteúdos; a biblioteca virtual; entre outros).

- ✓ Proporcionar um momento de Network aos pós-graduandos.

Avaliação do Desempenho do Aluno

O aluno deverá realizar as atividades propostas no ambiente virtual. A realização das atividades irá compor sua frequência no curso, que será considerada para a sua aprovação.

A atividade avaliativa que o aluno realizará para compor a sua média é a Avaliação Virtual (AV); essa atividade é obrigatória e estará disponível no Ambiente Virtual de Aprendizagem – AVA, conforme cronograma de seu curso.

Para a aprovação em cada uma das disciplinas, o aluno deverá obter frequência de, no mínimo, 75% (setenta e cinco por cento) e nota igual ou superior a 7,0 (sete).

As notas devem ser expressas no intervalo de 0 (zero) a 10 (dez).

O aluno que obtiver média inferior a 7,0 (sete) nas disciplinas terá direito ao Programa de Dependência e Recuperação – PDR, mediante a solicitação de requerimento e respeitando o período de jubileamento do curso.

O PDR será realizado no ambiente virtual de aprendizagem, sendo que o aluno terá acesso ao conteúdo da disciplina e realizará uma Avaliação Virtual - AV, e a nota obtida substituirá a média do aluno.

Para a obtenção do **Certificado** de Pós-graduação *Lato Sensu* – especialização, o aluno deverá cumprir todas condições seguintes:

- ✓ Frequência mínima de 75% (setenta e cinco por cento) em todas as disciplinas;
- ✓ Nota igual ou superior a 7,0 (sete) em todas as disciplinas.

Certificação

O Certificado de conclusão de curso de Especialização será acompanhado por histórico escolar, em cumprimento às exigências da Resolução CNE/CES nº1, de 06 de abril de 2018, da Câmara de Educação Superior do Conselho Nacional de Educação.

Composição do Corpo Docente

O corpo docente do curso é constituído por profissionais qualificados, com comprovado saber em sua área de atuação, conforme Resolução CNE/CES nº1, de 06 de abril de 2018, sendo integrado, no mínimo, por 30% (trinta por cento) de portadores de título de pós-graduação *stricto sensu*, isto é, portadores de títulos de Mestrado e Doutorado, obtidos em programas de pós-graduação *stricto sensu* devidamente reconhecidos pelo poder público em território nacional, ou revalidados, conforme legislação vigente. Os demais docentes são certificados em nível de especialização, pós-graduação *lato sensu*, de reconhecida capacidade técnico-profissional.

9. Estágio Não Obrigatório

O estágio curricular não obrigatório tem como finalidade estimular o aluno a desenvolver atividades extracurriculares, para que possa inter-relacionar os conhecimentos teóricos e práticos adquiridos durante o curso e aplicá-los na solução de problemas reais da profissão, proporcionando o desenvolvimento da análise crítica e reflexiva para os problemas socioeconômicos do país, de acordo com a Resolução de Estágio curricular não obrigatório vigente na Instituição.

Os principais objetivos da prática do estágio curricular não obrigatório são:

- I. proporcionar o exercício do aprendizado compromissado com a realidade socioeconômica-política do país;
- II. propiciar a realização de experiências de ensino e aprendizagem visando à educação profissional continuada, alicerçada no desenvolvimento de competências e habilidades e ao exercício do pensamento reflexivo e criativo; e
- II. incentivar o trabalho de pesquisa e investigação científica, visando ao desenvolvimento da ciência, da tecnologia e da cultura.

A carga horária é definida pela concedente de estágio, não podendo ultrapassar a carga horária máxima de 6 (seis) horas diárias e 30 (trinta) horas semanais, as quais podem ser realizadas em empresas públicas ou privadas, instituição de pesquisa, órgãos governamentais e não governamentais, e as próprias unidades da Universidade, desde que sigam às condições adequadas para que o

estagiário possa aprofundar os seus conhecimentos teóricos e práticos adquiridos no curso.

Para o Curso de Pós-Graduação EAD, a prática do estágio curricular não obrigatório é permitida durante a vigência do curso, não podendo exceder em um mesmo campo de estágio o período de 2 (dois) anos.

Os estágios curriculares não obrigatórios devem estar apoiados em Termo de Compromisso e de comum acordo com a Instituição, devendo explicitar não somente os aspectos legais específicos, como também os aspectos educacionais e de compromisso com a realidade social. O Planejamento do Estágio Curricular Não Obrigatório é de responsabilidade do coordenador de curso/professor orientador e também do Departamento de Estágios.

10. Matriz Curricular

DISCIPLINAS	CH PRÁTICA	CH TEÓRICA	CH TOTAL
Ambientação	0 h	0 h	0 h
Tecnologias descentralizadas	0 h	40 h	40 h
Governança de Dados	0 h	40 h	40 h
Lei Geral de Proteção de Dados	0 h	40 h	40 h
Interações entre big data e cloud computing	0 h	40 h	40 h
Fundamentos e regulamentação da privacidade e proteção de dados	0 h	40 h	40 h
Certificação DPO	0 h	40 h	40 h
Cybersecurity	0 h	40 h	40 h
Compliance digital	0 h	40 h	40 h
Cibercrimes, responsabilidade penal e civil	0 h	40 h	40 h

11. Carga Horária

A carga horária de 360h constitui o conteúdo ministrado em 9 (nove) disciplinas.

12. Conteúdo programático

Disciplina: Ambientação

Ementa: Ensino a distância: características desta modalidade de estudo. A tecnologia e o ensino à distância. Legislação do Ensino a Distância no Brasil. Aspectos relacionados ao perfil no Ensino a Distância.

Competências e Habilidades:

- Compreender a modalidade de ensino a distância.
- Identificar uma relação entre tecnologia e educação no contexto do EAD;
- Discutir elementos da legislação do ensino a distância no Brasil;
- Refletir sobre o perfil do aluno em ensino a distância.

Conteúdo Programático 1: Introdução ao Ensino a Distância.

Conteúdo Programático 2: Tecnologia e educação.

Conteúdo Programático 3: Legislação do Ensino a Distância no Brasil.

Conteúdo Programático 4: Perfil do aluno no Ensino a Distância.

Bibliografia básica:

BRASIL. Ministério da Educação. **Lei de Diretrizes e Bases da Educação Nacional - Lei n. 9.394/96**. Brasília, 1996. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9394.htm. Acesso em: 6 dez. 2022.

BRASIL. Ministério da Educação. **Resolução CNE/CP n. 7, de 18 de dezembro de 2018**. Brasília, 2018. Disponível em: https://normativasconselhos.mec.gov.br/normativa/view/CNE_RES_CNECESN72018.pdf. Acesso em: 6 dez. 2022.

GIL, H. A passagem da Web 1.0 para a Web 2.0 e... Web 3.0: potenciais consequências para uma 'humanização' em contexto educativo. 2014. **Boletim informativo Cybercentro Castelo Branco**. Castelo Branco, 2014. Disponível em: <https://repositorio.ipcb.pt/bitstream/10400.11/2404/1/A%20passagem%20da%20Web%20Henrique.pdf>. Acesso em: 6 dez. 2022.

MEYER, A. I. da S. (2022). Conceituando a Educação a Distância. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 8, n. 1, p. 590-601, [s. l.], 2022. Disponível em: <https://periodicorease.pro.br/rease/article/view/3835>. Acesso em: 6 dez. 2022.

VAZ, M. L. de L.; RIBEIRO, F.; COSTA, L. A. da. Os desafios da educação a distância on-line e a remotividade na nova engenharia educacional. **Brazilian Journal of Science**, v. 1, n. 4, p. 79-86. Goiás, 2022. Disponível em: <https://www.brazilianjournalofscience.com.br/revista/article/view/79>. Acesso em: 6 dez. 2022.

VIEIRA, D. M. L.; COSTA, L. A.; VAZ, M. L. L. Um novo olhar para a educação a distância. In: MACHADO, G. E.; COSTA, S. C.; SILVA, K. R. P. **Debates contemporâneos: perspectivas e reflexões atuais**. Santa Maria: Arco, 2021.

Bibliografia Complementar:

BAPTISTA, M. M. Internet: auxílio à educação. **BIBLOS - Revista do Instituto de Ciências Humanas e da Informação**, v. 16, p. 37- 44, [s. l.], 2004. Disponível em: <http://hdl.handle.net/20.500.11959/brapci/23717>. Acesso em: 6 dez. 2022.

MOORE, M.; KEARSLEY, G. **Educação a distância: uma visão integrada**. São Paulo: Thomson Learning, 2007.

MORAN, J. M.; MASETTO, M. T.; BEHRENS, M. A. **Novas tecnologias e mediação pedagógica**. 21. ed. Campinas: Papirus, 2013.

PIVA, D. J.; PUPO, R.; GAMEZ, L. et al. **EAD na prática**: planejamento, métodos e ambientes de educação on-line. São Paulo: Elsevier, 2011.

Disciplina: Tecnologias Descentralizadas.

Ementa: Tecnologia Descentralizada. Bitcoin. Blockchain. Smart Contracts. Smart Cities. Aplicações de DLT ao registro de imóveis. Aplicações de DLT ao registro de pessoas. Aplicações de DLT a notas e títulos.

Competências e Habilidades:

- Aproximar o aluno da concepção da revolução tecnológicas nos próximos anos
- Compreender a tecnologia que sustenta as criptomedas mais conhecidas.
- Fomentar a criação de novas possibilidade de produtos – jurídicos ou não.
- Capacitar o aluno a refletir sobre possíveis soluções tecnológicas utilizando tecnologia descentralizada.

Conteúdo Programático 1: Tecnologia Descentralizada

Conteúdo Programático 2: Blockchain. Bitcoin. Smart Contracts. Utilização de Blockchain nas juntas comerciais.

Conteúdo Programático 3: Smart Cities. Aplicações de DLT (Distributed Ledger Technology) ao registro de imóveis.

Conteúdo Programático 4: Uso de DLT (Distributed Ledger Technology) ao registro de pessoas e documentos estundantis. A DLT (Distributed Ledger Technology) e sua utilização em notas e títulos.

Bibliografia Básica:

MOUGAYAR, William. Blockchain para negócios: Promessa, prática e aplicação da nova tecnologia da Internet. Atlas Books. São Paulo. 2017

TAPSCOTT, Don, TAPSCOTT, Alex. Blockchain Revolution. Senai -SP. 2017.

CAMPOS, Emília Malgueiro. Criptomoedas e Blockchain. Lumen Juris. São Paulo. 2018.

LYRA, João Gomes. Blockchain e organizações descentralizadas. Brasport. 2019.

Bibliografia Complementar:

BLOCKCHAIN COMO SISTEMA DE CUSTÓDIA DE VALORES MOBILIÁRIOS NO ÂMBITO DO MERCADO DE CAPITAIS BRASILEIRO. Revista de Direito Bancário e do Mercado de Capitais | vol. 80/2018 | p. 93 - 106 | Abr - Jun / 2018 | DTR\2018\14473

PERSPECTIVAS PARA A TECNOLOGIA BLOCKCHAIN

Revista de Direito Bancário e do Mercado de Capitais | vol. 81/2018 | p. 141 - 158 | Jul - Set / 2018 | DTR\2018\19494

CONTRATOS INTELIGENTES, OAD E NOVA ECONOMIA INSTITUCIONAL: PERSPECTIVAS PARA A INTERPRETAÇÃO E APLICAÇÃO DE AJUSTES CELEBRADOS EM COMPUTAÇÃO DESCENTRALIZADA A PARTIR DE ESTUDO DE CASO SOBRE A VULNERABILIDADE DA CODIFICAÇÃO NO AMBIENTE DO ETHEREUM. Revista de Direito Civil Contemporâneo | vol. 18/2019 | p. 61 - 90 | Jan - Mar / 2019 | DTR\2019\27929.

Disciplina: Governança de dados

Ementa: Visão geral da gestão de dados, governança de dados, gestão da arquitetura de dados, desenvolvimento de dados, gestão de dados mestre e dados de referência.

Competências e Habilidades:

- Compreender o ciclo de vida do dado e o papel da governança
- Elaborar projetos usando princípios de governança de dados
- Esquematizar arquitetura de dados
- Aplicar princípios da gestão de dados

Conteúdo Programático 1: Introdução à governança de dados. Dado como ativo corporativo. Ciclo de vida do dado. Gestão de dados. O profissional de governança de dados.

Conteúdo Programático 2: Visão geral da gestão de dados. Missão, princípios e objetivos. Funções e atividades. Papéis e responsabilidades. Tecnologias.

Conteúdo Programático 3: Conceito de governança de dados. Conceitos e atividades. Detalhes de atividades da governança de dados. Desenvolvimento de dados. Estilos de modelagem de dados. Design de dados. Implementação de dados.

Conteúdo Programático 4: Arquitetura de dados. Gestão da arquitetura de dados. Conceitos e atividades. Princípios gerais. Gestão de dados mestre. Conceitos de dado mestre e dado de referência. Integração de dados. Gestão de mudanças.

Bibliografia Básica:

BRACKETT, Michael; EARLEY, Susan. **The DAMA Guide to The Data Management Body of Knowledge** (DAMA-DMBOK Guide), 2009.

BARBIERI, Carlos. **Governança de Dados:** Práticas, conceitos e novos caminhos. Alta Books, 2020.

RÊGO, Bergson Lopes. **Gestão e governança de dados:** promovendo dados como ativo de valor nas empresas. Brasport, 2013.

SHARDA, Ramesh; DELEN, Dursun; TURBAN, Efraim. **Business Intelligence e Análise de Dados para Gestão do Negócio.** Porto Alegre: Bookman, 2019.

Bibliografia Complementar:

HASHEM, I. A. T.; YAQOOB, I.; ANUAR, N.B.; MOKHTAR, S.; GANI, A.; KHAN, S.U. **The rise of “big data” on cloud computing: review and open research issues.** Information Systems 47 (2015), 98 - 115.

LOSHIN, David. **Master data management.** Morgan Kaufmann, 2010.

BAKSHI, Kapil. Considerations for big data: Architecture and approach. In: **2012 IEEE aerospace conference**. IEEE, 2012. p. 1-7.

Disciplina: Lei Geral de Proteção de Dados

Ementa: Direitos humanos. Direitos fundamentais. Direito à vida privada. Direito à proteção de dados. Legislação brasileira de proteção de dados: Marco Civil da Internet, Lei do Cadastro Positivo e Lei de Acesso à Informação. Regulamento Europeu de proteção de dados – GDPR. Privacy by design. Lei Geral de Proteção de Dados Pessoais - LGPD. Agentes de tratamento. Controlador. Operador. Responsabilidades. Bases Legais de tratamento de dados. Ressarcimentos de danos. Encarregado pelo Tratamento de Dados – DPO. Segurança da Informação. Boas práticas e governança. Autoridade Nacional de Proteção de Dados. Fiscalização. Sanções administrativas.

Competências e Habilidades:

- Compreender as legislações nacionais e internacionais de proteção de dados pessoais. Compreender as implicações da LGPD no Direito Empresarial. Desenvolver a habilidade de analisar violações de dados pessoais, avaliar riscos e propor soluções. Capacitar o aluno para que possa prestar consultoria ou analisar sua própria empresa em busca de uma adequação legal. Propiciar um conhecimento amplo sobre a proteção de dados pessoais e suas implicações nas empresas.

Conteúdo Programático 1: Direitos humanos. Direitos fundamentais. Direito à vida privada. Direito à proteção de dados pessoais. Background da legislação de proteção de dados pessoais. Legislação da União Europeia de proteção de dados (GDPR),

Conteúdo Programático 2: Princípios da Lei Geral de Proteção de Dados Pessoais. Fundamentos da LGPD. Âmbito de Aplicação. Encarregado de Dados pessoais. Conceito e atribuições.

Conteúdo Programático 3: Conceitos gerais da Lei Geral de Proteção de Dados Pessoais - LGPD. Bases Legais para o Tratamento de dados pessoais,

de dados pessoais sensíveis. Tratamento de dados pessoais de crianças e de adolescentes. Tratamento de dados pessoais pelo poder público. Agentes de tratamento. Controlador. Operador.

Conteúdo Programático 4: Autoridade Nacional de Proteção de Dados. Fiscalização. Sanções administrativas. Boas práticas e governança. Registro de Operações de tratamento de dados. Incidente de Segurança. Segurança da Informação. *Privacy by design*.

Bibliografia Básica:

DONEDA, Danilo ... [et al.]. Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021.

PALHARES, Felipe; PRADO, Luiz Fernando e VIDIGAL, Paulo. Compliance Digital e LGPD. São Paulo: Thomson Reuters Brasil, 2021 (Coleção Compliance; coordenação Irene Patrícia Diom Nohara, Luiz Eduardo de Almeida).

PALHARES, Felipe (coord). Temas Atuais de Proteção de Dados. Thomson Reuters Brasil, 2020.

TEIXEIRA, Tarcisio. GUERREIRO, Ruth Maria. Lei Geral de Proteção de Dados Pessoais comentada artigo por artigo. 4 ed. São Paulo: Saraiva, 2022.

Bibliografia Complementar:

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

TEIXEIRA, Tarcisio... [et al.]. DPO – Encarregado de Dados Pessoais [recurso eletrônico] – São Paulo: Expressa, 2022.

Disciplina: Interações entre big data e cloud computing.

Ementa: Introdução ao Big Data: Fundamentos, Infraestrutura e Interfaces. Gerenciamento de Big Data: Coleta e Processamento de Dados. Aplicação da Ciência de Dados no gerenciamento empresarial. Algoritmos de Aprendizado de

Máquina para minerar os dados. Big Data Analytics. Estruturas de Programação em Nuvem. Cloud Computing e Big Data.

Competências e Habilidades:

- Desenvolver a habilidade de raciocinar em ambientes computacionais de alta complexidade.
- Compreender os fundamentos da análise, gerenciamento e armazenamento de dados.
- Assimilar a importância do Aprendizado de Máquina na mineração de dados.
- Analisar a relação entre Cloud Computing e Big Data.

Conteúdo Programático 1: Introdução ao Big Data: Fundamentos, Infraestrutura e Interfaces.

Conteúdo Programático 2: Gerenciamento de Big Data: Coleta e Processamento de Dados.

Conteúdo Programático 3: Aplicação da Ciência de Dados no gerenciamento empresarial.

Conteúdo Programático 4: Big Data Analytics.

Conteúdo Programático 5: Algoritmos de Aprendizado de Máquina para minerar os dados.

Conteúdo Programático 6: Cloud Computing e Big Data.

Conteúdo Programático 7: Estruturas de Programação em Nuvem.

Bibliografia Básica:

MACHADO, F. N. R. **Big data:** o futuro dos dados e aplicações. São Paulo: Editora Erica, 2018

KELLEHER, J. D.; TIERNEY, B. **Data science.** Cambridge: MIT Press Essential Knowledge Series, 2018

RUPARELIA, N. B. **Cloud computing**. Cambridge: MIT Press Essential Knowledge Series, 2016

NETO, M. V. S. **Computação em nuvem**. Rio de Janeiro: Editora Brasport, 2015

SAGIROGLU, S.; SINANC, D. **Big data**: a review. International Conference on Collaboration Technologies and Systems (2013), 13681548.

HASHEM, I. A. T.; YAQOOB, I.; ANUAR, N.B.; MOKHTAR, S.; GANI, A.; KHAN, S.U. **The rise of “big data” on cloud computing**: review and open research issues. Information Systems 47 (2015), 98 - 115.

QI, H.; GANI, A. **Research on mobile cloud computing**: Review, trend and perspectives. Second International Conference on Digital Information and Communication Technology and it's Applications (2012), 12804207.

JULA, A.; SUNDARARAJAN, E.; OTHMAN, Z. **Cloud computing service composition**: A systematic literature review. Expert Systems with Applications 41 (2014), p. 3809-3824.

Bibliografia Complementar:

Data Science and Big Data Analytics: Making Data-Driven Decisions. Disponível em: <<https://bigdataanalytics.mit.edu>> Acesso em 13 nov.2018.

MIT-IBM Watson AI Lab. Disponível em: <<https://mitibmwatsonailab.mit.edu>> Acesso em 13 nov.2018. **What is Cloud Computing?** Disponível em: <<https://www.ibm.com/cloud/learn/what-is-cloud-computing>> Acesso em 13 nov.2018.

Nebula Cloud Computing Platform. Disponível em: <<https://www.nasa.gov/open/nebula.html>> Acesso em 13 nov.2018.

Disciplina: Fundamentos e regulamentação da privacidade e proteção de dados.

Ementa: Fundamentos e Princípios da Proteção de Dados Pessoais. Fundamentos e Regulamentação de Privacidade e Proteção de Dados. Práticas

de proteção e de privacidade de dados. Sistemas de Gestão de Privacidade. Gerenciamento de Identidade e acesso (IAM) e autodeterminação informativa. DPIA (Data Protection Impact Assessment) e DLM (Data Lifecycle Management). Direitos de titulares. Marcos legais da privacidade e suas bases. Privacy by Design, Security by Design e Ethics by Design. Zero Trust.

Competências e Habilidades:

- Conhecer e compreender os princípios legais acerca da legislação sobre privacidade e dados pessoais
- Conhecer os fundamentos do direito ao dado, titularidade e o histórico das leis
- Conceituar a proteção de dados de acordo com a legislação vigente
- Implantar práticas de privacidade dos dados e gestão da proteção, visando a redução de riscos;
- Compreender características básicas de sistema digitais seguros, infraestrutura e cloud computing.

Conteúdo Programático 1: História da regulamentação da proteção de dados, GDPR e definições.

Conteúdo Programático 2: Princípios do processamento de dados, propósitos e direitos de acesso.

Conteúdo Programático 3: Proteção de dados by Design e por padrão.

Conteúdo Programático 4: DPIA, DLM e auditoria.

Bibliografia Básica:

TOMASEVICIUS FILHO, Eduardo. **A lei geral de proteção de dados brasileira:** uma análise setorial (volume I) / coordenação Eduardo Tomasevicius Filho. São Paulo: Almedina, 2021.

PINHEIRO, Patrícia Peck. **Segurança digital:** proteção de dados nas empresas. SLEIMAN, Cristina. et al. São Paulo: Atlas, 2021.

PINHEIRO. Patrícia Peck. **Direito Digital**. 6. ed. São Paulo: Saraiva, 2016.

Bibliografia Complementar:

BESEMER, Leo. **Whitepaper**: EXIN Privacy & Data Protection Foundation. EXIN, 2020. Disponível em: http://bit.ly/PDPF_literature

European Commission.
General Data Protection Regulation (GDPR) Regulation EU 2016/679
Regulation of the European Parliament and the Council of the European Union.
Bruxelas, 2016. Disponível em: <http://eur-lex.europa.eu>

PINHEIRO. Patrícia Peck. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018.

Disciplina: Certificação DPO

Ementa: Data Protection Officer, agentes de tratamento de dados e o Encarregado de dados. Mapeamento e inventário de dados, processos e fluxos. Dados públicos e dados privados. ANPD, CNPD, seu funcionamento e funções. Ferramentas de monitoramento e prevenção à vazamentos de dados. DPMS (Data Protection Management System). Relatório de impacto, vazamentos, respostas a incidentes e BRP. Liderança e Soft Skills.

Competências e Habilidades:

- Planejar e aplicar a gestão eficiente em crises de segurança digital e governança de dados
- Atuar como orientador para empresas, instituições e governos sobre procedimentos relacionados à incidentes com dados, como vazamento ou roubo/furto;
- Orientar na criação de processos para levantamento e aquisição de dados, bem como tratamento e consumo, em observância da LGPD

- Salvar as informações dos titulares dos dados, sejam empresas, clientes ou colaboradores;
- Implementar e manter o sistema de gerenciamento de informações de privacidade

Conteúdo Programático 1: Política de proteção aos dados aplicada

Conteúdo Programático 2: Funções do DPO e o papel do Encarregado de dados na LGPD.

Conteúdo Programático 3: Gerenciamento e organização da proteção de dados e DPMS.

Conteúdo Programático 4: Vazamento de dados, notificação e resposta à incidente.

Bibliografia Básica:

GARCIA, Lara Rocha. **Lei Geral de Proteção de Dados Pessoais (LGPD):** guia de implantação. Lara Rocha Garcia; Edson Aguilera-Fernandes; Rafael Augusto Moreno Gonçalves; Marcos Ribeiro Pereira Barretto. São Paulo: Blucher, 2020.

LIMA, Ana Paula Moraes. **LGPD aplicada.** Ana Paula Moraes Canto de Lima [et al.]; coordenação Ana Paula Moraes Canto de Lima, Marcelo Crespo, Patrícia Peck Pinheiro. São Paulo: Atlas, 2021.

BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

Bibliografia Complementar (inserir 3 bibliografias atuais):

PINHEIRO. Patrícia Peck. **Proteção de dados pessoais:** comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018.

BESEMER, Leo. **Whitepaper:** EXIN Privacy & Data Protection Foundation. EXIN, 2020. Disponível em: http://bit.ly/PDPF_literature

Disciplina: Cybersecurity

Ementa: Arquitetura de Sistemas Seguros. Tecnologias de Desenvolvimento Seguro.

Competências e Habilidades:

- Desenvolver o conhecimento de arquitetura e infraestrutura de sistemas necessário para analisar e especificar controles de segurança para sistemas seguros;
- Desenvolver o conhecimento de estratégia e inteligência através de jogos e desenvolvimento de mecanismos de criptografia, aplicação da tecnologia e uso de certificados digitais e acesso a *deep web*.

Conteúdo Programático 1: Arquitetura de sistemas. Diferentes tecnologias de desenvolvimento e suas principais características.

Conteúdo Programático 2: Componentes de um sistema distribuído. Aspectos de segurança dos sistemas distribuídos. Análise de segurança.

Conteúdo Programático 3: Processo de desenvolvimento seguro. Top 10 OWASP. Testes de segurança em aplicações Web. Cloud computing: conceitos e aspectos de segurança.

Conteúdo Programático 4: Big Data Analytics. Armazenamento Seguro. Conceitos de inteligência. Conceitos de jogos.

Bibliografia Básica:

KIZZA, Joseph Migga. **Computer network security and cyber ethics**. 2nd ed. Jefferson: McFarland & Company, 2006.

RAY, John. **Maximum Linux security**: a hackers guide to protecting your Linux server and workstation]. 2nd ed. Indianapolis: SAMS, 2001.

KUROSE, James F.; ROSS, Keith W. **Redes de Computadores e a Internet**: Uma nova abordagem. São Paulo: Editora Pearson, 2017.

STALLINGS, William. **Criptografia e segurança de redes**: princípios e práticas. São Paulo: Pearson Education do Brasil, 2010.

BENANTAR, Messaoud. **Introduction to the public key infrastructure for the Internet**. Upper Saddle River, N.J.: Prentice-Hall: PTR, 2002.

SINGH, Simon; CALIFE, Jorge Luiz. **O livro dos códigos**. São Paulo: Record, 2007.

Bibliografia Complementar:

STALLINGS, William. **Criptografia e segurança de redes**: princípios e práticas. São Paulo: Pearson Education do Brasil, 2010.

MCCLURE, Stuart; SCAMBRAY, Joel; KURTZ, George. **Hackers expostos/ segredos e soluções para a segurança das redes**. São Paulo: Makron Books, 2000.

TANENBAUM, Andrew S.; WETHERALL, D. **Computer networks**. 5th ed. Boston, MA; Columbus, OH: Prentice Hall, 2011.

CORDEIRO, Luiz Gustavo. **Certificação digital**: conceitos e aplicações: modelos brasileiro e australiano. Rio de Janeiro: Ciência Moderna, 2008.

BUCHMANN, Johannes A. **Introduction to cryptography**. New York: Springer-Verlag, 2001

Disciplina: Compliance Digital

Ementa: Programas de compliance nacional e internacional. Compliance Empresarial e Due Diligence. Compliance Concorrencial Novo Estatuto Jurídico da Empresa Pública e Governança. Combate à Corrupção e Novos Modelos de Colaboração. Gestão de Conflitos e Soluções Alternativas para o Setor Público e Privado. Programas de Compliance e suas Etapas de Implantação. Acordo de Leniência e Certificações.. Marco civil na Internet.

Competências e Habilidades:

- Aprofundar os conhecimentos acerca do compliance habilitando o profissional a atuar como compliance officer de empresas; Capacitar o profissional para avaliar se as empresas estão em conformidade com previsões legais e regulamentos externos e internos;

- Aprofundar o debate e o conhecimento sobre compliance nas empresas nacionais e internacionais.
- Desenvolver o profissional para habilidades específicas com a finalidade de obtenção de certificação nacional e internacional.

Conteúdo Programático 1: Programas de compliance nacional e internacional. Compliance Empresarial e Due Diligence: Estrutura da Empresa, Contrato Social e Responsabilidade de Sócios, Dirigentes e Acionistas.

Conteúdo Programático 2: Contrato Entre Empresas e Responsabilização de Parceiros (terceirização, representação, distribuição, compras, fornecedores, parcerias, consórcios).

Conteúdo Programático 3: Compliance Concorrencial: Regulação Antitruste e Combate ao Dumping. Novo Estatuto Jurídico da Empresa Pública e Governança. Combate à Corrupção e Novos Modelos de Colaboração. Gestão de Conflitos e Soluções Alternativas para o Setor Público e Privado.

Conteúdo Programático 4: Etapas de Implantação. Acordo de Leniência e Certificações...

Bibliografia Básica:

FCPA. CARVALHO, André Castro; ALVIM, Tiago Cripa; BERTOCCELLI Rodrigo de Pinho; VENTURINI, Otávio (coord), **Manual de Compliance** – Rio de Janeiro. Forense. 2018.

SIMÃO, Valdir Moyses; VIANNA, Marcelo Pontes. **O acordo de leniência na lei anticorrupção: histórico, desafios e perspectivas**. São Paulo: Trevisan, 2017.

ACKMAN, David; The Compliance Revolution: How Compliance Needs to Change to Survive. Singapore: Wiley & Sons, 2015

GIAMUNDO NETO, Giuseppe. DOURADO, Guilherme Afonso. HADLICH, Luiz Felipe. **Compliance na administração pública**. CARVALHO, André Castro; ALVIM, Tiago Cripa; BERTOCCELLI Rodrigo de Pinho; VENTURINI, Otávio (coord), **Manual de Compliance** – Rio de Janeiro. Forense. 2018.

Controlling functions performed in startups. / Las funciones de la controladora desempeñadas en las empresas startups. By: Novaes Nocetti, Alaide Almeida; Facin Lavarda, Carlos Eduardo. Revista Ambiente Contábil. jan-

jun2019, Vol. 11 Issue 1, p182-200. 19p. Language: Portuguese. DOI: 10.21680/2176-9036.2019v11n1ID14813

Bibliografia Complementar:

CARVALHO, Itamar. ALMEIDA, Bruno. Programas de Compliance: Foco no programa de integridade. CARVALHO, André Castro; ALVIM, Tiago Cripa; BERTOCCELLI Rodrigo de Pinho; VENTURINI, Otávio (coord), Manual de Compliance – Rio de Janeiro. Forense. 2018.

BERTOCCELLI, Rodrigo de Pinho. Compliance. CARVALHO, André Castro; ALVIM, Tiago Cripa; BERTOCCELLI Rodrigo de Pinho; VENTURINI, Otávio (coord), Manual de Compliance – Rio de Janeiro. Forense. 2018.

RAMAKRISHNA, SALONI. Enterprise Compliance Risk Management. An Essential Toolkit for Banks and Financial Services. New Jersey: Wiley & Sons, 2015.

Disciplina: Ciber Crimes, Responsabilidade Penal e Civil

Ementa: Ciber criminologia e a fenomenologia dos delitos informáticos os reflexos da globalização no direito penal tradicional. A sociedade virtual do risco. A criminalidade complexa do século XXI. A engenharia social a serviço do crime. Regulação legislativa no âmbito penal nacional e internacional. Sobre ciber crimes. Breves considerações sobre a convenção internacional de budapest sobre cibercriminalidade. O tratamento legislativo no brasil relacionado aos delitos informáticos e a lei nº 12.737/2012 (lei carolina dieckman). A legislação penal mundial no combate e prevenção da delinquência informática. Conceito, características e a classificação dos ciber crimes. Conceito e evolução dos delitos informáticos. A classificação dos ciber crimes e o direito penal. O bem jurídico tutelado pelo direito penal. Tempo e lugar do crime. Dos crimes. Invasão ilegal à sistemas e dispositivos informáticos. A criação de vírus informático para fins ilícitos. O crime de pedofilia na internet e o estatuto da criança e do adolescente. Revenge porn ou sexting. A criminalização da fake news. Sequestro de dados na internet (ransomware). Dano informático.

Competências e Habilidades:

- Aprimorar a discussão acerca dos crimes virtuais.
- Abordar as consequências dos atos praticados no ambiente virtual - responsabilidade penal e civil.
- Capacitar o aluno a compreensão da fase de investigação de um ilícito virtual
- **Desenvolver a habilidade de produção de provas em ambiente virtual**

Conteúdo Programático 1: Cibercriminologia e a fenomenologia dos delitos informáticos. Os reflexos da Globalização no Direito Penal Tradicional. A Sociedade Virtual do Risco. A Criminalidade Complexa do Século XXI. A Engenharia Social a serviço do crime.

Conteúdo Programático 2: Regulação legislativa no âmbito penal nacional e internacional. Sobre cibercrimes. Breves considerações sobre a Convenção Internacional de Budapest sobre Cibercriminalidade. O tratamento legislativo no Brasil relacionado aos delitos informáticos e a Lei nº 12.737/2012 (Lei Carolina Dieckman). A legislação penal mundial no combate e prevenção da delinquência informática. Responsabilidade Penal e Civil.

Conteúdo Programático 3: Conceito, características e a classificação dos cibercrimes. Conceito e evolução dos Delitos Informáticos. A classificação dos Cibercrimes e o Direito Penal. O Bem Jurídico Tutelado pelo Direito Penal. Tempo e Lugar do Crime.

Conteúdo Programático 4: Dos crimes. Invasão ilegal à sistemas e dispositivos informáticos. A criação de vírus informático para fins ilícitos. O crime de pedofilia na Internet e o Estatuto da Criança e do Adolescente. Revenge Porn ou Sexting. A criminalização da Fake News. Sequestro de Dados na Internet (Ransomware). Dano informático.

Bibliografia Básica:

WENDT, Emerson. Direito e TI - CyberCrimes. Livraria do advogado. Rio de Janeiro:2019.

COLLI, Maciel. Cibercrimes. Limites e Perspectivas à Investigação Policial de Crimes Cibernéticos. Juruá. 2019.

BARRETO, Alessandro; BRASIL, Beatriz. Manual de Investigação Cibernética. À Luz do Marco Civil da Internet. Brasport. 2016

Bibliografia Complementar:

JORGE, Vigor Vinícios Nogueira. Investigação Criminal Tecnológica - Volume 1. Brasport. 2018.

NORAT, Markus, et. Al. Direito Digital. Responsabilidade Civil e Criminal na Internet. Clube dos Autores. 2018

BREWER, Russell, et. Al. Cybercrime Prevention: Theory and Applications. Palgrave Pivot; Edição: 1st ed. 2019

13. Infraestrutura Física e Pedagógica

O aluno encontrará todo o conteúdo do curso e assistirá às aulas gravadas no ambiente virtual. Para assistir às aulas é fundamental que as especificações abaixo sejam obedecidas, possibilitando, assim, uma recepção de maior qualidade dos vídeos.

Hardware:

- Processador Intel Core 2 Duo ou superior.
- 2Gb de Memória RAM.
- Placa de vídeo com resolução 1024x768, qualidade de cor 32 bits e compatível com Microsoft DirectShow.
- Microsoft DirectX 9.0c ou posterior.

Software:

- Navegador: Firefox, Google Chrome, Internet Explorer (sempre atualizado).
- Sistema Operacional: Windows XP ou posterior.

- Adobe Flash Player (atualizado).
- *Plugin* de vídeos SilverLigth (atualizado)

Rede:

- Conexão com a Internet banda larga de no mínimo 2 MB.
- Em caso de acesso em ambientes corporativos além da velocidade, é necessário verificar as condições de segurança de rede de sua empresa e se certificar que o site não estará bloqueado.

Adicionalmente, é prevista a utilização da biblioteca virtual para consultas bibliográficas e pesquisa de assuntos referentes às disciplinas ministradas.

