Desenvolvimento de Disciplinas / Cursos de curta duração para o Ensino Superior

Digitalização e Transição no Setor de Energia

(28/10/2020)

Nome da Disciplina:	Cibersegurança e ética de dados no Setor Elétrico
Carga horária recomendada	60 horas (4 horas/semana)
Competência geral (Que aptidão se espera do aluno/ profissional ao finalizar a disciplina/ o curso?)	Avaliar riscos de segurança cibernética e propor ações para reduzir riscos de ataques virtuais, considerando aspectos éticos de segurança de dados
Conhecimento prévios necessários (Requisitos de acesso)	✓ Conhecimentos básicos de algoritmos de programação (Python, Matlab) ✓ Conhecimento básicos de probabilidade, cálculo multivariável e álgebra linear ✓ Conhecimentos de sistemas elétricos de potência

Unidades de competência (Mais especificamente, quais são as principais aptidões e/ou conhecimentos que o aluno/ profissional deve desenvolver/ adquirir ao atender essa disciplina/ esse curso?)	Analisar e aplicar os conceitos principais de cibersegurança (malware, protocolos de conformidade)
	Avaliar riscos de segurança cibernética
	Propor ações para reduzir riscos de ataques virtuais com base na regulamentação vigente do setor elétrico, considerando aspectos éticos de segurança de dados
Funções/ Áreas de atividade (Quais as funções/ atividades se espera que esse aluno/ profissional desenvolva com qualidade após atender essa disciplina/ esse curso?)	Engenheiro de projeto e/ou de operação de sistemas elétricos
	Coordenação de centro de operação

Capacidades técnicas (Tendo em vista as unidades de competência e funções/ áreas de atividade, que habilidades técnicas devem ser desenvolvidas no aluno/ profissional durante o atendimento a essa disciplina/ esse curso?) * Uma capacidade técnica pode exigir mais de um conhecimento	**Conhecimentos** (Conteúdos que deverão ser abordados na disciplina/ no curso para o desenvolvimento da respectiva capacidade técnica)
1 Analisar e aplicar os conceitos principais de cibersegurança (malware, protocolos de conformidade)	1.1 Apresentação de conceitos de cibersegurança e de vulnerabilidade 1.2 Visão sistêmica do setor elétrico com identificação de fontes de dados e seus potenciais riscos de segurança (IoT, Cloud Computing) 1.3 Padrões de protocolos de conformidade e de comunicação (sistemas SCADA) e IEDs (Intelligent Electronic Devices) 1.4 Proteção contra malware (Virus, Worms, spyware, trojans, etc.)
2 Avaliar riscos de segurança cibernética, ética e uso de dados	2.1 Reconhecimento e análise de vulnerabilidades 2.2 Regulamentação relacionada a uso e segurança de dados (normas de segurança nacionais e internacionais, Lei LPGD 13.709 de 2018, EU GDPR 2016/679) 2.3 Compreensão dos aspectos éticos do uso e manipulação de dados (tratamento de dados pessoais, criptografia) 2.4 Certificação de segurança de hardwares 2.5 Avaliação dos riscos de segurança nos sistemas de comunicação e interface de transferência de dados
3 Propor ações para reduzir riscos de ataques virtuais com base na regulamentação vigente do setor elétrico, considerando aspectos éticos de segurança de dados	3.1 Aplicações para melhoria de segurança de hardware (certificação de seguranças) e de infraestrutura 3.2 Ações para redução de riscos de Cibersegurança (SQL Injection, XSS, Aurora, DoS, man-in the middle, Bus sniffer, etc). 3.3 Requisitos e sistemas de monitoramento para inibir manipulação de dados, por exemplo relacionado a consumo de energia

Infraestrutura necessária (Equipamentos/ Laboratórios/ Materiais específicos que a instituição deve ter para ofertar a disciplina/ o curso)	Laboratório de informática com rede para simulação de ataques cibernéticas
	Simuladores de software com uso de bibliotecas (Python, R, Matlab, Mathworks)

Bibliografia (Livros/ Artigos/ Apostilas que podem ser utilizados pelos docentes para ministrar a disciplina/ o curso)	Brooks, C. j. / Cybersecurity Essentials / 2018
	Kim, D. / Fundamentos de Segurança de Sistemas de Informação / 2014
	Brown, L. / Segurança de computadores / 2013