PROGRAMA DE CURSO
CIBERSEGURIDAD APLICADA A REDES ELÉCTRICAS

A. Antecedentes generales del curso:

Departamento	Ingeniería Eléctrica (DIE)					
Nombre del curso	Ciberseguridad aplicada a Redes Eléctricas		Código	EL6051	Créditos	6
Nombre del curso en inglés	*Cybersecurity applied to Electrical Networks*					
Horas semanales	Docencia	4	Auxiliares	--	Trabajo personal	6
Carácter del curso	Electivo Línea de especialización					
Requisitos	EL4103: Sistemas de energía y equipos eléctricos					

B. Propósito del curso:

El curso de "Ciberseguridad aplicada a las Redes Eléctricas" tiene como principal propósito que los estudiantes apliquen e implementen en el diseño de redes eléctricas los fundamentos de la ciberseguridad y, asimismo analizar las vulnerabilidades y amenazas cibernéticas que afectan hoy en día en los ámbitos de las tecnologías de la información (TI) y tecnologías operacionales (TO), y el estudio de metodologías, marcos normativos y mejores prácticas en ciberseguridad para la identificación, protección, detección, respuesta y recuperación de incidentes de ciberseguridad en entornos industriales.

Para aplicar los conocimientos entregados en el curso se espera que durante el curso los(as) estudiantes realicen un análisis del estado del arte referente a ciberataques industriales a Infraestructuras Críticas o ciberataques a dispositivos Industriales TO, que hayan comprometido equipos o plataformas (Scada, PLC´s, HMI, válvulas, motores, etc.) del sector eléctrico u otros sectores afines, se identifiquen las vulnerabilidades y amenazas, modelen las causas e impactos del problema de ciberseguridad y luego presenten una solución de protección, detección y respuesta temprana ante incidentes de ciberseguridad, basado en metodologías, marcos normativos y mejores prácticas vistos en clases con una visión holística de la solución a la problemática.

El curso tributa a las siguientes competencias específicas (CE) y genéricas (CG):

CE2: Concebir y aplicar conocimientos de ciencias físicas y matemáticas para el desarrollo de soluciones tecnológicas a problemáticas de la Ingeniería Eléctrica y áreas afines.

CE4: Concebir, diseñar y evaluar, dispositivos, sistemas y desarrollos científico- tecnológicos para la solución de problemas en el ámbito de la Ingeniería Eléctrica, considerando especificaciones técnicas, así como requerimientos económicos, ambientales, sociales y éticos.

CG1: Comunicación académica y profesional

Comunicar en español de forma estratégica, clara y eficaz, tanto en modalidad oral como escrita, puntos de vista, propuestas de proyectos y resultados de investigación fundamentados, en situaciones de comunicación compleja, en ambientes sociales, académicos y profesionales.

CG4: Trabajo en equipo Trabajar en equipo, de forma estratégica y colaborativa, en diversas actividades formativas, a partir de la autogestión de sí mismo y de la relación con el otro, interactuando con los demás en diversos roles: de líder, colaborador u otros, según requerimientos u objetivos del trabajo, sin discriminar por género u otra razón.

C. Resultados de aprendizaje:

Competencias específicas	Resultados de aprendizaje
CE2	RA1. Investiga el estado del arte en ciberseguridad relacionado con amenazas y vulnerabilidades cibernéticas presentes en ataques cibernéticos a infraestructuras críticas (utilities), considerando el caso que se le presenta, a fin de resolver problemas asociados al mismo.
CE4	RA2. Modela e implementa, utilizando fundamentos de ciberseguridad, enfoques metodológicos (NIST, Mitre Attack, entre otros), cuadros normativos (NERC-CIP, ISA/IEC 62443, ISO 27001, entre otros) y mejores prácticas (CIS Control, SANS Institute, INCIBE, entre otros) para el diseño de soluciones de ciberseguridad en el ámbito industrial en sistemas eléctricos.
Competencias genéricas	**Resultados de aprendizaje**
CG4	RA3: Trabaja en equipo, para proponer una solución a un caso que se le presenta, aplicando el conocimiento producto de las investigaciones realizadas, a partir de la autogestión de sí mismo y de la relación con el otro, interactuando con los demás en diversos roles:
CG1	RA4: Redacta informes de investigación y realiza presentaciones orales, relacionadas con una problemática de ciberseguridad aplicada a redes eléctricas, expresando de manera efectiva, clara y precisa los resultados obtenidos en cada fase de la investigación realizada a fin de comunicar dichos resultados.

D. Unidades temáticas:

Número	RA al que tributa	Nombre de la unidad	Duración en semanas
1	RA1, RA2	Fundamentos de Ciberseguridad	3 semanas
Contenidos		**Indicador de logro**	
1.1. Principales conceptos de Seguridad de la Información, Ciberseguridad Industrial y Protección de Datos y Datos Personales. 1.2. Principales normativas, mejores prácticas y metodologías para la aplicación de controles y soluciones en Ciberseguridad para redes TI/OT. 1.3. Definición de Infraestructuras Críticas de la Información.		El/la estudiante: 1. Aplica los principales conceptos de la Ciberseguridad para la Gestión de Riesgos, Gobernanza, Cumplimiento Normativo y Continuidad del Negocio en aplicaciones en Ingeniería Eléctrica. 2. Analiza las diferencias entre las diferentes normativas y enfoques metodológicos en ciberseguridad (ISO 27001, NIST, NERC-CIP, ISA/IEC 62443, entre otros) para su aplicación en la Ingeniería Eléctrica. 3. Evalúa los planes de infraestructuras críticas de países como USA y España, así como la Política Nacional de Ciberseguridad en Chile para entender el grado de importancia de la Ciberseguridad.	
Bibliografía de la unidad		[1], [3]	

Número	RA al que tributa	Nombre de la unidad	Duración en semanas
2	RA1, RA2	Introducción a las Redes Eléctricas Inteligentes Seguras	4 semanas
Contenidos		**Indicador de logro**	
2.1. Análisis de Entorno: Industria 4.0 y Transformación Digital en el Sector Eléctrico. 2.2. Definición de Smart Grid y Principales Componentes de una Smart Grid Segura. 2.3. Tecnologías Avanzadas aplicadas a una Smart Grid Segura. 2.4. Aplicaciones y Casos de uso de Smart Grid Seguras.		El/la estudiante: 1. Evalúa los principales componentes, elementos y características de una Arquitectura Smart Grid Segura. 2. Analiza las principales tecnologías TIC habilitantes en una Arquitectura Smart Grid Segura (Inteligencia Artificial, Big Data, 5G, Blockchain). 3. Analiza y deduce las principales aplicaciones y casos de uso en Smart Grid Segura en: Smart Metering, Electromovilidad, Smart Cities, Microgrids, etc.	
Bibliografía de la unidad		[2], [4]	

Número	RA al que tributa	Nombre de la unidad	Duración en semanas
3	RA1, RA2,	Amenazas y Vulnerabilidades Cibernéticas	4 semanas
Contenidos		**Indicador de logro**	
3.1. Tipos de vulnerabilidades en TI/TO. 3.2. Tipos de amenazas y técnicas de hackeo en ambientes TI/TO. 3.3. Equipos de Respuesta ante Incidentes de Seguridad (CSIRT). 3.4. Técnicas y Herramientas de Ciberinteligencia aplicadas al mundo industrial.		El/la estudiante: 1. Analiza y deduce las principales Vulnerabilidades de Ciberseguridad en Ambientes Industriales. 2. Deduce las principales amenazas cibernéticas, tipos de malwares (ramsomware, pishing, SQL injection, etc.), técnicas de hackeo (man in the middle, DDoS, etc) y principales ataques cibernéticos (Stuxnet, BlackEnergy, Indutroyer, WannaCry, etc 3. Evalúa diferentes equipos de respuesta ante incidentes de ciberseguridad basado en mejores prácticas a nivel de: recursos humanos, roles, infraestructura tecnológica, modelos de entrenamiento (Blue/Red Team) y procesos para hacer frente a ataques cibernéticos. 4. Analiza las herramientas y metodologías de Inteligencia de Amenazas (Ciberinteligencia) aplicadas a la Ciberseguridad.	
Bibliografía de la unidad		[1], [4]	

Número	RA al que tributa	Nombre de la unidad	Duración en semanas
4	RA1, RA2, RA3, RA4	Principales Contramedidas, Herramientas y Servicios Consultivos en Ciberseguridad	4 semanas
Contenidos		**Indicador de logro**	
4.1. Principales Contramedidas en una Arquitectura de Defensa en Profundidad y Zero Trust en el modelo de referencia Purdue (ISA 95). 4.2. Herramientas de Gestión y Simulación de Ciberseguridad. 4.3. Principales Servicios Consultivos en Ciberseguridad: Ethical Hacking (tipos), Pentesting, Risk Assessment, Análisis Forense, Planes de Concienciación entre otros.		El/la estudiante: 1. Diseña las principales soluciones de contramedidas aplicadas a las distintas capas de una Arquitectura de Ciberseguridad convergente TI/TO segura y confiable. 2. Modela las principales herramientas de gestión y simulación de un SOC (Security Operation Center) y SOC Integrado para Infraestructuras Críticas. 3. Aplica Contramedidas, Herramientas y Servicios Consultivos a un problema específico de ciberseguridad en el proyecto del curso y analiza su efecto en la mitigación del riesgo informático e industrial. 4. Evalúa los principales controles de ciberseguirdad en entornos industriales del sector eléctrico, de tal manera de incorporarlo. al diseño de un proyecto	

	Smart Grid Seguro (Smart Metering, Microgrids, Subestaciones Digitales, etc). 5. Trabaja en equipo en la selección de un caso a investigar, logrando demostrar el conocimiento desarrollado, la responsabilidad, respeto hacia el otro, así como el manejo de conflictos, estrés e incertidumbre, alcanzando acuerdos. 6. Redacta un informe escrito de manera clara y concisa, con lenguaje técnico, asimismo presenta las principales conclusiones de manera oral.
Bibliografía de la unidad	[3], [4]

E. Estrategias de enseñanza - aprendizaje:

La metodología de trabajo para conseguir los resultados planteados para el proceso de enseñanza—aprendizaje está basada en la participación activa de los estudiantes. Las principales actividades para realizar son:

- Análisis de casos
- Clase expositiva.
- Investigación
- Análisis de artículos

F. Estrategias de evaluación:

La evaluación estará orientada a verificar avances de parte de los estudiantes y demostración de resultados de aprendizaje mediante:

Tipo de evaluación	Resultado de aprendizaje asociado a la evaluación	Ponderación
▪ Trabajo de investigación, basados en casos que se le presentan para analizar. 1.1 Presentaciones orales. 1.2 Elaboración de informes.	RA1, RA2, RA3, RA4	50%
▪ Trabajo de Análisis de casos de manera individual.	RA1, RA2	50%

Al inicio de cada semestre, el cuerpo académico informará sobre los tipos de evaluación, la cantidad y las ponderaciones correspondientes.

G. Recursos bibliográficos:

Bibliografía obligatoria:

[1] Cybersecurity Fundamentals Glossary, ISACA, 2016.
[2] Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82 Revision 2, May 2015.
[3] Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, NIST, April 16, 2018.
[4] Libro Ciberseguridad Industrial e Infraestructuras Críticas, Fernando Sevillano, Ra-Ma Editorial, 2021.

Bibliografía complementaria:

[5] Zero Trust Architecture, NIST Special Publication 800-207, August 2020.
[6] Guidelines for Planning an Integrated Security Operations Center, EPRI, December 2013.
[7] NISTIR 7628 Revision 1, Guidelines for Smart Grid Cybersecurity.
[8] Política Nacional de Ciberseguridad, agosto 2017, Ministerio del Interior, Chile
[9] Estándar de Ciberseguridad para el Sector Eléctrico, Publicación Coordinador Eléctrico Nacional, octubre 2020.
[10] Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), Version 1.1 February 2014, DOE-DHS, USA.
[11] Plan Director de Ciberseguridad para el Sector Eléctrico 2021 – 2023, Cigré Chile, Agosto 2020.
[12] National Energy Security Strategy, July 2015, Presidencia del Gobierno, España.
[13] Technical Brochure: Cybersecurity: Future threats and impact on electric power utility organizations and operations, Reference: 796, WG D2.46_CIGRE, March 2020.
[14] Technical Brochure: Electric Power Utilities' Cybersecurity for Contingency Operations, Reference: 840, WG D2.50_CIGRE, June 2021.
[15] ENISA Report - How to setup up CSIRT and SOC, December 2020.
[16] Ten Strategies of a World-Class Cybersecurity Operations Center, MITRE, Carson Zimmerman, 2014.
[17] G DATA Whitepaper, El nuevo Reglamento de Protección de Datos de la UE (GDPR) – Lo que las empresas deben saber, septiembre 2017.
[18] Anexo Técnico: Sistemas de Medición, Monitoreo y Control, CNE, agosto 2019.
[19] Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies Industrial Control Systems Cyber Emergency Response Team, September 2016, Homeland Security.
[20] Glosario de Términos de Ciberseguridad, INCIBE, España, 2017.
[21] ENISA Baseline security recommendations for IoT in the context of Critical Information Infraestructure.

H. Datos generales sobre elaboración y vigencia del programa de curso:

Vigencia desde:	Diciembre del 2021
Elaborado por:	Eduardo Morales Cabello
Validado por:	Comité Técnico Docente DIE
Revisado por:	Área de Gestión Curricular- Académicos del área de Energía DIE