Universidad Tecnológica Nacional
Facultad Regional Buenos Aires

ANEXO I

RESOLUCIÓN Nº...../21

ASIGNATURA:	CIBERSEGURIDAD INDUSTRIAL	**CÓDIGO:**	
DEPARTAMENTO:	INGENIERÍA EN SISTEMAS DE INFORMACIÓN	**CLASE:**	Cuatrimestral
ÁREA:	INGENIERÍA EN SISTEMAS DE INFORMACIÓN	**HORAS SEM.:**	6 hs.
BLOQUE:	ELECTIVAS	**HORAS / AÑO:**	Reloj 72hs./ Cátedra 96hs

Fundamentación:

En esta última década, la evolución hacia un mundo cada vez más interconectado e interdependiente, propone que el nuevo desafío de los responsables de Sistemas y Seguridad de la Información (CIO (Chief Information Officer), CISO (Chief Information Security Officer) y CIRO (Chief Information Risk Officer)) sea la integración y convergencia de estos mundos, respetando las características y necesidades del mismo (de allí nace el nuevo concepto de Ciberseguridad Industrial). Actualmente, este concepto, está reconocido y avalado por diversas organizaciones internacionales, incluyendo la UE (Unión Europea) y el DHS (Department of Homeland Security), quienes impulsan diversas normativas y apoyan a organizaciones varias especializadas en el tema.

La Ciberseguridad es una rama de especialización dentro de la Tecnología de la información y su proyección sobre el mundo OT tiende a crear una nueva especialidad orientada a los procesos industriales. El Ingeniero en sistemas de información tiene el desafío de cubrir el crecimiento exponencial de las tecnologías de la información hacia otras áreas como por ejemplo, la tecnología de las operaciones, la Ciberseguridad en convergencia IT-OT y conectividad a Internet.

Los sistemas industriales existen desde hace décadas y siempre han sido vistos de forma reticente por las Gerencias de Sistemas y de IT debido a sus diferencias en la evolución, en la necesidad y metodología para instalar actualizaciones, parches y modificaciones que no son con la misma frecuencia y bajo el mismo paradigma que se acostumbra en el mundo de TI.

La necesidad de conexión con el mundo financiero de TI, accesos remotos para monitoreo, mantenimiento y operación y la ineludible unión e interconectividad al mundo de Internet, ha evidenciado y potenciado la necesidad de aplicar la madurez obtenida en Seguridad de la Información a las Tecnologías de la Operación (OT por sus siglas en inglés).

A diferencia del mundo de IT, en OT, cualquier acción no deseada puede provocar daños a las personas en forma directa (a diferencia de los sistemas que IT acostumbra operar). Los sistemas industriales siguen funcionando sobre sistemas operativos antiguos y hasta EOS (end of support) ya que uno de sus axiomas es no tocar aquello que funciona. Por ejemplo, hay sistemas productivos bajo Windows 98 que ni siquiera poseen antivirus y tampoco se puede reiniciar porque se requeriría, para el proceso de producción industrial, parar una planta entera.

Los futuros profesionales deberán abordar la convergencia con este mundo industrial con el actual de IT y para ello es necesario comprender sus necesidades y características básicas que difieren de las del mundo TI, pero que a la vez necesitan de la experiencia y madurez adquirida en estos años y que el mundo OT no posee. Este nuevo campo representa, no solo un desafío para el nuevo ingeniero, sino la puerta de acceso a la industria 4.0 del IoT y del IIoT (Internet of Thing e Industrial Internet of Things).

Objetivos:

Identificar los rudimentos de sistemas y procesos industriales.
Distinguir sistemas industriales de los tradicionales de TI (OT (Tecnología Operacional) vs. IT (Tecnología de la Información)).
Reconocer la importancia de la CiberSeguridad en los sistemas industriales desde una perspectiva analítica, crítica y reflexiva en una realidad hiperconectada.
Reconocer las principales vulnerabilidades de los sistemas industriales y su entorno.
Distinguir procesos y sectores industriales de una organización junto a sus requerimientos y necesidades en CiberSeguridad.
Aplicar normas COBIT5, ISO27000, ISA95, IEC 62443 (ISA99) en CiberSeguridad industrial.
Reconocer el modelo de marco normativo para gobernar la CiberSeguridad industrial en una organización.
Aplicar herramientas de control y cumplimiento de la CiberSeguridad industrial en las organizaciones.

Programa analítico:

Unidad I – Rudimentos de Sistemas Industriales.
Presentación de sus componentes (PLC, sensores, actuadores, DCS, HMI, PCS, SCADA, etc.) Definiciones. Terminología, Conceptos y Modelos. Arquitecturas. Repaso de conceptos de Redes (TCP/IP, Modelo OSI). Protocolos de comunicaciones industriales (MODBUS, ProfiBus, DNP3, OPC, etc).
Logros pedagógicos: El estudiante será capaz de comprender y reconocer los sistemas industriales y sus dispositivos y partes.

Unidad II – Introducción a la CiberSeguridad industrial.
¿Qué entendemos por Ciberseguridad Industrial? Control y Triada de seguridad industrial (Disponibilidad, Integridad, Confidencialidad). Diferencias entre los mundos de OT (Operation Technology) e IT. Historia y Contexto Nacional e Internacional. Entidades especializadas. Ampliación del mundo de IT hacia una convergencia con el de OT.
Logros pedagógicos: El estudiante será capaz de reconocer diferencias frente al mundo conocido de IT y entender las diferencias de necesidades.

Unidad III – Principales Normativas de referencia
Normas internacionales de Seguridad de la información (ISO27000, COBIT5). Normas internacionales de Ciberseguridad Industrial (ISA95, ISA99/IEC62443). Estructura. Marco normativo. Glosario. Gestión de la CiberSeguridad industrial. Selección y Políticas para el Personal de Operación.
Logros pedagógicos: El estudiante conocerá las normas más importantes internacionales y será capaz de comprender y reconocer las mismas con aplicación práctica en los sistemas industriales.

Unidad IV – Norma Internacional IEC62443 (ISA99)
Estructura. Definiciones. Terminología, Conceptos y Modelos. Desarrollo de los principales documentos del estándar ISA99. Roles y Responsabilidades de los Vendors, Owners, Partners, Solution Suppliers. Zonas y conductos. Niveles de seguridad. Requerimientos y recomendaciones.
Logros pedagógicos: El estudiante hará foco en la norma más importante del mercado, conocerá a fondo su estructura, será capaz de entenderla y estará listo para poder aplicarla en el mundo real.

Unidad V – Sistema de Gestión de CiberSeguridad Industrial
Definición de una estrategia de CiberSeguridad industrial. Inventario. Análisis de procesos e interdependencias. Gestión de riesgos. Difusión y concientización de cultura en CiberSeguridad industrial. Normas y cumplimiento. Continuidad de la operación. Revisión, Mejora y sustentabilidad de la gestión.
Logros pedagógicos: El estudiante empezará a aplicar los conocimientos de las unidades anteriores en el marco de un sistema de gestión de ciberseguridad. Esto le permitirá empezar a unir el mundo teórico y normativo con el real.

Unidad VI – Aplicación en entorno corporativo
Modelo de Marco Normativo basado en normas internacionales. Política. Normas Generales y Verticales por negocios. Concepto de propiedad de activos de información. Clasificación de la Información. Homologaciones y arquitecturas (incluyendo infraestructura, aplicaciones, base de datos, etc.). Gobierno, Control y cumplimiento en la Gestión de Seguridad basado en dominios.
Logros pedagógicos: El estudiante continuará con aplicaciones prácticas viendo ejemplos de marcos normativos de gobiernos y corporativos. Estos le darán visión del mundo real y el estado actual de la industria.

Unidad VII – Trabajo de aplicación
Herramientas y conceptos de CiberSeguridad aplicados (Firewall, IDS/IPS, SIEM, WAF, accesos remotos, antimalware, etc).
Logros pedagógicos: El estudiante volcará en este trabajo los conceptos y conocimientos teóricos llevados a un caso práctico y produciendo un análisis de situación actual y un plan de mejoras y remediaciones.

Distribución de carga horaria entre actividades teóricas y prácticas:

Tipo de actividad	Carga horaria total en hs. reloj	Carga horaria total en hs. cátedra
Teórica	51,75	69
Formación practica	20.25	27
Formación experimental	0	0
Resolución de problemas	0	0
Proyectos de diseño	0	0
Practica de supervisada	0	0
Total	72	96

Articulación Horizontal y vertical con otras materias

La asignatura Ciberseguridad Industrial se articula en forma vertical con disciplinas técnicamente relacionadas y que la preceden en el plan de estudio como, Redes de Información, Comunicaciones y Seguridad en Redes. Desde el punto de vista operacional con Teoría de Control. Cada estudiante deberá tener cursada y regularizada cada una de estas asignaturas al momento de comenzar la cursada ya que brindan los conocimientos mínimos necesarios para afrontar el estudio de equipos y dispositivos de la tecnología de la operación (OT), SCADA, PLC, HMI, etc. que son conocimientos que se dan durante la materia.
En cuanto a la articulación horizontal, la ciberseguridad industrial brinda conocimientos que son compatibles y complementarios con conceptos y contenidos de otras asignaturas, y de aplicación cruzada en el mundo actual de IT y de OT, relacionados a la prevención, vigilancia, monitoreo y resiliencia de los activos de una organización y de la privacidad de datos de las personas.

Cronograma estimado de clases:

Unidad temática	**Duración en horas cátedra**
Unidad 1 - Clase 1: Rudimentos de Sistemas Industriales	6 horas
Unidad 1 – Clase 2: Rudimentos de Sistemas Industriales	6 horas
Unidad 2 – Clase 3: Introducción a la CiberSeguridad industrial.	6 horas
Unidad 2 – Clase 4: Introducción a la CiberSeguridad industrial.	6 horas
Unidad 3 – Clase 5: Principales Normativas de referencia	6 horas
Unidad 3 y 4 – Clase 6: Principales Normativas de referencia. Norma Internacional IEC62443 (ISA99)	6 horas
Unidad 4 – Clase 7: Norma Internacional IEC62443 (ISA99) Revisión Integral	6 horas
Clase 8: Evaluación 2do parcial	**6 horas**
Unidad 5 – Clase 9: Sistema de Gestión de CiberSeguridad Industrial	6 horas
Unidad 6 – Clase 10: Aplicación en entorno corporativo. Armado de Equipos y propuesta de temas p/TP	6 horas
Unidad 6 y 7 – Clase 11: Aplicación en entorno corporativo. Asignación de TP	6 horas
Unidad 7 – Clase 12:	6 horas

Unidad 7 – Clase 13:	6 horas
Unidad 7 -- Clase 14:	6 horas
Clase 15: Evaluación 2do parcial	**6 horas**
Clase 16: Entrega de TP	6 horas

Bibliografía:

-Betty Biringer, Eric Vugrin, Drake Warren (2013). Critical Infrastructure System Security and Resiliency,, CRC Press.
-Robert Radvanovsky, Jacob Brodsk (2013). Handbook of SCADA/Control Systems Security,y, CRC Press.
-Ronald L. Krutz PhD (2017) Industrial Automation and Control System Security Principles, Protecting the Critical Infrastructure.
-Tyson Macaulay, Bryan L. (2011). Singer Cybersecurity for Industrial Control Systems: SCADA, DCS, --PLC, HMI, and SIS,, Auerbach Publications.
(S/F). Norma ISO 27000, COBIT5, ISA95, ISA99, IRAM 17550, IEC 62443, ISA99 IACS.

PÁGINAS WEB DE INTERÉS

-HOMELAND SECURITY https://www.dhs.gov/
-Norma IEC62443 http://isa99.isa.org/ISA99%20Wiki/Home.aspx ISA99
-Centro de Ciberseguridad Industrial https://www.cci-es.org/
-National Institute Standards Tecnologies https://www.nist.gov/
-North American Electric Reability Corp http://www.nerc.com/Pages/default.aspx
-Agencia Europea de Seguridad de Redes y de Información https://www.enisa.europa.eu/
-Centro Criptológico Nacional Computer Emergency Response Team https://www.ccn-cert.cni.es/
-ICS- CSIRT USA https://us-cert.cisa.gov/ics
-Cibersecurity & Infraestructure Security Agency https://us-cert.cisa.gov/ics
-Centro de Ciberseguridad Industrial http://www.cci-es.org

Correlativas:

PARA CURSAR:

Cursadas: Administración de recursos
Redes de información
Simulación
Ingeniería de software

Aprobadas: Diseño de sistemas
Sistemas operativos
Gestión de datos

Universidad Tecnológica Nacional
Facultad Regional Buenos Aires

PARA RENDIR:

Aprobadas: Administración de recursos
ingeniería en software
Redes de información
Simulación