UTN.BA
DEPARTAMENTO
INGENIERIA EN SISTEMAS DE INFORMACION

ASIGNATURA:	CIBERSEGURIDAD INDUSTRIAL
DEPARTAMENTO:	ING. EN SIST. DE INFORMACION
AREA:	ELECTIVAS
BLOQUE	TECNOLOGÍAS APLICADAS

MODALIDAD:	Cuatrimestral
HORAS SEM.:	6 horas
HORAS/AÑO:	96 horas
HORAS RELOJ	72
NIVEL:	5º
AÑO DE DICTADO:	2018

Objetivos

- Conocer y entender los rudimentos de sistemas y procesos industriales.
- Comprender las diferencias y similitudes de los sistemas industriales con los sistemas tradicionales de TI (mundos OT (Tecnología Operacional) vs IT (Tecnología de la Información))
- Desarrollar concientización acerca de la importancia de la CiberSeguridad en los sistemas industriales.
- Desarrollar en el alumno una actitud analítica, crítica y reflexiva respecto de la CiberSeguridad industrial en una realidad hiperconectada.
- Comprender la ampliación de entorno y alcance de la seguridad de la información hacia la convergencia con sistemas industriales que interactúan con procesos reales.
- Comprender las principales vulnerabilidades de los sistemas industriales y sui entorno.
- Comprender las implicancias de los ciber-riesgos que afectan a directamente a las vidas humanas.
- Reconocer los distintos procesos y sectores industriales de una organización y sus particulares requerimientos y necesidades en CiberSeguridad.
- Conocer y saber utilizar las principales normas de CiberSeguridad (COBIT5, ISO27000, ISA95), comprender y explicar en profundidad la IEC 62443 (ISA99) en CiberSeguridad industrial.
- Comprender y conocer un modelo de marco normativo para gobernar la CiberSeguridad industrial en una organización.
- Incorporar las herramientas necesarias para el control y cumplimiento de la CiberSeguridad industrial en las organizaciones y la coordinación de sus distintos sectores.

Contenidos Mínimos (Programa Sintético).

- Conceptos de sistemas industriales y su CiberSeguridad. Necesidades específicas.
- Nociones básicas de arquitectura de sistemas industriales y sus procesos básicos
- Contenidos básicos de normas internacionales de seguridad de la información. Especial desarrollo de la Norma IEC62443 en CiberSeguridad industrial
- Organización de una Gerencia de Seguridad de la Información en una empresa con procesos industriales
- Detección de vulnerabilidades, riesgos y amenazas. Prevención y acciones correctivas.
- Como confeccionar un marco normativo a medida de la Organización basado en sus procesos
- Gobierno, Control y cumplimiento (GRC) en CiberSeguridad industrial.

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).

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.

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.

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.

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.

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.

Unidad VII: Trabajo de aplicación

Herramientas y conceptos de CiberSeguridad aplicados (Firewall, IDS/IPS, SIEM, WAF, accesos remotos, antimalware, etc).

Realizar un trabajo práctico analizando un escenario propuesto en base a los contenidos dados.

Bibliografía

- Norma ISO 27000, COBIT5, ISA95, ISA99, IRAM 17550, etc.
- IEC 62443, ISA99 IACS
- Documentos y trabajos publicados por distintas entidades especializadas en el tema, entre otras:

  https://www.dhs.gov/ HOMELAND SECURITY
  http://isa99.isa.org/ISA99%20Wiki/Home.aspx ISA99 Norma IEC62443
  https://www.cci-es.org/ Centro de Ciberseguridad Industrial
  https://www.nist.gov/ National Institute Standards Tecnologies
  http://www.nerc.com/Pages/default.aspx North American Electric Reability Corp
- Material Didáctico desarrollado por la cátedra

Correlativas

Para Cursar:

Cursadas:

- Administración de Recursos
- Redes de Información
- Simulación
- Ingeniería de Software

Aprobadas:

- Diseño de Sistemas
- Sistemas Operativos
- Gestión de Datos

Para rendir:

Aprobadas:

- Administración de Recursos
- Redes de Información
- Simulación
- Ingeniería de Software