UNIVERSIDAD DE SONORA
Unidad Regional Centro
División de Ingeniería
Departamento de Ingeniería Industrial
LICENCIATURA INGENIERÍA EN MECATRÓNICA

Nombre de la Asignatura: CIBERSEGURIDAD INDUSTRIAL					
Clave:	**Créditos:** 8	**Horas totales:**80	**Horas Teoría:** 2	**Horas Práctica:** 4	**Horas Semana:** 5
Modalidad: Presencial			**Eje de formación:** Especializante		
Elaborado por: DR. VÍCTOR HUGO BENÍTEZ BALTAZAR**,** DR. CARLOS FIGUEROA NAVARRO					
Antecedente:			**Consecuente:**		
Carácter: Optativa			**Departamento de Servicio:** Ingeniería industrial		

Propósito:

La asignatura pertenece al eje especializante y es de carácter optativa. El principal propósito es proporcionar a los estudiantes los aspectos fundamentales y básicos para analizar los riesgos y vulnerabilidades que integran los ciber entornos industriales, asi como lograr tener capacidad técnica de determinar acciones para mitigar estos riesgos.

I. Contextualización

Introducción:

Esta materia hace una introducción a la ciber seguridad industrial e infraestructura crítica mediante el concepto ICS (Industrial CyberSecurity). La idea es que el Ingeniero en Mecatrónica pueda conocer la tecnología que se ocupa de analizar los riesgos y vulnerabilidades que integran los ciber entornos industriales y pueda determinar acciones para mitigar estos riesgos.

Según la definición estándar la ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciber entorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios y los sistemas de comunicaciones.

Esta área del conocimiento es relativa a la seguridad de tecnologías de la información, que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software (bases de datos, metadatos, archivos), hardware. Las unidades didácticas del curso son:

la Unidad didáctica I trata de las definiciones importantes de ciberespacio e infraestructuras inteligentes también se presenta el modelo de amenazas para infraestructuras inteligentes. también se incluye los estándares, marcos de gestión y tecnologías aplicables.

En la Unidad didáctica II se estudia la superficie de ataque en infraestructuras inteligentes. La idea es saber cómo utilizar técnicas de desarrollo que cumplan con los criterios de seguridad en el uso para todo tipo de software.

En la Unidad didáctica III se analiza el desarrollo de aplicaciones robustas. El fin se saber cómo diseñar sistemas a

prueba de ataques con alto grado de confiabilidad, donde sistema debe realizar un seguimiento en tiempo real.	
Perfil del(los) instructor(es):	Poseer Licenciatura en Ingeniería en Mecatrónica o ingeniería en sistemas de información Preferentemente con grado académico de maestría o especialidad Con experiencia docente y desarrollo profesional comprobada cuando menos de dos años en el campo de la materia.

II. Competencias a lograr

Competencias genéricas a desarrollar:

- **Capacidadde aprendery actualizarse permanentemente.** Articula saberes de diversos campos y
- Establece relaciones entre ellos y su vida cotidiana.
- **Trabajo colaborativo.** Asume una actitud constructiva, congruente con los conocimientos y habilidades con los que cuenta dentro de distintos equipos de trabajo.
- **Capacidadparala toma dedecisiones.** Evalúa y sopesa información importante para identificar los aspectos relevantes. Define la prioridad para la solución del problema en términos de impacto y urgencia.
- **Capacidad para realizar investigación básica y aplicada.** Identifica los sistemas y reglas o principios medulares que subyacen a una serie de fenómenos.
- **Competencia Digital.** Aplica herramientas digitales para el pensamiento reflexivo, la creatividad y la innovación.

Competencias específicas:

- HABILIDAD PARA UTILIZAR PROTOCOLOS DE COMUNICACIÓN DE DATOS PARA APLICACIONES INDUSTRIALES.
  - Resolver problemas dentro del área de seguridad informática y de las comunicaciones. Proponer soluciones en el entorno industrial y empresarial en el campo de la ciberseguridad. Aplicar los conceptos de ciberseguridad para proteger de manera autónoma la recolección de datos y la ejecución de instrucciones a bajo nivel.

Objetivo General:

Obtener una visión global de la ciberseguridad y la ciber inteligencia, así como aprender a diseñar e implementar sistemas seguros de acceso y transmisión de datos; detectar y responder ante incidentes de seguridad informática.

Objetivos Específicos:

1. Adquirir conocimientos sobre los aspectos generales de la protección de infraestructuras críticas y la ciberseguridad Industrial
2. Adquirir los conocimientos de los diferentes tipos de técnicas para asegurar el sistema, así como utilizar técnicas de desarrollo.
3. Diseñar sistemas robustos de alta confiabilidad cibernética.

Unidades Didácticas:
Unidad Didáctica I – DEFINICIONES IMPORTANTES DE CIBERESPACIO E INFRAESTRUCTURAS INTELIGENTES
Unidad Didáctica II – SUPERFICIE DE ATAQUE EN INFRAESTRUCTURAS INTELIGENTES
Unidad Didáctica III–DESARROLLO DE APLICACIONES ROBUSTAS

III. Didáctica del programa

Unidades Didácticas:

Unidad didáctica I. Definiciones importantes de ciberespacio e infraestructuras inteligentes
En la unidad I, el alumno adquiriere conocimientos sobre los aspectos generales de la protección de infraestructuras críticas y la ciberseguridad Industrial, también se incluye los estándares, marcos de gestión y tecnologías aplicables.

- Introducción
- Términos y conceptos generales
- Estado del arte internacional
- Relación entre protección de infraestructuras críticas y ciberseguridad en entornos industriales
- Aproximación a los sistemas de control industrial
- Vulnerabilidades y amenazas de los sistemas de control industrial.

Unidad didáctica II. Superficie de ataque en infraestructuras inteligentes
En la unidad II, el alumno adquiere los conocimientos de los diferentes tipos de técnicas para asegurar el sistema, así como utilizar técnicas de desarrollo que cumplan con los criterios de seguridad en el uso para todo tipo de software. De igual manera, la unidad trata sobre como implantar medidas de seguridad físicas: sistemas anti incendios, vigilancia de los centros de proceso de datos, sistemas de protección contra inundaciones, protecciones eléctricas contra apagones y sobretensiones, sistemas de control de accesos y vigilancia de la red.
,

- Técnicas de desarrollo
- Criptografía
- Vigilancia de la red
- Redes perimetrales de seguridad
- Modelo Bell-LaPadula
- Ciberseguridad inteligente.

Unidad de didáctica III. **Desarrollo de aplicaciones robustas**
En la unidad IV, el alumno debe diseñar sistemas a prueba de ataques con alto grado de confiabilidad. El sistema debe realizar un seguimiento en tiempo real y es diseñada para ayudar a crear sistemas de defensa adaptativos, evolutivos e inteligentes.

- Sistemas Robustos en ciberseguridad
- Proyecto final.

Criterios de desempeño

1. Participación activa en clase.
2. Ser puntuales.
3. Asistencia. Es muy importante. Tomar en cuenta el Reglamento Escolar.
4. Cumplir cabal y puntualmente con todas las actividades y trabajos.
5. Hacer los exámenes en las fechas programadas.
6. Trabajar en equipo los proyectos del curso.

Experiencias de Enseñanza / procesos y objetos de aprendizaje requeridos

1. Exposición del maestro de conceptos teóricos
2. Exposición de alumnos de aplicaciones industriales

Experiencias de aprendizaje.

1. Investigación de artículos de ciencia y tecnología.
2. Exposición de proyectos.

Recursos didácticos y tecnológicos (material de apoyo):

1. Laptop del instructor.
2. Cañón.
3. Pintarrón.
4. Conexión a internet.
5. Software comercial de ciber seguridad.

Bibliografía	***Básica/ Complementaria***
Singer Peter W., and Allan Friedman. (2014). Cybersecurity: What Everyone Needs to Know. Edit. Oxford University Press,	***Básica***
Dua Sumeet, and Xian Du. (2016). Data mining and machine learning in cybersecurity. Edit. CRC press	***Básica***
Dejan Kosutic. (2012). Ciberseguridad en 9 pasos. Edit. EPPS Services Ltd.	***Básica***
Fundación Telefónica. (2016). Ciberseguridad, la protección de la información en un mundo digital. Edit. Ariel.	***Básica***

IV. Evaluación Formativa de las Competencias

#	Tipo (C,H, A)	Evidencias a evaluar	Criterios de evaluación	Técnicas e Instrumentos de Evaluación	Ponderación %
1	C	Examen parcial	Se evaluará el nivel de conocimientos adquiridos en relación a la unidad I	Examen escrito	20 %
2	C,H, A	Exposiciones de proyectos de estudio	Se evaluará la capacidad, habilidades y actitudes en relación a trabajo en equipo, lectura y análisis de proyectos, exposición, organización de ideas.	Diseño, debate, organización y presentación de proyectos aplicados	30 %
3	C	Examen parcial	Se evaluará el nivel de conocimientos adquiridos en relación a la unidad II	Examen escrito	20 %
4	C	Examen parcial	Se evaluará el nivel de conocimientos adquiridos en relación a la unidad III	Examen escrito	20 %
5	H, A	Participación activa en clase	Se evaluarán las habilidades de comunicación, organización yactitudes de trabajo y compromiso del alumno	Participación en clases y asistencia	10 %
				Total	**100 %**

C: Conocimientos H: Habilidades A: Actitudes