ASSESS

2133 – Assessment (IC33)

Análisis de Vulnerabilidades y Evaluación de Riesgos Cibernéticos en Sistemas Industriales Nuevos y Existentes – IC33

Requiere IC32

La primera fase en el ciclo de vida de CiberSeguridad de los sistemas industriales (IACS – definida en ISA/IEC-62443-1-1) consiste en identificar y documentar los activos industriales (IACS) y realizar un análisis de vulnerabilidad de seguridad cibernética y evaluación de riesgos con el fin de identificar y comprender las vulnerabilidades de alto riesgo que requieren mitigación.

Por la ISA/IEC-62443-2-1 estas evaluaciones deben realizarse tanto en las aplicaciones existentes (Brownfield) como nuevas (Greenfield). Parte del proceso de evaluación implica el desarrollo de un modelo de zonas y de conductos de los sistemas bajo consideración, la identificación de objetivos de nivel de seguridad y la documentación de los requisitos de seguridad cibernética en una especificación de requisitos de seguridad cibernética (CSRS).

Al finalizar el curso estará en condiciones de:

- Identificar y documentar el alcance de los IACSs en evaluación y bajo consideración
- Especificar, reunir o generar la información de seguridad cibernética necesaria para realizar la evaluación
- Identificar o descubrir las vulnerabilidades de seguridad cibernética inherentes al producto o sistema bajo consideración
- Organizar y facilitar una evaluación de riesgos de seguridad cibernética para un sistema integrado
- Identificar y evaluar escenarios de amenaza realistas
- Identificar las lagunas en las políticas, procedimientos y las normas existentes en la compañía
- Establecer y documentar zonas y conductos de seguridad
- Preparar la documentación de los resultados de la evaluación.

ISA certificate program
ISA APPROVED

Ejercicios prácticos por realizar en clase:

- Discutir y criticar a la arquitectura de los sistemas y sus diagramas
- Inventario de activos de los sistemas bajo consideración
- Evaluación de las deficiencias
- Evaluación de la vulnerabilidad (Windows)
- Ejercicios de captura de tráfico Ethernet
- Escaneo de puertos
- Uso de las herramientas de análisis de vulnerabilidades
- Realización de una evaluación de riesgos de alto nivel
- Creación de un diagrama de zonas y de conductos
- Realización de una evaluación de riesgos cibernéticos detallada
- Discutir y criticar una especificación de requisitos de seguridad cibernética

Este curso proporcionará a los estudiantes la información y las habilidades necesarias para evaluar la seguridad cibernética de un nuevo IACS o en IACSs existentes y desarrollar una especificación de requisitos de seguridad cibernética que se puede utilizar para documentar los requisitos de seguridad cibernética del proyecto.

Certificación N° 2 “ISA/IEC 62443 Cybersecurity Risk Assessment Specialist”

- Créditos CRE: 2,1
- Créditos CEU: 2,1 (Otorgados por ISA)
- El examen para obtener la certificación profesional (incluido en la matrícula) se rinde aparte con un plazo máximo de hasta 6 meses de realizado el curso. Por el momento el examen se rinde únicamente en idioma inglés..

Modalidad y horarios:

Disponible en idiomas español y portugués, en modalidades presenciales y virtuales en línea, sincrónico y asincrónico en el Campus Académico de WiseCourses. Contiene examen de práctica que se realizará en línea dentro del nuestro Campus Educativo, empleando la misma metodología que la evaluación de certificación de ISA. De esta forma el estudiante se sentirá más confiado para luego rendir el examen oficial bajo el sistema SCANTRON.

Duración: 24 horas con el docente

Resumen de las características destacadas del curso:

- Disponible en idiomas español y portugués, tanto la locución como el material completo del curso. El material del curso estará disponible para consultar en el Campus Educativo (asincrónica) tanto en idioma español como en idiomas portugués e inglés.
- Incluye ejercicios prácticos en línea. Cada asistente accede desde el campus de forma remota a una computadora dedicada conectada en red con el resto de las computadoras del curso para realizar varios ejercicios prácticos de CiberSeguridad con software y aplicaciones específicas.
- Abundante material de lectura complementaria (Incluyendo la Norma ISA/IEC 62443).
- Reuniones virtuales grupales de estudio hasta rendir el examen aún luego de finalizado el curso.
- Múltiples oportunidades para rendir el examen hasta 6 meses después de finalizado el curso por el sistema SCANTRON.
- El asistente puede ingresar al Campus para consultar el material del curso por un plazo de 1 año.
- Coaching, chat y blog 7×24 por un plazo de 1 año asistiendo en la implementación de los conocimientos adquiridos prácticos en su organización.

Entregables:

Los participantes recibirán en la clase (presenciales) en su domicilio (virtuales) acceso los siguientes materiales. Se podrá suministrar material impreso opcional con costo adicional: Lecciones del curso impresas, Normas ISA/IEC-62443 empleadas en el curso, Campus educativo para bajar información complementaria y software, Cursos prácticos de laboratorio, y Elegibilidad para obtener del certificado oficial. (Requiere asistencia 100%).

Desde WiseCourses estamos inspirados por la innovación en educación para crear procesos de capacitación que sean representativos del mundo en el que vivimos actualmente. Crear y soportar nuevos sistemas potenciando a los educadores y profesionales que adquieren la experiencia.