GOVERN

2132 – Fundamentals (IC32)
Empleando el estándar ISA/IEC-62443 para proteger a los Sistemas de Control.

Este curso proporciona una mirada detallada de cómo los estándares ISA/IEC-62443 pueden ser usados para proteger sus sistemas de control críticos. Esto también explora las diferencias procedurales y técnicas entre la seguridad tradicional para los ambientes de IT y aquellas soluciones apropiadas para SCADA o ambientes del piso de planta. Este curso contiene las bases para comprender cómo está organizada la serie de normas ISA/IEC-62443.

Al finalizar el curso estará en condiciones de:

- Discutir los principios detrás de un Programa de Ciberseguridad Industrial de largo plazo.
- Interpretar las normas y guías de Ciberseguridad de ISA/IEC-62443 y aplicarlas en su operación.
- Definir los fundamentos de riesgo y metodologías de análisis de vulnerabilidades.
- Describir los principios para el desarrollo de sus políticas de seguridad.
- Explicar los conceptos de defensa en profundidad y los modelos de referencia.
- Analizar las tendencias actuales en incidentes de seguridad industrial.
- Definir los principios detrás de las técnicas de mitigación de riesgo claves, el antivirus y actualizar parches, firewalls y redes privadas virtuales.

ISA certificate program
ISA APPROVED

Cubrirá en el curso los siguientes tópicos:

- Entendimiento del ambiente de seguridad industrial actual: ¿Qué es la seguridad electrónica para sistemas de control y automatización industriales?, ¿Qué tienen de diferente y en común los sistemas de IT y los industriales?
- ¿Cómo suceden los Ciber-Ataques?: comprendiendo los vectores de ataque y sus pasos.
- Creando un Programa de Ciberseguridad Industrial: factores críticos del éxito y un entendimiento acabado de la norma ISA/IEC-62443-2-1 (ANSI/ISA.99.02.01-2009).
- Análisis de Riesgo: racionalidad del negocio, identificación del riesgo, clasificación y auditoria de seguridad. Metodología DNSAM.
- Estudio del nivel de riesgo con sus políticas de seguridad, organización y concientización: alcance CSMS, seguridad organizacional, entrenamiento del personal y concientización.
- Estudio del nivel de riesgo con las medidas de remediación seleccionadas: seguridad del personal, seguridad física y ambiental, segmentación de redes y control de acceso.
- Alcanzado el nivel de riesgo, con la implementación de mediciones: gestión del riesgo e implementación, desarrollo del sistema y mantenimiento, y gestión de la documentación.
- Monitoreo y Mejora del CSMS: cumplimiento y revisión para mejorar y mantener el CSMS.

Certificado N° 1: Especialista en Fundamentos de Ciberseguridad Industrial:

- Créditos CEU: 1,4
- El examen para obtener la certificación profesional 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.

SCANTRON.
SMART STARTS HERE

Modalidad y horarios:

Este curso se encuentra disponible en todas las modalidades presenciales (en Oficinas de WisePlant, en Planta del Cliente, en Academia) y Virtuales (Sincrónica, Asincrónica y Bajo Demanda). Aun en modalidades presenciales el curso requiere que los participantes utilicen la Plataforma Educativa para poder acceder al abundante material complementario y para rendir la Evaluación Final.

- Duración: 16 horas con el docente, incluyendo la evaluación final.

Ejercicios Prácticos:

- Desarrollo de casos de negocios para la Ciberseguridad Industrial.
- Ejemplos y casos prácticos demostrados por el instructor.
- Este curso no tiene ejercicios prácticos de laboratorio.

Resumen de las características destacadas del curso:

- Disponible en idiomas Español, Portugués e Inglés 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 en redes con software y aplicaciones específicas.
- Abundante material de lectura complementaria (Únicamente en sus idiomas originales)
- Reuniones virtuales grupales de estudio hasta rendir el examen aún luego de finalizado el curso.
- Todas las oportunidades que precise 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) los siguientes materiales. La entrega y/o envío de material impreso es opcional y podrá ser realizada con costo adicional.

- Acceso a las lecciones del curso impresas.
- Acceso a las normas ISA/IEC-62443 empleadas en el curso.
- Acceso al campus educativo para bajar información complementaria y software.
- Elegibilidad para obtener del certificado oficial SCANTRON. (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.