USIL EPG

Innovación, IA y Tecnología

CURSO INTERNACIONAL EN

RESPONSABLE DE CIBERSEGURIDAD INDUSTRIAL

INICIO: 19 de octubre

DURACIÓN:
24 horas académicas

MODALIDAD:
Virtual sincrónica

HORARIO:
Sábado
9:00 a. m. a 1:00 p. m.

CERTIFICACIÓN:
A nombre de la Escuela de Posgrado USIL

epg.usil.edu.pe

Descripción del curso

En un mundo cada vez más interconectado, la ciberseguridad industrial OT se ha vuelto una necesidad crítica, especialmente en sectores que dependen de infraestructuras críticas. Este programa abarca temas esenciales como la implementación del marco NIST SP 800-82 para ciberseguridad en sistemas de control industrial, gestión de riesgos en entornos OT y medidas de ciberseguridad específicas para sistemas industriales. Al finalizar el curso, los participantes estarán equipados con el conocimiento y las habilidades necesarios para proteger eficazmente las infraestructuras industriales de ciberamenazas, garantizando la continuidad y la seguridad operativa. Según un estudio de Gartner, se prevé que, para 2025, el 75 % de las empresas industriales habrá sufrido ciberataques, subrayando la urgencia de esta capacitación.

Objetivos

1. Conocer los fundamentos y principios del marco NIST SP 800-82 aplicados a entornos OT.
2. Comprender la gestión de riesgos y su aplicación en infraestructuras industriales.
3. Aplicar técnicas de ciberseguridad específicas para sistemas de control industrial.
4. Analizar vulnerabilidades y amenazas en entornos OT.
5. Evaluar la eficacia de las medidas de ciberseguridad implementadas.

Perfil del participante

Este curso está diseñado para profesionales de tecnología de operaciones, tecnología de la informática y ciberseguridad, ingenieros industriales, responsables de seguridad de la información en infraestructuras críticas, y cualquier persona encargada de la protección de sistemas de control industrial.

Skills

Al finalizar el curso, el alumno obtendrá las siguientes capacidades:

- Gestión de riesgos en entornos industriales.
- Implementación del marco NIST SP 800-82 en OT.
- Análisis de vulnerabilidades en sistemas de control industrial.
- Desarrollo de políticas de ciberseguridad para infraestructuras críticas.
- Respuesta a incidentes en entornos industriales.
- Monitorización de sistemas OT.
- Configuración segura de dispositivos industriales.
- Evaluación de cumplimiento normativo.
- Gestión de proyectos de ciberseguridad industrial.

Temario

- Introducción a la ciberseguridad industrial OT.
- Normativa NIST SP 800-82 en entornos industriales.
- Gestión de riesgos y amenazas en sistemas OT.
- Análisis y mitigación de vulnerabilidades en infraestructuras críticas.
- Implementación de medidas de ciberseguridad en sistemas de control industrial.
- Respuesta a incidentes y recuperación de sistemas OT.
- Monitorización y auditoría de sistemas industriales.
- Cumplimiento normativo y auditoría de seguridad.
- Desarrollo de políticas y procedimientos de ciberseguridad OT.
- Proyecto integrador: desarrollo de un plan de ciberseguridad industrial.

Trabajo aplicativo final:

Desarrollar un *roadmap* de ciberseguridad para una infraestructura industrial, aplicando el marco NIST SP 800-82 y las mejores prácticas de seguridad para sistemas OT.

Profesor *practitioner*

Sebastián Vargas

Gerente general en TTPSEC SPA ® Consultoría de Estrategia, Tecnología y Ciberseguridad.

- Tiene más de 18 años de experiencia en el ámbito de la ciberseguridad y ha ocupado diversos cargos como OSI, CISO o CSO en el sector público, financiero y en empresas vinculadas con la infraestructura crítica de Chile.
- Máster en Ciberseguridad Industrial por el Centro de Ciberseguridad Industrial en España.
- Máster en Gestión de Tecnologías de la Información por la Universitat Oberta de Catalunya en España.
- Máster en Ciberseguridad, Ciberterrorismo y Ciberguerra por la Universidad Pegaso en Italia.
- Ingeniero civil en informática e ingeniero en ciberseguridad por la Universidad Tecnológica de Chile.
- Posee diversas certificaciones tales como:
  - Certified Ethical Hacker (Practical).
  - eLearnSecurity Certified Incident Responder (eCIR).
  - eLearnSecurity Certified Digital Forensics Professional (eCDFP).
  - eLearnSecurity Junior Penetration Tester (eJPT).
  - MITRE ATT&CK Fundamentals.
  - MITRE ATT&CK PurpleTeam.
  - MITRE ATT&CK for Cyber Threat Intelligence.
  - MITRE ATT&CK for Security Operations Center Assessments.
  - MITRE ATT&CK for Adversary Emulation Methodology.
  - MITRE ATT&CK for Threat Hunting Detection Engineering.
  - Implementador y auditor de ISO 27001.
  - C|CISO.

Inversión
S/ 1800

Certificación

Asistencia mínima 70 %	Nota mínima 11

Para obtener la certificación, el alumno no debe superar el 30 % de inasistencias del total de horas de clases y debe tener una nota final aprobatoria.

Requisitos de admisión

- Copia o foto de DNI (ambos lados)
- Ficha de inscripción
- Acuerdo de matrícula
- Un año de experiencia laboral mínima

La EPG-USIL se reserva el derecho de cancelar o modificar las fechas de sus cursos y comunicarlas con la debida anticipación.

Una vez iniciadas las clases no se podrá solicitar la devolución de la primera cuota.

El dictado de clases del curso se iniciará siempre que se alcance el número mínimo de alumnos matriculados establecido por USIL.

Para la entrega de certificados son requisitos indispensables tener una nota aprobatoria, no haber superado el 30 % de inasistencias y haber cancelado la inversión económica total del curso.

Más información

981 458 741
informes.epg@usil.edu.pe
@usileducacionejecutiva
EPGUSIL

#EducaciónEjecutivaUSIL

epg.usil.edu.pe

Universidad San Ignacio de Loyola S.R.L. RUC: 20297868790