ZIBERSEGURTASUN INDUSTRIALA IKASTAROA (ONLINE)

GAIA	Informatika, Telekomunikazio Sistemak eta Sistema Txertatuak
ECTS/ORDUAK	25 ORDU
EGUTEGIA	2022/10/17 - 2022/12/16 As-At-Az-Og-Or
HIZKUNTZA	Gaztelania
MODALITATEA	Online

Informazio gehiago eta izen-ematea

HELBURUAK

Los avances tecnológicos han traído, y traen, una gran cantidad de ventajas, beneficios y aportes a la actividad empresarial, tanto en las Tecnologías de la Información como de Operación. Sin embargo, su puesta en marcha trae consigo hacer frente a una serie de riesgos, los cuales, deberán ser mitigados, reducidos o transferidos hasta un punto que sea asumibles por la organización.
Las compañías tienen una transparencia sin precedentes a lo largo de todas sus operaciones que no solo mejorarán sus procesos, sino que también desarrollarán nuevos modelos de negocio que incrementarán sus beneficios.
Reducir los tiempos de producción, aumentar la flexibilidad, posibilitar la producción individualizada en masa, optimizar el consumo de energía y recursos, son algunos de los desafíos a los que se enfrentan las empresas en la actualidad, debiendo optimizar toda la cadena de valor, desde el diseño, la planificación e ingeniería de la producción hasta los servicios. El aumento de la disponibilidad, mejora continua, optimización de procesos y la resiliencia frente a interrupciones no planificadas sobre cualquier tipo de infraestructura, son algunos de los objetivos más destacados; encontrando ejemplos claros en sectores como industria manufacturera, energía, máquina herramienta o automoción.
Así pues, al recopilar, contextualizar y analizar la gran cantidad de datos disponibles, las empresas obtendrán información transformadora para tomar decisiones informadas y realizar cambios que mejoren la rentabilidad. Esta generación, acceso, tratamiento y explotación de la información de procesos o, coligados a ellos, favorece un aspecto clave en la puesta en marcha de nuevas soluciones, la interoperabilidad. La cual, junto con la integración de tecnologías, ofrece un aumento en el grado de exposición de tales sistemas, componentes y dispositivos.
La Ciberseguridad Industrial es el conjunto de acciones, métodos y procedimientos, tanto técnicos como operativos, que permiten materializar que dicho nivel de riesgo sea el mínimo aceptable y, que el impacto para la organización a través de un incidente, en caso de haber un uso o acceso indebido de las mismas; también sea igualmente mínimo. Es decir, resulta necesario evitar que algo o alguien, de una manera intencionada, o no intencionada, pueda alterar total o parcialmente la actividad de una empresa,

organización o institución, provocando así, un daño material o inmaterial derivado de los nuevos riesgos tecnológicos introducidos y en donde amenazas y vulnerabilidades encuentran la vía por donde alcanzar sus propósitos.
Es por ello que resulta obligado proteger tales sistemas, dispositivos y componentes que intervienen en las actividades y procesos industriales sobre los que se basan distintos modelos de negocio de las compañías, así como aquéllos que participan en la creación, acceso, tratamiento y almacenamiento de la información de procesos.

NORI ZUZENDUA

personal vinculado a las Tecnologías de Información, como administradores de redes, sistemas o desarrolladores; y de Operación, como programadores, personal de mantenimiento o ingeniería

PROGRAMA

1. Módulo “Introducción a la Ciberseguridad Industrial” (Duración: 1 hora)
a. Definición de Tecnologías de Operación.
b. Evolución de las Distintas Revoluciones Industriales.
c. Situación pasada y actual.
d. Diferencias y Prioridades en entornos IT y OT.
e. Beneficios Ciberseguridad Industrial.
f. Ejemplos de incidentes.
2. Módulo “Equipos y Dispositivos Industriales” (Duración: 2h 20m)
a. Sensores, Actuadores.
b. PLCs y Controladores.
c. Seguridad Funcional, SIS.
d. Periferia Descentralizada.
e. HMI, sistemas de Visualización.
f. Software de Programación.
g. Robots.
h. DCS.
i. VFD.
j. Networking Industrial.
k. Pasarelas.
l. Servidores SCADA, MES y ERP.
m. Máquina Herramienta.
n. Actividad 1; “Identificar y situar los principales equipos y dispositivos sobre un escenario propuesto”.
3. Módulo “Redes y comunicaciones industriales” (Duración: 1h 43m)
a. Introducción a las Comunicaciones.
b. Modelo de Referencia OSI.
c. Pila TCP/IP.
d. Identificadores de equipos.
e. VLAN
f. Tipos y Características de comunicaciones industriales.
g. Requisitos.
h. Modelos de comunicaciones industriales.
i. Dispositivos.

j. Protocolos y Buses de Campo.
k. Topologías de Redes Industriales.
l. Medios Físicos e inalámbricos.
m. Evolución de comunicaciones.
n. Actividad 1; “Análisis de tráfico a partir de capturas .pcap”
4. Módulo “Modelo Purdue e ISA- 95” (Duración: 10m)
a. Introducción.
b. Modelo por capas.
c. Definición de Capas.
d. Tipos de Procesos.
e. Actividad 1; “Situar, según modelo Purdue, los equipos y dispositivos de la Actividad 1”
5. Módulo “Amenazas en entornos Industriales” (Duración: 24m)
a. Definición de amenazas.
b. Intencionadas.
c. No intencionadas.
d. Internas.
e. Externas.
f. Vía de acceso.
g. Factores de Riesgo.
6. Módulo “Vulnerabilidades en entornos industriales” (Duración: 36m)
a. Definición.
b. Clasificación y categorización.
c. Presencia de vulnerabilidades en entornos industriales.
7. Módulo “Vectores de Ataque en entornos industriales” (Duración: 20m)
a. Definición.
b. Mecanismos y métodos empleados.
8. Módulo “Modelo de Defensa en Profundidad” (Duración: 2h 5m)
a. Definición.
b. Diferencia Security y Safety.
c. Desafíos de los entornos industriales para su protección.
d. Diferencia entre estrategia de defensa IT y OT.
e. Métodos y recursos de protección.
f. Modelo por Capas y su significado.
g. Explicación de cada una de ellas.
h. Limitaciones.
i. Componentes y elementos que interviene en el Modelo Defensa en Profundidad.
j. Modelo de implementación.
9. Módulo “Medidas de seguridad sobre Infraestructuras de Comunicaciones” (Duración: 2 h 25 m)
a. Definición.
b. Objetivos.
c. Entornos.
d. NGFW.
e. Zonas.
f. Separación.
g. Segmentación.
h. Micro Segmentación.
i. Virtual Patching.

j. VPNs.
k. Monitorización.
l. Otras consideraciones.
m. Tareas asociadas.
n. Actividad 1; “Respuesta a preguntas y situar equipos cortafuegos en el esquema de la Actividad 1 del módulo “Modelos de Referencia”.
o. Demo 1; “Captura de Tráfico”, Port Mirror y TAP.
p. Demo 2; “Cortafuegos de Red, Parte I”; Funcionalidades y ejemplos con equipos Fortinet Fortigate y SIEMENS Scalance S y X.
q. Demo 3; “Cortafuegos de Red, Parte II; NGFW, modos de operación, DPI, etc. Ejemplos con equipos Fortinet Fortigate y SIEMENS Scalance S y X.”
10. Módulo “Medidas de seguridad en Equipos Finales” (Duración: 1h 37m)
a. Definición.
b. Bastionado.
c. Whitelisting.
d. Control de Accesos.
e. Monitorización.
f. Antivirus.
g. Gestión de Parches.
h. Cifrado.
i. Gestión de Activos.
j. Copias de Respaldo.
k. Acceso Remoto.
l. Sistemas de Detección de Intrusi
