Solucionario de

ejercicios de autoevaluación

Ejercicios de autoevaluación
Unidad de Aprendizaje 1

1. Indica si las siguientes afirmaciones son verdaderas o falsas.

a. En el ámbito industrial, la ciberseguridad cobra una importancia aún mayor, debido a la creciente digitalización y conexión de los sistemas críticos.

- **Verdadero**
- Falso

b. Los ataques cibernéticos causan exclusivamente pérdidas económicas.

- Verdadero
- **Falso**

c. La comprensión de los fundamentos de la ciberseguridad permite a los profesionales, y en general a todos los miembros de una organización, tener conciencia sobre las amenazas a las que están expuestos.

- **Verdadero**
- Falso

2. ¿Cuál de los siguientes no es un pilar fundamental de la ciberseguridad?

a. Confidencialidad
b. Integridad
c. Redundancia
d. Disponibilidad

3. ¿Qué representa la A en el triángulo CID (CIA en inglés) en ciberseguridad?

a. Disponibilidad
b. Autenticación
c. Autorización
d. Acceso

4. ¿Qué técnica se usa para garantizar que una persona es quien dice ser al acceder a un sistema?

a. Autenticación
b. *Firewall*
c. Criptografía
d. Autorización

5. ¿Qué tipo de amenaza implica la manipulación de empleados para obtener acceso a sistemas sensibles?

a. Ataque DDoS
b. Denegación de servicio (DoS)
c. Ingeniería social
d. *Phishing*

6. ¿Qué es un ataque de denegación de servicio (DoS)?

a. Un ataque que satura los sistemas con tráfico excesivo para interrumpir el servicio.
b. Un ataque que compromete la confidencialidad de los datos.
c. Un ataque que infecta los sistemas con *malware*.
d. Un ataque que roba credenciales de usuario.

7. ¿Cuál de las siguientes fases forma parte de una metodología de gestión de riesgos?

a. Monitoreo y revisión
b. Implementación de parches
c. Escaneo de virus
d. Desconexión de redes

8. ¿Qué son los activos críticos en ciberseguridad?

a. Solo los servidores web.
b. Bases de datos desactualizadas.
c. Recursos esenciales cuya pérdida afectaría gravemente a la organización.
d. Dispositivos de *hardware* de la organización.

9. ¿Qué significa la continuidad del negocio en el contexto de la ciberseguridad?

a. La capacidad de una organización para seguir operando después de un incidente.
b. El proceso de realizar evaluaciones de seguridad cada año.
c. La implementación solo de medidas de prevención de ataques.
d. La restauración de sistemas tras un ataque de *malware*.

10. ¿Qué estándar proporciona directrices específicas para la gestión de la seguridad de la información?

a. OWASP
b. PCI-DSS
c. NIST 800-82
d. ISO 27001

Ejercicios de autoevaluación Unidad de Aprendizaje 2

1. Indica si las siguientes afirmaciones son verdaderas o falsas.

a. Es fundamental comprender que la gestión de riesgos juega un papel decisivo en la protección de los sistemas de información de cualquier tipo de organización. Este proceso es fundamental para asegurar la resiliencia de la organización ante eventos imprevistos, ayuda a minimizar las pérdidas y aprovechar las oportunidades que puedan surgir.

- **Verdadero**
- Falso

b. La gestión de riesgos en la seguridad de los sistemas es un proceso puntual que permite identificar posibles vulnerabilidades o amenazas, evaluar el impacto potencial y la probabilidad de que se materialicen, tomando medidas para mitigarlas o gestionarlas adecuadamente.

- Verdadero
- **Falso**

c. El plan de tratamiento de riesgos permite definir claramente los controles necesarios para mitigar los riesgos y cuáles de estos se van a tratar, pero no define quién será responsable de implementarlos, el tiempo en el que deben cumplirse y los recursos asignados para garantizar una gestión adecuada de los riesgos.

- Verdadero
- **Falso**

2. ¿Qué proceso implica identificar las posibles amenazas que podrían afectar a una organización?

a. Análisis de riesgos
b. Evaluación de riesgos
c. Identificación de riesgos
d. Monitoreo de riesgos

3. ¿Qué acción busca reducir la probabilidad o el impacto de un riesgo?

a. Evitar
b. Mitigar
c. Transferir
d. Aceptar

4. ¿Cuál es la función de las auditorías de seguridad?

a. Detectar amenazas internas.
b. Revisar periódicamente las políticas de seguridad.
c. Eliminar amenazas.
d. Detectar virus.

5. ¿Qué *cmdlet* de *PowerShell* permite automatizar la instalación de actualizaciones en sistemas *Windows?*

a. Install-WindowsUpdate
b. Set-ExecutionPolicy
c. Enable-BitLocker
d. New-NetFirewallRule

6. En el proceso de gestión de riesgos, ¿qué etapa implica priorizar los riesgos en función de su importancia?

a. Proteger datos mediante encriptación.
b. Desactivar servicios innecesarios para reducir la superficie de ataque.
c. Implementar un cortafuego en la red.
d. Aceptar los riesgos.

7. ¿Qué herramienta permite automatizar la gestión de dispositivos móviles en entornos empresariales?

a. Kerberos
b. *Microsoft Intune*
c. *Ansible*
d. *PowerShell*

8. ¿Qué componente de seguridad es responsable de limitar el tráfico no autorizado en una red?

a. Antivirus
b. IDS
c. *Firewall*
d. Monitorización

9. ¿Qué significa "cifrado de datos en reposo"?

a. Cifrar datos cuando se están utilizando.
b. Cifrar datos almacenados.
c. Cifrar datos durante la transmisión.
d. Cifrar datos al ser eliminados.

10. ¿Qué protocolo es utilizado en la capa de aplicación del modelo OSI para la navegación web?

a. FTP
b. TCP
c. HTTP
d. UDP

Ejercicios de autoevaluación Unidad de Aprendizaje 3

1. Indica si las siguientes afirmaciones son verdaderas o falsas.

a. Conocer los fundamentos industriales de las tecnologías de la operación (OT) en el control de procesos resulta básico, debido al impacto directo que tienen en la eficiencia y seguridad de las infraestructuras críticas.

- **Verdadero**
- Falso

b. La convergencia entre OT e IT permite una mayor automatización y recopilación de datos.

- **Verdadero**
- Falso

c. No es necesario comprender cómo funcionan los sistemas de control y la instrumentación de OT para crear estrategias de protección adecuadas, aplicar medidas de *hardening* y gestionar los riesgos de forma eficaz, con idea de garantizar la continuidad y resiliencia de los procesos industriales ante posibles ciberataques.

- Verdadero
- **Falso**

2. ¿Qué caracteriza a los sistemas de control automático?

a. Requieren supervisión constante.
b. Funcionan independientemente una vez configurados.
c. Son poco precisos en el control de temperatura.
d. Son más comunes en la industria tradicional.

3. ¿Qué representa la Cuarta Revolución Industrial?

a. La integración avanzada de tecnologías digitales en la industria.
b. La introducción de los sistemas manuales de control.

c. El desarrollo de la electricidad.
d. El uso de cadenas de montaje en producción.

4. ¿Qué elemento permite a los sistemas de control mantener variables críticas dentro de rangos seguros?

a. Control PID
b. Control SCADA
c. DCS
d. HMI

5. ¿Qué tecnología industrial ayuda a predecir la necesidad de mantenimiento de maquinaria?

a. *Big data*
b. *Fieldbus*
c. *HMI*
d. *Control PID*

6. ¿Qué es una RTU?

a. Unidad terminal remota
b. Un tipo de sensor de presión
c. Un sistema de monitoreo humano
d. Un conversor de voltaje a corriente

7. ¿Cuál es la principal función de un sistema SCADA?

a. Recopilar datos en tiempo real de dispositivos de control.
b. Ejecutar procesos manuales en planta.
c. Controlar redes de área amplia.
d. Realizar pruebas de penetración.

8. ¿En qué consiste la transformación digital en la industria?

a. Crear más sistemas manuales de producción.
b. Aumentar el uso de energía eléctrica.
c. Monitorear y optimizar procesos en tiempo real.
d. Reducir el uso de tecnologías avanzadas.

9. ¿Qué sistema permite la interacción directa entre operarios y máquinas?

a. HMI (interfaz hombre-máquina)
b. DCS
c. SCADA
d. RTU

10. ¿Cuál es un ejemplo de un proceso discreto en la industria?

a. Fabricación de alimentos en lotes
b. Refinado de petróleo
c. Tratamiento de agua
d. Producción de automóviles

Ejercicios de autoevaluación Unidad de Aprendizaje 4

1. Indica si las siguientes afirmaciones son verdaderas o falsas.

a. La Industria X.0 o industria inteligente se caracteriza por el uso de herramientas innovadoras como la inteligencia artificial, el internet de las cosas, los gemelos digitales y la robotización colaborativa, tecnologías que transforman no solo los procesos productivos, sino también las formas de interacción entre máquinas, datos y personas.

- **Verdadero**
- Falso

b. *EtherCAT (Ethernet for Control Automation Technology)* es un protocolo de comunicación desarrollado por Beckhoff Automation para entornos industriales que requieren transmisión de datos en tiempo real.

- **Verdadero**
- Falso

c. Aunque está diseñado para responder a las exigencias de precisión, velocidad y flexibilidad, *EtherCAT* no consigue optimizar procesos críticos con la eficiencia deseada.

- Verdadero
- **Falso**

2. ¿Qué estándar internacional organiza e integra los sistemas industriales?

a. ISO 9001
b. GMP
c. ISA-95
d. FDA

3. ¿Qué nivel de ISA-95 interactúa directamente con los sensores y los actuadores?

a. Nivel 4
b. Nivel 2
c. Nivel 0
d. Nivel 1

4. ¿Qué nivel de ISA-95 corresponde a la gestión empresarial?

a. Nivel 1
b. Nivel 3
c. Nivel 0
d. Nivel 4

5. ¿Qué función cumplen los sistemas MES en una fábrica?

a. Supervisan las tareas administrativas.
b. Controlan las redes industriales.
c. Gestionan, monitorizan y optimizan los procesos de fabricación en tiempo real.
d. Conectan los dispositivos IoT en la nube.

6. ¿Qué tipo de maquinaria está diseñada para transformar las materias primas en productos finales?

a. Maquinaria de manipulación
b. Maquinaria de producción
c. Maquinaria de inspección
d. Robots articulados

7. ¿Qué nivel de automatización tiene una máquina que requiere intervención humana para iniciar procesos?

a. Automática
b. Semiautomática
c. Manual
d. Computerizada

8. ¿Qué nivel de ISA-95 usa ERP para coordinar inventarios?

a. Nivel 1
b. Nivel 2
c. Nivel 3
d. Nivel 4

9. ¿Qué protocolo estándar utilizan los sistemas MES para conectarse con las máquinas industriales?

a. HTTP
b. *OPC UA*
c. *Bluetooth*
d. *Ethernet*

10. ¿Qué tecnología permite rastrear y gestionar objetos sin contacto físico?

a. Códigos de barras
b. RFID
c. *Bluetooth* clásico
d. *Ethernet*

Ejercicios de autoevaluación Unidad de Aprendizaje 5

1. Indica si las siguientes afirmaciones son verdaderas o falsas.

a. La ciberseguridad industrial se ha convertido en un pilar esencial en las plantas industriales modernas, donde la digitalización y la interconectividad traen consigo tanto oportunidades como importantes riesgos.

- **Verdadero**
- Falso

b. En un entorno industrial, el cumplimiento de las normas de seguridad y salud laboral, junto con las instrucciones técnicas de instalación, no solo protege a los trabajadores y las operaciones, sino que también garantiza la integridad de los sistemas críticos.

- **Verdadero**
- Falso

c. Conocer los conceptos de seguridad y los riesgos asociados en las instalaciones industriales permite al personal cualificado identificar y mitigar vulnerabilidades antes de que se traduzcan en fallos catastróficos.

- **Verdadero**
- Falso

2. ¿Qué significa SCADA en el contexto industrial?

a. Supervisión de sistemas avanzados
b. Supervisión, control y adquisición de datos
c. Sistema de control automatizado
d. Supervisión y control de aparatos

3. ¿Cuál es la función principal de los PLC en un sistema ICS?

a. Supervisar sistemas IT.
b. Ejecutar tareas específicas, como encender o apagar máquinas.

c. Monitorizar redes de comunicación.
d. Procesar datos empresariales.

4. En un sistema ICS, las RTU:

a. Procesan datos financieros.
b. Ejecutan acciones físicas.
c. Transmiten datos de sensores al sistema central.
d. Gestionan redes inalámbricas.

5. La ciberseguridad IT se enfoca principalmente en:

a. Seguridad y continuidad de procesos físicos
b. Supervisión de redes industriales
c. Protocolo de gestión de energía
d. Confidencialidad, integridad y disponibilidad de datos

6. ¿Qué prioridad tiene la ciberseguridad OT?

a. Confidencialidad de datos
b. Optimización de redes
c. Disponibilidad y seguridad de procesos físicos
d. Monitoreo en tiempo real

7. ¿Qué diferencia clave hay entre los sistemas IT y OT?

a. IT gestiona datos, mientras OT controla procesos físicos.
b. Los sistemas IT operan en tiempo real, mientras que los OT no.
c. OT utiliza redes inalámbricas, mientras IT usa redes cableadas.
d. IT se enfoca en sensores, mientras OT usa actuadores.

8. La ISO 45001 está relacionada con:

a. Salud y seguridad laboral
b. Seguridad eléctrica
c. Gestión de datos empresariales
d. Normas de diseño de redes

9. ¿Qué normativa regula los sistemas instrumentados de seguridad?

a. NFPA 70E
b. IEC 61511
c. ISO 45001
d. OPC UA

10. ¿Qué característica se destaca en una red LAN industrial?

a. Comunicación entre plantas
b. Uso exclusivo de Wi-Fi
c. Conexión entre servidores empresariales
d. Alta velocidad de transmisión

Ejercicios de autoevaluación Unidad de Aprendizaje 6

1. Indica si las siguientes afirmaciones son verdaderas o falsas.

a. La transformación digital en la industria ha permitido la automatización de procesos y la conexión de sistemas industriales con la tecnología de la información y otras tecnologías emergentes.

- **Verdadero**
- Falso

b. Los entornos industriales, a diferencia de los sistemas de TI tradicionales, deben garantizar la continuidad operativa y la seguridad de los procesos físicos.

- **Verdadero**
- Falso

c. Para lograr una protección efectiva, se requiere una segmentación adecuada de la red industrial que permita controlar, aislar y proteger los diferentes niveles de los sistemas de control.

- **Verdadero**
- Falso

2. ¿Cuál es el objetivo principal de la ciberseguridad industrial?

a. Proteger los sistemas de información de la empresa.
b. Asegurar la continuidad operativa y la seguridad de los sistemas de control industrial (ICS).
c. Incrementar la eficiencia operativa mediante la automatización.
d. Reducir los costos de producción de la planta industrial.

3. ¿Qué diferencia la ciberseguridad de los sistemas de TI de la ciberseguridad de los sistemas OT?

a. La ciberseguridad OT prioriza la disponibilidad y la seguridad física.
b. La ciberseguridad de TI prioriza la disponibilidad y la seguridad física.
c. La ciberseguridad de TI no utiliza herramientas de *hacking* ético.

d. La ciberseguridad OT solo se aplica en entornos de la nube.

4. ¿Cuál de las siguientes afirmaciones sobre la transformación digital en la industria es correcta?

a. La automatización de procesos reduce la exposición a ciberamenazas.
b. La transformación digital elimina la necesidad de controladores lógicos programables.
c. La transformación digital se aplica solo en la red corporativa.
d. La transformación digital expone los sistemas industriales a nuevas amenazas cibernéticas.

5. ¿Cuántos niveles conforman el modelo Purdue?

a. 5
b. 6
c. 7
d. 4

6. ¿Cuál es la amenaza principal a la que se enfrenta el nivel 0 del modelo Purdue?

a. Acceso no autorizado a sistemas de control.
b. *Ransomware* dirigido a servidores de bases de datos.
c. Manipulación física de sensores y actuadores.
d. Acceso remoto no controlado a sistemas SCADA.

7. ¿Cuál de las siguientes técnicas de ataque permite interceptar la comunicación de protocolos industriales no cifrados?

a. *Sniffing*
b. *Fuzzing*
c. Explotación de vulnerabilidades
d. Análisis de riesgos

8. ¿Cuál de los siguientes estándares está enfocado a la protección de la

energía eléctrica en Estados Unidos?

a. NIST SP 800-82
b. IEC 62443
c. NERC CIP
d. ISO 27001

9. ¿Qué herramienta de simulación de ataques es utilizada para entrenar la ciberseguridad en entornos OT/IT?

a. *Nmap*
b. *Wireshark*
c. *Nessus*
d. *CALDERA*

10. ¿Cuál de las siguientes medidas es esencial para proteger los sistemas SCADA?

a. Cifrado TLS para la comunicación
b. Uso de Modbus sin autenticación
c. Acceso remoto no controlado
d. Exposición pública de sistemas SCADA

Ejercicios de autoevaluación Unidad de Aprendizaje 7

1. Indica si las siguientes afirmaciones son verdaderas o falsas:

a. Las plataformas como *Cybertrix-Cybring* permiten simular ataques para evaluar la seguridad de los sistemas industriales.

- **Verdadero**
- Falso

b. En la ciberseguridad industrial, la disponibilidad garantiza que los sistemas estén accesibles solo durante el horario laboral.

- Verdadero
- **Falso**

c. El *pentesting* es una técnica para analizar y explotar vulnerabilidades en sistemas de control industrial.

- **Verdadero**
- Falso

2. ¿Qué objetivo persigue la simulación de ataques en plataformas como *Cybertrix-Cybring*?

a. Verificar la usabilidad del sistema.
b. Evaluar la efectividad de las medidas de seguridad implementadas.
c. Aumentar la capacidad de almacenamiento del sistema.
d. Detectar vulnerabilidades solo en redes wifi.

3. ¿Qué elemento clave define la seguridad en los sistemas industriales?

a. Redundancia
b. Confidencialidad
c. Conexión constante a la nube
d. Escalabilidad

4. ¿Qué se entiende por *pentesting* en la ciberseguridad industrial?

a. El monitoreo en tiempo real de datos sensibles
b. Un análisis para identificar y explotar vulnerabilidades
c. La implementación de medidas de seguridad física
d. El control de acceso biométrico en plantas industriales

5. ¿Cuál es la principal ventaja de realizar pruebas de seguridad en entornos simulados?

a. Garantizar la disponibilidad constante del sistema.
b. Reducir costes operativos de la infraestructura.
c. Minimizar riesgos en los sistemas reales.
d. Mejorar la estética de los paneles de control.

6. ¿Qué función cumple la autenticación en la seguridad industrial?

a. Asegurar el acceso autorizado a los sistemas.
b. Garantizar la disponibilidad del sistema.
c. Proteger los datos en tránsito.
d. Bloquear completamente el acceso remoto.

7. ¿Qué se entiende por ciberamenaza?

a. Un usuario que no tiene entrenamiento adecuado
b. Una prueba de rendimiento en un sistema de control
c. Una herramienta de auditoría automatizada
d. Una debilidad explotada para dañar sistemas o datos

8. ¿Qué ventaja ofrece la utilización de plataformas como *Cybertrix-Cybring?*

a. La implementación automática de contraseñas seguras
b. El acceso remoto sin necesidad de autenticación
c. El análisis en tiempo real del tráfico en redes sociales
d. La simulación segura de ataques cibernéticos

9. ¿Qué principio fundamental busca asegurar la disponibilidad en sistemas industriales?

a. Prevenir interrupciones en los procesos operativos.
b. Aumentar la velocidad de procesamiento.
c. Diseñar interfaces más intuitivas para los usuarios.
d. Reducir el tamaño físico de los equipos.

10. ¿Cuál de las siguientes medidas es clave para proteger la integridad de los datos en los sistemas industriales?

a. Garantizar que los datos no sean modificados sin autorización.
b. Permitir el acceso remoto a los datos sin restricciones.
c. Asegurar la disponibilidad constante de los sistemas.
d. Proporcionar copias de seguridad solo en horario laboral.

Ejercicios de autoevaluación Unidad de Aprendizaje 8

1. Indica si las siguientes afirmaciones son verdaderas o falsas.

a. En un mundo empresarial cada vez más interconectado, la ciberseguridad industrial se ha convertido en una necesidad crítica para la protección de infraestructuras esenciales.

- **Verdadero**
- Falso

b. No todos los enfoques *red team* y *blue team* permiten a los profesionales simular ataques reales y desarrollar respuestas efectivas para mitigar riesgos.

- Verdadero
- **Falso**

c. Aunque un *ransomware* es un código malicioso muy peligroso, no termina de ser una amenaza crítica en los entornos industriales.

- Verdadero
- **Falso**

2. ¿Cuál es el objetivo principal de la ciberseguridad industrial?

a. Mejorar la eficiencia de los procesos industriales.
b. Minimizar vulnerabilidades y reducir el impacto de ciberataques.
c. Eliminar cualquier tipo de conexión en infraestructuras críticas.
d. Evitar completamente la automatización en redes OT.

3. ¿Qué enfoques se utilizan en la ciberseguridad para evaluar y mitigar amenazas en redes industriales?

a. *White team y black team*
b. *Ethical hacking y pentesting*
c. *Red team y blue team*
d. *Offensive security y passive security*

4. ¿Cuál de los siguientes es un riesgo principal del *ransomware* en entornos industriales?

a. Reducción de la velocidad de producción
b. Paralización de la producción y riesgo para la seguridad de los trabajadores
c. Mayor consumo de energía en la red OT
d. Pérdida de conectividad temporal sin daños significativos

5. ¿Cuál de los siguientes es un objetivo común de los ataques de *ransomware* en sistemas OT?

a. Espionaje empresarial
b. Pruebas de control de calidad
c. Sabotaje industrial
d. Monitoreo del rendimiento de la red

6. ¿Cuál es el método más común de distribución de *ransomware* en redes OT?

a. *Phishing* y engaño al personal
b. Ataques físicos a servidores
c. Correos electrónicos corporativos legítimos
d. Uso de *firewalls* para detectar ataques

7. ¿Qué representa un gran riesgo en redes industriales debido a su falta de actualizaciones?

a. Uso de servidores redundantes
b. Dispositivos OT antiguos sin parches de seguridad
c. Implementación de inteligencia artificial
d. Virtualización de entornos

8. ¿Cuál de los siguientes es un impacto del *ransomware* en entornos industriales?

a. Reducción de la capacidad de cómputo
b. Mejora en la segmentación de red
c. Aumento de la eficiencia de la producción
d. Riesgo para la seguridad de los trabajadores

9. ¿Qué incidente histórico de *ransomware* afectó gravemente a la empresa Maersk?

a. *NotPetya*
b. *WannaCry*
c. *Stuxnet*
d. *Pegasus*

10. ¿Qué aspecto clave pudo haber prevenido el ataque a Maersk?

a. Uso de cifrado de extremo a extremo
b. Segmentación de redes y actualización de parches de seguridad
c. Desconexión total de la red de internet
d. Deshabilitación de todos los servidores en horario nocturno