Principios de seguridad

Conozca la tríada de la seguridad, los modelos y los principios de seguridad más comunes.

Tarea 1: Introducción.

La seguridad se ha convertido en una palabra de moda a día de hoy y todas las empresas afirman que la tienen, y que se puede confiar en ello. Pero ¿es así?
Antes de empezar debemos pensar ¿qué es lo que queremos proteger?

- Impedir que un niño pequeño acceda a tu portátil.
- O proteger los datos que tiene el portátil que contienen diseños técnicos valorados en millones de dólares.

Son situaciones y cuidados muy diferentes en contra del acceso de un niño, y contra los actores del espionaje industrial.

- **Respuesta:** Simplemente hacer clic para Enviar (no se necesita respuesta).

Tarea 2: CIA.

Antes de calificar algo por lo seguro, hay que analizar mejor en qué consiste la seguridad. Cuando se quiere juzgar la seguridad de un sistema, hay que pensar en términos de la tríada de la seguridad: **confidencialidad**, **integridad** y **disponibilidad** (CIA).

- **Confidencialidad:** garantiza que sólo las personas o destinatarios previstos puedan acceder a los datos.
- **Integridad:** pretende garantizar que los datos no puedan ser alterados; además, podremos detectar cualquier alteración en caso de que se produzca.
- **Disponibilidad:** pretende garantizar que el sistema o servicio esté disponible cuando se necesite.

- **Pregunta:** Click on "View Site" and answer the five questions. What is the flag that you obtained at the end?
  - **Respuesta: THM{CIA_TRIAD}**

Tarea 3: DAD.

La seguridad de un sistema se ve atacada por uno de varios medios. Puede ser mediante la revelación de datos secretos, la alteración de datos o la destrucción de datos.

- **Divulgación:** es lo contrario de la confidencialidad. En otras palabras, la divulgación de datos confidenciales sería un ataque a la confidencialidad.
- **Alteración:** es lo contrario de la integridad. Por ejemplo, la integridad de un cheque es indispensable.
- **Destrucción/Denegación:** es lo contrario de Disponibilidad.

❖ **Pregunta:** The attacker managed to gain access to customer records and dumped them online. What is this attack?
  ➢ **Respuesta: Disclosure**

❖ **Pregunta:** A group of attackers were able to locate both the main and the backup power supply systems and switch them off. As a result, the whole network was shut down. What is this attack?
  ➢ **Respuesta: Destruction/Denial**

Tarea 4: Conceptos fundamentales de los modelos de seguridad.

Cómo podemos crear un sistema que garantice una o varias funciones de seguridad.
La respuesta estaría en utilizar modelos de seguridad garantizada. En esta tarea, presentaremos tres modelos de seguridad fundamentales:

- El Modelo Bell-LaPadula
- El Modelo de Integridad Biba
- El Modelo Clark-Wilson

❖ **Pregunta:** Click on "View Site" and answer the four questions. What is the flag that you obtained at the end?
  ➢ **Respuesta: THM{SECURITY_MODELS}**

Tarea 5: Defensa en profundidad.

La defensa de profundidad se refiere a la creación o organización de seguridad de múltiples niveles, también conocida como multinivel.
Considerando este caso, digamos que disponemos de nuestros documentos privados en un cajón bajo llave, pero ¿quieres que esa cerradura sea lo único que impide al ladrón obtener tus documentos privados?
Si pensamos en seguridad multinivel, pensaríamos mejor en que los documentos estén en el cajón bajo llave, la puerta del cuarto esté cerrada, la puerta principal esté cerrada, que el portón esté cerrado, todo bajo llave y hasta poner un sistema de cámaras de vigilancia.
Aunque estos múltiples niveles de seguridad no pueden detener a todos los ladrones, bloquearan a la mayoría y frenarían a los demás.

❖ **Respuesta:** Simplemente hacer clic para Enviar (no se necesita respuesta).

Tarea 6: ISO/IEC 19249.

La Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (CEI) han creado la norma ISO/IEC 19249.
En esta tarea, repasamos brevemente la norma ISO/IEC 19249:2017 Tecnología de la información - Técnicas de seguridad - Catálogo de principios arquitectónicos y de diseño para productos, sistemas y aplicaciones seguros.

- **Respuesta: “2”**
- **Respuesta: “1”**
- **Respuesta: “5”**

Tarea 7: Confianza cero Vs. Confiar pero verificar.

La confianza es esencial pero debe gestionarse con principios de seguridad como "Confía pero verifica" y "Confianza Cero", que promueven la verificación constante y la reducción de riesgos al no asumir confianza por defecto. Zero Trust se implementa, por ejemplo, con microsegmentación, aunque debe aplicarse sin afectar la operatividad del negocio.

- **Respuesta:** Simplemente hacer clic para Enviar (no se necesita respuesta).

Tarea 8: Amenaza O Riesgo.

Vulnerabilidad, amenaza y riesgo son conceptos clave en seguridad. Una vulnerabilidad es una debilidad, una amenaza es el peligro potencial asociado, y el riesgo es la probabilidad e impacto de que una amenaza explote una vulnerabilidad. Estos conceptos se aplican tanto en seguridad física como en sistemas informáticos.

- **Respuesta:** Simplemente hacer clic para Enviar (no se necesita respuesta).

Tarea 9: Conclusión.

- **Respuesta:** Simplemente hacer clic para Enviar (no se necesita respuesta).