

## Documentación Sala Security Principles (Principios de Seguridad).

### Tarea 1 Introduction

Acá solo veremos la importancia de conocer quién es nuestro adversario. Solo debemos presionar complete.

Pregunta

Think how you would describe something as secure.

Respuesta

Complete

### Tarea 2 CIA

En esta tarea tenemos que leer los conceptos de CIA (confidencialidad, Integridad y disponibilidad)

Presionamos en view site y nos abrirá una ampliación del sitio donde nos harán unas preguntas y responderemos haciendo click en las opciones que están abajo.

IMPORTANTE: las preguntas pueden cambiar de orden.

Pregunta

Two companies are negotiating a certain agreement; however, they want to keep the details of the agreement secret. Which security pillar are they emphasizing?

Respuesta

C

Pregunta

At a police checkpoint, the police officer suspected that the vehicle registration papers were fake. Which security function does the officer think is lacking?

Respuesta

I

Pregunta

You went to cash out a cheque, and the bank teller made you wait for five minutes as they confirmed the signature of the cheque's issuer. Which security function is the bank teller checking?

Respuesta

I

Pregunta

One hotel is stressing that the Internet over its WiFi network must be accessible 24 hours a day, seven days a week. Which security pillar is the hotel requiring?

Respuesta

A

Pregunta

As the troops got deployed, the leader stressed that they should not communicate their location to anyone while the mission was ongoing. Which security function did the leader want to have?

Respuesta

C

Luego de responder las 5 preguntas nos dara la FLAG para pegar en la respuesta

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

Aca leeremos la teoría sobre DAD (divulgación, alteración y destrucción/denial)

#### 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 Fundamental Concepts of Security Models (Conceptos Fundamentales de los Modelos de Seguridad)

En esta tarea vamos a leer la teoría sobre los modelos de seguridad más utilizados.

Presionamos en view site y nos abrirá una ampliación del sitio donde nos harán unas preguntas y responderemos haciendo click en las opciones que están abajo.

IMPORTANTE: las preguntas pueden cambiar de orden.

#### Pregunta

Which model dictates "no read down"?

#### Respuesta

Biba

#### Pregunta

Which model states "no read up"?

#### Respuesta

Bell

#### Pregunta

Which model teaches "no write down"?

#### Respuesta

Bell

#### Pregunta

Which model forces "no write up"?

#### Respuesta

Biba

Al responder correctamente las 4 preguntas nos dará la FLAG para pegar al final de la tarea

#### 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 Defence-in-Depth (Defensa en Profundidad)

En esta tarea vamos a conocer los conceptos sobre defensa en profundidad. No necesitas responder ninguna pregunta solo presionar Complete

#### Tarea 6 ISO/IEC 19249

Vamos a leer la teoría referente a las normas ISO y IEC con respecto a los principios de la seguridad.

Pregunta

Which principle are you applying when you turn off an insecure server that is not critical to the business?

Respuesta

2

Pregunta

Your company hired a new sales representative. Which principle are they applying when they tell you to give them access only to the company products and prices?

Respuesta

1

Pregunta

While reading the code of an ATM, you noticed a huge chunk of code to handle unexpected situations such as network disconnection and power failure. Which principle are they applying?

Respuesta

5

#### Tarea 7 Zero Trust versus Trust but Verify (Cero Confianza versus Confianza, pero Verificar)

En esta tarea vamos a ver la teoría sobre confianza cero y confía, pero verifica. Leer atentamente ya que es importante. No tenemos que responder preguntas solo presione Complete.

#### Tarea 8 Threat versus Risk (Amenaza versus Riesgo)

En esta tarea vamos a ver la teoría sobre los 3 términos para evitar cualquier confusión. No tenemos que responder preguntas solo presione Complete.

#### Tarea 9 Conclusión

No es más q un breve resumen de lo q se vio.