Documentación Sala Governance & Regulation (Gobernanza y Regulación)

Tarea 1: Introducción

Vamos a leer una pequeña reseña de lo que consiste la sala y vamos a ver los objetivos de aprendizaje y los prerrequisitos que tenemos que tener para comprender las tareas. No necesitas responder preguntas solo presionar Complete

Tare 2: Why is it important? (¿Por qué es importante?)

Vamos a leer la importancia de la gobernanza en la seguridad de la información. Viendo terminologías, procesos reglamentos, beneficios y leyes que nos ayudarán en el día a día.

Pregunta

A rule or law enforced by a governing body to ensure compliance and protect against harm is called?

Respuesta

Regulation

Pregunta

Health Insurance Portability and Accountability Act (HIPAA) targets which domain for data protection?

Respuesta

Healthcare

Tarea 3: Information Security Frameworks (Marcos de Seguridad de la Información)

En esta tarea vamos a leer sobre conceptos de seguridad de la información, como desarrollar documentos de gobernanza, como preparar una política de contraseñas y procedimientos de respuesta a incidentes.

Pregunta

The step that involves monitoring compliance and adjust the document based on feedback and changes in the threat landscape or regulatory environment is called?

Respuesta

Review and update

Pregunta

A set of specific steps for undertaking a particular task or process is called?

Respuesta

Procedures

Tarea 4: Governance Risk and Compliance (GRC)(Riesgo de Gobernanza y Cumplimiento)

Vamos a leer teroria complementaria sobre la gobernanza, componentes guías para desarrollar el programa de gobernanza y un ejemplode gobernanza en el sector financiero.

Pregunta

What is the component in the GRC framework involved in identifying, assessing, and prioritising risks to the organisation?

Respuesta

Risk Management

Pregunta

Is it important to monitor and measure the performance of a developed policy? (yea/nay)

Respuesta

yea

Tarea 5: Privacy and Data Protection(Privacidad y Protección de Datos)

En esta tarea vamos a conocer sobre la importancia de la seguridad de la información en la UE y las penalidades que se pueden dar en distintos casos.

Pregunta

What is the maximum fine for Tier 1 users as per GDPR (in terms of percentage)?

Respuesta

4

Pregunta

In terms of PCI DSS, what does CHD stand for?

Respuesta

cardholder data

Tarea 6: NIST Special Publications(NIST Special Publications)

En esta tarea veremos sobre las publicaciones NIST 800-53 y 800-63B que serían publicaciones donde se informa de prácticas para organizar las practicas con identidades digitales.

Pregunta

Per NIST 800-53, in which control category does the media protection lie?

Respuesta

Physical

Pregunta

Per NIST 800-53, in which control category does the incident response lie?

Respuesta

Administrative

Pregunta

Which phase (name) of NIST 800-53 compliance best practices results in correlating identified assets and permissions?

Respuesta

Map

Tarea 7: Information Security Management and Compliance (Gestión y Cumplimiento de la Seguridad de la Información)

En esta tarea leeremos sobre las normas ISO/IEC 27001 y cómo planifica una auditoría SOC

Pregunta

Which ISO/IEC 27001 component involves selecting and implementing controls to reduce the identified risks to an acceptable level?

Respuesta

Risk treatment

Pregunta

In SOC 2 generic controls, which control shows that the system remains available?

Respuesta

Availability

Tarea 8: Conclusión

En esta parte leeremos un breve resumen y al presionar view site jugaremos un juego donde dispararemos un misil a unas burbujas y si estamos en lo correcto se destruirán en caso contrario nos hará una pregunta.

Pregunta

Click the View Site button at the top of the task to launch the static site in split view. What is the flag after completing the exercise?

Respuesta

THM{SECURE_1001}