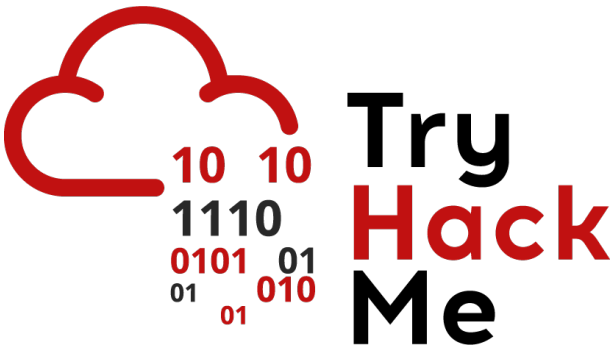
Writeup: Sala *Governance and Regulation*

Autor: Ismaeldevs

Plataforma: TryHackMe

4 de julio de 2025



Índice

1. Introducción

La sala Governance and Regulation ofrece una introducción esencial a los marcos normativos y de cumplimiento que rigen la ciberseguridad en las organizaciones. Está diseñada para ayudar a comprender cómo las políticas, estándares y regulaciones internacionales se integran en una estrategia de seguridad efectiva.

2. Sala

2.1. Tarea 1 - Introducción

Comenzamos con una introducción donde se establece un contexto de el aprendizaje sobre gobernanza y regulación en ciberseguridad. Destaca la importancia de implementar políticas y marcos regulatorios sólidos para proteger los activos de información y garantizar el cumplimiento normativo.

Además, nos dejan en cuenta cuales son los objetivos de aprendizaje los cuales son:

- Comprender el papel fundamental de la gobernanza y la regulación en la ciberseguridad.
- Familiarizarse con leyes, regulaciones, políticas, estándares y directrices internacionales relevantes.
- Explorar el marco de Gobernanza, Gestión de Riesgos y Cumplimiento (GRC).
- Desarrollar y mejorar la postura de ciberseguridad conforme a estándares internacionales como ISO 27001 y NIST 800-53.

Una vez que comprendemos la introducción podemos comenzar la sala.

Respuesta: **No requiere respuesta** (Hacemos clic en **Submit**).

2.2. Tarea 2 - Por qué es importante?

En está tarea se destaca la relevancia de la gobernanza y la regulación en la ciberseguridad organizacional. Se enfoca en cómo estas prácticas fortalecen la postura de seguridad, aseguran el cumplimiento normativo y alinean las operaciones con los objetivos empresariales.

En esta parte se ve temas como la gobernanza de la seguridad de la información, regulaciones claves donde se aborda regulaciones internacionales fundamentales que

las organizaciones deben cumplir para proteger los datos y mantener la confianza de las partes interesadas, también, algunos beneficios claves sobre implementar una sólida gobernanza en seguridad de la información y por último algunas leyes y reglamentos pertinentes.

Después de un aprendizaje sobre estos temas podemos proceder a responder las preguntas:

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**

2.3. Tarea 3 - Marcos de seguridad de la información

La tarea nos introduce a los componentes esenciales que conforman los marcos de seguridad en las organizaciones. Estos marcos proporcionan una estructura organizada para proteger los activos de información y garantizar el cumplimiento normativo.

Aprenderemos elementos claves de un marco de seguridad (Políticas, Estándares, Directrices, etc), también el desarrollo de documentos de gobernanza que es un proceso que incluye la evaluación periódica de políticas y la incorporación de comentarios de las partes interesadas para realizar ajustes necesarios, luego la preparación de una política de contraseñas y para finalizar la elaboración de un procedimiento de respuesta a incidentes.

Una vez que finalizamos nuestro aprendizaje en esta tarea podemos responder las siguientes preguntas:

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: **Procedure**

2.4. Tarea 4 - Gobernanza, Riesgo y Cumplimiento (GRC)

Ahora aprenderemos sobre el marco GRC, que ayuda a las organizaciones a alinear sus objetivos empresariales con las mejores prácticas de seguridad, regulaciones y estándares, manteniendo el cumplimiento normativo. Además, este marco consta de tres componentes los cuales son

- Gobernanza
- Gestión de Riesgos
- Cumplimiento

Otros temas que se abordan en esta tarea son cómo desarrollar un programa GRC y el comprender la importancia de monitorear y medir las políticas que es esencial supervisar y evaluar el desempeño de las políticas desarrolladas para garantizar su eficacia y realizar ajustes cuando sea necesario.

Después de comprender el GRC responderemos las siguientes preguntas:

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**

2.5. Tarea 5 - Privacidad y protección de datos

Ahora en esta tarea vamos a centrarnos en la importancia de salvaguardar la información personal y financiera dentro de las organizaciones. Esta tarea destaca cómo las regulaciones internacionales, como el Reglamento General de Protección de Datos (GDPR) y el Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI DSS), establecen directrices para proteger los datos sensibles y garantizar el cumplimiento normativo.

También en esta tarea se abordan temas claves como el GDPR: Establece que las organizaciones pueden enfrentar multas de hasta el 4 porciento de su facturación anual global por infracciones graves relacionadas con la privacidad de los datos y por último el PCI DSS que se enfoca en la protección de los datos del titular de la tarjeta, asegurando que las empresas que procesan pagos mantengan altos estándares de seguridad.

Después de estudiar estos temas nos toca responder las siguientes preguntas:

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

2.6. Tarea 6 - Publicaciones especiales del NIST

En esta tarea nos enfocaremos en aprender las directrices del Instituto Nacional de Estándares y Tecnología (NIST), especialmente la publicación 800-53, que proporciona un marco para implementar controles de seguridad y privacidad en sistemas de información. Abordaremos temas que son clave los cuales son los siguientes:

- **NIST 800-53** que categoriza los controles en cuatro tipos (administrativos, técnicos, físicos y operacionales), abarcando 20 familias diferentes.
- Controles como la protección de medios se clasifican bajo controles físicos, mientras que la respuesta a incidentes se considera un control administrativo.
- Por último, las mejores prácticas de cumplimiento incluyen fases como Descubrir y Clasificar, Mapear, Gestionar y Monitorear

Ahora que aprendimos sobre estas publicaciones especiales del NIST podemos pasar a responder las siguientes preguntas:

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

2.7. Tarea 7 - Gestión y cumplimiento de la seguridad de la información

En esta tarea vamos a centrarnos en dos estándares clave para garantizar la seguridad y cumplimiento en las organizaciones que son:

- **ISO/IEC 27001**: Este es un estándar internacional que establece los requisitos para implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI).
- **SOC 2**: Este estandar es un informe de auditoría que evalúa cómo los proveedores de servicios gestionan los datos para proteger la privacidad y los intereses de sus clientes.

El objetivo de esta tarea es el aprender la importancia de adoptar y cumplir con estos estándares para fortalecer la postura de seguridad de la información y asegurar la confianza de las partes interesadas.

Después de estudiar estos estándares vamos a proceder en responder las siguientes preguntas:

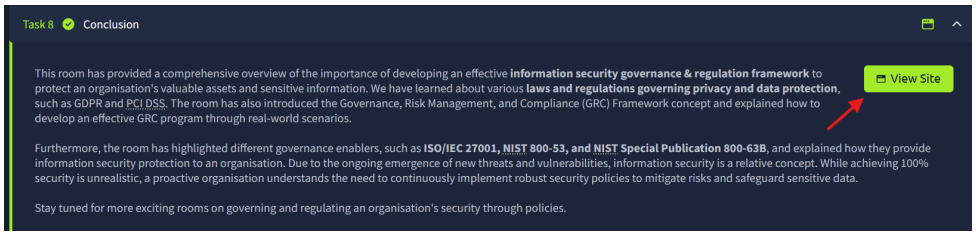
Pregunta: Which ISO/IEC 27001 component involves selecting and implementing controls to reduce the identified risks to an acceptable level?
Respuesta: **Risk treatment**

Pregunta: In SOC 2 generic controls, which control shows that the system remains available?
Respuesta: **Availability**

2.8. Tarea 8 - Conclusión

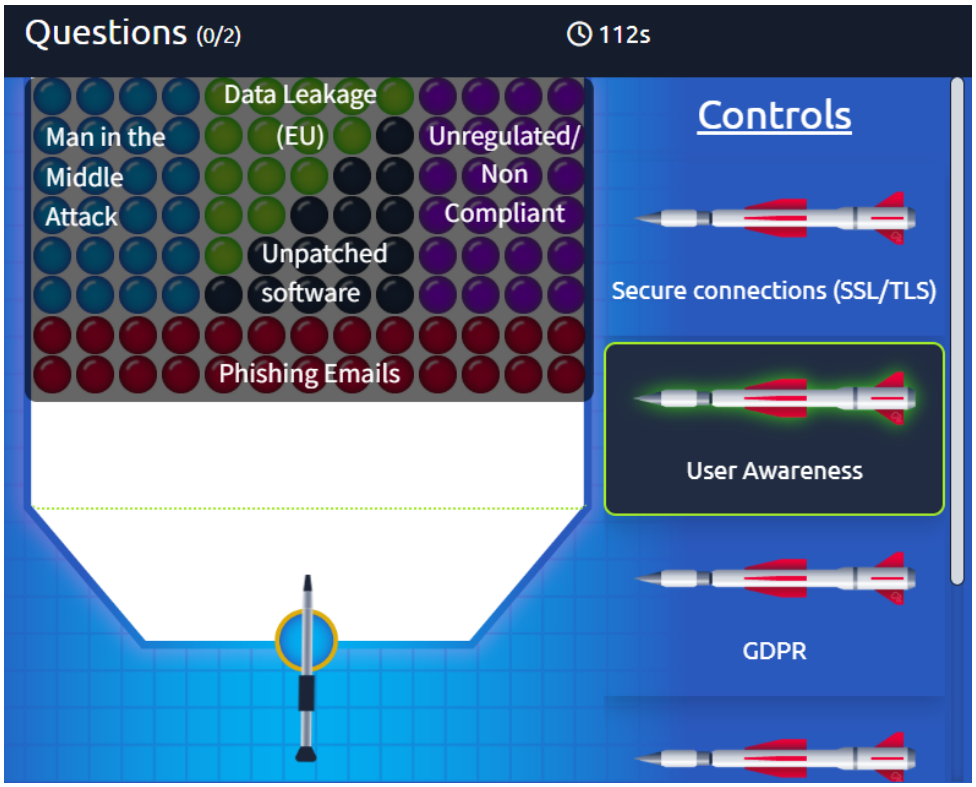
Terminamos la sala con esta última tarea donde resalta lo clave que fue aprender sobre gobernanza y regulación en ciberseguridad. La importancia de implementar marcos como **ISO/IEC 27001**, **NIST 800-53** y **SOC 2** para establecer políticas, procedimientos y controles que protejan los activos de información y aseguren el cumplimiento normativo. Además, se destaca cómo la adopción de prácticas de gobernanza, gestión de riesgos y cumplimiento (**GRC**) fortalece la postura de seguridad de una organización y alinea las operaciones con los objetivos empresariales.

Para dar por finalizado la sala debemos completar un ejercicio y obtener la flag de respuesta para completar. Para ello debemos ir a la parte superior de la tarea 8 y darle click en **View Site**.



Una vez que le damos de nos desplegara un sitio estático donde procederemos a jugar un juego donde debemos responder correctamente para conseguir la flag.

Para responder la primera pregunta debemos seleccionar a la derecha la opción de **User Awareness** y hacer clic en medio para indicar que se relaciona con la vulnerabilidad de **Phishing Emails**.

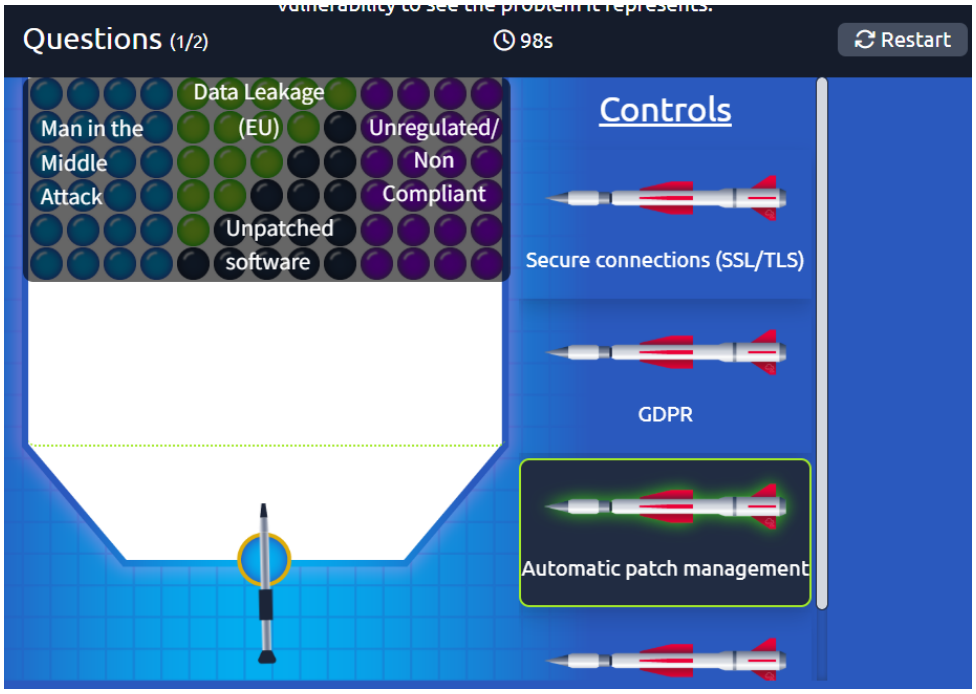


Una vez que acertamos se nos va a desplegar una pregunta con diferentes opciones de respuesta.

Pregunta: Which of the following is a valid NIST publication dealing with Security and Privacy Controls for Information Systems and Organisations?

Respuesta: **NIST 800-53**

Ahora procederemos a destruir la siguiente burbuja, para ello, vamos a seleccionar el misil de **Automatic path managment** y haremos clic apuntando a la vulnerabilidad de **Unpatched Software**.

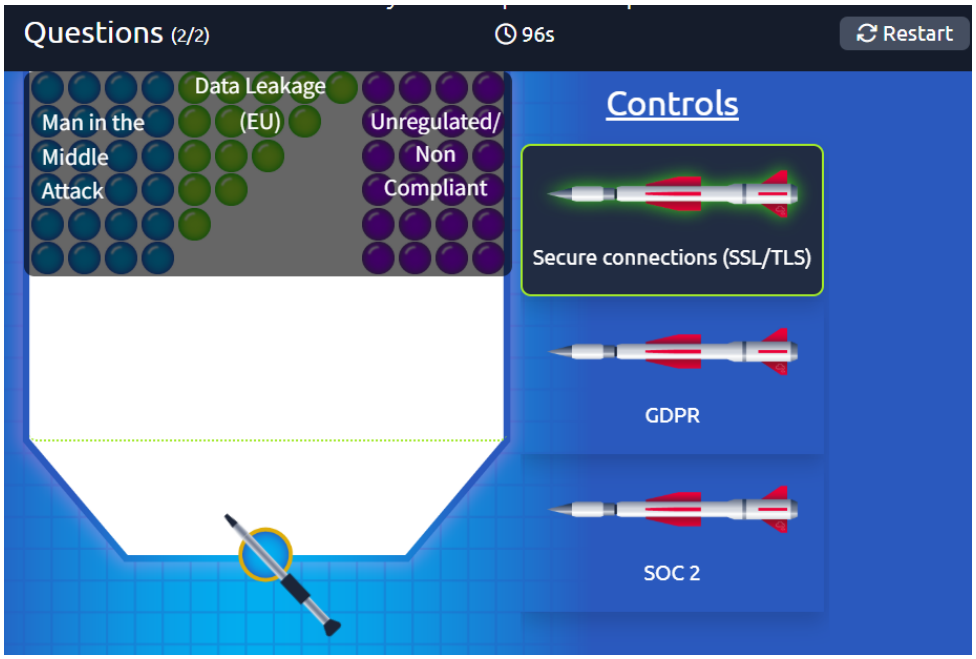


Nuevamente se nos desplegara una pregunta con múltiples opciones de respuesta.

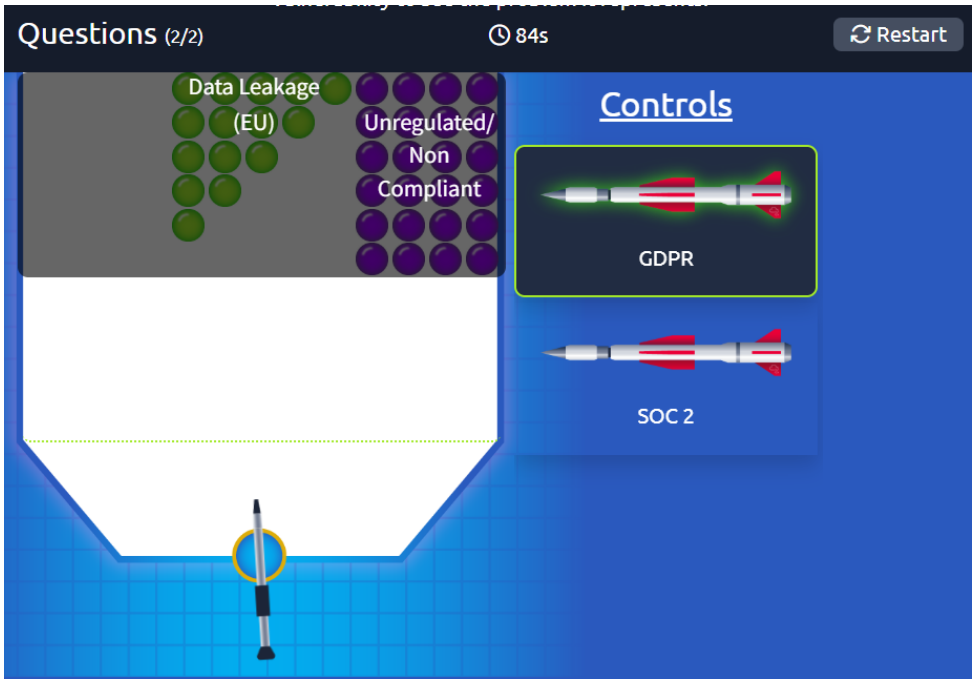
Pregunta: Which of the following frameworks primarily assists in Information Security Management and Compliance?

Respuesta: **SOC 2**

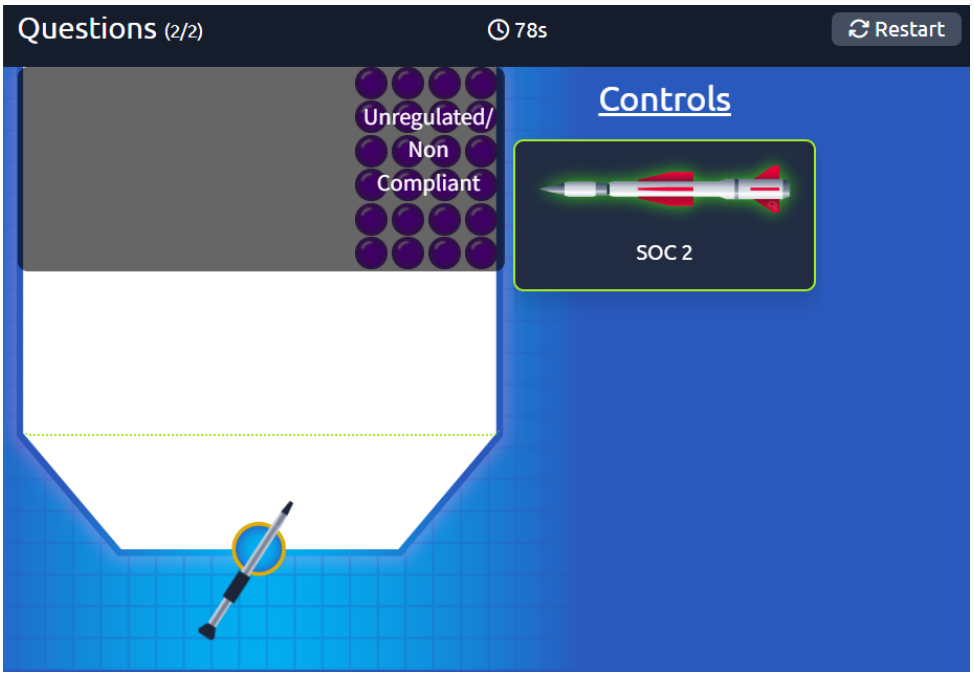
Una vez que respondemos las dos preguntas del juego podemos proceder a terminar de romper el resto de burbujas. Vamos a seleccionar el **Secure connections (SSL/TLS)** y le damos clic apuntando a la vulnerabilidad **Man in the Middle Attack**.



Después seleccionaremos el de **GDPR** y hacemos nuevamente clic apuntando a la burbuja **Data Leakage (EU)**.



Por último, con el **SOC 2** vamos a finalizar de romper todas las burbujas con la vulnerabilidad de **Unregulated / Non Compliant**.



Una vez rompemos la última burbuja nos proporcionara la flag de respuesta de la tarea y completaremos la sala de Gobernanza y regulación.

Respuesta: **THM{SECURE_1001}**

3. Conclusión sobre la Sala

Esta sala fue una buena introducción integral a los principios fundamentales de la gobernanza y la regulación en ciberseguridad. A través de ocho tareas interactivas abordando diferentes temas claves donde se aprendió cómo las organizaciones pueden establecer políticas, marcos y controles para proteger sus activos de información y garantizar el cumplimiento normativo.

Al completar esta sala, logramos adquirir una comprensión sólida de cómo las políticas, estándares y regulaciones se combinan para formar una estrategia de seguridad efectiva.