

Gobernanza y regulación

Tarea 1: Introducción

P: Estoy listo para iniciar la sala.

R: No se necesita respuesta

Tarea 2: ¿Por qué es importante?

P1: ¿Cómo se llama una regla o ley aplicada por un órgano de gobierno para garantizar el cumplimiento y proteger contra daños?

R1: Regulation / Reglamento

P2: ¿A qué ámbito de protección de datos se dirige la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA)?

R2: Healthcare / Salud

Tarea 3: Marcos de seguridad de la información

P1: ¿Cómo se llama el paso que implica monitorear el cumplimiento y ajustar el documento en función de la retroalimentación y los cambios en el panorama de amenazas o el entorno regulatorio?

R1: Review and update / Revisar y actualizar

P2: ¿Cómo se llama un conjunto de pasos específicos para llevar a cabo una tarea o proceso en particular?

R2: Procedure / Procedimiento

Tarea 4: Gobernanza, Riesgo y Cumplimiento (GRC)

P1: ¿Cuál es el componente del marco GRC involucrado en la identificación, evaluación y priorización de los riesgos para la organización?

R1: Risk Management / Gestión de riesgos

P2: ¿Es importante monitorear y medir el desempeño de una política desarrollada? (sí/no)

R2: Yea / Si

Tarea 5: Privacidad y protección de datos

P1: ¿Cuál es la multa máxima para los usuarios de Nivel 1 según el RGPD (en términos de porcentaje)?

R1: 4

P2: En términos de PCI DSS, ¿qué significa CHD?

R2: cardholder data / datos del titular de la tarjeta

Tarea 6: NIST Special Publications

P1: Según NIST 800-53, ¿en qué categoría de control se encuentra la protección de los medios?

R1: Physical / Físico

P2: Según NIST 800-53, ¿en qué categoría de control se encuentra la respuesta a incidentes?

R2: Administrative / Administrativo

P3: ¿Qué fase (nombre) de las mejores prácticas de cumplimiento de NIST 800-53 da como resultado la correlación de los activos y permisos identificados?

R3: Map

Tarea 7: Information Security Management and Compliance

P1: ¿Qué componente de la norma ISO/IEC 27001 implica la selección e implementación de controles para reducir los riesgos identificados a un nivel aceptable?

R1: Risk treatment / Tratamiento de riesgos

P2: En los controles genéricos SOC 2, ¿qué control muestra que el sistema permanece disponible?

R2: Availability / Disponibilidad

Tarea 8: Conclusion

P: Haga clic en el botón "Ver sitio" en la parte superior de la tarea para abrir el sitio estático en vista dividida. ¿Cuál es la bandera después de completar el ejercicio?

Nos aparecera el siguiente desafío, a medida que avancemos nos haran preguntas:

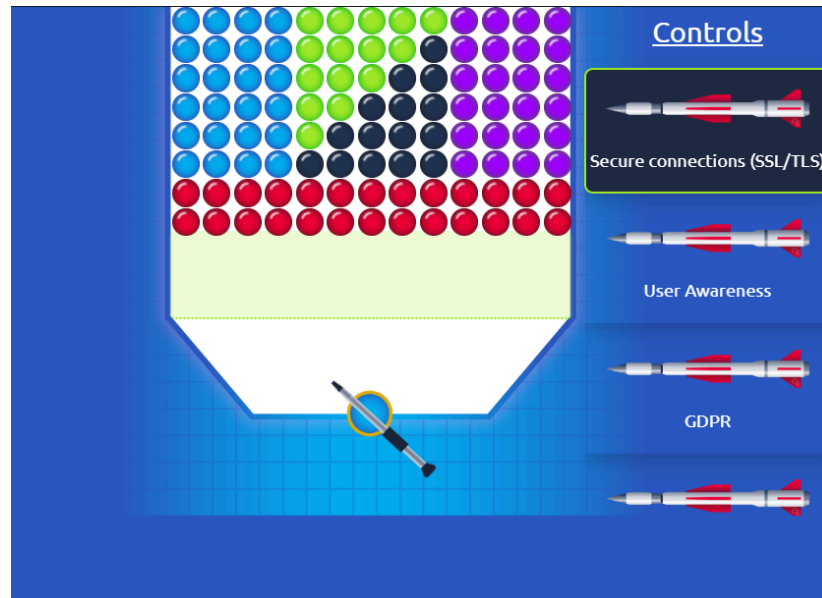


Figura 1 (Lab)

User Awareness (Rojo) - Automatic patch management (Negro)

Secure connections (Azul) - SOC 2(Violeta) - GDPR (Verde)

La primera pregunta es:

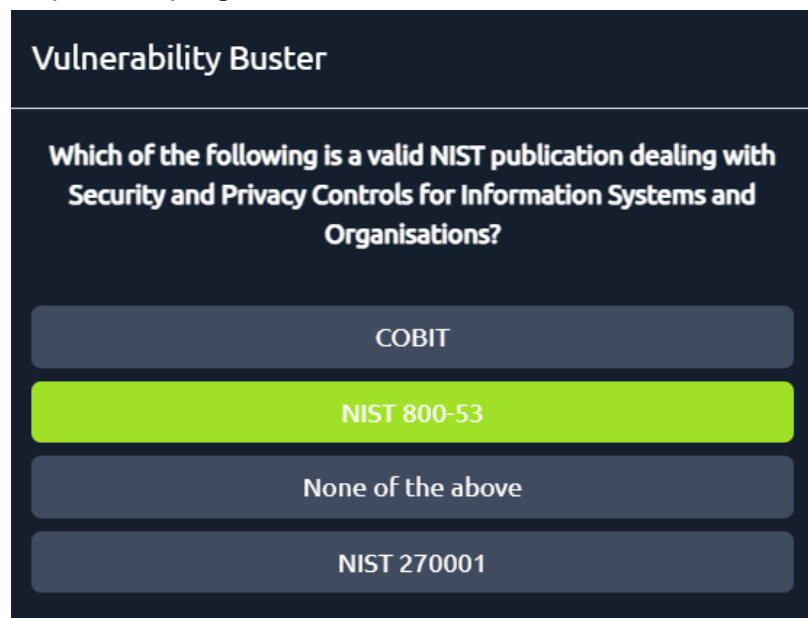


Figura 2 (Pregunta 1)

La segunda pregunta es:

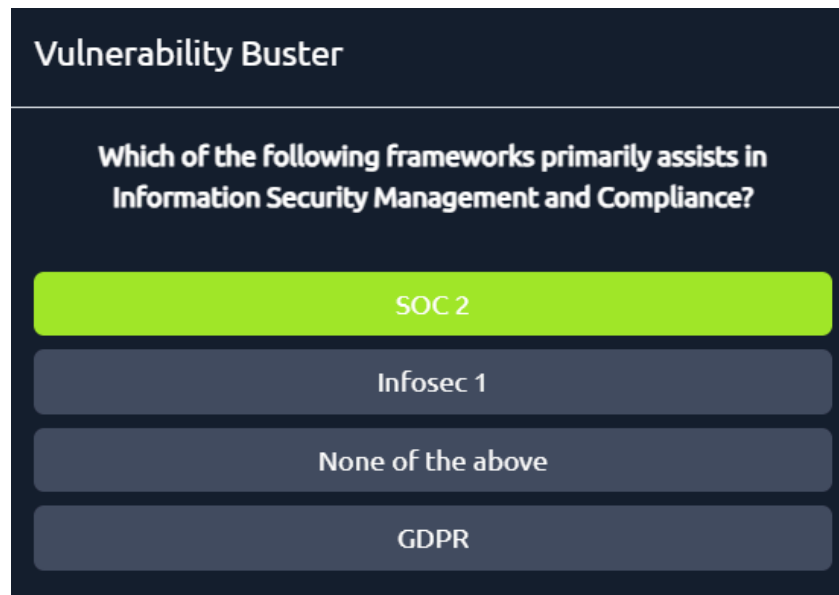




Figura 3 (Pregunta 2)

Bandera conseguida con éxito



Figura 4 (Flag)

R: THM{SECURE_1001}

 **LinkedIn:** <https://www.linkedin.com/in/mateo-rodr%C3%ADguez-suar-202695249/>
 **GitHub:** <https://github.com/MaateoSuar>