Gobernanza y Regulación

Explore políticas y marcos vitales para regular la seguridad cibernética en una organización.

Tarea 1: Introducción.

La ciberseguridad requiere un enfoque integral con políticas, monitoreo y cumplimiento para proteger sistemas sensibles de actores maliciosos y evitar daños o robos de datos.

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

Tarea 2: ¿Por qué es importante?.

En este apartado, veremos 3 Terminologías, que son las más importantes. son:

- **Gobernanza:** Gestionar y dirigir una organización o sistema para lograr sus objetivos y garantizar el cumplimiento de las leyes, reglamentos y normas.
- **Regulación:** Una regla o ley aplicada por un órgano rector para garantizar el cumplimiento y proteger contra daños.
- **Cumplimiento:** El estado de adhesión a las leyes, reglamentos y normas que se aplican a una organización o sistema.

- **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: Marcos de seguridad de la información.

Es un conjunto completo de documentos que describe la información de la seguridad y rigen como se emplean, gestiona y hace cumplir la seguridad de la organización. Esto incluye principalmente:

- **Politii:** Una declaración formal que describe las metas, principios y pautas de una organización para lograr objetivos específicos.
- **Normas:** Un documento que establece requisitos o especificaciones específicas para un proceso, producto o servicio en particular.
- **Directrices:** Un documento que proporciona recomendaciones y mejores prácticas (no obligatorias) para lograr metas u objetivos específicos.
- **Procedimientos:** Conjunto de pasos específicos para llevar a cabo una tarea o proceso en particular.
- **Bases:** Un conjunto de estándares o requisitos mínimos de seguridad que una organización o sistema debe cumplir.

❖ **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: Riesgo de gobernanza y cumplimiento (GRC).

La gobernanza y el cumplimiento son claves para la seguridad organizacional. El marco GRC integra gobernanza, gestión de riesgos y cumplimiento, alineando la seguridad con los objetivos y regulaciones de la organización.

❖ **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: Privacidad y protección de datos.

Las regulaciones de privacidad son esenciales para proteger la información personal (PII) y asegurar su manejo ético. Aplican en sectores como salud, finanzas e industria, fortaleciendo la confianza y el cumplimiento normativo.

❖ **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: Publicaciones especiales del NIST.

NIST 800-53 es una guía del NIST que proporciona controles de seguridad y privacidad para proteger la confidencialidad, integridad y disponibilidad (CIA) de los sistemas. Ayuda a las organizaciones a cumplir regulaciones y mitigar riesgos mediante un marco basado en buenas prácticas. La Revisión 5 organiza estos controles en 20 familias, cubriendo amenazas como ataques, errores, desastres y problemas de privacidad.

- **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: Gestión y cumplimiento de la seguridad de la información

La gestión de la Seguridad de la Información protege los activos frente a accesos y daños no autorizados mediante controles, evaluaciones y capacitación. El cumplimiento asegura que se sigan normas legales y del sector. Se abordarán dos estándares clave.

- **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.

Esta sala presentó la importancia de un marco eficaz de gobernanza y regulación en seguridad de la información, destacando leyes como RGPD y PCI DSS, y el enfoque GRC. También se abordaron estándares clave como ISO/IEC 27001 y NIST 800-53. Aunque la seguridad total no es posible, implementar políticas sólidas ayuda a mitigar riesgos y proteger los datos.

- **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}**