📘 Glosario: Evaluación Continua en Seguridad y APIs RESTful

🔍 1. KPI (Key Performance Indicator)

Indicador clave de rendimiento que permite **medir la eficacia de procesos o controles**, como la tasa de mitigación de vulnerabilidades o el tiempo medio de respuesta a incidentes.

⏱️ 2. MTTR (Mean Time to Remediate/Respond)

Tiempo promedio que tarda una organización en **detectar, analizar, contener y resolver una vulnerabilidad o incidente**. Cuanto menor es el MTTR, mejor es la capacidad de reacción.

🧪 3. Pentesting (Pruebas de Penetración)

Simulación controlada de ciberataques reales contra un sistema, aplicación o API para **evaluar la solidez de sus controles de seguridad**.

📚 4. Auditoría de Seguridad

Proceso sistemático y documentado para **evaluar el cumplimiento de políticas, controles y normas de seguridad**, como ISO 27001, NIST o COBIT.

📈 5. Mejora Continua

Ciclo iterativo de **evaluar, ajustar y reforzar** las medidas de seguridad basándose en datos, métricas y hallazgos de auditorías o análisis.

📊 6. SIEM (Security Information and Event Management)

Plataforma que permite **correlacionar, analizar y visualizar eventos de seguridad** en tiempo real. Ejemplos: Splunk, ELK Stack, IBM QRadar.

🧱 7. IDS/IPS (Intrusion Detection/Prevention System)

Herramientas que **detectan (IDS) o bloquean (IPS)** actividades maliciosas dentro de una red o sistema. Ejemplos: Snort, Suricata.

📜 8. ISO/IEC 27001

Estándar internacional para la **gestión de seguridad de la información (ISMS)**, que define requisitos para establecer, implementar y mejorar políticas y controles.

🧰 9. NIST SP 800-53

Publicación del Instituto Nacional de Estándares y Tecnología (NIST) de EE. UU. que establece un **conjunto de controles de seguridad y privacidad para sistemas de información**.

🌐 10. API RESTful

Interfaz de programación basada en el protocolo HTTP que permite a sistemas externos interactuar con una aplicación web. Son **puntos críticos de exposición** y deben protegerse adecuadamente.

🔐 11. Autenticación y Autorización en APIs

Controles que aseguran que **solo los usuarios correctos accedan a recursos autorizados**, mediante mecanismos como tokens JWT, OAuth2 o claves API.

🛑 12. Error 500 / 401 / 403 en APIs

Códigos de estado HTTP que indican fallas:

- 500: Error interno del servidor
- 401: No autenticado
- 403: No autorizado
  Su análisis es útil para detectar **fallas lógicas, configuraciones incorrectas o intentos de ataque**.

🔄 13. Monitoreo Continuo

Práctica de observar en tiempo real el comportamiento del sistema o API, recolectando logs, eventos y métricas para **detectar anomalías o amenazas activas**.

🧬 14. Tasa de Detección de Incidentes

Métrica que indica la capacidad de un sistema para **identificar eventos de seguridad relevantes**, como ataques, accesos sospechosos o cambios no autorizados.

📦 15. Registro de Eventos (Logs)

Información generada por sistemas y aplicaciones que **documenta acciones, accesos, errores y cambios**, útil para auditoría, análisis forense y cumplimiento normativo.
