ENS (Esquema Nacional de Seguridad): Guía práctica para su implementación y cumplimiento

El Esquema Nacional de Seguridad (ENS) es un marco regulatorio fundamental en España que establece los principios y requisitos de seguridad para la protección adecuada de la información manejada por las administraciones públicas y entidades del sector privado que colaboran con ellas. A continuación, se presentan los aspectos clave que deben tenerse en cuenta, recomendaciones prácticas y una guía.

1. Análisis de código y pruebas

- **Metodología de desarrollo seguro:** Implementar una metodología que incluya prácticas de codificación segura y revisión de código. Utilizar herramientas de análisis estático y dinámico para detectar vulnerabilidades.
- **Testing:** Realizar pruebas de seguridad exhaustivas, incluyendo pruebas de penetración (pentesting) y análisis de vulnerabilidades. Incorporar pruebas automatizadas en el ciclo de desarrollo continuo (CI/CD).

2. Infraestructura en la nube

- **Arquitectura sin servidor:** Aprovechar los servicios serverless de AWS para reducir la superficie de ataque y mejorar la escalabilidad. Configurar adecuadamente los roles y políticas de IAM (Identity and Access Management) para limitar el acceso.
- **Controles de seguridad:** Implementar las mejores

prácticas de seguridad de AWS, como la gestión de claves, el cifrado de datos en reposo y en tránsito, y la configuración de registros y auditorías.

3. Análisis de amenazas

- **Principales amenazas:** Conocer y mitigar las principales amenazas de seguridad web identificadas por OWASP, como la inyección SQL, XSS (Cross-Site Scripting) y la configuración incorrecta de seguridad.
- **Integración en el desarrollo:** Incorporar los controles y medidas de OWASP en el ciclo de vida del desarrollo de software.

4. Niveles de seguridad y declaración de aplicabilidad

- **Mapa de arquitectura de producción:** Crear un mapa detallado de la arquitectura de producción que identifique todos los componentes y sus interacciones. Asegurarse de que todos los componentes cumplan con los requisitos del ENS.
- **Declaración de aplicabilidad:** Documentar los controles de seguridad aplicables y justificar la inclusión o exclusión de cada control. Esta declaración debe ser revisada y aprobada regularmente.

5. Monitorización y herramientas de seguridad

- **SIEM (Security Information and Event Management):** Implementar una herramienta SIEM para la recolección, análisis y correlación de eventos de seguridad. Esto ayudará a identificar y responder a incidentes de manera oportuna.
- **Monitorización:** Establecer una monitorización continua

de los sistemas y redes para detectar actividades sospechosas. Utilizar IDS (Intrusion Detection Systems) e IPS (Intrusion Prevention Systems) para proteger contra intrusiones.
- **Antivirus y seguridad de dispositivos:** Asegurarse de que todos los dispositivos, especialmente portátiles, cuenten con soluciones antivirus actualizadas y configuradas correctamente.

6. Proceso de auditoría

- **Auditorías regulares:** Realizar auditorías de seguridad periódicas para evaluar el cumplimiento del ENS. Estas auditorías pueden incluir revisiones documentales y auditorías remotas.
- **Informe de auditoría:** El auditor jefe preparará un informe de auditoría identificando cualquier no conformidad.
- **Resolución de no conformidades:** Disponer de un mes para resolver las no conformidades detectadas. Priorizar las áreas críticas como la monitorización, la seguridad de los dispositivos y la autenticación.

7. Recomendaciones finales

- **Monitorización proactiva:** Implementar una monitorización proactiva para anticiparse a posibles incidentes de seguridad.
- **Formación y concienciación:** Capacitar al personal en prácticas de seguridad y concienciación sobre amenazas. Esto es fundamental para mantener una postura de seguridad robusta.
- **Autenticación y gestión de accesos:** Implementar sistemas de autenticación fuerte y gestionar los accesos de manera granular para minimizar riesgos.