Publicación sobre el Método y Criterios para la Evaluación de Seguridad

blocked URL

Se ha publicado una importante actualización sobre los **métodos y criterios** a seguir en la **Evaluación de Seguridad** dentro del ámbito de la Oficina de Calidad de la STIC. Pretende servir de guía para la realización de pruebas de seguridad de las aplicaciones y servicios web cuyo objetivo es reforzar la protección de la aplicación ante posibles amenazas. Esta normativa, que ya está disponible en su por tal oficial, introduce una serie de directrices clave para garantizar una mayor protección de los sistemas y servicios frente a las amenazas cibernéticas y otros riesgos asociados a la seguridad de la información.

¿Por qué es importante?

En un mundo cada vez más digitalizado, la seguridad de los datos y sistemas administrativos es esencial para proteger tanto a los usuarios como a las instituciones. La nueva normativa establece un marco más robusto y detallado para evaluar los riesgos de seguridad, identificando no solo las amenazas potenciales, sino también los controles necesarios para mitigarlas.

A través de la implementación de un enfoque sistemático y actualizado, se busca:

- **Fortalecer la protección de la información** sensible que maneja la administración.
- **Asegurar la continuidad** de los servicios públicos, minimizando los riesgos derivados de incidentes de seguridad.
- **Garantizar el cumplimiento** de las normativas y regulaciones europeas y nacionales en materia de protección de datos y ciberseguridad.

¿Qué incluye?

Los puntos clave de la publicación incluyen:

1. **Métodos para la evaluación de riesgos:** Se detalla cómo se deben llevar a cabo las evaluaciones de seguridad, proporcionando una metodología clara y efectiva para la identificación, análisis y gestión de riesgos asociados a la tecnología y los sistemas utilizados en los desarrollos software.
2. **Criterios para la implementación de medidas de seguridad:** Además de los métodos de evaluación, también se especifican los criterios para la adopción de medidas correctivas y preventivas, lo que facilita hacer frente a cualquier amenaza que pueda surgir.
3. **Monitoreo y mejora continua:** Un aspecto fundamental contemplado es la obligación de llevar a cabo un proceso de seguimiento continuo, con el objetivo de adaptar las estrategias de seguridad a las nuevas amenazas y avances tecnológicos. La mejora constante es clave para mantener la protección a largo plazo.

¿A quién afecta?

La publicación está dirigida principalmente a todas las áreas de la STIC, entidades y organismos que forman parte de la DGSIC , incluyendo servicios, departamentos y dependencias que manejan información sensible y sistemas críticos. Todos estos actores deberán ajustar sus procedimientos y prácticas de seguridad a los criterios establecidos, asegurando que las evaluaciones de seguridad sean rigurosas y efectivas.

¿Cómo acceder?

La normativa está disponible en el portal público Gobernanza y Calidad de la Subdirección de las Tecnologías de la Información y Comunicaciones (STIC), a través de este enlace directo, donde los interesados pueden consultar todos los detalles sobre el método y los criterios para la evaluación de la seguridad.

Un paso hacia una administración más segura

Este avance refuerza el compromiso con la **seguridad cibernética** y la **protección de datos personales**, y es un paso fundamental hacia la consolidación de una administración pública más **transparente, moderna y segura**. Sin duda, ésta normativa contribuirá a mejorar la confianza de los ciudadanos en los servicios digitales, al mismo tiempo que fortalece las capacidades de los organismos públicos para afrontar los desafíos de la seguridad informática.

¡ La seguridad es tarea de todos !