NEWSLETTER

Subcomité de Seguridad

13 de marzo 2026| nº 28

Noticias de Ciberseguridad

La AEPD publica orientaciones sobre IA agéntica y protección de datos: foco en riesgos, vulnerabilidades y medidas

La Agencia Española de Protección de Datos (AEPD) ha publicado orientaciones sobre Inteligencia Artificial agéntica aplicada a tratamientos de datos personales. Estos sistemas no solo responden, sino que pueden actuar con autonomía para alcanzar objetivos, lo que incrementa los retos de control, trazabilidad y seguridad en entornos digitales.

El documento ofrece una visión práctica para responsables y encargados, con una estructura que incluye: explicación de qué es la IA agéntica, análisis de cumplimiento normativo, identificación de vulnerabilidades y amenazas asociadas, y un conjunto de medidas para reducir impactos sobre los derechos y libertades de las personas. La AEPD subraya, además, la necesidad de comprender esta tecnología, en constante evolución, y aprovecharla para reforzar la protección de datos desde el diseño.



Ver noticia

CERT-EU publica su Marco de Inteligencia sobre Ciberamenazas para unificar criterios y priorizar riesgos en la UE

El CERT-EU, equipo de respuesta a incidentes y servicio de ciberseguridad que da soporte a las instituciones, órganos y agencias de la Unión Europea, ha presentado su Marco de Inteligencia sobre Amenazas Cibernéticas, un documento de referencia que formaliza cómo el equipo clasifica, evalúa y prioriza la actividad cibernética maliciosa para las entidades de la Unión y su ecosistema. El objetivo: respaldar la elaboración de informes, alertas y concienciación coherentes sobre ciberamenazas, y permitir una reacción más rápida, una comunicación más clara y una respuesta más eficaz.

El marco define un vocabulario común y métodos consistentes, incorporando elementos clave como actividades maliciosas de interés, categorías y dominios de amenaza, niveles de actores, criterios de confianza e incertidumbre, atribuciones técnicas basadas en evidencias y modelos de puntuación para orientar la mitigación priorizada. Asimismo, se alinea con las regulaciones de ciberseguridad de la UE, MITRE ATT&CK, los estándares de inteligencia de la OTAN y las buenas prácticas de FIRST.

Se trata de un “documento vivo” que evolucionará con el panorama de amenazas y el desarrollo de nuevas regulaciones.



Ver noticia

ENISA publica una metodología para diseñar y evaluar ejercicios de ciberseguridad con plantillas y guías prácticas

La Agencia de la Unión Europea para la Ciberseguridad (ENISA) ha presentado su Metodología de Ejercicios de Ciberseguridad, un marco de referencia para planificar, ejecutar y evaluar simulacros y ejercicios (técnicos u operativos) de forma ordenada y medible. La propuesta busca asegurar que participen los perfiles adecuados en el momento oportuno y que los ejercicios generen resultados útiles para mejorar capacidades reales.

El documento se apoya en lecciones aprendidas, buenas prácticas del sector y experiencia acumulada, y está pensado para usarse junto a un kit de herramientas de apoyo con plantillas, checklists y material de orientación para facilitar la organización de ejercicios eficaces.



Ver noticia