NEWSLETTER

Subcomité de Seguridad

16 de octubre | nº 34

CTEAJE
Comité Técnico Estatal de la Administración Judicial Electrónica

1 Noticias de Ciberseguridad

La AEPD advierte sobre los retos de privacidad de la futura cartera europea de identidad digital

La Agencia Española de Protección de Datos (AEPD) viene alertando sobre los desafíos que plantea la implantación de la cartera europea de identidad digital prevista en el marco del reglamento eIDAS2, especialmente en materia de privacidad, seguridad y protección de datos personales.

En una nueva publicación de su serie de análisis sobre eIDAS2, la AEPD examina riesgos como la detección de actividades de los usuarios, las brechas de datos y la divulgación excesiva de información personal. El organismo advierte de que, incluso sin compartir datos directamente, determinados actores podrían inferir información sensible mediante la observación de comportamientos, registros o comunicaciones asociadas a la cartera digital.

La agencia también destaca que una posible filtración de datos biométricos, documentos de identidad o historiales de transacciones podría tener consecuencias especialmente graves para los ciudadanos, incluyendo riesgos de robo de identidad o vigilancia indebida.

Para reducir estos riesgos, la AEPD recomienda aplicar medidas de protección de datos desde el diseño, como el almacenamiento local de información, el cifrado de copias de seguridad, el uso de técnicas de divulgación selectiva y la minimización de la recopilación de datos personales.

eIDAS2, la cartera europea de identidad digital y el RGPD (VI)



2 Noticias en Ciberseguridad

Panorama de amenazas ENISA 2026

ENISA analizó 8.257 incidentes que afectaron a la Unión Europea entre el 1 de enero y el 31 de diciembre de 2025, recopilados de fuentes abiertas y datos compartidos.

Los ataques de denegación de servicio distribuido (DDoS) representaron el 51,3% de la actividad observada, y los accesos no autorizados alcanzaron el 39,5%.

El phishing representó el 77,8% de los casos identificados de ingeniería social, mientras que la explotación de vulnerabilidades continuó siendo una vía relevante para obtener accesos no autorizados (60,4%).

Los acontecimientos geopolíticos continuaron teniendo influencia sobre las amenazas que afectaron a la Unión Europea durante el periodo analizado. Las operaciones impulsadas por motivos ideológicos representaron el 57,3% de la actividad observada, principalmente a través de campañas DDoS realizadas por grupos hacktivistas contra servicios públicos, entidades esenciales y organizaciones relacionadas con acontecimientos políticos.

El análisis sectorial de ENISA sitúa a la **Administración Pública** como el sector más afectado por la actividad ciberdelictiva, con un 31,8% de los incidentes registrados, seguida de los servicios empresariales y la industria manufacturera.

Otro de los aspectos destacados por ENISA es la creciente integración de la inteligencia artificial en las actividades cibernéticas maliciosas.

ENISA destaca como elemento crítico el potencial efecto en cadena de los incidentes que afecten a proveedores de software, servicios y entornos cloud.

En conjunto, el informe refleja un escenario en el que convergen ciberdelincuencia, hacktivismo, amenazas estatales y vulnerabilidades técnicas, reforzando la necesidad de proteger especialmente los servicios expuestos, las credenciales y las dependencias de terceros.

ENISA Threat Landscape 2026 | ENISA

3 Noticias en Ciberseguridad

Directrices para proteger los tokens de identidad y acceso en línea frente al mal uso

El Instituto Nacional de Estándares y Tecnología (NIST) y la Agencia de Ciberseguridad y Seguridad de Infraestructuras (CISA), ambos de Estados Unidos, han publicado el informe **NIST IR 8587, Protección de Tokens y Afirmaciones contra la Falsificación, el Robo y el Uso Indebido**, que ofrece directrices para proteger los tokens digitales utilizados en la autenticación y el acceso a muchos servicios que usamos en línea basados en la nube.

Los tokens permiten identificar a los usuarios, acceder a recursos protegidos y utilizar funciones como el inicio de sesión único. Sin embargo, si no se protegen adecuadamente, pueden ser robados o falsificados para acceder a información sensible. Un ataque citado en el informe permitió a actores extranjeros robar más de 60.000 correos electrónicos de una agencia mediante tokens falsificados a partir de una clave de firma robada.

El documento está dirigido principalmente a las agencias federales y a los proveedores de servicios en la nube, aunque también resulta útil para otras organizaciones.

3 Noticias en Ciberseguridad

Sus principales recomendaciones y novedades incluyen:

- **Protección de claves criptográficas**: orientaciones sobre su uso, almacenamiento y seguridad.
- **Adaptación a nuevas tecnologías**: consideraciones iniciales sobre inteligencia artificial y criptografía poscuántica.
- **Referencias a estándares actuales y emergentes** para facilitar la revocación de tokens y el intercambio de señales alrededor de tokens.

En conclusión, el informe busca **reforzar la seguridad de los sistemas de identidad y control de acceso**, reduciendo el riesgo de robo, falsificación y uso indebido de tokens mediante mejores prácticas y una mayor colaboración entre organizaciones y proveedores tecnológicos.

NIST finaliza directrices para proteger los tokens de identidad y acceso en línea frente al mal uso | NIST

