NEWSLETTER

Subcomité de Seguridad

04 de noviembre 2024 | nº 15

Noticias de Ciberseguridad

El CEPEJ avanza en Ciberjusticia e Inteligencia Artificial

El Grupo de Trabajo sobre Ciberjusticia e Inteligencia Artificial (CEPEJ-GT-CYBERJUST) se reunió los días 17 y 18 de octubre de 2024 para evaluar los progresos en su programa de actividades bienal. Durante el encuentro, se trabajó en el desarrollo de un glosario tecnológico, una guía sobre videoconferencia en procedimientos judiciales y directrices para la publicación en línea de decisiones judiciales, con el fin de presentarlos en la plenaria de diciembre.

La reunión también incluyó un debate sobre inteligencia artificial en el entorno judicial, seguido de la demostración de herramientas automáticas de grabación y transcripción de Eslovenia y España. Estas herramientas buscan facilitar la labor de los jueces y se añadirán al Centro de Recursos sobre Ciberjusticia e IA, el cual ofrece un panorama detallado de la implementación de sistemas de inteligencia artificial en el ámbito judicial en Europa y el mundo.



Ver noticia

La Comisión Europea impulsa la certificación de las Carteras de Identidad Digital en la UE con el apoyo de ENISA

Cada octubre, Europa celebra el Mes Europeo de la Ciberseguridad (ECSM), una iniciativa impulsada por la **Agencia Europea de Ciberseguridad (ENISA)** con el apoyo de la Comisión Europea y los Estados miembros de la UE. Este mes tiene como objetivo fomentar la conciencia sobre la importancia de la ciberseguridad, ofreciendo a los ciudadanos herramientas y conocimientos para protegerse en un entorno digital cada vez más complejo.

Noticias en Ciberseguridad

En 2024, el tema principal es nuevamente la ingeniería social, una técnica de manipulación psicológica utilizada por ciberdelincuentes para obtener información sensible o acceso a sistemas mediante el engaño de sus víctimas. La ingeniería social abarca amenazas como el phishing, smishing, vishing y pretexting, todas dirigidas a explotar vulnerabilidades humanas más que técnicas. Según el informe de ENISA Panorama de Amenazas de 2024, el phishing sigue siendo uno de los métodos más utilizados por los atacantes, responsables de gran parte de los incidentes de ciberseguridad prolongados.

ENISA también ha subrayado la importancia de educar a diversos sectores de la sociedad, adaptando sus campañas a las particularidades culturales y nacionales. En este sentido, se han lanzado materiales educativos y entrevistas con representantes de distintos países de la UE, para destacar cómo cada nación aborda el desafío de la ciberseguridad desde su propia perspectiva.
Este enfoque no solo busca prevenir ciberataques, sino también fortalecer la confianza del público en las tecnologías digitales. La creciente sofisticación de amenazas como los deepfakes o la inteligencia artificial maliciosa hace que la concienciación y la colaboración internacional sean más cruciales que nunca.



Ver noticia

La Comisión adopta nuevas normas de ciberseguridad para redes y entidades críticas bajo la Directiva NIS2

La Comisión Europea ha aprobado en el mes de octubre las primeras normas de ejecución de la Directiva NIS2, que establece medidas de gestión de riesgos de ciberseguridad para infraestructuras y redes críticas en la Unión Europea. Esta nueva regulación específica los casos en los que un incidente debe considerarse significativo y obliga a las empresas clave digitales, como proveedores de servicios en la nube, centros de datos y plataformas de redes sociales, a notificar los incidentes a las autoridades.

La norma aprobada coincide con la fecha límite para que los Estados miembros transpongan la Directiva NIS2 a su legislación nacional. Con estas nuevas normas, la UE refuerza su ciberresiliencia ante posibles amenazas digitales y fortalece la supervisión y ejecución en todos los sectores críticos. Este marco representa un avance crucial en la protección de las infraestructuras digitales críticas de Europa, mejorando la ciberseguridad y promoviendo la cooperación transfronteriza.

Ver noticia