NEWSLETTER

Subcomité de Seguridad

08 de mayo 2024 | nº 10

Noticias de Ciberseguridad

La AEPD recibe por tercer año consecutivo el mayor número de reclamaciones de su historia

Recientemente, el 11 de abril de 2023, la AEPD ha publicado su Memoria de Actuación 2023, que contiene, las iniciativas de concienciación, difusión, colaboración e inspección puestas en marcha, los informes y procedimientos más relevantes del año, un análisis de las tendencias normativas y jurisprudenciales y los desafíos para la privacidad, tanto en un plano nacional como internacional.

Cada año son más numerosas las reclamaciones presentadas ante la Agencia, según se recoge en las memorias publicadas, en 2023 se presentaron 21.590 reclamaciones, lo que supone un incremento de un 43% respecto a 2022 y un 55% más que en 2021, batiéndose el récord en cuanto al número de reclamaciones recibidas por la agencia.

Las reclamaciones planteadas con mayor frecuencia por los ciudadanos en 2023 corresponden a recepción de publicidad no deseada (+114%), servicios de internet (+30%), videovigilancia (+29%), comercio, transporte y hostelería (+66%), y las relacionadas con entidades financieras/acreedoras (+78%). En lo relativo a los procedimientos sancionadores, se finalizaron 419, siendo las áreas más frecuentes la videovigilancia (33%), los servicios de internet (14%), los procedimientos relacionados con las Administraciones Públicas (6%) y publicidad (spam email/SMS) (6%).

Ver más

La Memoria recoge, los principales hitos de 2023, entre otros, los desafíos para la privacidad tanto jurídicos como tecnológicos, y la protección de las personas en el mundo digital, que puede verse en detalle en el siguiente enlace, Memoria de actuación 2023.

Noticias en Ciberseguridad

Aprobado el Reglamento de Cibersolidaridad

El pasado 24 de abril, el Parlamento Europeo aprobó el Reglamento del Parlamento Europeo y del Consejo, por el que se establecen medidas destinadas a reforzar las capacidades de la Unión para detectar, prepararse y responder a las amenazas e incidentes de ciberseguridad.
El Reglamento reforzará la solidaridad a escala de la Unión a la hora de detectar, afrontar y superar los incidentes de ciberseguridad importantes o a gran escala, mediante la creación de un Ciberescudo Europeo y un Mecanismo de Ciberemergencia global.

Para detectar las principales amenazas cibernéticas de forma rápida y eficaz, la Comisión propone la creación de un Ciberescudo Europeo, entidades encargadas de detectar las ciberamenazas y de actuar frente a ellas, utilizando la inteligencia artificial (IA) y el análisis avanzado de datos. A su vez, las autoridades y las entidades pertinentes podrán reaccionar de manera más eficiente y eficaz ante los incidentes graves.

Ver más

El Reglamento de Cibersolidaridad de la UE también incluye la creación de un mecanismo de ciberemergencia para aumentar la preparación y mejorar las capacidades de respuesta ante incidentes en la UE.

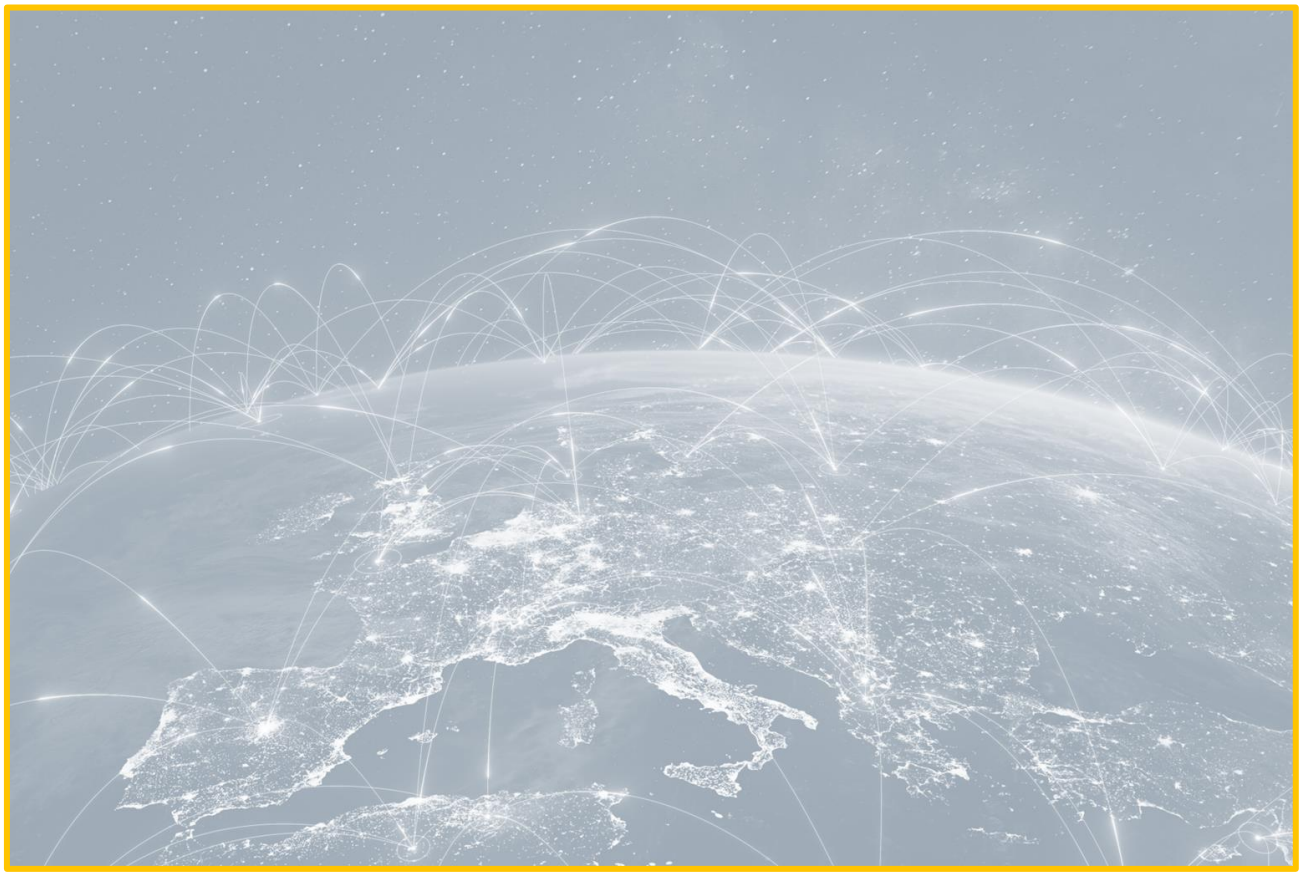
Hacia una Europa segura y confiable en materia de Ciberseguridad

El 17 de abril, la Agencia de Ciberseguridad de la Unión Europea (ENISA), la Comisión Europea y la presidencia belga del Consejo de la Unión Europea organizaron la 2ª Conferencia de Política de Ciberseguridad de la UE.

En el evento se destacó que la ciberseguridad y su política futura es un tema de suma importancia para Europa, porque es una piedra angular de nuestro futuro crecimiento digital y económico.

Implementar el marco legal de ciberseguridad y garantizar las capacidades operativas para hacer frente a los desafíos cibernéticos emergentes, son las variables que garantizarán el éxito. Por ello, estas conferencias son el foro que permitirán a la Agencia proponer recomendaciones en el que será el primer informe sobre el estado de la ciberseguridad en la Unión, que orientará la misión estratégica de Europa hacia un alto nivel común de ciberseguridad.

Noticias en Ciberseguridad



Ver más

Se abordaron cuestiones como el despliegue de medidas de Ciberprotección Activa (ACP) por parte de los Estados miembros dentro de la legislación y el marco político existente de la UE, los requisitos de certificación de productos y servicios digitales, el proceso de implementación de las disposiciones de la Directiva NIS2 y su impacto en los sectores de infraestructura crítica.