Con la colaboración de

# La Cátedra de Ciberseguridad INCIBE-UPV destaca en una jornada la necesidad de que la UE cuente con infraestructuras satelitales propias

- **El encuentro destacó la necesidad de regular las operaciones con drones y que estas tengan como requisito certificarse en algún esquema de seguridad como el Esquema Nacional de Seguridad (ENS)**

- **Del total de 83.517 incidentes de ciberseguridad que se produjeron en 2023, según el balance de ciberseguridad de INCIBE, 237 fueron en operadores esenciales y críticos**

**València, 6 de marzo de 2025**.- La Cátedra de Ciberseguridad INCIBE-UPV, que es fruto del convenio entre el Instituto Nacional de Ciberseguridad (INCIBE), entidad dependiente del Ministerio para la Transformación Digital y de la Función Pública, a través de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, y la Universitat Politècnica de Valencia, ha destacado la necesidad de que la UE cuente con infraestructuras satelitales propias para suministrar este tipo de servicios a los países que la componen sin necesidad de terceros. Esta ha sido una de las conclusiones de la "**I Jornada sobre Ciberseguridad en el Sector Aeroespacial"** celebrada en València.

Esta jornada es parte de la Cátedra de Ciberseguridad INCIBE-UPV, incluida en el programa de Cátedras de Ciberseguridad en España, en el marco del Plan de Recuperación, Transformación y Resiliencia, con la financiación de los Fondos *Next Generation-EU*.

Organizada por la **Cátedra de Ciberseguridad INCIBE-UPV,** en colaboración con el Clúster **Espai Aero CV**, este encuentro ha incidido además en cómo, con la tecnología nacional actual, está garantizada la seguridad del segmento tierra pero es esencial garantizar también la ciberseguridad en los satélites para que puedan reportar las amenazas.

Además de la importancia de que la ciberdefensa esté implementada en toda la cadena de suministro de los satélites para su completa y perfecta securización.

El acto ha contado en su inauguración con el director de Sectores Estratégicos de INCIBE, **Jesús Feliz,** el director de la Cátedra de Ciberseguridad INCIBE-UPV, **Santiago Escobar**, el presidente de Espai Aero CV, **José Nieto** y el director del Consorcio Valenciano del Espacio (VSC), **Vicente Boria,** que han hablado de cómo la red es el principal foco de ataques cibernéticos y cómo la motivación siempre es geopolítica y, finalmente, estratégica y económica.

Además, han analizado la reciente directiva NIS2, que se está trasponiendo a nivel de la UE, y que amplía a muchos más sectores el calificativo de "sectores críticos" e incide en la implicación de la cúpula directiva de las compañías en cuanto a concienciación en materia de ciberseguridad.

**Incidentes en operadores esenciales y críticos**

Del total de 83.517 incidentes de ciberseguridad que se produjeron en 2023, según el balance de ciberseguridad de INCIBE, el 52,83% tuvieron una peligrosidad alta, el 5,76% muy alta, el 15,23% media y el 26,18% baja. Del total de incidentes, 237 fueron en operadores esenciales y críticos.

En la parte de experiencias institucionales, el teniente coronel, director interino de Ciberdefensa, Jefatura de Servicios Técnicos y Ciberespacio del Ejército del Aire, Miguel Ángel Valle García, ha explicado la evolución y la estrategia nacional en ciberseguridad, tanto a nivel nacional como la que corresponde a España en la ciberdefensa internacional.

Mientras que la subdirectora General de Ciberseguridad en la Generalitat Valenciana, Carmen Serrano Durbá, se ha adentrado en los pasos que se han dado desde 2007, momento en el que se creo el centro de ciberseguridad CSIRT-CV, hasta la actualidad.

Durante su intervención, **el director de la Cátedra de Ciberseguridad INCIBE-UPV, Santiago Escobar**, ha incidido en la "*necesidad de la formación para que los recién egresados tengan los conocimientos más actualizados posibles que está demandando el mercado de la ciberseguridad en el sector aeroespacial. Aunque la superespecialización, en este campo, que es tan amplio, es complicada para el estudiantado que termina la Universidad, por lo que es necesaria una continua formación*".

**Necesidad de regular operaciones con drones**

También, como conclusión de la jornada, se ha destacado la necesidad de regular las operaciones con drones y que estas tengan como requisito certificarse en algún esquema de seguridad como pueda ser el Esquema Nacional de Seguridad (ENS). Certificar estos sistemas permitiría aumentar su nivel de madurez en ciberseguridad y evitar posibles ataques.

La jornada ha contado además con **experiencias empresariales en ciberseguridad en el sector aeronáutico y aeroespacial** de la mano del responsable de Operaciones Criptoespacio Cipherbit-Grupo Oesía, Diego Ruano, el responsable de gestión de infraestructuras Cloud y Ciberseguridad de Sopra Steria, Arsenio Pérez, el director de Ciberseguridad de Vig-Sec Drone, Alejandro Aliaga, el CEO de Emxys, José Antonio Carrasco, y el director del Máster en sistemas de aeronaves no tripuladas y tecnologías asociadas, Israel Quintanilla.

Para cerrar esta **"I Jornada sobre Ciberseguridad en el sector Aeroespacial",** el director de la Cátedra de Ciberseguridad INCIBE-UPV, **Santiago Escobar,** la

investigadora predoctoral FPU de Derecho Civil en la Universitat de València y miembro del Consejo Asesor Joven de la Secretaría General de la Unión Internacional de Telecomunicaciones (ITU), **Roser Almenar,** el catedrático de Derecho Civil de la Universitat de València y delegado de protección de datos, **Javier Plaza**, la miembro del Equipo Jurídico Marzo, **Ana Marzo**, y el técnico y auditor jefe de ENS y ISO 27001 de European Quality Assurance, **Esteban Susquillo,** han analizado el Esquema Nacional de Seguridad y directiva NIS2 y su aplicación en empresas y sector aeroespacial.

En esta mesa, moderada por la gerente de Espai Aero CV, Angélica Robles, se han destacado los principales problemas que encuentran las compañías en torno a la ciberseguridad como son la falta de percepción del riesgo, la debilidad de los eslabones dentro de las empresas, tanto en personas como en cadena de suministro, la inversión en ciberseguridad, así como la inflación normativa.

**Programa de Cátedras de Ciberseguridad en España**

INCIBE, dentro del Programa Global de Innovación en Seguridad, tiene como misión particular la elevación de las capacidades y recursos en ciberseguridad, en los ecosistemas académico, empresarial y tecnológico, dirigidos a impulsar las capacidades en ciberseguridad de la sociedad y la economía en general. Esta iniciativa tiene el propósito de disponer de un programa que persiga la promoción y generación del conocimiento y la transferencia del mismo al sector productivo, especialmente estableciendo sinergias entre los ámbitos sociales y económicos de la ciberseguridad. Con el objetivo de desarrollar este propósito se lanzó el pasado 1 de diciembre de 2022 la invitación pública para la colaboración en la promoción de cátedras de ciberseguridad en España.

Las iniciativas y actuaciones del programa de Cátedras de Ciberseguridad en España se engloban dentro del **Programa Global de Innovación en Seguridad,** contemplado en el Plan de Recuperación, Transformación y Resiliencia (PRTR) a través del Componente 15. Inversión 7 Ciberseguridad: Fortalecimiento de las capacidades de ciudadanos, PYMES y profesionales e impulso del sector. Actúa especialmente en tres de los seis aspectos claves de la industria recogidos en el hito 245 del PRTR: impulsar la industria nacional de la ciberseguridad para el surgimiento, crecimiento y desarrollo de empresas en este sector; desarrollar soluciones y servicios de alto valor añadido en el ámbito de la ciberseguridad; y formar y desarrollar talentos especializados en el ámbito de la ciberseguridad.

***Sobre INCIBE***

*El Instituto Nacional de Ciberseguridad es una entidad dependiente del Ministerio para la Transformación Digital y de la Función Pública, a través de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, consolidado como entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de los ciudadanos y las empresas. Además, es un motor de transformación social y oportunidad para la innovación, fomentando la I+D+i y el talento.*

Con la colaboración de

***Sobre UPV***

*La Universitat Politècnica de València (UPV) es, según el Academic Ranking of World Universities (ARWU), conocido como ranking de Shanghai, la mejor universidad tecnológica de España. Más del 70% del alumnado de la UPV ya trabaja al año de haber finalizado sus estudios. Y ello se debe en buena medida a las prácticas en empresa que son remuneradas. La UPV mantiene más de mil convenios que permiten el intercambio de estudiantes con otras universidades europeas, de América Latina, Estados Unidos, Canadá, Australia, China y Japón. En sus poco más de 50 años de historia, ha producido más de 145.000 publicaciones científicas. Es líder nacional en número de patentes y una de las instituciones académicas españolas que más ingresos obtiene gracias a su actividad investigadora.*