Con la colaboración de FEDACOVA

Una jornada de la Cátedra de Ciberseguridad INCIBE-UPV estima en 100 millones de euros anuales el coste de los ciberataques en el sector agroalimentario de la Comunitat

- **El 70% de los ciberincidentes a nivel mundial afecta a pymes, tiene un coste medio de 35.000 euros, y 6 de cada 10 de ellas cesa su actividad en los 6 meses siguientes, según se ha expuesto en la I Jornada sobre Ciberseguridad en la Industria Agroalimentaria**

València,2de julio de 2025.- Una jornada de 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 estimado en un rango de 75 a 100 millones de euros anuales el coste de los ciberincidentes** en la industria agroalimentaria de la Comunitat Valenciana.

En esta "**I Jornada sobre Ciberseguridad en la Industria Agroalimentaria"**, organizada por la **Cátedra de Ciberseguridad INCIBE-UPV,** en colaboración con la **Federación Empresarial de Agroalimentación de la Comunidad Valenciana (FEDACOVA),**diferentes expertos en tecnología de industrias agroalimentarias valencianas han coincidido en resaltar que este dato, no solo refleja los daños directos de los ciberataques, sino también las consecuencias colaterales de una digitalización que avanza más rápido que las medidas de protección implantadas.

Esta jornadaes partede 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*.

Así, los expertos han destacado que los ataques mayoritarios que generan estas pérdidas son ransomware que paralizan líneas de producción enteras durante días, malware y phishing. Suplantación de identidad (BEC) en pagos a proveedores o clientes internacionales. Sabotajes digitales que alteran sistemas de control de temperatura o trazabilidad. Fugas de información confidencial, como datos de exportación, fórmulas de producto o registros de clientes. Y colapso de sistemas logísticos y ERP que afectan a las cadenas de distribución y entregas clave.

Estos ciberincidentes se traducen en paralización de operaciones con impactos económicos en la exportación e incumplimiento de contratos, pérdidas de clientes

internacionales, por falta de confianza, daño reputacional de las compañías que pueden afectar a toda su cadena de valor. Y sanciones legales, por filtración de datos personales que pueden ascender desde 3.000 hasta 20.000 euros.

El sector agroalimentario de la Comunitat Valenciana, con más de 8.000 millones de euros anuales de facturación y más de 2.000 empresas es un sector crítico, reconocido como tal por la normativa en materia de ciberseguridad NIS2, que entró en vigor el 17 de octubre de 2024, y que debe cumplir con obligaciones de notificación y medidas de seguridad establecidas por la directiva.

El 70% de los ataques afecta a pymes y tiene un coste medio de 35.000 euros

Sin embargo, tal y como destacaron los expertos de esta jornada, al estar compuesto mayoritariamente por pymes, la mayoría piensa que son pocos empleados, que no les van a atacar, que las pérdidas las cubrirá el seguro o que no tienen nada importante que quieran los ciberatacantes.

De hecho, el 70% de los ciberataques a nivel mundial afecta a pymes, tiene un coste medio de 35.000 euros y 6 de cada 10 de ellas cesa su actividad en los 6 meses siguientes a un ciberincidente, según los datos de la consultora Forrester.

Por ello, en este encuentro se explicó cómo las empresas deben pasar de creer que están protegidas a tener la certeza de que sí los están, con certificaciones que inciden en este ámbito como la ISO 27001, ISO 27701, ISO 27017, ISO 27018, Esquema Nacional de Seguridad, o ISO 42001.

Además, tal y como subrayaron un plan básico de ciberseguridad para cualquier pyme, con instalación de un ativirus/EDR, realización de copias de seguridad, activación del doble factor de autenticación, sensibilización a los empleados, evaluación de riesgos, elaboración de un plan de respuesta y la mejora de los controles, cuesta menos de 5.000 euros anuales, un coste asumible para cualquier pyme.

Estas fueron algunas de las principales conclusiones de la mesa de**“experiencias empresariales en ciberseguridad en la industria agroalimentaria”**dentro de la jornadaque ha contado con el Business Developer-Digital Trust de **SGS**, Luis Villanueva, elCTO Corporativo de **Familia Martínez**, Roberto López, el director global de Servicios de Ciberseguridad de **Ayesa**, Álvaro Fraile, el director de IT de **Vicky Foods**, Robert Tro, el director de IT de **Jumel Alimentaria,** José Llorca, y el director de IT de**Agua Mineral San Benedetto**, Juan Francisco Cerezo.

Ante estas cifras, y tal y como ha resaltado el **director de la Cátedra de Ciberseguridad INCIBE-UPV, Santiago Escobar,** en la apertura de esta jornada “*la ciberseguridad ya no es opcional. No se trata de un gasto, sino de una inversión a futuro para las compañías que va a hacer posible que tengan un camino para su supervivencia y en la que las empresas deben buscar compañeros de viaje especialistas para que los acompañen pero sobre todo es importante que todas las*

personas de la organización estén formados y concienciados en materia de ciberseguridad".

La jornada, que se ha celebrado en el salón de actos del cubo rojo de la ciudad Poiltècnica de la Innovación (CPI) ha contado con una afluencia masiva de empresas y más de 50 personas inscritas. En este sentido, el secretario general de FEDACOVA, Sergio Barona, ha subrayado que el éxito de esta iniciativa "*pone de manifiesto la creciente preocupación del sector por anticiparse a los riesgos digitales y proteger sus procesos productivos y su cadena de valor. La ciberseguridad ya no es una opción, sino una necesidad estratégica para garantizar la competitividad, la trazabilidad y la confianza. Esta jornada nos ha permitido identificar amenazas concretas, compartir buenas prácticas y abrir un espacio de colaboración que es clave para afrontar los desafíos del presente y del futuro*".

La clausura de la jornada ha contado con una mesa de debate bajo el título "**Aplicación real de herramientas de ciberseguridad y LOPD para pymes de la industria agroalimentaria**" que ha incidido de un modo más práctico en el ámbito normativo vigente. Bajo la moderación del adjunto a Dirección y agente de innovación en FEDACOVA, Juan José Rico, han participado de ella el director de la Cátedra de Ciberseguridad INCIBE-UPV, Santiago Escobar, el abogado especializado en derecho tecnológico, LOPD y Ciberseguridad de Leynet Consultores, Luis López, el director de Infonegoci, Artur Yusá, el CTO de Ontinet, Alejandro Aliaga, y el jefe de Desarrollo Estratégico de Negocio Digital y Alianzas de AINIA, David Martínez.

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 Ciberseguridades una entidad dependiente del Ministerio para la Transformación Digital y de la Función Pública, a través de laSecretaría 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.

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.

Para más información:
Nebo Comunicación
Raquel Bascuñana 622 15 25 80
raquel.bascunana@nebocomunicacion.com