Octubre 2025

Ciber Eguraldia

Noticias generales

Incidentes de ciberseguridad

Estafas y fraudes

Malware y vulnerabilidades

Fugas de información

Ciberseguridad industrial

Noticias generales

El Estado español, el quinto país europeo más afectado por los ciberataques en el primer semestre de 2025

Así se recoge en el sexto informe anual “Microsoft Digital Defence”, que analiza las tendencias entre julio 2024 y junio 2025. El impacto de los ciberataques a nivel mundial posiciona a España en la 14ª posición, y en el quinto a nivel europeo.

Solo el 27% de las pymes cuenta con una estrategia de ciberseguridad sólida

El Observatorio de Competitividad Empresarial de la Cámara de Comercio de España (2024) reveló que menos de la mitad de las empresas (solo un 46,8%) dispone de un plan formal de seguridad digital, y entre las microempresas la cifra desciende al 29%. Además, únicamente un 34% de las compañías ofrece formación específica en ciberseguridad a sus empleados.

Comienza el Mes Europeo de la Ciberseguridad 2025 centrándose en las amenazas de phishing

Este mes comienza el mes Europeo de la Ciberseguridad, se trata de una campaña anual de sensibilización que ofrece orientaciones prácticas para que los ciudadanos de la UE se mantengan seguros en línea. En este artículo te proporcionamos más información.

Incidentes de ciberseguridad

Incidente grave en F5

F5 ha informado sobre un incidente de seguridad detectado en agosto de 2025, en el que un grupo altamente sofisticado, presuntamente vinculado a un Estado, mantuvo acceso persistente a sistemas internos y exfiltró archivos de entornos críticos, incluidos el desarrollo de BIG-IP y plataformas de gestión del conocimiento. Tras contener la intrusión, F5 ha reforzado sus controles de seguridad y publicado actualizaciones para mitigar riesgos.

El grupo de ransomware Qilin asegura haber hackeado a la Agencia Tributaria

La Agencia Tributaria, que cuenta con más de 25.000 trabajadores y se encarga de la gestión de impuestos de todo tipo ha desmentido estas afirmaciones e indica que, tras revisar los documentos que se han hecho públicos, puede señalar que no provienen de sus sistemas internos. Así pues, el hackeo no se habría hecho directamente a Hacienda.

Desmantelan una sofisticada red de cibercrimen como servicio

La red criminal y su infraestructura eran técnicamente muy sofisticadas y permitían a delincuentes de todo el mundo utilizar su servicio de SIM-box para cometer una amplia gama de ciberdelitos relacionados con las telecomunicaciones, entre otros delitos.

Estafas y fraudes

Alertan de una nueva estafa con la que buscan datos personales y bancarios

VOST Euskadi informa que Sanidad "no está solicitando la renovación de tu tarjeta sanitaria con motivo de la implantación de un nuevo sistema de verificación".

El fraude telefónico se dispara y Europol advierte que millones de europeos están en riesgo

La suplantación del identificador de llamadas no es una simple molestia telefónica: es un vector de fraude que mueve billones (en euros) y afecta tanto a ciudadanos a pie como a grandes instituciones.

Oracle y Google alertan de una ola de correos de extorsión masiva contra empresas

Oracle y Google han detectado una campaña de extorsión a gran escala dirigida a clientes corporativos que usan Oracle E-Business Suite. Aunque Oracle no ha revelado cuántas organizaciones se han visto afectadas ni en qué países, la compañía ha confirmado que el ataque se aprovecha de fallos conocidos y corregidos en actualizaciones previas. De ahí su insistencia en aplicar los parches de seguridad más recientes.

Malware y vulnerabilidades

Vulnerabilidades identificadas en el primer semestre de 2025

A continuación, se indican los datos cuantitativos y cualitativos de las vulnerabilidades identificadas en el primer semestre de 2025, de modo que permitan evaluar la situación actual y la tendencia para este año.

Microsoft corrige 167 vulnerabilidades, 16 de ellas calificadas como críticas, y 6 zero-day

Microsoft ha publicado su Boletín de Seguridad mensual (Patch Tuesday) en octubre de 2025 con el total de 252 vulnerabilidades identificadas, de las cuales 167 tienen descripción específica.

Oracle publica parches, tras confirmarse explotación de EBS, en su actualización trimestral de seguridad

Se han identificado 12 vulnerabilidades críticas que afectan a diversos productos Oracle, incluyendo Oracle Managed File Transfer, Oracle Retail Xstore Office, Oracle Agile PLM, Oracle Agile Engineering Data Management, Oracle Hospitality Cruise Shipboard Property Management System, Oracle Communications, Oracle Marketing, Oracle Financial Services Analytical Applications Infrastructure, Oracle Identity Manager, Oracle Business Intelligence Enterprise Edition y JD Edwards EnterpriseOne Tools.

Privacidad y fugas de información

Las campañas de phishing en auge: Microsoft continúa como la marca más suplantada

Microsoft sigue siendo la marca preferida de los ciberdelincuentes para suplantar, según el Brand Phishing Report de Check Point Research correspondiente al tercer trimestre de 2025. Google se coloca en el segundo puesto, con un 9% de los intentos de suplantación vinculados con marcas, seguida de Apple, con un 6%. En conjunto, las tres compañías que ocupan el podio coparon más de la mitad de toda la actividad de phishing registrada durante el trimestre.

Plugin de seguridad expone información sensible de más de 100.000 páginas de Wordpress

Un 'plugin' de seguridad de Worpress, que ofrece características como un escáner de 'malware' y protección frente ataques de fuerza bruta, ha puesto en riesgo a las más de 100.000 páginas web donde está instalado, debido a una vulnerabilidad.

183 millones de correos y contraseñas quedan al descubierto tras una nueva macrofiltración

Lejos de ser un ataque aislado a un proveedor o una plataforma concreta, esta filtración tiene su origen en una recolección masiva de logs procedentes de infostealers, un tipo de malware diseñado específicamente para extraer información sensible directamente desde los equipos infectados.

Ciberseguridad industrial

Ciberseguridad cotidiana e industrial: dos mundos unidos por la conectividad

La conectividad se ha vuelto el lenguaje común de nuestro tiempo. Desde los hogares inteligentes hasta las fábricas automatizadas, todo está vinculado a Internet. Si bien se habla mucho de la Ciberseguridad, hay conceptos que no están claros, y muchas personas, asocian el concepto con mega estructuras, empresas de gran porte y que no aplica a todo lo cotidiano. Y en la realidad partimos del concepto de que cualquier usuario de un smartphone y que realiza transacciones electrónicas está dentro del campo.

Ciberseguridad OT: ¿Qué es la seguridad de tecnología operativa?

La digitalización de los procesos industriales, representa también un reto sin precedentes en cuestiones de vulnerabilidad. Surge así la necesidad de atender a la Ciberseguridad de la Tecnología Operativa (OT) adoptando medidas, tecnologías y prácticas que protejan los sistemas industriales y la infraestructura crítica que controlan y monitorizan procesos físicos, como la fabricación, el suministro eléctrico o la logística.

La industria manufacturera blanco preferente del cibercrimen

Se trata de un sector en el que el coste de un ataque ya no se mide solo en pérdida de datos, sino también en paradas de producción, interrupciones en la cadena de suministro y pérdidas millonarias.