Septiembre 2025

Ciber Eguraldia

Noticias generales

Incidentes de ciberseguridad

Estafas y fraudes

Malware y vulnerabilidades

Fugas de información

Ciberseguridad industrial

Noticias generales

Modus operandi de grupos criminales con impacto en Euskadi en elprimersemestre de2025

A lo largo del primer semestre de 2025, se ha seguido un proceso de identificación y monitorización de las amenazas que han tenido un impacto en Euskadi con objetivo de poner en marcha iniciativas que mitiguen el riesgo de las entidades tanto públicas como privadas, así como de la ciudadanía. Por este motivo, en la Agencia Vasca de Ciberseguridad, Cyberzaintza, hemos analizado un total de 67 incidentes de alto impacto.

Aumentan los ciberataques dirigidos a sectores críticos y esenciales

España sufrió el pasado agosto una media de 2.024 ciberataques semanales, lo que supone un 16% más que en el mismo mes de 2024, según un estudio de Check Point Research. Los sectores más atacados fueron las administraciones, el sector de bienes y servicios de consumo, el de telecomunicaciones y la industria facturera. A nivel mundial, los ciberataques bajaron un 1% respecto a julio, pero subieron un 1% interanual.

Las ciberamenazas a empresas europeas aumentan con respecto a 2024

Las ciberamenazas a empresas europeas continúan aumentando durante este año 2025, según dos de cada cinco profesionales europeos de TI y ciberseguridad (39 por ciento), que han detallado que su organización está sufriendo más ciberataques que hace un año, por lo que los presupuestos, el personal y las competencias de las compañías no logran mantener el ritmo de los actores maliciosos y frenar los ataques.

Incidentes de ciberseguridad

Aceros Olarra reanuda la producción tras una semana de parada porel ciberataque

Tras el susto producido hace una semana tras sufrir un ataque informático, que obligó a paralizar prácticamente al completo la actividad en la factoría, Aceros Inoxidables Olarra ha dado luz verde este lunes a la reincorporación progresiva de la plantilla a las instalaciones a fin de reanudar la producción. La siderúrgica de Loiu salva así a priori sin mayores consecuencias una adversidad que generó la semana pasada una gran incertidumbre en el entorno de la compañía.

Unciberataque provoca elcaos envarios aeropuertoseuropeos

Horas de espera, retrasos y cancelaciones de vuelos: estas son las consecuencias del ciberataque sufrido el viernes por la noche por un proveedor de servicios de sistemas y asistencia a pasajeros en el aeropuerto Berlin Branderburg (BER). El proveedor de servicios presta servicio a varios aeropuertos europeos. El aeropuerto de Bruselas también se vio afectado por el ciberataque.

2.000 Ciberataques semanales en agosto: gobierno y telecomunicaciones, enelpuntode mira

Según el "Índice Global de Amenazas" de Check Point Software correspondiente al mes de agosto, el volumen de ciberataques que se han producido en España ha aumentado un 16% si lo comparamos con el mismo mes del año anterior, para llegar a una media de 2.024 ataques por semana, ligeramente por encima de la media global, que fue de 1.994 ataques.

Estafas y fraudes

Alerta por estafas suplantando a Hacienda: buscan robar claves bancarias mediante correos y SMS falsos

Losataques consistenenenviar notificacionesfalsas que aparentan ser de la Agencia Tributaria utilizando técnicas de phishing y smishing. En estos mensajes, se informa al destinatario sobre supuestas incidencias fiscales, deudas pendientes o reembolsos de impuestos, instándole a acceder a un enlace para obtener más información. Una vez dentro, se solicita información confidencial como números de cuenta, tarjetas bancarias e incluso imágenes del DNI.

Aumentan las ciberestafas durante el regreso a clases con material escolar y becas falsas

Con el iniciodel curso escolar, lasfamiliasespañolasse enfrentannosolo aun incremento del gasto, sino también a una oleada de fraudes digitales que aprovechan este periodo de mayor consumo. Durante campañas anteriores se detectaron portales falsos de material escolar con precios irresistibles, webs fraudulentas que simulaban matrículas e incluso supuestas becas en las que las familias terminaban perdiendo dinero y exponiendo información personal.

Evita fraudes: los datos del DNI que nunca debes compartir, según expertos en ciberseguridad

Tener quedejar nuestro DNI para quele hagan una foto en un alojamiento o para muchas otras gestiones, es un hábito tan rutinario que ni siquiera hemos caído en la cuenta de que no deberíamos hacerlo. Y lo peor de todo es que hay datos que no debería caer en manos de terceros bajo ninguna premisa.

Malware y vulnerabilidades

Actividades de ransomware identificadas en el primer semestre de 2025

Enel informe se destacanlos grupos de ransomware quehan mostrado mayoractividad, en cuanto al número de víctimas durante el período analizado, así como las nuevas amenazas emergentes que han surgido tras la desaparición o desmantelamiento de grupos que en el pasado fueron muy activos.

Microsoft corrige 91 vulnerabilidades, siendo 13 de ellas calificadas como críticas, y 2 zero-day

Actualización de seguridadde septiembrede2025.Esta actualización consiste en la corrección de 91 vulnerabilidades de Microsoft.

Se descubre el primer ransomware basado en IA

Elequipode investigación de ESET, compañía líder endetección proactiva de amenazas, ha identificado un malware, al que han llamado PromptLock, que tiene la capacidad de filtrar, cifrar y posiblemente incluso destruir datos. Este descubrimiento ha sido considerado “el primer ransomware impulsado por IA”.

Privacidad y fugas de información

Aumentan los fraudes con criptomonedas impulsados por estafas de inversión y suplantación digital

Uninforme reciente del FBIsitúa a España entre los veinte países más golpeadospor fraudes relacionados con criptomonedas, una realidad que preocupa tanto a las autoridades como a los inversores. La naturaleza descentralizada de estas monedas, junto con la rapidez de las transacciones y la dificultad para rastrear los fondos a nivel internacional, convierte a este ecosistema en un terreno fértil para los ciberdelincuentes.

BMW sufre una brecha de datos a través de un proveedor externo

Elfabricante de automóvilesBMW ha confirmado queha sufrido un incidentecibernético. La compañía ha bloqueado el acceso a las cuentas afectadas y ha llevado a cabo "exhaustivas comprobaciones" de seguridad. Por ahora no se han encontrado evidencias de que la infraestructura de la empresa haya sido comprometida.

Alerta sobre VPN falsas que acceden a datos personales y cuentas bancarias

Aunque lasVPN sonherramientas para reforzar la privacidad y garantizar las conexiones seguras, algunos programas están desarrollados con fines maliciosos. Lejos de proteger al usuario, abren una puerta directa hacia los datos bancarios, contraseñas y credenciales de acceso. Kaspersky, firma de referencia en el sector de la ciberseguridad, ha revelado recientemente la existencia de seis aplicaciones de este tipo que comprometen seriamente la integridad digital de quienes las instalan.

Ciberseguridad industrial

Menos del 30% de la industria revisa sus vulnerabilidades mensualmente

Elinforme “Asegurar la Tecnología Operativa (OT) con soluciones diseñadas específicamente”, elaborado por Kaspersky y VDC Research en base a entrevistas a 250 responsables de la toma de decisiones en el sector industrial de EMEA, muestra el estado de la seguridad en un sector que es crítico. Y a juzgar por cómo trabajan en los parches y en la revisión de vulnerabilidades, queda mucho por hacer.

Ciberseguridad industrial: las pérdidas y filtraciones de datos de las organizaciones siguen aumentando

ElInformesobreSeguridaddeDatos 2025 deFortinet y CybersecurityInsiders confirma que muchos responsables de seguridad están adoptando un enfoque más programático para proteger los datos confidenciales, dejando atrás una mentalidad puramente tecnológica, y destinando una mayor partida presupuestaria a su protección.

CyberVolk: el ransomware que paraliza la ciencia y las infraestructuras críticas en Europa y Asia

Los investigadoresde seguridad han informado sobre CyberVolk, un nuevo ransomware que apareció por primera vez en mayo de 2024 y evolucionó rápidamente para transformarse en una sofisticada amenaza que trae de cabeza a muchas víctimas hoy en día.