ARAINTEL SEMANAL

Nº 94 - SEMANA DEL 8 AL 14 - JUNIO 2026

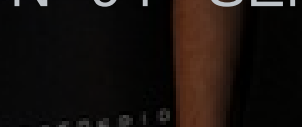
3 artículos destacados



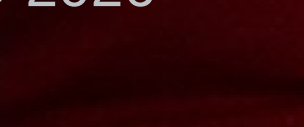
IA para empresas: NEXVIUM, Digital Hand Made, Golive y SMF Monclús abordarán ciberseguridad, el AI Act y la



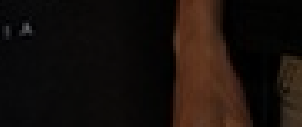
13 empresas del Hub de Defensa de Aragón participarán en Eurosatory, una de las principales ferias de



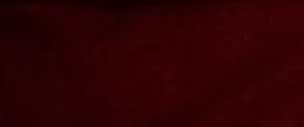
No, Claude Fable 5 no se ha filtrado en The Pirate Bay



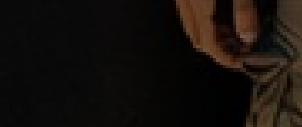
Qué es el Ghostpairing y cómo evitar accesos ocultos a nuestras redes sociales como WhatsApp



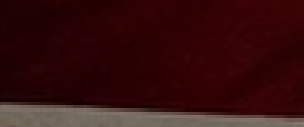
La Guardia Civil celebra el XI Curso de Verano de Inteligencia y Seguridad junto a la UNIRIOJA



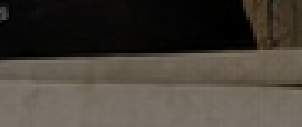
Denuvo, hipervisores y cuando piratear sale caro



Deveco impulsa un afterwork sobre IA práctica para pymes junto a CEOE Aragón y Tecnara



El CUD y la AGM celebran su primer Seminario Internacional de Liderazgo



Comprometidas 20.225 cuentas de Instagram por una vulnerabilidad en el soporte con IA de Meta



La aplicación de la IA en la industria reúne a representantes empresariales y agentes de innovación en el ITA

Comunidad y medio de tecnología y seguridad de referencia en Aragón.

SUMARIO

ARTíCULOS

Miembros de Araintel participan en C1b3rtr4cks 2026 (UAM)(p. 009) **11 JUN 2026** Diego Julián Adell

Qué es el Ghostpairing y cómo evitar accesos ocultos a nuestras redes sociales como WhatsApp(p. 012) **12 JUN 2026** Ruben Marcu

Denuvo, hipervisores y cuando piratear sale caro(p. 014) **12 JUN 2026** Dede

NOTICIAS

La Brigada ‘Aragón’ I conmemora su XL aniversario (p. 018) **8 JUN 2026** Ruben Marcu

Comprometidas 20.225 cuentas de Instagram por una vulnerabilidad en el soporte con IA de Meta(p. 019) **9 JUN 2026** Ruben Marcu

La aplicación de la IA en la industria reúne a representantes empresariales y agentes de innovación en el ITA(p. 020) **9 JUN 2026** Ruben Marcu

La Guardia Civil celebra el XI Curso de Verano de Inteligencia y Seguridad junto a la UNIRIOJA(p. 021) **9 JUN 2026** Ruben Marcu

La Policía Nacional desarticula en Zaragoza un coro de los Dominican Don’t Play (p. 023) **11 JUN 2026** Ruben Marcu

Deveco impulsa un afterwork sobre IA práctica para pymes junto a CEOE Aragón y Tecnara(p. 024) **12 JUN 2026** Ruben Marcu

IA para empresas: NEXVIUM, Digital Hand Made, Golive y SMF Monclús abordarán ciberseguridad, el AI Act y la búsqueda de financiación(p. 024) **12 JUN 2026** Ruben Marcu

El RPEI-12 instruye a las Fuerzas Armadas libanesas en desactivación de explosivos en Zaragoza(p. 025) **12 JUN 2026** Ruben Marcu

Integra Security Day reúne a expertos nacionales para abordar la anticipación y la respuesta empresarial ante los ciberataques (p. 026) **12 JUN 2026** Araintel

Colorín colorado, este cuento se ha acabado. EE. UU. ordena a Anthropic suspender sus modelos Fable y Mythos por 'motivos de seguridad nacional' (p. 027)
13 JUN 2026 Ruben Marcu

13 empresas del Hub de Defensa de Aragón participarán en Eurosatory, una de las principales ferias de defensa y seguridad de Europa(p. 030)
13 JUN 2026 Ruben Marcu

No, Claude Fable 5 no se ha filtrado en The Pirate Bay(p. 032)
13 JUN 2026 Ruben Marcu

El CUD y la AGM celebran su primer Seminario Internacional de Liderazgo(p. 033)
14 JUN 2026 Ruben Marcu

Trece startups y pymes tecnológicas participan en la tercera edición de StartTech+ del IAF y Aragón EDIH(p. 034)
14 JUN 2026 Ruben Marcu

ALERTAS

Inyección SQL en productos de Nemon(p. 037)
8 JUN 2026 INCIBE-CERT

Boletín de seguridad de SAP: junio de 2026(p. 037)
9 JUN 2026 INCIBE-CERT

Múltiples vulnerabilidades en productos de Check Point(p. 038)
9 JUN 2026 INCIBE-CERT

Boletín de seguridad de Microsoft: junio de 2026(p. 038)
10 JUN 2026 INCIBE-CERT

Inyección de comandos en FortiSandbox de Fortinet(p. 039)
10 JUN 2026 INCIBE-CERT

Múltiples vulnerabilidades en OpenSSL(p. 039)
10 JUN 2026 INCIBE-CERT

[Actualización 11/06/2026] Múltiples vulnerabilidades en productos Ivanti(p. 039)
11 JUN 2026 INCIBE-CERT

Denegación de servicio en Serv-U de SolarWinds(p. 040)
11 JUN 2026 INCIBE-CERT

Inyección de cadena de formato autenticada en Tapo C110 de TP-Link (p. 040)
12 JUN 2026 INCIBE-CERT

Múltiples vulnerabilidades en MobaXterm Personal Edition (Portable) de Mobatek(p. 040)
12 JUN 2026 INCIBE-CERT

Toma de control de PeopleSoft de Oracle(p. 041) **12 JUN 2026** INCIBE-CERT

ALERTAS SCI

Boletín de seguridad de Siemens: junio de 2026(p. 043) **9 JUN 2026** INCIBE-CERT

Múltiples vulnerabilidades en productos de Schneider Electric (p. 043) **9 JUN 2026** INCIBE-CERT

Múltiples vulnerabilidades en LabX Standard de Mettler Toledo (p. 043) **10 JUN 2026** INCIBE-CERT

Múltiples vulnerabilidades en Universal Gateways de MBS(p. 044) **10 JUN 2026** INCIBE-CERT

Credenciales embebidas en productos de Mitsubishi Electric(p. 044) **12 JUN 2026** INCIBE-CERT

Múltiples vulnerabilidades en Cámaras de Brickcom(p. 045) **12 JUN 2026** INCIBE-CERT

Múltiples vulnerabilidades en la plataforma IoT de Naxclow (p. 045) **12 JUN 2026** INCIBE-CERT

Múltiples vulnerabilidades en productos de B&R(p. 045) **12 JUN 2026** INCIBE-CERT

Securiza tus Operaciones Industriales

Empoderamos a las industrias con tecnología de vanguardia que garantiza la seguridad, conformidad y eficiencia de sus operaciones.

Aprende más →



Safetybits

Safetybits

La buena seguridad te impulsa

La plataforma OTSPM de Safetybits aborda la seguridad de manera integral, cubriendo todas las áreas clave en una única herramienta, integrándose con tus procesos y anticipándose a tus necesidades

Dedica menos tiempo a realizar comprobaciones manuales de inventario y a investigar falsos positivos, y pasa directamente a la acción.

Leer Más →



Safetybits es el líder innovador en soluciones de ciberseguridad para entornos de tecnología operativa (OT). Nuestra misión es empoderar a las industrias con tecnología de vanguardia que garantice la seguridad, conformidad y eficiencia de sus operaciones.

¿Y SI LA SOLUCIÓN A TU PROBLEMA NO FUERA COMPRAR MÁS TECNOLOGÍA?

El método de la pregunta incómoda de **XELAB**

Descubre más

www.xelab.io

xelab

Email
carlos@palominomoreno.com

Teléfono
+34 635 31 10 59

Horario
Lun - Vier 9:00 - 15:00

Seguro de Ciberriesgo

LA PROTECCIÓN DIGITAL QUE TU EMPRESA NECESITA

¿Qué es un seguro de ciberriesgo?

En un mundo cada vez más conectado, los ciberataques ya no son cosa de grandes corporaciones. Cualquier empresa, por pequeña que sea, puede **sufrir un robo de datos**, un ataque de ransomware o una suplantación de identidad digital.

Un seguro de ciberriesgo **te protege frente a estos incidentes**, cubriendo tanto las pérdidas económicas como los costes técnicos y legales que pueden derivarse de un ataque informático.

Protección de datos

Cubre los costes derivados del robo, filtración o pérdida de datos personales o sensibles almacenados por tu empresa.

Asistencia técnica

Incluye servicios de expertos en ciberseguridad que actúan rápidamente para contener el ataque y evitar daños mayores.

Responsabilidad

Te protege frente a reclamaciones de terceros si un fallo de seguridad en tus sistemas causa perjuicio a clientes.

Gastos asociados

Desde costes legales hasta sanciones por incumplimiento de la RGPD, pasando por recuperación de información.

Interrupción del negocio

Si un ciberataque paraliza tu actividad (por ejemplo, bloqueando tus sistemas o webs), el seguro cubre la pérdida de ingresos mientras recuperas la operativa, ayudándote a minimizar el impacto financiero.

Extorsión digital y ransomware

Cubre los costes derivados de amenazas como el secuestro de datos (ransomware), incluyendo negociaciones, pagos de rescate bajo supervisión y restauración de archivos.

Auditoría y prevención

Incluye servicios de análisis de vulnerabilidades, formación para tu equipo y asesoramiento técnico para reducir los riesgos antes de que ocurra un ataque.

UNA BARRERA EFICAZ FRENTE A LAS AMENAZAS DIGITALES MÁS CRÍTICAS

¿Qué cubre el seguro de ciberriesgo?

El seguro de ciberriesgo **no solo actúa cuando el daño ya está hecho**: también te acompaña en la prevención, la detección y la respuesta ante cualquier incidente digital. Desde ataques informáticos hasta errores humanos o fallos en el software, esta cobertura **te permite operar con tranquilidad** en un entorno cada vez más vulnerable.

SECCIÓN

ARTíCULOS

3 PIEZAS EN ESTA SECCIÓN

Miembros de Araintel participan en C1b3rtr4cks 2026 (UAM)



DIEGO JULIáN ADELL · 11 JUN 2026

Miembros de **Araintel** asistieron a la V edición de C1b3rtr4cks 2026 celebrada el 29 de mayo en la Universidad Autónoma de Madrid (UAM).

La jornada contó con seis ponencias orientadas a **promover la cultura de la seguridad digital entre cualquier público interesado**, mediante la difusión de conocimiento en **ciberseguridad y ciberinteligencia** El evento fue organizado por la **SEIF, la Asociación de Seguridad Informática de la Universidad Autónoma de Madrid**



Apertura del evento

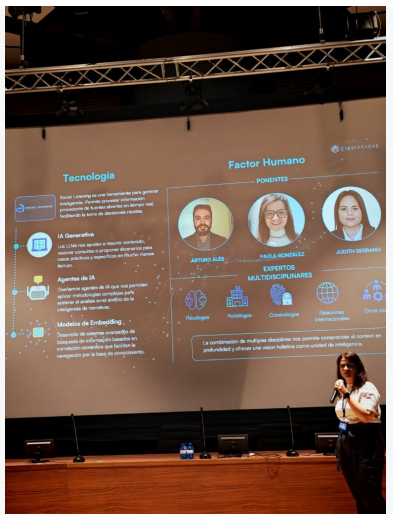
El evento comenzó en el salón de actos de la Politécnica. Durante la espera en la fila, dos de nuestros miembros, Diego y Christian coincidieron con varios asistentes, entre ellos Daniel Ferrer Acio. **A todos los participantes se les entregó como acreditación un badge PCB, que tuvo un papel relevante a lo largo de la jornada.**

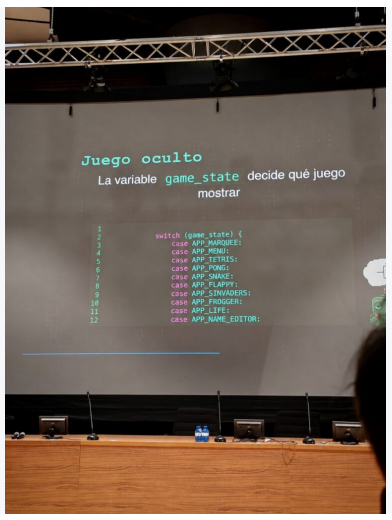
La acreditación entregada consistía en una matriz LED RGB de 8x16 con un microcontrolador MCU CH32V003, **cinco botones y ocho juegos programados**, entre ellos Tetris, Snake y Flappy Bird. Uno de ellos permanecía oculto y estaba basado en el Juego de la Vida de Conway.

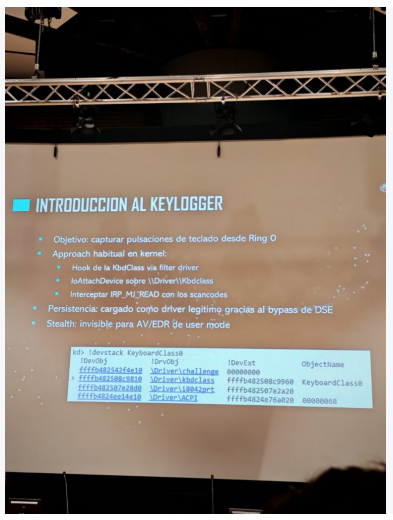
Descubrir cómo acceder a ese contenido fue precisamente el eje de la primera ponencia, impartida por Javier Balboa, de Future Space, quien evidenció un cuidado especial tanto en el desarrollo del badge como en la presentación. Este es uno de los motivos por los que conviene acudir puntual al evento y no quedarse sin acreditación, ya que los badges son limitados.











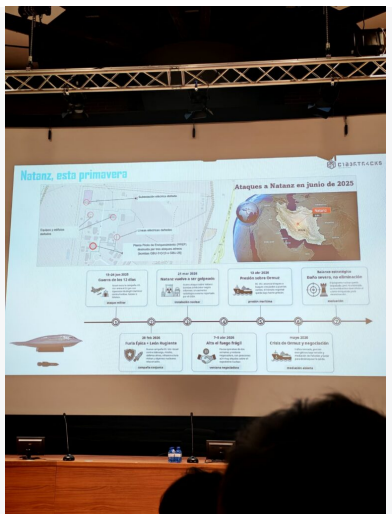
Desarrollo del evento

El evento continuo con un tema de actualidad, **la guerra cognitiva y la IA aplicada al OSINT** en el contexto actual de Groenlandia. Paula González, Judith Serrano y Arturo Alés nos dieron una masterclass de los retos que se desarrollan en este tipo de campañas, sus riesgos, y como se pueden enfrentar,

A continuación tuvo lugar la ponencia «Evadiendo DSE para carga de drivers no firmados», impartida por Adrián Zamora. La sesión abordó la amenaza que supone el uso de drivers legítimos firmados en operaciones de malware y las medidas que pueden aplicarse para mitigar este tipo de técnicas. Durante la presentación se utilizó un keylogger como ejemplo práctico para mostrar cómo pueden desarrollarse estos ataques.

Ángel Veloy, con su exposición sobre «Stuxnet», abordó el contexto de ciberguerra entre Estados Unidos e Irán y explicó cómo esta ciberarma fue utilizada contra el programa de enriquecimiento de uranio iraní.

Una de las ponencias que más sorprendió fue «Hacking Cranes Mama», impartida por Pedro C., alias s4ur0n. En ella se **explicó el hacking RF aplicado a los sistemas de radiocontrol de grúas** Para hacerlo más claro, el ponente utilizó una mini grúa en el escenario y un mando radiocontrol. A través de la presentación, fue mostrando las vulnerabilidades de estos sistemas y **realizó una demostración en vivo con Flipper Zero, capturando la señal de radio del mando inalámbrico y replicándola sobre la mini grúa**.





Joel Serna y David Marugán realizaron una demostración sobre cómo pudo llevarse a cabo la llamada «Operación Grim Beeper», atribuida a Israel contra equipos de radiocomunicaciones utilizados por Hezbolá en Líbano y Siria. La operación terminó con la detonación simultánea de buscapersonas y walkie-talkies vinculados a este grupo armado.

La demostración se centró en dos aspectos: **la modificación interna del hardware de los buscapersonas**, y el uso del protocolo de radio **POCSAG** para activar el dispositivo. De esta forma, los ponentes explicaron de manera práctica cómo una alteración física del equipo podía combinarse con señales de radio para provocar su activación remota.



Como cierre del evento, no podía faltar una ponencia dedicada a la inteligencia artificial. Jaime Morales, con «Cuando la IA se autocrea agujeros de seguridad», explicó cómo el uso cada vez más extendido de esta tecnología puede hacer que vulnerabilidades conocidas y no corregidas se propaguen y se repliquen dentro de los propios sistemas de IA.

Cierre y reflexión

Después del viaje, entre nervios y cansancio el evento nos dejo una grata impresión, con mas dudas, preguntas y ganas de saber de las que llegamos **Es un evento para ir, disfrutar y querer reflexionar.**

Sus miembros **Iván Sánchez** y **Juan Fernández**, nos ofrecieron una gran bienvenida a todos los asistentes. También cabe reconocer el trabajo de toda la asociación por el éxito de la jornada y por la calidad de los ponentes participantes. El año que viene sin duda repetiremos.



Síguenos en araintel.com

Qué es el Ghostpairing y cómo evitar accesos ocultos a nuestras redes sociales como WhatsApp



RUBEN MARCU · 12 JUN 2026

El ghostpairing es una técnica de fraude basada en ingeniería social que busca vincular una cuenta digital a un dispositivo o sesión controlada por el atacante sin que la víctima pierda necesariamente el acceso principal.

A diferencia del robo tradicional de cuentas, el objetivo no siempre es cambiar la contraseña o expulsar al usuario, sino añadir una presencia oculta dentro de la cuenta.

El caso se ha detectado especialmente en WhatsApp y WhatsApp Web por el uso de **dispositivos vinculados**, pero la lógica del ataque no se limita a esta aplicación.

Cualquier plataforma que permita mantener sesiones abiertas, conectar dispositivos, autorizar aplicaciones externas o aprobar accesos desde otro equipo puede ser intervenida de manera similar.

Cómo funciona el engaño

El ataque empieza con un mensaje diseñado para generar confianza o urgencia. Puede llegar desde una cuenta previamente comprometida, lo que hace que la víctima lo perciba como legítimo. El contenido suele incluir un enlace con un pretexto simple: una supuesta foto, una etiqueta, una revisión de seguridad, una invitación o una comprobación de identidad.

Al acceder al enlace, la víctima llega a una página fraudulenta que imita un servicio conocido. El sitio puede simular una pantalla de Meta, Google, Microsoft, una red social, una plataforma de mensajería o cualquier servicio usado por la víctima.

A partir de ahí, el atacante no siempre intenta robar directamente una contraseña. En muchos casos busca que el usuario complete una acción legítima: escanear un código QR, introducir un número de teléfono, aprobar una notificación, iniciar sesión en una versión web falsa o autorizar la vinculación de un nuevo dispositivo.

El resultado es una sesión añadida a la cuenta. La víctima puede seguir utilizando el servicio, pero el atacante también obtiene acceso.

Por qué es más difícil de detectar

El aspecto más problemático del ghostpairing es que no siempre produce una señal evidente. En un robo clásico, la víctima suele notar que no puede entrar, que la contraseña ha cambiado o que la cuenta ha sido recuperada por un tercero. En este caso, el acceso principal puede seguir funcionando.

Esa continuidad reduce la sospecha. El usuario abre la aplicación, ve sus mensajes o su perfil y no percibe una pérdida inmediata de control. Mientras tanto, el atacante puede consultar información, observar actividad, descargar archivos o preparar nuevos fraudes desde dentro de la cuenta.

La técnica resulta especialmente útil cuando el valor está en la vigilancia, la lectura de mensajes, la suplantación progresiva o el acceso a información sensible, no solo en el bloqueo de la cuenta.

Plataformas donde puede aplicarse la misma lógica

En aplicaciones de mensajería, como WhatsApp, Telegram o servicios con versión web, el atacante puede buscar el acceso a conversaciones, archivos, grupos y contactos. La cuenta comprometida también puede servir para enviar enlaces fraudulentos a otras personas con mayor credibilidad.

En redes sociales, el objetivo puede ser acceder a mensajes privados, publicar contenido, modificar datos del perfil, contactar con seguidores o utilizar la cuenta para campañas de fraude y suplantación.

En servicios de correo electrónico, el riesgo es mayor. Una sesión no autorizada puede permitir leer comunicaciones, recuperar contraseñas de otros servicios, acceder a facturas, documentos, contratos o información profesional, y preparar ataques dirigidos.

En plataformas corporativas, como suites de productividad, almacenamiento en la nube o herramientas de colaboración, el atacante puede obtener acceso a documentos internos, conversaciones de equipo, calendarios, archivos compartidos o credenciales almacenadas de forma indirecta.

En cuentas bancarias o servicios financieros, el margen suele estar más protegido por controles adicionales, pero el riesgo puede aparecer si el usuario autoriza accesos, entrega códigos, instala aplicaciones falsas o permite operaciones desde un dispositivo no reconocido.

WhatsApp como caso visible

WhatsApp es uno de los casos más claros porque su función de dispositivos vinculados permite utilizar la cuenta desde varios equipos. El atacante puede intentar que la víctima complete el proceso como si estuviera accediendo a una foto, verificando su identidad o entrando en un servicio legítimo.

Una vez vinculada la sesión, el atacante puede consultar parte de la actividad disponible, enviar mensajes y aprovechar la confianza de los contactos. La víctima, al no perder el acceso desde su teléfono, puede tardar más en detectar el problema.

Por eso la revisión periódica de **Dispositivos vinculados** es una medida básica. Cualquier sesión desconocida debe cerrarse de inmediato.

Qué hacer si se sospecha de una sesión no autorizada

La primera medida es revisar las sesiones activas de la cuenta afectada. En cada plataforma puede aparecer con nombres distintos: dispositivos vinculados, sesiones activas, actividad de inicio de sesión, aplicaciones conectadas, dispositivos de confianza o accesos recientes.

Si aparece un dispositivo, navegador, ubicación o aplicación no reconocida, debe cerrarse la sesión. Después conviene cambiar la contraseña y activar o revisar la autenticación en dos factores.

También es recomendable revocar permisos de aplicaciones externas. Muchas cuentas permiten conectar servicios de terceros que mantienen acceso aunque el usuario cambie algunos datos de inicio de sesión.

Si la cuenta ha sido utilizada para suplantar la identidad de la víctima, enviar enlaces fraudulentos o cometer un fraude económico, deben conservarse pruebas. Capturas de pantalla, mensajes, correos, enlaces, números de teléfono, registros de actividad y justificantes pueden ser útiles para una denuncia.

Prevención: revisar accesos, no solo contraseñas

La prevención no debe limitarse a usar contraseñas fuertes. El ghostpairing demuestra que una cuenta puede verse comprometida aunque la contraseña no haya cambiado. El punto crítico está en las sesiones abiertas y en las autorizaciones concedidas.

Conviene revisar de forma periódica los dispositivos vinculados, cerrar sesiones antiguas, eliminar aplicaciones conectadas que ya no se utilicen y desconfiar de cualquier enlace que pida aprobar un acceso, escanear un QR o verificar una cuenta.

La autenticación en dos factores sigue siendo necesaria, pero no elimina por completo el riesgo si el usuario aprueba manualmente una acción fraudulenta. Ningún código, aviso de verificación o solicitud de acceso debe aceptarse sin comprobar antes qué se está autorizando.

EL ghostpairing no es solo un problema de WhatsApp. Es una forma de abuso de confianza contra el modelo actual de cuentas multiplataforma. Su eficacia depende de una idea sencilla: conseguir que la víctima abra la puerta pensando que está realizando una acción normal.

Denuvo, hipervisores y cuando piratear sale caro



DEDE · 12 JUN 2026

Los sistemas de protección de videojuegos como Denuvo llevan años dificultando la distribución de copias no autorizadas. Ante la ausencia de cracks tradicionales para algunos títulos recientes, han aparecido métodos alternativos basados en hipervisores personalizados**capaces de alterar el entorno de ejecución del juego**.

La técnica no elimina las protecciones del software. En su lugar, **intenta engañarlas desde una capa con privilegios superiores al propio sistema operativo**. El enfoque ha generado interés entre comunidades de cracking, pero también plantea riesgos de seguridad que van más allá de los habituales asociados a este tipo de herramientas.

Qué está ocurriendo

Algunos grupos han comenzado a experimentar con bypass basados en hipervisores para ejecutar videojuegos protegidos por Denuvo sin necesidad de modificar directamente el ejecutable del juego.

A diferencia de un crack tradicional, que altera el software protegido para neutralizar sus mecanismos de defensa, este enfoque busca modificar el entorno donde se ejecuta el juego. El objetivo es responder de forma controlada a determinadas comprobaciones realizadas por el sistema anti-tamper.

La propuesta surge en un contexto donde ciertos títulos permanecen largos periodos sin cracks funcionales debido a la complejidad técnica de las protecciones actuales.

Qué significa crackear un videojuego

Un videojuego es software sujeto a mecanismos de licencia y protección frente a la copia o distribución no autorizada. Para ello suelen utilizarse tecnologías DRM (Digital Rights Management) y sistemas anti-tamper diseñados para detectar modificaciones.

Uno de los ejemplos más conocidos es Denuvo, una tecnología utilizada por numerosos estudios para dificultar la ingeniería inversa y retrasar la aparición de versiones modificadas.

Tradicionalmente, los crackers analizan el funcionamiento interno del programa y modifican partes concretas del ejecutable para desactivar estas protecciones. Se trata de un proceso complejo que requiere conocimientos avanzados de bajo nivel, depuración y análisis de código. La OWASP define este tipo de actividades dentro del ámbito de la ingeniería inversa aplicada al software.

Qué cambia con el uso de hipervisores

Un hipervisor es una capa de virtualización que se sitúa entre el hardware y el sistema operativo. Su función habitual es gestionar máquinas virtuales o entornos aislados. Microsoft ofrece una descripción detallada de este modelo en su documentación sobre Hyper-V.

Existen hipervisores de tipo 1, que se ejecutan directamente sobre el hardware, e hipervisores de tipo 2, que funcionan como aplicaciones dentro de un sistema operativo ya cargado.

En el ecosistema Windows, Hyper-V es un ejemplo de hipervisor de tipo 1. Este componente opera en una capa de privilegios superior al kernel del sistema operativo, conocida habitualmente como Ring -1, una arquitectura basada en las extensiones de virtualización descritas por Intel VT-x

Desde esa posición privilegiada puede observar e interceptar determinadas interacciones entre el software y el hardware antes de que lleguen al procesador.

Cómo intenta evitarse Denuvo

Denuvo no se limita a verificar una licencia válida. También incorpora mecanismos anti-manipulación que monitorizan continuamente el comportamiento del juego durante su ejecución, según explica su desarrollador, Irdeto.

Entre otras funciones, puede detectar herramientas de depuración, analizar tiempos de ejecución, verificar la integridad de determinadas rutinas o utilizar técnicas de virtualización y cifrado para dificultar el análisis de código.

El objetivo de estas medidas no es impedir permanentemente la creación de un crack, sino aumentar el coste técnico y temporal necesario para desarrollarlo.

Los bypass basados en hipervisores intentan aprovechar su posición privilegiada para alterar determinadas respuestas observadas por Denuvo. En lugar de eliminar las comprobaciones, la estrategia consiste en presentar al sistema anti-tamper un entorno aparentemente legítimo.

No existen demasiados detalles públicos y verificables sobre algunas de estas implementaciones, por lo que parte de la información disponible procede de comunidades especializadas y análisis independientes.

El riesgo para el usuario

El principal problema no es técnico sino de confianza. Un crack tradicional puede incorporar código malicioso, pero normalmente sigue estando sujeto a distintas capas de protección del propio sistema operativo, mecanismos de seguridad del kernel y funciones de virtualización modernas.

Un bypass basado en un hipervisor personalizado opera en una posición mucho más sensible. Para funcionar necesita acceso privilegiado al sistema y modifica componentes relacionados con el arranque y la virtualización.

Esto implica que el usuario está concediendo un nivel de control extraordinariamente elevado a software desarrollado por terceros cuya procedencia, auditoría o seguridad suelen ser desconocidas.

Desde una perspectiva de ciberseguridad, instalar un hipervisor no verificado supone asumir riesgos significativamente mayores que ejecutar una aplicación convencional. La agencia estadounidense CISAadvierte de la importancia de proteger adecuadamente estas capas de virtualización debido a su elevado nivel de privilegio.

Una capa difícil de supervisar

Las soluciones de seguridad tradicionales están diseñadas para supervisar procesos que se ejecutan en el sistema operativo o en el kernel.

Un componente que opera en una capa inferior puede resultar más complejo de analizar, monitorizar o desactivar en caso de comportamiento malicioso. TantoCISAcomo la documentación de Microsoft sobre seguridad basada en hardwaredestacan la relevancia de estas tecnologías dentro de la superficie de confianza del sistema.

Esto no significa que cualquier bypass basado en hipervisor sea necesariamente peligroso, pero sí que introduce una superficie de riesgo adicional que debe valorarse antes de su instalación.

Qué deben tener en cuenta los usuarios

La aparición de estas técnicas refleja la evolución constante entre los sistemas de protección comercial y los métodos utilizados para intentar eludirlos.

Sin embargo, el interés técnico del enfoque no elimina los riesgos asociados a instalar componentes con acceso privilegiado al hardware y al proceso de arranque del sistema.

Para el usuario, la cuestión principal no es únicamente si el método funciona, sino qué nivel de acceso está otorgando y qué garantías existen sobre el software que está ejecutando. Como señala la Agencia de la Unión Europea para la Ciberseguridad (ENISA), la confianza en la procedencia y la cadena de suministro del software es un elemento clave para evaluar los riesgos asociados a cualquier tecnología.

En este tipo de escenarios, la falta de transparencia suele ser un factor de riesgo más relevante que la propia protección que se pretende evitar.

QUALIXIS

SERVICIOS DE DEFENSA Y AEROESPACIAL

Calidad y Certificaciones para el Sector Defensa y Aeroespacial



Especialistas en EN 9100, PECAL 2110/2310, ENS e ISO 9001 para pymes industriales del ecosistema de defensa.

EN 9100 / AS 9100

Implantación y certificación de sistemas de gestión de la calidad para la industria aeroespacial y de defensa.

PECAL 2110 / 2310

Adecuación a los requisitos específicos de calidad para proveedores del Ministerio de Defensa.

ENS + ISO 27001

Seguridad de la información y cumplimiento del Esquema Nacional de Seguridad para organizaciones críticas.

Responsable de Calidad por Horas

Profesionales senior integrados en tu equipo para impulsar tu sistema de calidad con flexibilidad y eficiencia.

¿Por qué Qualixis en defensa?

Experiencia real

Amplia experiencia implantando y certificando normas clave en empresas del sector defensa y aeroespacial.

Integración en equipo

Nos integramos en tu organización como un miembro más, entendiendo tu realidad y aportando soluciones prácticas.

Resultados medibles

Conseguimos mejoras tangibles en procesos, cumplimiento y competitividad. Enfocados en resultados, no solo en documentación.



MIEMBRO DEL ECOSISTEMA | Aragon Defence Hub

https://reversea.me

RME

RME-DISCO RESEARCH GROUP

RME is composed of people with special interest on security, mainly focused on software and systems security

FOLLOW US

» See our GitHub's projects

» Follow us in Twitter

» Join to our Telegram's channel!



SECCIÓN

NOTICIAS

14 PIEZAS EN ESTA SECCIÓN

La Brigada ‘Aragón’ I conmemora su XL aniversario



RUBEN MARCU · 8 JUN 2026

La Brigada ‘Aragón’ I conmemoró el **lunes 1 de junio de 2026** en Zaragoza el XL aniversario de su creación con un acto militar que rindió homenaje a los 40 años de trayectoria de esta unidad del Ejército de Tierra y a su contribución a la defensa de España.

La jornada comenzó con una **ofrenda floral a la Virgen del Pilar** en la basílica del Pilar. Posteriormente, se celebró el acto central, presidido por el **general de división Cepeda**, con los honores a la autoridad, la revista a las tropas, el nombramiento de Cazadores de Honor, la despedida de la Enseña Nacional del personal que pasa a la reserva y el homenaje a los caídos.

El acto concluyó con el desfile de las unidades participantes ante las autoridades y el público asistente. La ceremonia formó parte del programa conmemorativo organizado por la Brigada ‘Aragón’ I con motivo de sus cuatro décadas de historia.



La conmemoración también incluyó semanas antes una exposición en el antiguo Palacio de Capitanía General de Zaragoza, inaugurada el **jueves 14 de mayo de 2026** y clausurada el **miércoles 20 de mayo de 2026**. La muestra recorrió la historia de la brigada mediante imágenes de misiones, ejercicios y operaciones, junto con una colección de uniformes representativos.

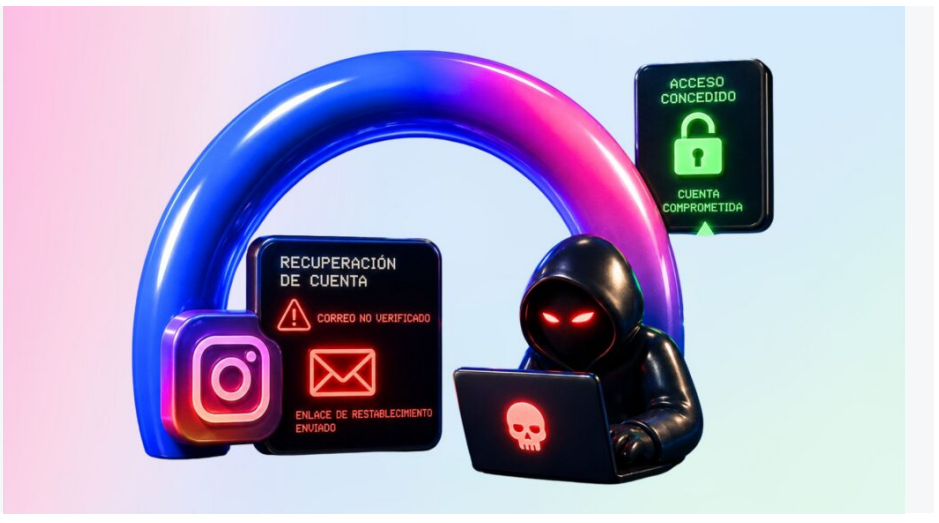
También incorporó un espacio dedicado a su antecesora, la Brigada de Caballería ‘Castillejos’ II.

Más de **5.000 personas** visitaron la exposición durante los días en los que permaneció abierta. La iniciativa permitió acercar a la ciudadanía la evolución histórica de la unidad, su actividad actual y el papel que desempeñan sus militares en distintos ámbitos operativos.

La unidad fue creada el **1 de junio de 1986**. Desde entonces, sus efectivos han participado en numerosas operaciones en territorio nacional e internacional, además de misiones de apoyo a la población civil y actividades de colaboración con la sociedad.

Los actos del XL aniversario culminaron el **sábado 6 de junio de 2026** con una jornada de puertas abiertas orientada especialmente al público juvenil, con el objetivo de mostrar de cerca el trabajo diario de sus soldados y reforzar el vínculo de la unidad con la sociedad aragonesa.

Comprometidas 20.225 cuentas de Instagram por una vulnerabilidad en el soporte con IA de Meta



RUBEN MARCU · 9 JUN 2026

Meta comunicó la semana pasada a las autoridades estadounidenses que un error en el código de **High Touch Support (HTS)**, su herramienta de recuperación de cuentas asistida por inteligencia artificial, habría permitido a terceros no autorizados recibir enlaces de restablecimiento de contraseña, facilitando el secuestro de perfiles sin doble autentificación.

Según notificaciones regulatorias, Meta detectó la brecha el 31 de mayo, aunque se habría producido el 17 de abril, lo que sugiere que la herramienta habría estado comprometida, como mínimo, durante al menos seis semanas. Algunas investigaciones iniciales han demostrado que el método para robar cuentas ya circulaba en grupos de Telegram días antes.

Durante esa ventana se estima que **se pudieron comprometer hasta 20.225 cuentas de usuarios**. Es importante resaltar que **la cifra es un máximo**, no los secuestros confirmados, es decir, algunos de esos restablecimientos los pudieron hacer los propios titulares de la cuenta.

¿Por qué falló 'High Touch Support'?

High Touch Support permite a quien ha perdido el acceso a su perfil pedir ayuda y solicitar que se envíe un enlace de restablecimiento a una dirección de correo a través de un chatbot. Según **Amber Hannah**, Associate General Counsel de Incident Response en **Legal HTS** de Meta, la vulnerabilidad en el sistema se habría debido a una ruta separada del código que no comprobaba correctamente el correo introducido durante la recuperación.

Esa ruta debía verificar que la dirección facilitada coincidiera con la asociada a la cuenta de Instagram, pero no lo hacía. Como consecuencia, el sistema podía enviar enlaces de restablecimiento a correos no vinculados al perfil. En la práctica, el fallo permitió abusar del proceso de recuperación de cuentas y completar un **secuestro de cuenta** account takeover si el perfil **no tenía activada la autenticación de dos factores**.

Según **Andy Stone**, portavoz y director de comunicación de Meta, la vulnerabilidad habría sido parcheada horas después de conocerse el caso y resuelta el día 1 de junio. Algunas fuentes como **404 Media** han documentado que el método circulaba días antes en grupos de Telegram, donde se compartían vídeos, capturas y listas de nombres de usuario de alto valor junto a las guías sobre la explotación, la cual involucraba el uso de VPN para simular la región de la cuenta objetivo.

Recibir el enlace no garantizaba por sí solo el acceso; una vez restablecida la contraseña el secuestrador de cuentas solo podía iniciar sesión **si el titular no tenía activada la autenticación de dos factores (2FA)**.

Qué datos han podido quedar expuestos

Meta afirma desconocer qué información personal ha podido llegar a ser consultada, aunque señala categorías como los datos de contacto como el correo y el teléfono, la fecha de nacimiento,

las publicaciones y el contenido como fotos, vídeos e historias, los mensajes directos, el historial de actividad e interacción, la información del perfil y las cuentas o servicios conectados.

Varios portales como 404 Media vincularon el incidente con varios secuestros de cuentas de alto perfil, entre ellas la antigua cuenta de la Casa Blanca asociada a **Barack Obama**, la cuenta de **Sephora** y la del Chief Master Sergeant de la Fuerza Espacial de Estados Unidos, **John Bentivegna**. Meta, sin embargo, negó que el fallo hubiera afectado a cuentas de líderes mundiales o expuesto mensajes privados, una versión que Andy Stone calificó como «totalmente falsa».

Mitigación y recuperación

Meta ha aplicado un control de seguridad obligatorio a las cuentas potencialmente afectadas, **exigiendo volver a autenticarse antes de recuperar el acceso**, buscando bloquear cualquier sesión o recuperación iniciada a través del flujo vulnerable. También retiró de producción el código defectuoso.

Meta introdujo **HTS** en marzo de 2026 como un asistente de soporte con inteligencia artificial pensado para agilizar tareas de cuenta y seguridad, entre ellas el restablecimiento de contraseñas, la activación de la autenticación de dos factores y la recuperación de accesos.

Meta tiene previsto avisar a los usuarios afectados el día 19 de junio y recomendarles revisar la seguridad de su cuenta así como activar el 2FA.

La aplicación de la IA en la industria reúne a representantes empresariales y agentes de innovación en el ITA



RUBEN MARCU · 9 JUN 2026

Más de **50** representantes de empresas industriales y agentes de innovación han participado en la jornada «Fabricación avanzada impulsada por IA», organizada por el **Instituto Tecnológico de Aragón** en el edificio **DIC** (Digital Imagination Center).

El encuentro se ha centrado en la aplicación de la **inteligencia artificial en entornos productivos**, con casos reales de uso industrial y soluciones orientadas a mejorar procesos, reducir ineficiencias y reforzar la toma de decisiones basada en datos.

IA para fabricación avanzada

La jornada se ha celebrado en el marco del proyecto europeo **AI-MATTERS**, una iniciativa dirigida a acelerar la adopción de soluciones de inteligencia artificial en empresas manufactureras europeas.

El proyecto ofrece infraestructuras de **experimentación, validación y demostración tecnológica**, con el objetivo de que las compañías puedan probar tecnologías avanzadas antes de incorporarlas a sus líneas de producción.

Durante la sesión se han abordado aplicaciones vinculadas a la **fabricación avanzada**, la automatización, la robótica, el análisis de datos y la integración de sistemas inteligentes en plantas industriales.

Casos reales en planta

Uno de los bloques principales ha estado dedicado a casos de us empresariales en ámbitos como **mantenimiento predictivo**, el **control de calidad**, la **optimización de procesos** y la **gestión avanzada de la producción**.

Estas soluciones permiten anticipar fallos, detectar desviaciones en la fabricación, ajustar operaciones y mejorar la eficiencia de los sistemas industriales.

El ITA también ha presentado los servicios de apoyo técnico disponibles a través de **AI-MATTERS**, orientados a reducir las barreras técnicas y económicas que dificultan la implantación de estas tecnologías en la industria.

Empresas, clústeres y capacidades tecnológicas

El encuentro ha contado con la participación de **Mar Paños**, directora general de Industria, Competitividad, Innovación y Transformación Digital Empresarial del Gobierno de Aragón, junto a representantes de distintos **clústeres industriales aragoneses**.

La sesión ha terminado con un espacio de encuentro entre empresas y una visita a las instalaciones tecnológicas del **ITA**, donde los asistentes han podido conocer de cerca las capacidades del centro y explorar posibles colaboraciones con otros agentes del ecosistema industrial.

La Guardia Civil celebra el XI Curso de Verano de Inteligencia y Seguridad junto a la UNIRIOJA



RUBEN MARCU · 9 JUN 2026

La **Guardia Civil** celebrará del **16 al 18 de junio de 2026** la XI edición del Curso de Verano de Inteligencia y Seguridad, bajo el lema **«Innovación y transformación digital cibersegura»**.

La formación se plantea como una **microcredencial de verano** de carácter intensivo y aplicado. El curso abordará cómo la transformación digital, la inteligencia artificial, la gestión del dato y la ciberseguridad están modificando los servicios públicos, la seguridad y la operativa de las organizaciones.

La actividad está alineada con los marcos europeos de competencias digitales y con la evolución estratégica de la Guardia Civil. Su objetivo es que cada participante pueda diseñar una hoja de ruta de innovación y transformación digital adaptada a su unidad, área de responsabilidad o entorno profesional.

El curso se desarrollará en modalidad híbrida, con sesiones presenciales en la Universidad de La Rioja, en Logroño, y seguimiento online a través del campus virtual. Cuenta con **200 plazas**, reconoce **1,5 créditos ECTS** y ofrece diploma acreditativo tras superar un examen final online.

La matrícula estará abierta hasta el **15 de junio de 2026**. La modalidad presencial tiene un coste de **10 euros**, mientras que la online es gratuita. La microcredencial tiene además carácter solidario: todo lo recaudado en inscripciones y aportaciones irá destinado a **Proyecto Hombre en La Rioja**.

Transformación digital aplicada a la seguridad

El programa combina **15 horas presenciales**, distribuidas en tres jornadas, con **22,5 horas de trabajo autónomo** a través del campus virtual. Este formato permite facilitar la participación de profesionales de distintas unidades y comandancias, reducir desplazamientos y mantener la continuidad formativa en contextos operativos exigentes.

Los contenidos se organizan en torno a varios ejes: inteligencia artificial, analítica de datos, automatización, infraestructuras digitales, **ciberseguridad**, soberanía tecnológica y aplicación de capacidades digitales en el ámbito de la seguridad pública.

El curso también analizará los retos organizativos y culturales de la digitalización en estructuras jerarquizadas, así como su impacto en la operativa policial, la toma de decisiones y la prestación de servicio al ciudadano.

Ciberseguridad, inteligencia artificial y datos

La primera jornada estará dedicada a las perspectivas generales de la transformación digital. Tras la inauguración institucional, el programa incluirá una conferencia inaugural a cargo de **Horacio Morell**, presidente de IBM España.

Durante ese primer módulo se abordarán experiencias de transformación digital en los sectores público, privado y académico. También se celebrará un panel sobre seguridad y defensa en la era digital, con participación de representantes de la Guardia Civil, Mossos d'Esquadra, Policía Nacional y Ejército del Aire.

El segundo módulo se centrará en los elementos clave de la transformación digital. La jornada incluirá una mesa sobre infraestructura digital y otra sobre **ciberseguridad en la era de la inteligencia artificial**, con representantes del **Centro Criptológico Nacional**, **INCIBE** y el **Mando Conjunto del Ciberespacio**.

También se tratará el papel de los datos, los procesos y la inteligencia artificial en la transformación de las organizaciones. En este bloque participarán perfiles vinculados al Estado Mayor de la Defensa, la Guardia Civil, Gartner, la Universidad de Castilla-La Mancha e ISDEFE.

Innovación tecnológica en la Guardia Civil

La última jornada estará orientada al futuro de la innovación y la transformación digital. El programa incluye un panel específico sobre proyectos de innovación en la Guardia Civil, con responsables de unidades vinculadas a ciberseguridad, sistemas de información, formación y transformación digital.

El curso incorporará además una ponencia sobre la **Cibercomandancia de la Guardia Civil**, introducida por el general de división **Santiago Martín Gómez**, jefe de la Jefatura de Transformación Digital y Ciberseguridad de la Guardia Civil. La intervención principal correrá a cargo del coronel **José Luis Cano Camarero**, jefe de la Sección de Planeamiento Operativo de Estado Mayor de la Guardia Civil.

La jornada concluirá con una mesa sobre innovación tecnológica, tendencias, desafíos y soberanía, con representantes del CDTI, la Fundación Dialnet e Indra.

Dirigido a perfiles de seguridad, administración y sector privado

La formación está dirigida a miembros de las **Fuerzas y Cuerpos de Seguridad**, Fuerzas Armadas, oficiales de enlace de cuerpos extranjeros acreditados en España, personal de la Administración

Pública, profesionales del sector privado vinculados a la seguridad, estudiantes universitarios y personas interesadas en la materia.

La Policía Nacional desarticula en Zaragoza un coro de los Dominican Don’t Play



RUBEN MARCU · 11 JUN 2026

La **Policía Nacional** ha desarticulado en Zaragoza un “coro” de los **Dominican Don’t Play** y ha detenido a **doce personas** por su presunta participación en delitos de pertenencia a organización criminal, tráfico de drogas, tenencia ilícita de armas, usurpación de bien inmueble y defraudación de fluido eléctrico.

El operativo se ha desarrollado en la capital aragonesa contra un grupo que, según la investigación, mantenía una actividad especialmente intensa en los distritos de **Delicias** y **San José**. El coro habría estado implicado en varios enfrentamientos con bandas rivales como los **Black Panther** o los **Trinitarios**.

La investigación comenzó hace varios meses, cuando agentes especializados en grupos juveniles violentos detectaron un aumento de la actividad de la organización y del número de integrantes del grupo en Zaragoza.

La operación ha sido dirigida por el Tribunal de Instancia de Zaragoza, Sección de Instrucción, Plaza 12, y desarrollada por la **Comisaría General de Información** y la **Brigada Regional de Información de Zaragoza**.

Un grupo estructurado y con reparto de tareas

Los investigadores consideran que el coro estaba formado principalmente por los doce detenidos. El grupo presentaba una estructura interna cohesionada, con reparto de funciones entre sus miembros y una implantación progresiva en distintas zonas de Zaragoza.

La Policía Nacional sostiene que la organización ejercía influencia sobre jóvenes de la ciudad y que su actividad se había consolidado en varios puntos de la capital aragonesa. La investigación también vincula al grupo con episodios de violencia frente a otras bandas juveniles.

Drogas, delitos contra la propiedad y armas intervenidas

La principal vía de financiación del grupo habría sido el **tráfico de drogas** y la comisión de **delitos contra la propiedad**. El operativo culminó con doce detenciones y dos registros domiciliarios en Zaragoza.

Durante los registros, los agentes intervinieron **armas blancas**, instrumentos peligrosos, armas de fuego simuladas, sustancias estupefacientes, balanzas de precisión, pañuelos tipo bandana, varios vehículos de movilidad personal y diferentes dispositivos tecnológicos, que están siendo analizados.

Los detenidos han sido puestos a disposición judicial. El titular del Tribunal de Instancia de Zaragoza, Sección de Instrucción, Plaza 1, ha decretado **prisión provisional para siete de los arrestados**. La investigación continúa abierta y la Policía Nacional no descarta nuevas detenciones.

Deveco impulsa un afterwork sobre IA práctica para pymes junto a CEOE Aragón y Tecnara



RUBEN MARCU · 12 JUN 2026

La **Oficina Acelera Pyme** de CEOE Aragón celebrará el próximo **23 de junio** a las 18:00 la segunda sesión del **Ciclo Afterwork Acelera Pyme** con la colaboración de **DEVECO** y **TECNARA, Clúster TIC de Aragón**

El encuentro, de carácter gratuito, se plantea como una sesión empresarial en la que la digitalización se combina con el networking en espacios cercanos y singulares de Aragón.

De la mano de DEVECO, la jornada mostrará cómo aplicar la inteligencia artificial en una pyme de forma práctica y sencilla, con el objetivo de ahorrar tiempo, mejorar la organización interna y aumentar la productividad.

Durante la sesión se abordará cómo automatizar tareas habituales como la atención al cliente, la gestión de correos o la generación de documentos. También se analizarán herramientas de IA accesibles para pequeñas y medianas empresas, criterios para identificar procesos con potencial de automatización y errores frecuentes que conviene evitar al empezar a trabajar con estas soluciones.

El programa incluirá además una aproximación a **Commander**, una herramienta orientada a empresas industriales, manufactureras e ingenierías para mejorar la gestión de recursos, equipos y toma de decisiones.

Las plazas son limitadas y la solicitud de plaza debe realizarse a través del correo **oap@ceoearagon.es**.

Fuente: Oficina Acelera Pyme CEOE Aragón.

IA para empresas: NEXVIUM, Digital Hand Made, Golive y SMF Monclús abordarán ciberseguridad, el AI Act y la búsqueda de financiación



RUBEN MARCU · 12 JUN 2026

CEOE Aragón celebrará el próximo **2 de julio** la jornada «IA para empresas: el momento es ahora», una sesión centrada en el impacto de la inteligencia artificial en la actividad empresarial.

El encuentro abordará la aplicación de la IA en la toma de decisiones, la organización interna, la ciberseguridad, el cumplimiento normativo y la financiación de proyectos tecnológicos. La jornada contará con la participación de **NEXVIUM**

,**Digital Hand Made**,**Golive**y**SMF Monclús Abogados**

Durante la sesión se analizarán casos reales y usos prácticos de la inteligencia artificial en el negocio. Entre los temas previstos figuran la IA decisional para mejorar la toma de decisiones, los retos de ciberseguridad asociados a esta tecnología, la preparación de las empresas ante el**AI Act**y las ayudas disponibles para impulsar proyectos de IA.

El programa contará con intervenciones de**Antonio Santacruz**, de **NEXVIUM**;**David Lozano**, de**Digital Hand Made**;**Javier Ferrando**y**Carlos Saad**, de**Golive**; y**Álvaro Monclús**, de**SMF Monclús Abogados**

La jornada comenzará a las**9:30 horas**y finalizará con un café networking. La**inscripción**es imprescindible y debe realizarse a través de la web de CEOE Aragón.

Fuente:CEOE Aragón.

El RPEI-12 instruye a las Fuerzas Armadas libanesas en desactivación de explosivos en Zaragoza



RUBEN MARCU · 12 JUN 2026

El**Regimiento de Pontoneros y Especialidades de Ingenieros Nº12** (RPEI-12), con sede en Zaragoza, ha acogido la fase práctica del primer curso de desactivación de explosivos de nivel 2 impartido por personal español a miembros de las**Fuerzas Armadas de Líbano**.

La formación se ha desarrollado durante ocho semanas. Las seis primeras tuvieron lugar en Beirut, mientras que las dos últimas se realizaron en Zaragoza, donde los participantes completaron prácticas con explosivos y municiones reales.

El curso ha estado dirigido a la adquisición de capacidades propias de la especialidad**EOD**, siglas en inglés de Explosive Ordnance Disposal. Esta disciplina se centra en la identificación, manipulación y desactivación de artefactos explosivos y municiones convencionales.



Durante su estancia en el Regimiento de Pontoneros, los militares libaneses realizaron ejercicios prácticos bajo la supervisión del **Equipo Móvil de Instructores**español, conocido por sus siglas en inglés como MTT. Las prácticas permitieron aplicar los conocimientos adquiridos en la fase teórica desarrollada previamente en Líbano.

Tras completar la instrucción, los participantes deberán superar los exámenes oficiales en la**Escuela Regional para el Desminado Humanitario en Líbano**, ubicada en Hammana. La certificación les habilitará para ejercer esta especialidad en

la República del Líbano.

La actividad se enmarca en el **Military Technical Committee for Lebanon**, MTC4L, constituido en marzo de 2024 y del que España es miembro fundador. Este organismo trabaja para reforzar la eficacia y la capacidad operativa de las Fuerzas Armadas libanesas.

La formación confirma el papel de Zaragoza como punto de instrucción especializada en capacidades EOD dentro de la cooperación militar española con Líbano.

Integra Security Day reúne a expertos nacionales para abordar la anticipación y la respuesta empresarial ante los ciberataques



ARAINTEL · 12 JUN 2026

Integra Tecnología ha celebrado este martes en Zaragoza una nueva edición de **Integra Security Day**, un encuentro orientado a analizar los principales retos de la ciberseguridad empresarial desde la anticipación, la visibilidad, la respuesta ante incidentes y la protección continua.

La jornada reunió a **José Luis Latorre**, consejero de Organización en Integra Tecnología; **Deepak Daswani**, ingeniero en informática y experto en ciberseguridad; **Álvaro Lancho**, Microsoft Security Evangelist en Glueckkanja; **Aitor de la Pinta**, System Engineer en Fortinet; **Fernando Bonet**, Sales Specialist en Integra Tecnología; **Aída Morfioli**, directora de Servicios Gestionados en Integra; y **Pablo Moreno**, Cybersecurity Engineer en Integra.

El encuentro, celebrado en **Finca La Alquería**, abordó la ciberseguridad como un proceso que no empieza cuando se detecta un incidente, sino antes. La sesión puso el foco en la necesidad de identificar riesgos, ganar visibilidad sobre los sistemas, coordinar la respuesta y reducir la superficie de ataque en organizaciones cada vez más conectadas y distribuidas.

El ataque como punto de partida

La apertura contó con la intervención de **José Luis Latorre**, consejero de Organización en Integra Tecnología, quien situó el riesgo digital como una realidad que muchas veces permanece oculta hasta que el incidente ya se ha producido.

Uno de los bloques centrales estuvo protagonizado por **Deepak Daswani**, ingeniero en informática, hacker y experto en ciberseguridad. Su intervención mostró cómo puede desarrollarse un ciberataque y por qué las decisiones adoptadas en los primeros momentos resultan determinantes para contener su impacto.

La sesión acercó a los asistentes a una cuestión clave para cualquier organización: cuánto tiempo tarda una empresa en detectar que ha sido atacada y qué capacidad real tiene para reaccionar cuando la amenaza ya está dentro.

SOC, SASE y Zero Trust

El papel del **SOC**, centro de operaciones de seguridad, fue otro de los ejes del encuentro. **Microsoft** y **Álvaro Lancho**, Microsoft Security Evangelist en **Glueckkanja**, abordaron la importancia de contar con visibilidad suficiente para detectar, investigar y responder ante incidentes.

La jornada también analizó la reducción de la superficie de ataque mediante enfoques como **SASE** y **Zero Trust**, dos modelos orientados a reforzar la seguridad corporativa en entornos híbridos y distribuidos. Este bloque contó con la participación de **Aitor de la Pinta**, System Engineer en **Fortinet**, y **Fernando Bonet**, Sales Specialist en **Integra Tecnología**.

Durante el encuentro se trataron cuestiones como la detección temprana, la respuesta coordinada, la defensa moderna, la protección continua y la evolución de la ciberseguridad hacia modelos gestionados y estratégicos.

Seguridad como proceso continuo

El cierre corrió a cargo de **Aída Morfioli**, directora de Servicios Gestionados en Integra, y **Pablo Moreno**, Cybersecurity Engineer en Integra. Ambos defendieron que la seguridad no debe entenderse como un proyecto puntual, sino como un proceso permanente de prevención, detección, respuesta y mejora.

Bajo el enfoque de **Security Care**, Integra Tecnología planteó la necesidad de acompañar a las organizaciones de forma continuada frente a un escenario de amenazas en evolución constante.

La jornada finalizó con un espacio de comida y networking entre asistentes, ponentes y partners tecnológicos. Con esta nueva edición, **Integra Security Day** refuerza su posición como un encuentro dirigido a empresas, instituciones y profesionales interesados en mejorar su preparación ante los riesgos digitales.

Araintel, presente en Integra Security Day

Varios miembros de Araintel asistieron a la jornada, donde compartieron experiencias y posibles nuevas oportunidades laborales con otros asistentes.



Fuente: Integra Tecnología.

Colorín colorado, este cuento se ha acabado. EE. UU. ordena a Anthropic suspender sus modelos Fable y Mythos por ‘motivos de seguridad nacional’



RUBEN MARCU · 13 JUN 2026

La compañía de Dario Amodei ha acatado la directiva de control de exportaciones del Gobierno estadounidense, pero discrepa de la medida, la atribuye a un malentendido y asegura estar trabajando para restablecer el servicio. El acceso al resto de sus modelos no se ha visto afectado.

El **Gobierno de Estados Unidos** ha emitido una directiva de control de exportaciones que ha obligado a Anthropic a suspender el acceso a Claude Fable 5 y Claude Mythos 5 por parte de cualquier ciudadano extranjero, tanto dentro como fuera del país.

Anthropic ha indicado que recibió dicha directiva a las 17:21, hora del Este de Estados Unidos, **en torno a las 23:21 en la España peninsular**. La compañía sostiene que la carta se ampara en motivos de seguridad nacional, pero no concreta cuál es el riesgo específico que habría llevado a imponer la restricción.

La compañía ha explicado que el efecto práctico de la orden ha sido **la desactivación abrupta de Fable 5 y Mythos 5 para todos sus clientes**, con el objetivo de garantizar el cumplimiento de la directiva, no viéndose afectado el uso del resto de sus modelos.

La decisión ha provocado malestar en parte de la comunidad tecnológica. Las críticas apuntan a que **Anthropic habría contribuido a sobredimensionar el riesgo de Fable 5** con un discurso demasiado alarmista sobre sus capacidades, una narrativa que ahora podría haberse vuelto en su contra.

A ello se suma el malestar de usuarios que dependían de Fable 5 para trabajar o que habían contratado Claude Max precisamente para acceder al nuevo modelo. La retirada abrupta del servicio ha abierto **dudas sobre posibles reembolsos**, y sobre la confianza de la clientela en lanzamientos sujetos a restricciones regulatorias de este tipo.

El caso también amplía el debate sobre el acceso a la inteligencia artificial avanzada. Algunos observadores ven en esta decisión un posible punto de inflexión: **los modelos frontera podrían dejar de ofrecerse como productos comerciales abiertos**. Ello podría derivar en accesos diferenciados según país, nacionalidad o tipo de cliente.

Gobiernos aliados, grandes laboratorios, contratistas de defensa y empresas autorizadas podrían quedar en una posición preferente, mientras **usuarios, investigadores independientes, pequeñas empresas o clientes de países considerados sensibles perderían acceso a los sistemas más avanzados.**

Un posible jailbreak

Según **Anthropic**, el Gobierno estadounidense habría actuado tras conocer un posible método para sortear la seguridad de **Fable 5**. Esta técnica, conocida como jailbreak, permite intentar obtener respuestas que el modelo debería bloquear o restringir.

La compañía afirma que revisó una demostración del método. Según su versión, solo sirvió para identificar un pequeño número de vulnerabilidades menores y ya conocidas. Anthropic sostiene que otros modelos públicos también podrían detectar esos fallos sin recurrir a un jailbreak.

Hasta ahora, el Gobierno solo le habría trasladado pruebas verbales de un posible jailbreak específico, no generalizado. El caso consistiría en pedir al modelo que lea una base de código concreta y corrija posibles fallos de software.

La compañía añade que ha revisado un informe que considera la base de la directiva. Según su análisis, la capacidad mostrada en ese documento ya está disponible en otros modelos, incluido **GPT-5.5** de OpenAI.

Las salvaguardas de Fable 5

Anthropic defiende que **Fable 5** incorpora controles de seguridad reforzados para limitar su uso indebido en ciberseguridad y otros ámbitos sensibles. La compañía afirma que esas restricciones son amplias y que algunos usuarios las han considerado excesivas.

Antes del lanzamiento, Anthropic asegura que sometió el modelo a miles de horas de pruebas con el **Gobierno estadounidense**, el **Instituto de Seguridad de la IA del Reino Unido**, organizaciones privadas externas y equipos internos. El objetivo era comprobar hasta qué punto podían sortearse sus defensas.

Según la empresa, esas pruebas mostraron que las salvaguardas de Fable 5 son más eficaces que las de modelos anteriores. Anthropic sostiene que ningún equipo ha logrado hasta ahora un jailbreak universal, es decir, una técnica capaz de anular de forma general las defensas del modelo y desbloquear capacidades avanzadas en ciberseguridad.

La compañía admite, aun así, que ningún sistema es inmune. Según Anthropic, cualquier modelo puede ser vulnerable a técnicas de evasión concretas, capaces de obtener cierta información sensible en casos específicos.

Por ese motivo, Anthropic afirma que diseñó Fable 5 con una estrategia de seguridad por capas. La idea es limitar el alcance de los posibles jailbreaks, hacer más difícil su desarrollo y combinar esas barreras con monitorización para detectar y cerrar abusos.

La empresa también vincula esta estrategia con la retención de datos de clientes durante 30 días en Fable 5. Anthropic reconoce que esta política tiene un coste en su relación con los usuarios, pero sostiene que le permite investigar y mitigar posibles técnicas de evasión.

Discrepancia con la decisión del Gobierno

Anthropic ha cumplido hasta ahora la directiva legal del Gobierno estadounidense, pero discrepa de la medida. La compañía considera que el hallazgo de un posible jailbreak limitado no justifica retirar un modelo comercial desplegado, según la propia empresa, para “cientos de millones de personas”.

La empresa advierte de que, si ese criterio se aplicara al conjunto del sector, podría frenar en la práctica todos los nuevos lanzamientos de **modelos frontera**

Anthropic sostiene que el Gobierno debe poder bloquear despliegues inseguros, pero dentro de un proceso transparente, justo, claro y basado en hechos técnicos. A juicio de la compañía, esta actuación no cumple esos principios.

La empresa ha pedido disculpas a sus clientes por la interrupción del servicio. También ha señalado que considera el episodio un malentendido y que trabaja para restablecer cuanto antes el acceso a **Fable 5** y **Mythos 5**

Reacciones en redes sociales

Parte de la comunidad tecnológica ha cuestionado la estrategia de **Anthropic**. La crítica se centra en que la compañía habría contribuido a sobredimensionar el riesgo de **Fable 5** con un discurso demasiado alarmista sobre sus capacidades. Según esta lectura, esa narrativa habría terminado volviéndose en su contra.

A esa crítica se suma la frustración de usuarios que dependían de **Fable 5** para trabajar o que habían contratado suscripciones específicas para acceder al nuevo modelo. Algunos clientes de **Claude Max** han planteado si podrán recuperar el dinero tras contratar el servicio precisamente para utilizar Fable 5.

Otros observadores ven en este caso un posible punto de inflexión.

La IA más avanzada podría dejar de venderse como un producto comercial

abierto y pasar a gestionarse como tecnología estratégica. En la práctica, eso podría traducirse en accesos diferenciados según país, nacionalidad o tipo de cliente.

Gobiernos aliados, grandes laboratorios, contratistas de defensa y empresas autorizadas podrían mantener acceso a los modelos más potentes, mientras usuarios, investigadores independientes, pequeñas empresas o clientes de países considerados sensibles quedarían fuera.

También han surgido lecturas políticas que interpretan la medida como parte de una disputa mayor entre el **Gobierno estadounidense** y las empresas que desarrollan inteligencia artificial avanzada. Estas posiciones plantean que los controles de exportación podrían utilizarse no solo como instrumento de seguridad nacional, sino también como mecanismo de presión sobre compañías que no se alineen con determinadas prioridades políticas, militares o económicas.

13 empresas del Hub de Defensa de Aragón participarán en Eurosatory, una de las principales ferias de defensa y seguridad de Europa



RUBEN MARCU · 13 JUN 2026

El Hub de Defensa de Aragón participará por primera vez con un stand agrupado en **Eurosatory**, una de las principales ferias internacionales de defensa y seguridad. La cita se celebrará del **15 al 19 de junio** en el recinto **Paris-Nord Villepinte**, en París, y reunirá a empresas, instituciones, delegaciones oficiales y profesionales del sector.

La participación aragonesa reunirá a **13 empresas** y superará los **180 metros cuadrados** de superficie expositiva entre el stand agrupado del **Hub de Defensa de Aragón**, el Pabellón de España y varios espacios independientes. Las empresas presentes serán **Aragon Photonics, ARPA, Cigüeñales Sanz, Equimodal, Kepar, Modisprem, TBO Logistics, Teltronic, Instalaza, Zfoam, ANMOPYC, Mecanus Innovación y Up Lifting**

El objetivo es dar visibilidad internacional a las capacidades industriales, tecnológicas y logísticas de Aragón, además de abrir contactos comerciales en el mercado francés y europeo de defensa. La presencia estará coordinada por **AREX**, la Dirección General de Industria, Competitividad, Innovación y Transformación Digital Empresarial del Gobierno de Aragón y el **Instituto Aragonés de Fomento**

Qué es Eurosatory

Eurosatory es la mayor feria europea especializada en defensa y seguridad. El encuentro reúne a empresas, instituciones, delegaciones oficiales y profesionales vinculados a ámbitos como seguridad interior, ciberseguridad, espacio, drones, gestión de crisis, protección civil, logística, sistemas de mando y control, vehículos, sensores y soluciones duales.

En su última edición congregó a más de **2.000 expositores** y más de **60.000 visitantes profesionales**. Para las empresas aragonesas, la feria supone una vía de acceso a potenciales clientes, proveedores, contratistas principales, delegaciones internacionales y ecosistemas industriales de defensa.

La cita llega en un contexto de mayor atención europea hacia la industria de defensa, la seguridad y las tecnologías de doble uso, con especial interés en reforzar capacidades industriales propias y cadenas de suministro estratégicas.

La presencia de Aragón en París

El centro de la actividad aragonesa durante los cinco días de feria será el stand del **Hub de Defensa de Aragón**, ubicado en el **pabellón 4**. El espacio tendrá **63 metros cuadrados** y contará con zona institucional, mostradores individuales para empresas y área de reuniones.

El stand agrupado funcionará como punto común de representación para las compañías integradas en el espacio del Hub. La superficie total aragonesa será superior porque incluye también la presencia de empresas en el Pabellón de España y en stands independientes.

La participación permite presentar bajo una misma imagen capacidades vinculadas a fabricación avanzada, logística, comunicaciones, fotónica, soluciones modulares, maquinaria, movilidad y tecnologías con posible uso dual.

Más de 1.000 contactos comerciales previos

La presencia en Eurosatory no se limita a la participación física en la feria. AREX e IAF han desarrollado un trabajo previo de análisis comercial centrado en los ecosistemas de defensa de **Francia y Alemania**, dos mercados relevantes para la industria europea del sector.

Ese trabajo se ha realizado con apoyo de consultoras especializadas y ha permitido identificar empresas, agentes industriales y posibles socios de interés para las compañías aragonesas. En total, se han realizado más de **1.000 contactos** y se han abierto conversaciones con empresas internacionales.

También se ha elaborado un catálogo específico del **Hub de Defensa de Aragón**, en inglés y francés, con información sobre las capacidades de las empresas participantes, sus sectores de actividad, certificaciones, ubicación en feria e información corporativa.

AREX e IAF han coordinado además actuaciones con la **Oficina de Apoyo Exterior del Ministerio de Defensa**, conocida como **OFICAEX**, y con **TEDAE**, entidad organizadora del Pabellón de España. El objetivo es facilitar la visita de delegaciones internacionales y reforzar la presencia de las compañías aragonesas en las acciones vinculadas al pabellón nacional.

Un sector con acceso exigente

La entrada en el mercado internacional de defensa requiere una labor comercial sostenida. Es un sector especializado, regulado y con procesos de compra largos, en el que pesan las certificaciones, la solvencia técnica, la capacidad industrial y las relaciones estables con contratistas y administraciones.

Por ese motivo, la participación aragonesa en Eurosatory se plantea como una acción de medio y largo plazo. La feria permitirá generar reuniones, abrir conversaciones y detectar oportunidades de colaboración, pero la consolidación de esos contactos dependerá del seguimiento posterior de cada empresa.

La agenda aragonesa incluirá también la jornada **"Intercambio de experiencias entre regiones europeas de defensa – Foro ADR Eurosatory"** que buscará explorar posibilidades de cooperación con regiones europeas que desarrollan programas de apoyo a su industria de defensa.

El Hub de Defensa de Aragón

El **Hub de Defensa de Aragón** es una iniciativa estratégica del Gobierno de Aragón, a través del Instituto Aragonés de Fomento, el Instituto Tecnológico de Aragón y AREX, junto con el

Ayuntamiento de Zaragoza, la Delegación del Gobierno de España en Aragón, los clústeres **AERA, ALIA y TECNARA**, CEOE Aragón, CEPYME Aragón y el Consejo Aragonés de Cámaras de Comercio, en colaboración con el Ministerio de Defensa.

Su finalidad es ampliar la base industrial y tecnológica de defensa en Aragón mediante la conexión entre empresas, innovación, logística, formación, infraestructuras y colaboración público-privada.

La participación en Eurosatory da continuidad a la presencia agrupada del Hub en **FEINDEF**, celebrada en Madrid, donde participaron **33 empresas aragonesas**

No, Claude Fable 5 no se ha filtrado en The Pirate Bay



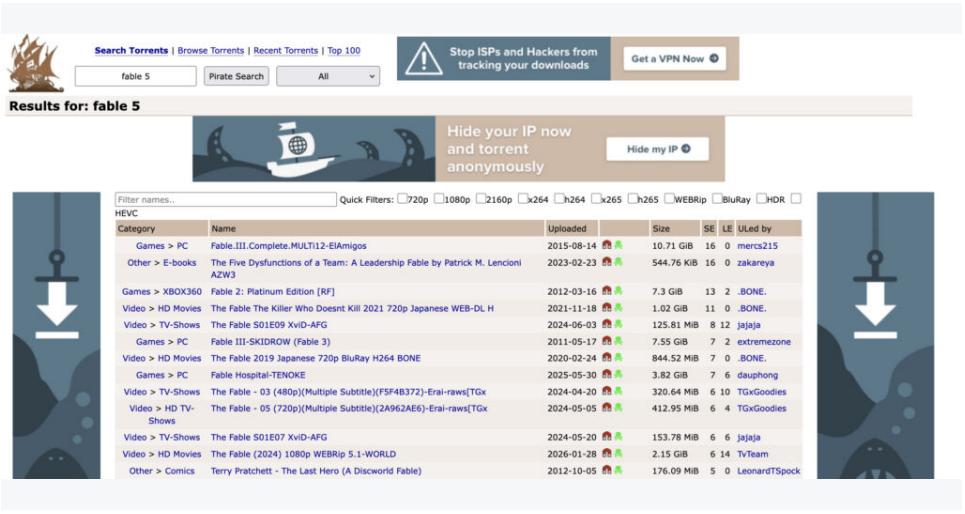
RUBEN MARCU · 13 JUN 2026

Una supuesta captura de pantalla de un torrent de 3,4 TB de **Claude Fable 5**, el modelo de Anthropic [suspendido tras una orden del Gobierno de Estados Unidos](), lleva desde ayer circulando en redes. No obstante, todo parece apuntar a que la imagen, una entrada en **The Pirate Bay**, es un montaje.

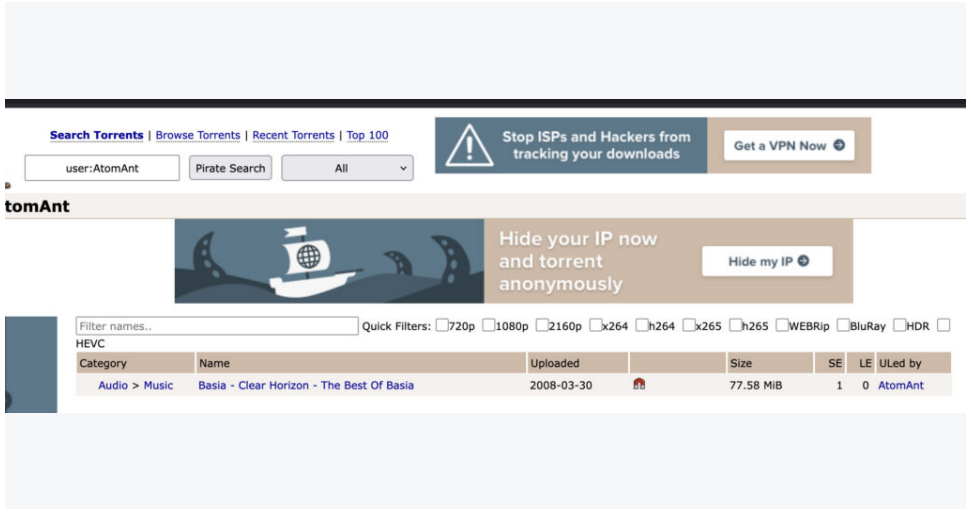
X TWITTER

Someone put Fable 5 on the pirate bay, 3.4TB ?
pic.twitter.com/VV9609KAIF
@PtrPomorski
https://x.com/PtrPomorski/status/2065743732792512621...

Hemos comprobado varios espejos de The Pirate Bay y **no aparece ninguna filtración del modelo**, solo resultados genéricos asociados al mundo de fantasía Fable, como videojuegos, películas, series, libros y otros archivos que nada tienen que ver con Anthropic.



Tras investigar al usuario **"AtomAnt"**, quien supuestamente habría filtrado el modelo, solo figura en su perfil un archivo musical subido en 2008. Además, **no existe la categoría Other > Models**. En general, todo apunta a ser una publicación troll.



En comentarios, [la comunidad ha revivido la clásica cultura P2P]() . Algunos han apostado a que dentro hay **un rickroll de 3,4 TB** mientras que otros han señalado que parece **"más cuento"**. Además, más allá de los chistes, varios usuarios han

señalado lo obvio: que aunque el archivo fuese real, casi nadie tendría el hardware para mover un modelo así.

La precaución nunca está de más

Más allá de los memes, estas situaciones pueden parecer inofensivas hasta que se comparten como si fuera una filtración de verdad. A partir de ahí pueden aparecer archivos infectados que prometen el modelo, una versión sin límites o accesos alternativos a Anthropic.

En estos casos no conviene fiarse. La recomendación, no solo con Anthropic sino en general, es no descargar archivos que prometan modelos cerrados, accesos filtrados o versiones sin restricciones a través de redes P2P o canales no oficiales.

El CUD y la AGM celebran su primer Seminario Internacional de Liderazgo



RUBEN MARCU · 14 JUN 2026

El **Centro Universitario de la Defensa** y la **Academia General Militar** han celebrado del **9 al 11 de junio de 2026** el primer Seminario Internacional de Liderazgo. El encuentro ha reunido a **36 participantes de ocho países** para analizar cómo se forma el liderazgo en las academias militares europeas.

El seminario se enmarca en el **programa EMILYO**, la iniciativa europea para el intercambio de jóvenes oficiales inspirada en Erasmus. Se ha planteado como un foro de cooperación académica, intercambio internacional y desarrollo del liderazgo en un entorno multinacional. El encuentro ha abordado la formación en liderazgo desde tres perspectivas: el ámbito académico, la instrucción y el adiestramiento militar, y la investigación e innovación docente.

El seminario ha incluido **21 comunicaciones orales**, **cuatro presentaciones en formato póster** y **una conferencia inaugural**. La sesión de apertura se ha centrado en el **Modelo K2 de Liderazgo**, una referencia en el Ejército de Tierra.

Un foro europeo sobre liderazgo militar

El encuentro parte de una idea central: el liderazgo debe considerarse una de las habilidades más importantes que cualquier oficial debe adquirir durante su proceso formativo. Esta formación no se limita al aprendizaje de competencias técnicas o capacidades de mando, sino que también exige interiorizar actitudes y valores que permitan distinguir qué decisiones deben adoptarse en contextos complejos.

Durante el seminario se ha analizado cómo estudian y desarrollan el liderazgo los cadetes en diferentes academias militares europeas. El objetivo ha sido identificar buenas prácticas, compartir experiencias y abrir nuevas líneas de colaboración entre instituciones académicas militares.

La dimensión internacional del encuentro ha permitido fomentar el diálogo intercultural, el trabajo en red y el intercambio de metodologías docentes. La organización también ha destacado la importancia de reforzar competencias como la comunicación, el trabajo en equipo y la capacidad de liderazgo en entornos multinacionales.

Tres líneas de trabajo

El programa se ha articulado en torno a tres grandes áreas. La primera ha abordado la dimensión académica del liderazgo, con atención a los contenidos que estudian los cadetes durante su formación. La segunda se ha centrado en la dimensión militar, vinculada a las actividades de instrucción y adiestramiento destinadas a fortalecer las aptitudes y actitudes de liderazgo.

La tercera línea se ha dedicado a la investigación y la innovación docente. En este bloque se han analizado proyectos, trabajos y experiencias orientadas a mejorar el conocimiento y la formación del alumnado en materia de liderazgo.

Celebrado en la Academia General Militar

El seminario se ha desarrollado en la **Academia General Militar** y en el **Centro Universitario de la Defensa**, en Zaragoza. La organización ha contado con un equipo de coordinación integrado por el coronel **Juan Jesús Pavón Coto**, como oficial de proyecto; **Julia Sánchez García**, responsable de cuestiones académicas; **Ángel Óscar Corona Beomont**, coordinador de administración y logística; y **Andy Tunnicliffe**, coordinador Erasmus.

Con esta primera edición, el CUD y la AGM han abierto un espacio europeo de intercambio sobre liderazgo militar. La iniciativa contribuye a fortalecer la cooperación internacional y a avanzar hacia un marco educativo común orientado a preparar a futuros líderes ante los desafíos del entorno de seguridad contemporáneo.



RUBEN MARCU · 14 JUN 2026

Trece startups y pymes tecnológicas participan en la tercera edición de StartTech+ del IAF y Aragón EDIH

El **Instituto Aragonés de Fomento (IAF)** ha puesto en marcha la tercera edición de **StartTech+ 2026**, el programa de aceleración dirigido a startups y pymes innovadoras o de base tecnológica que se desarrolla en el marco de **Aragón European Digital Innovation Hub (Aragón EDIH)**.

En esta edición participan **trece empresas emergentes y pymes innovadoras**, que seguirán entre junio y septiembre un itinerario de aceleración especializado y personalizado. Estas son **Autonality, Alan Tech Academy, Licia, MyNomina, Naxion, Visiora, Biopredx, GPONDoctor, Fidex, Prymerisk, Ingeniables, Try Business Solutions y Peryton Medical Solutions**.

El objetivo es impulsar su crecimiento mediante una hoja de ruta adaptada a las necesidades de cada proyecto, mejorar sus modelos de negocio, reforzar sus capacidades de gestión, facilitar el acceso a nuevas oportunidades de financiación e inversión y acelerar la escalabilidad de sus tecnologías.

Los proyectos participantes tienen presencia en localidades aragonesas como **Calanda, Santa Eulalia y Zaragoza**.

Diagnóstico, formación y mentoring

Tras la presentación oficial de los proyectos participantes, se ha celebrado la primera de las cinco sesiones presenciales de formación

especializada previstas dentro del programa, que se desarrollarán entre los meses de junio y septiembre.

De forma paralela a las acciones formativas, cada empresa participante recibirá acompañamiento para realizar un diagnóstico inicial a través de **Modelo de Gestión para la Competitividad y la Innovación del IAF**. Esta herramienta permitirá identificar las necesidades específicas de cada proyecto y orientar su evolución dentro del itinerario de aceleración.

A lo largo de los próximos meses, las empresas seleccionadas participarán también en procesos de **mentoring individual** con expertos, accederán a un mapeo personalizado de fuentes de financiación y oportunidades de inversión adaptadas a su fase de desarrollo, y formarán parte de actividades de networking orientadas a generar nuevas oportunidades de negocio y colaboración.

El programa concluirá en septiembre con la celebración del **Demo Day StartTech+ 2026**, un evento abierto a empresas, instituciones, entidades financieras e inversores. En esta jornada, los participantes presentarán la evolución de sus proyectos y los resultados obtenidos tras su paso por el programa.

Una iniciativa integrada en Aragón EDIH

StartTech+ forma parte de las acciones de apoyo al emprendimiento innovador impulsadas por **Aragón EDIH**, una iniciativa desarrollada conjuntamente por el **Instituto Aragonés de Fomento**, el **Instituto Tecnológico de Aragón (ITA)**, la **Universidad de Zaragoza**, **TECNARA**, **CEOE Aragón**, **CEPYME Aragón** y **Cámaras de Aragón**.

Aragón EDIH fue reconocido por la **Comisión Europea** en 2023 como Centro Europeo de Innovación Digital. El hub forma parte de la red europea de EDIHs y está especializado en **inteligencia artificial, sistemas cognitivos y computación de alto rendimiento HPC-Cloud**.

Para el periodo **2026-2028**, Aragón EDIH cuenta con un presupuesto cercano a los **4,4 millones de euros**, cofinanciado al 50 % a través del programa europeo **Digital Europe**. Su finalidad es impulsar la adopción de la inteligencia artificial y acelerar la transformación digital de las pequeñas y medianas empresas y del sector público.

Síguenos en araintel.com

SECCIÓN

ALERTAS

11 PIEZAS EN ESTA SECCIÓN

Inyección SQL en productos de Nemon

INCIBE-CERT · 8 JUN 2026

INCIBE-2026-402 · Importancia 5 - Crítica · Publicado el 08/06/2026

Recursos afectados: Nemon Trade Energy y Nemon Trade Energy CRM en las versiones 2.95.55.

Descripción:INCIBE ha coordinado la publicación de una vulnerabilidad de severidad crítica, que afecta a Trade Energy...

Solución: La vulnerabilidad reportada fue completamente mitigada por el equipo de Nemon el 26/05/2026. No se tiene constancia de que la vulnerabilidad haya sido explotada, ni de que haya tenido impacto alguno sobre clientes o datos gestionados por la plataforma. Al tratarse de una solución SaaS, la corrección fue aplicada de forma centralizada por Nemon, sin requerir ninguna acción por parte de los clientes. La vulnerabilidad ha sido corregida y no resulta explotable en la actualidad.

CVE:CVE-2026-10731.

Boletín de seguridad de SAP: junio de 2026

INCIBE-CERT · 9 JUN 2026

INCIBE-2026-407 · Importancia 5 - Crítica · Publicado el 09/06/2026

Recursos afectados:SAP NetWeaver AS ABAP y ABAP Platform, versiones SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 751, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758, SAP_BASIS 816, SAP_BASIS 918 y SAP_BASIS 919. SAP NetWeaver AS ABAP y ABAP Platform, versiones KRNL64NUC 7.22, 7.22EXT, KRNL64UC 7.22, 722EXT, 7.53, KERNEL 7.22, 7.53, 7.54, 7.77, 7.89, 7.93, 9.16, 9.18 y 91.9. SAP Commerce Cloud y SAP Data Hub, versiones HY_COM 2205, HY_DHUB 2205, COM_CLOUD 2211, 2211-JDK21 y DHUB_CLOUD 2211. SAP NetWeaver Application Server Java (Web Container), versión ENGINEAPI 7.50. SAP Commerce Cloud, versiones HY_COM 2205, COM_CLOUD 2211 y 2211-JDK21. SAP NetWeaver AS ABAP y ABAP Platform, versiones SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 751, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758 y SAP_BASIS 816. ODP Data Replication APIs, versiones DW4CORE 200, 300, 400, PI_BASIS 2006_1_700, 701, 702, 731, 740, SAP_BW 750 y 816. SAP S/4HANA, versiones S4FND 102, 103, 104, 105, 106, 107, 108 y 109. SAP NetWeaver AS Java (JDBC Test Servlet), versión BI_UDI 7.50. SAP Wily Introscope Enterprise Manager, versión WILY_INTRO_ENTERPRISE 10.8. SAP MDG (Review Match Groups Application), versiones S4CORE 108, SAP_BASIS 916, SAP_BASIS 917 y SAP_ABA 816. SAP Business Objects Business Intelligence Platform, versiones ENTERPRISE 430, 2025 y 2027. SAP Fiori (launchpad), versiones SAP_UI 754, 755, 756, 757, 758 y 816. SAP Business Objects, versiones ENTERPRISE 430, 2025 y 2027. SAP NetWeaver AS Java, versiones SERVERCORE 7.50, CORE-TOOLS 7.50 y J2EE-APPS 7.50.

Descripción:SAP ha publicado su boletín mensual en el que se incluyen 15 vulnerabilidades: 4 de severidad crítica, 2...

Solución: Actualizar a la última versión disponible indicada por el fabricante.

CVE:CVE-2026-44748, CVE-2026-27671, CVE-2026-22732, CVE-2026-40128.

Múltiples vulnerabilidades en productos de Check Point

INCIBE-CERT · 9 JUN 2026

INCIBE-2026-406 · Importancia 5 - Crítica · Publicado el 09/06/2026

Recursos afectados: Mobile Access / SSL VPN, Remote Access VPN, Spark Firewall y Security Gateways, Spark Firewall: R80.20.X (EOS), R80.40 (EOS), R81 (EOS), R81.10 (EOS), R81.10.X, R81.20, R82, R82.00.X, R82.10.

Descripción: Check Point Research, tras realizar una investigación, ha publicado 2 vulnerabilidades: 1 de severidad...

Solución: Check Point puede proporcionar una revisión (Hotfix) para R81.20, R82 y R82.10. Descargar la revisión correspondiente según lo indicado por el fabricante. Para Security Gateway / Maestro Orchestrator / Security Group: R82.10 Jumbo Hotfix Accumulator Take 19. R82.10 Jumbo Hotfix Accumulator Take 6. R82 Jumbo Hotfix Accumulator Take 103. R82 Jumbo Hotfix Accumulator Take 91. R81.20 Jumbo Hotfix Accumulator Take 141. R81.20 Jumbo Hotfix Accumulator Take 127. R81.20 Jumbo Hotfix Accumulator Take 120. R81.20 Jumbo Hotfix Accumulator Take 113. Para Check Point Spark Firewalls: R82.00.10 Build 998002216 para Local Installation. R82.00.10 Build 998002216 para Central Deployment en SmartConsole. R82.00.10 Build 998002216 para SmartUpdate. R81.10.17 Build 996004901 para Local Installation. R81.10.17 Build 996004901 para Central Deployment en SmartConsole. R81.10.17 Build 996004901 para SmartUpdate. En caso de no poder actualizar la versión afectada, se recomienda revisar las medidas de mitigación descritas por el fabricante en su aviso oficial enlazado en las referencias.

CVE:CVE-2026-50751, CVE-2026-50752.

Boletín de seguridad de Microsoft: junio de 2026

INCIBE-CERT · 10 JUN 2026

INCIBE-2026-410 · Publicado el 10/06/2026

Recursos afectados:NET ASP.NET Core Active Directory Domain Services Azure HorizonDB Azure Stack Edge Copilot Chat (Microsoft Edge) Function Discovery Service (fdwsd.dll) GitHub Copilot and Visual Studio Code HTTP/2 Linux MANA Driver M365 Copilot Microsoft Azure Attestation service and Device Health Attestation Service Microsoft Azure Kubernetes Service Microsoft Bing Microsoft Copilot Microsoft Defender for Endpoint Microsoft Dynamics 365 (on-premises) Microsoft Exchange Online Microsoft Exchange Server Microsoft Graph Microsoft Graphics Component Microsoft Kinect Microsoft Live Share Canvas SDK Microsoft Office Microsoft Office Click-To-Run Microsoft Office Excel Microsoft Office Project Microsoft Office SharePoint Microsoft Office Word Microsoft PC Manager Microsoft PowerToys Microsoft Teams for Android Microsoft UxTheme Library (uxtheme.dll) Microsoft Windows DNS Nuance PowerScribe Office for Android Remote Desktop Client Role: Windows Hyper-V UI Automation Manager (uiamanager.dll) Universal Plug and Play (upnp.dll) Visual Studio Code Windows Administrator Protection Windows Ancillary Function Driver for WinSock Windows Application Identity (AppID) Subsystem Windows BitLocker Windows Bluetooth Port Driver Windows Bluetooth Service Windows Boot Manager Windows Collaborative Translation Framework Windows Common Log File System Driver Windows Cryptographic Services Windows DHCP Client Windows DHCP Server Windows DWM Core Library Windows Deployment Services Windows HTTP.sys Windows Hotpatch Monitoring Service Windows Hyper-V Windows Internet (wininet.dll) Windows Kerberos Windows Kernel Windows

Kernel-Mode Drivers Windows Mark of the Web (MOTW) Windows Media Windows NT OS Kernel Windows NTFS Windows NTLM Windows Narrator Braille Windows Network Controller (NC) Host Agent Windows Performance Monitor Windows Program Compatibility Assistant Service Windows Projected File System Filter Driver Windows Push Notifications Windows RDP Windows SDK Windows Secure Boot Windows Shell Windows Sto…

Descripción: Microsoft ha publicado su boletín mensual de seguridad en el que se incluyen 206 vulnerabilidades: 10 de...

Solución: Actualizar a la última versión disponible indicada por el fabricante.

CVE:CVE-2026-26142, CVE-2026-42904, CVE-2026-44815, CVE-2026-45602, CVE-2026-45657, CVE-2026-47281, CVE-2026-47291, CVE-2026-47643, CVE-2026-48567, CVE-2026-48579.

Inyección de comandos en FortiSandbox de Fortinet

INCIBE-CERT · 10 JUN 2026

INCIBE-2026-411 · Importancia 5 - Crítica · Publicado el 10/06/2026

Recursos afectados: FortiSandbox 5.0: versiones afectadas 5.0.0 a 5.0.5. FortiSandbox 4.4: versiones afectadas 4.4.0 a 4.4.8. FortiSandbox Cloud 5.0: versiones afectadas 5.0.4 a 5.0.5. FortiSandbox PaaS 5.0: versiones afectadas 5.0.4 a 5.0.5.

Descripción: FortiGuard Labs ha publicado una vulnerabilidad de severidad crítica, que es caso de ser explotada...

Solución: Actualizar a alguna de las siguientes versiones: FortiSandbox 5.0.6 o superior. FortiSandbox 4.4.9 o superior. FortiSandbox Cloud 5.0.6 o superior. FortiSandbox PaaS 5.0.6 o superior.

CVE:CVE-2026-25089.

Múltiples vulnerabilidades en OpenSSL

INCIBE-CERT · 10 JUN 2026

INCIBE-2026-412 · Importancia 5 - Crítica · Publicado el 10/06/2026

Recursos afectados: Las siguientes versiones OpenSSL están afectadas: 4.0 3.6 3.5 3.4 3.0 1.1.1 1.0.2 Las versiones que carecen de soporte: 3.1, 3.2 y 3.3 no han sido analizadas y se desconoce si están afectadas por alguna de las vulnerabilidades.

Descripción: OpenSSL ha informado de 18 vulnerabilidades nuevas, 1 de severidad crítica, 10 altas, 3 medias y 4 bajas...

Solución: Según la versión que disponga, actualizar el producto a alguna de las siguientes versiones: OpenSSL 4.0: actualizar a OpenSSL 4.0.1 OpenSSL 3.6: actualizar a OpenSSL 3.6.3. OpenSSL 3.5: actualizar a OpenSSL 3.5.7. OpenSSL 3.4: actualizar a OpenSSL 3.4.6. OpenSSL 3.0: actualizar a OpenSSL 3.0.21. OpenSSL 1.1.1: actualizar a OpenSSL 1.1.1zh (únicamente para usuarios con soporte premium) OpenSSL 1.0.2 users should upgrade to OpenSSL 1.0.2zq (únicamente para usuarios con soporte premium)

CVE:CVE-2026-45447, CVE-2026-34182, CVE-2026-34183, CVE-2026-35188, CVE-2026-42764, CVE-2026-45445, CVE-2026-7383, CVE-2026-9076, CVE-2026-34180, CVE-2026-34181, CVE-2026-42765.

[Actualización 11/06/2026] Múltiples vulnerabilidades en productos Ivanti

INCIBE-CERT · 11 JUN 2026

INCIBE-2026-413 · Importancia 5 - Crítica · Publicado el 11/06/2026

Recursos afectados: Ivanti Sentry, versiones 10.5.1, 10.6.1, 10.7.0 y anteriores; Endpoint Manager Mobile, versiones 12.9.0, 12.8.0.2 y 12.7.0.1.

Descripción: Ivanti ha publicado dos avisos de seguridad donde informan de 4 vulnerabilidades, 2 de severidad crítica y 2 altas. Si se explotan, un atacante podría elevar sus privilegios a nivel de root, obtener acceso completo como administrador o ejecutar código en remoto. Identificador INCIBE-2026-413

Solución: Actualizar los productos a alguna de las siguientes versiones: Ivanti Sentry, versiones 10.5.2, 10.6.2 o 10.7.1. Ivanti Endpoint Manager Mobile, versiones 12.9.0.1, 12.8.0.3 o 12.7.0.2.

CVE:CVE-2026-10520, CVE-2026-10523, CVE-2026-6973, CVE-2026-10727.

Denegación de servicio en Serv-U de SolarWinds

INCIBE-CERT · 11 JUN 2026

INCIBE-2026-415 · Importancia 4 - Alta · Publicado el 11/06/2026

Recursos afectados SolarWinds Serv-U: versiones 15.5.4 y anteriores.

Descripción: SolarWinds ha publicado una vulnerabilidad de severidad alta, cuya explotación podría permitir a un...

Solución: SolarWinds recomienda a los usuarios afectados actualizar a la versión 15.5.4 HF1 de Serv-U.

CVE:CVE-2026-28318.

Inyección de cadena de formato autenticada en Tapo C110 de TP-Link

INCIBE-CERT · 12 JUN 2026

INCIBE-2026-442 · Importancia 4 - Alta · Publicado el 12/06/2026

Recursos afectados: Tapo C110 v2, versiones anteriores a 1.5.4 Build 260428 Rel.64344n.

Descripción:TP-Link ha publicado una vulnerabilidad de severidad alta que podría permitir a un atacante remoto autenticado redirigir el flujo de ejecución a funciones internas existentes, lo que desencadenaría un restablecimiento de fábrica. Identificador INCIBE-2026-442

Solución: Se recomienda seguir las instrucciones para actualizar a la última versión del firmware y solucionar las vulnerabilidades

CVE:CVE-2026-6250.

Múltiples vulnerabilidades en MobaXterm Personal Edition (Portable) de Mobatek

INCIBE-CERT · 12 JUN 2026

INCIBE-2026-421 · Importancia 4 - Alta · Publicado el 12/06/2026

Recursos afectados: MobaXterm Personal Edition (Portable) 26.3 (Build 5154).

Descripción:INCIBE ha coordinado la publicación de 2 vulnerabilidades de severidad alta que afectan a MobaXterm...

Solución: Las vulnerabilidades han sido solucionadas por el equipo de Mobatek en la versión 26.4.

CVE:CVE-2026-11879, CVE-2026-11967.

Toma de control de PeopleSoft de Oracle

INCIBE-CERT · 12 JUN 2026

INCIBE-2026-420 · Importancia 5 - Crítica · Publicado el 12/06/2026

Recursos afectados: PeopleSoft Enterprise PeopleTools de Oracle, versiones 8.61 y 8.62. Es posible que haya versiones anteriores afectadas, pero como carecen de mantenimiento no se han analizado.

Descripción: Bobby Gould, Lucas Miller y Minh Giang de TrendAI Zero Day Initiative y TrendAI Research han descubierto...

Solución: El fabricante aporta unas indicaciones de seguridad que se recomienda seguir (es preciso estar registrado) . En líneas generales se recomienda deshabilitar el servicio Environment Management Hub en configuraciones de múltiples servidores o eliminar la aplicación PSEMHUB directamente en configuraciones de un solo servidor. Si no es posible hacer ninguno de los dos, se recomienda bloquear el acceso externo a /PSEMHUB/* (especialmente /PSEMHUB/hub) y /PSIGW/HttpListeningConnector en el perímetro.

CVE:CVE-2026-35273.

SECCIÓN

ALERTAS SCI

8 PIEZAS EN ESTA SECCIÓN

Boletín de seguridad de Siemens: junio de 2026

INCIBE-CERT · 9 JUN 2026

INCIBE-2026-405 · Importancia 5 - Crítica · Publicado el 09/06/2026

Recursos afectadosSIMATIC WinCC Unified PC Runtime v16, v17, v18, v19, v20 y v21; SIPROTEC 5 - CP100, 150 200, 300 y Compact 7SX800 (CP050); AI Lightweight Inference Server Connector for Azure Databus HiMed Cockpit SCALANCE LPE9403, LPE9413, LPE9433, familia M-800, familia SC-600, W-700 IEEE 802.11ax y XC-300/XR-300/XC-400/XR-500WG/XR-500; Shopfloor IT Suite; SIDIS Prime; Siemens OPC UA Modelling Editor (SiOME); SIMATIC Comfort/Mobile RT, eaSie Core Package, eaSie PCS 7 Skill Package, HMI Operator Device, IOT2050, IPC BX-21A, IPC MD-57A, IPC ORCLA, PDM V9.3, RTLS Locating Manager, STEP 7 V5, Target, WinCC, WinCC OA, WinCC Runtime Advanced V17 y WinCC Unified Sequence; SIMOTION OACAMGEN; SINAMICS G200, G220, S200, S210 y S220; SINEC INS, NMS y Security Monitor; SINUMERIK Access MyMachine /OPC UA; SITRANS ASM IQ, Soft Sensor Engine IQ (SITRANS SSE IQ); User Management Component (UMC); Visual Inspection Cockpit.

Descripción: Siemens ha publicado su boletín mensual de seguridad en el que se incluyen 7 vulnerabilidades: 1 de...

Solución: Actualizar a la última versión disponible indicada por el fabricante.

CVE:CVE-2025-15467, CVE-2026-46746, CVE-2026-46748, CVE-2026-46749, CVE-2026-24349, CVE-2025-40808, CVE-2026-46747.

Múltiples vulnerabilidades en productos de Schneider Electric

INCIBE-CERT · 9 JUN 2026

INCIBE-2026-404 · Importancia 4 - Alta · Publicado el 09/06/2026

Recursos afectados EcoStruxure™ IT Data Center ExpertVersiones 9.1.1 y anteriores. EasyLogic T150 (anteriormente Saitel DR RTU)Versiones 11.06.31 y anteriores para CVE-2026-9650; Versiones 11.06.32 y anteriores para CVE-2026-9651. Saitel DP Remote Terminal Unit & ControllerVersiones 11.06.35 y anteriores para CVE-2026-9650; Versiones 11.06.37 y anteriores para CVE-2026-9651. PowerLogic™ P7Versiones V02.003.001.000 y anteriores.

Descripción: Schneider Electric ha publicado 6 vulnerabilidades: 4 de severidad alta y 2 medias que, en caso de ser...

Solución: Schneider Electric recomienda actualizar los productos afectados a las siguientes versiones que corrigen la vulnerabilidad: EcoStruxure™ IT Data Center Expert: 9.1.2. EasyLogic T150: 11.06.32. Saitel DP RTU: 11.06.38. PowerLogic™ P7: V02.004.001.000.

CVE:CVE-2026-9716, CVE-2026-9650, CVE-2026-9717, CVE-2026-8045, CVE-2026-9718, CVE-2026-9651.

Múltiples vulnerabilidades en LabX Standard de Mettler Toledo

INCIBE-CERT · 10 JUN 2026

INCIBE-2026-408 · Importancia 5 - Crítica · Publicado el 10/06/2026

Recursos afectados LabX Standard v21.3.22 LabX Standard v21.4.23

Descripción:CERT@VDE en coordinación con Mettler Toledo ha publicado 21 vulnerabilidades: 2 de severidad crítica y 19...

Solución: Mettler-Toledo GmbH recomienda actualizar todas las instalaciones de LabX Standard a la versión 21.4.23, donde se corrigen la mayoría de las vulnerabilidades identificadas. No obstante, las vulnerabilidades CVE-2025-69419, CVE-2026-0915, CVE-2025-15467 y CVE-2025-58187 permanecen sin resolver en el momento de publicación del aviso, estando previstas correcciones en futuras versiones del producto.

CVE:CVE-2025-68121, CVE-2018-15727, CVE-2025-15467, CVE-2023-36414, CVE-2024-0056, CVE-2025-68154, CVE-2026-24737, CVE-2021-24112, CVE-2025-58187, CVE-2025-9230, CVE-2025-15281, CVE-2026-21218, CVE-2026-26127, CVE-2026-26130, CVE-2026-0915, CVE-2026-2391, CVE-2026-22036, CVE-2024-43483, CVE-2023-29331, CVE-2025-69419, CVE-2025-46817.

Múltiples vulnerabilidades en Universal Gateways de MBS

INCIBE-CERT · 10 JUN 2026

INCIBE-2026-409 · Importancia 5 - Crítica · Publicado el 10/06/2026

Recursos afectados: Todas las pasarelas Universal Gateway (UGW) de MBS con firmware anterior a V6_0_0_7, incluyendo: Double-A Profibus Double-A x-link Double-X CAN Double-X DALI Double-X KNX Double-X LON Double-X M-Bus Double-X PROFINET Double-X x-link Single-A Single-X Triple-X KNX+DALI Triple-X KNX+LON Triple-X KNX+M-Bus Triple-X PROFINET+DALI Triple-X PROFINET+KNX Triple-X PROFINET+LON Triple-X PROFINET+M-Bus

Descripción: Daniel Hulliger, Damian Pfammatter y Adrien Rey en coordinación con el CERT@VDE y MBS han publicado 11...

Solución:MBS recomienda actualizar los dispositivos afectados a la versión de firmware V6_0_0_7 o posterior.

CVE:CVE-2026-35075, CVE-2026-35076, CVE-2026-35077, CVE-2026-35078, CVE-2026-35079, CVE-2026-35080, CVE-2026-35081, CVE-2026-35082, CVE-2026-35083, CVE-2026-35084, CVE-2026-35085.

Credenciales embebidas en productos de Mitsubishi Electric

INCIBE-CERT · 12 JUN 2026

INCIBE-2026-419 · Importancia 4 - Alta · Publicado el 12/06/2026

Recursos afectados:Múltiples modelos de equipos de aire acondicionado domésticos Mitsubishi Electric equipados con conectividad Wi-Fi: Serie B: Modelos MSZ-BKR y MSZ-BXV. Serie E: Modelos MSZ-EM y MSZ-EX. Serie F: Modelos MSZ-FD, MSZ-FZ y MSZ-FZV. Serie H / J / N: Modelos MSZ-HXV, MSZ-JXV y MSZ-NXV. Serie R: Modelos MSZ-R y MSZ-RK. Serie V / X: Modelos MSZ-VXV, MSZ-X, MSZ-XD y MSZ-XK. Serie Z / Y: Modelos MSZ-ZD, MSZ-ZW, MSZ-ZXV y MSZ-ZY. Unidades de Suelo / Consola (Prefijo MFZ): Serie MFZ-KT Serie MFZ-KW Unidades de Pared (Prefijo MSZ): Serie MSZ-AP Serie MSZ-AY (una de las gamas más comunes actualmente) Serie MSZ-BT Serie MSZ-DA Serie MSZ-EF (gama de diseño Kirigamine Zen) Serie MSZ-FT Serie MSZ-HR Serie MSZ-LN (gama Kirigamine Style / diseño premium) Serie MSZ-LZ Serie MSZ-RW Serie MSZ-RZ Consultar el aviso del fabricante para obtener el listado completo de productos afectados.

Descripción: El investigador Zachary Mitev ha reportado una vulnerabilidad en Mitsubishi Electric de severidad alta...

Solución: Mitsubishi Electric irá lanzando actualizaciones progresivamente para corregir la vulnerabilidad en sus diferentes productos, recomendamos comprobar el aviso del fabricante para saber exactamente en que fecha saldrá el parche de seguridad para tu dispositivo. Como medidas adicionales, Mitsubishi Electric recomienda configurar el equipo afectado con un router Wi-Fi siguiendo las instrucciones proporcionadas por el fabricante inmediatamente después de la instalación. Además se recomienda restringir el acceso físico y lógico a las redes inalámbricas donde se encuentren desplegados los dispositivos afectados, así como monitorizar accesos no autorizados a las mismas.

CVE:CVE-2026-5667.

Múltiples vulnerabilidades en Cámaras de Brickcom

INCIBE-CERT · 12 JUN 2026

INCIBE-2026-417 · Importancia 4 - Alta · Publicado el 12/06/2026

Recursos afectados: Versiones 3.2.3.5.6 de los siguientes productos: Brickcom Cube Brickcom Dome Brickcom Bullet Brickcom Box

Descripción:CISA ha publicado dos vulnerabilidades de severidad alta que podrían permitir que un atacante remoto, no...

Solución: Se recomienda a los usuarios que se comuniquen con Brickcom para obtener asistencia.

CVE:CVE-2026-50245, CVE-2026-50005.

Múltiples vulnerabilidades en la plataforma IoT de Naxclow

INCIBE-CERT · 12 JUN 2026

INCIBE-2026-416 · Importancia 5 - Crítica · Publicado el 12/06/2026

Recursos afectados: Las todas las versiones de los siguientes modelos de la plataforma IoT de Naxclow se ven afectadas: Timbre inteligente X3; X Smart Home; Versión V720; ix cam.

Descripción: Temuri Takalandze ha publicado 7 vulnerabilidades: 2 de severidad crítica, 2 de severidad alta y 3 de...

Solución: No existe solución para estas vulnerabilidades. Los usuarios deben ponerse en contacto con Naxclow para obtener más información.

CVE:CVE-2026-50101, CVE-2026-28742, CVE-2026-42947, CVE-2026-50108.

Múltiples vulnerabilidades en productos de B&R

INCIBE-CERT · 12 JUN 2026

INCIBE-2026-418 · Importancia 4 - Alta · Publicado el 12/06/2026

Recursos afectados: Linux for B&R, versión 12 y anteriores; APROL versiones anteriores a APROL-AutoYaST-DVD-V4.4-010.10.260602; X20EDS410, todas las versiones.

Descripción:B&R ha publicado 5 vulnerabilidades de severidad alta presentes en el kernel Linux y componentes de...

Solución: El fabricante recomienda aplicar las actualizaciones de seguridad correspondientes en cuanto estén disponibles. Para el producto APROL ya se dispone de la versión corregida APROL-AutoYaST-DVD-V4.4-010.10.260602. Para el resto de productos afectados, las versiones corregidas se encuentran pendientes de publicación. Mientras tanto, se recomienda aplicar medidas de mitigación como la restricción del acceso local al sistema, la aplicación de principios de mínimo privilegio y la deshabilitación de módulos del kernel afectados cuando sea posible sin impactar la operativa del sistema.

CVE:CVE-2026-31431, CVE-2026-43284, CVE-2026-46333, CVE-2026-46300, CVE-2026-43494.

Conecta Con Audiencias Técnicas

Marketing técnico y de producto para startups



CONECTA CON TUS CLIENTES

Sé como VHS, Aprende de Betamax

La mejor tecnología no vale nada si no conecta con un público.

Primero analizamos tu mensaje y lo ajustamos para que se alinee con las necesidades de tus clientes.

Después, creamos contenido educativo y de producto que transmite de forma natural el mensaje y resalta el valor de tu producto.

Explora Más Ejemplos →



RootNode.es

Marketing técnico y de producto para humanos.

ARAINTEL Magazine

EDICIóN SEMANAL · Nº 94 - SEMANA DEL 8 AL 14 - JUNIO 2026

Edición publicada por Araintel. Todos los contenidos pertenecen a sus autores.

ARAINTEL.COM