Boletín de Ciberseguridad

Riesgo de vulnerabilidades IT y OT

Diciembre - 2025

Sobre Axus

Axus es una empresa especializada en ciberseguridad, con presencia en el Perú y Latinoamérica. Asesora a clientes en la protección de su información e infraestructura tanto en ámbitos industriales (OT) como en ámbitos corporativos (IT) y viene registrando una creciente participación en el ámbito de Internet de las Cosas (IoT) y en la protección de entornos Cloud e Híbridos.

En base a su reputación como especialista con los principales fabricantes de la industria y su equipo profesional en permanente capacitación, Axus genera valor a través de una visión consultiva que busca definir soluciones a la medida de las necesidades de cada cliente.

Alertas de Ciberseguridad

A continuación, compartimos con ustedes algunas de las alertas más relevantes de Diciembre.

Alertas de Seguridad IT:

- Oltenia Energy, complejo minero de carbón, sufre ataque de Ransomware Gentlemen
- Ransomware afecta infraestructura IT de Romanian Waters, autoridad nacional de gestión hídrica en Rumania
- Filtrado de 2.3 millones de registros de suscriptores de WIRED, publicación digital de Condé Nast

Alertas de Seguridad OT/ICS:

- Aeropuertos de India sufren ataques de GPS spoofing que afectan navegación aérea
- Ciberataque disruptivo en PDVSA, empresa estatal petrolera venezolana (sector hidrocarburos)
- Ciberataque a la Red Eléctrica de Polonia (infraestructura energética)

Oltenia Energy, complejo minero de carbón, sufre ataque de Ransomware Gentlemen

Tipo de Ataque: **Ransomware (familia Gentlemen)**

Medio de Propagación: **Servicios expuestos a Internet y credenciales comprometidas (acceso inicial)**

1. **PRODUCTOS AFECTADOS:**
   - ERP corporativo y servicio de correo electrónico de la compañía
   - Sitio web corporativo (indisponible temporalmente)
   - Infraestructura IT de negocio (servidores y estaciones afectadas por cifrado)
2. **RESUMEN:**

En la madrugada del 26 de diciembre de 2025, Oltenia Energy Complex sufrió un ataque de ransomware Gentlemen que derribó su infraestructura IT y cifró archivos y documentos. Como consecuencia, ERP, gestor documental, correo y web quedaron temporalmente indisponibles. La organización aisló los sistemas comprometidos, notificó a las autoridades (DNSC, Ministerio de Energía, entre otras) y presentó denuncia ante DIICOT. Los equipos IT iniciaron la reconstrucción en nueva infraestructura usando copias de seguridad. La empresa investiga si hubo exfiltración de datos antes del cifrado. Pese al impacto, el Sistema Energético Nacional no se vio en peligro y la actividad operativa continuó parcialmente.

3. **DETALLE:**

El grupo Gentlemen emergió en agosto de 2025 y es conocido por aprovechar credenciales comprometidas y servicios expuestos a Internet para lograr acceso inicial y desplegar su carga de cifrado. En este caso, tras la intrusión, los atacantes encriptaron documentos y dejaron notas (README-GENTLEMEN.txt) con canales de contacto; los archivos presentan la extensión .7mtzhh, consistente con muestras atribuidas al grupo. El ERP y sistemas de gestión documental/correo fueron indisponibilizados, lo que sugiere compromiso de servidores de aplicaciones y file servers dentro del dominio corporativo. La respuesta inmediata incluyó aislamiento, apagado controlado, reconstrucción en entorno limpio y restauración desde backups. A la fecha del reporte, los actores no habían publicado a Oltenia en su sitio Tor de filtraciones, lo que indica negociación en curso o evaluación del impacto. No se reportan indicios de movimiento lateral hacia redes OT ni de afectación de SCADA/PLC, y la operación eléctrica nacional no fue comprometida. La investigación continúa para determinar persistencia, puntos de entrada (posible exposición de RDP/VPN/servicios web) y exfiltración de datos sensibles.

4. **RECOMENDACIONES:**
   - Implementar segmentación estricta entre redes IT y OT, con firewalls y listas de control de acceso granulares.
   - Actualizar y parchear sistemas y aplicaciones críticas; endurecer configuraciones (CIS benchmarks) en servidores y endpoints.

5. **REFERENCIAS:**
   - https://www.bleepingcomputer.com/news/security/romanian-energy-provider-hit-by-gentlemen-ransomware-attack/

Ransomware afecta infraestructura IT de Romanian Waters, autoridad nacional de gestión hídrica en Rumania

Tipo de Ataque: Ransomware

Medio de Propagación: No confirmado; posible explotación de servicios expuestos o credenciales comprometidas

1. **PRODUCTOS AFECTADOS:**
   - Servidores con GIS, bases de datos, correo electrónico y servicios web
   - Windows workstations y servidores DNS
2. **RESUMEN:**

El 20 de diciembre de 2025, la autoridad nacional de aguas de Rumania (Romanian Waters) notificó que sufrió un ataque de ransomware que afectó cerca de 1,000 sistemas IT en su sede central y 10 oficinas regionales. El incidente comprometió servidores con GIS, bases de datos, correo, web y DNS, además de estaciones Windows. Los atacantes utilizaron BitLocker para cifrar archivos y dejaron una nota de rescate solicitando contacto en 7 días. Las operaciones críticas y sistemas OT no fueron afectados; la coordinación de activos hidráulicos continuó mediante canales de voz y radio. La investigación está en curso y no se ha atribuido el ataque a ningún grupo específico.

3. **DETALLE:**

El ataque se ejecutó mediante el cifrado de sistemas usando la funcionalidad BitLocker integrada en Windows, lo que indica que los atacantes lograron privilegios administrativos en los equipos comprometidos. Fueron afectados servidores que alojaban GIS, bases de datos, correo electrónico, servicios web y DNS, además de estaciones de trabajo Windows en la red corporativa. La nota de rescate exigía contacto en un plazo de 7 días, sin especificar monto, lo que sugiere un enfoque manual de negociación. No se han identificado vectores iniciales, aunque se presume explotación de servicios expuestos o credenciales comprometidas. La autoridad notificó a la DNSC, al Centro Nacional Cibernético y a otros organismos, quienes trabajan en contención y restauración. No hay evidencia de movimiento lateral hacia redes OT ni afectación de sistemas SCADA; las operaciones hidráulicas se mantuvieron seguras mediante control local y comunicación por radio. El incidente resalta la falta de integración previa con el sistema nacional de protección para infraestructura crítica, que ahora se está implementando. No se ha atribuido el ataque ni se ha confirmado exfiltración de datos.

4. **RECOMENDACIONES:**
   - Implementar segmentación estricta entre redes IT y OT, con firewalls y ACL.
   - Desplegar soluciones EDR/XDR para detectar abuso de herramientas nativas (Living-off-the-Land).
   - Instrumentar monitoreo de eventos y correlación SIEM para detectar anomalías.
5. **REFERENCIAS:**
   - https://www.bleepingcomputer.com/news/security/romanian-water-authority-hit-by-ransomware-attack-over-weekend/

Filtrado de 2.3 millones de registros de suscriptores de WIRED, publicación digital de Condé Nast

Tipo de Ataque: **Exfiltración de datos (violación de privacidad)**

Medio de Propagación: **Fallo en API/web endpoint (Insecure Direct Object References – IDOR)**

1. **PRODUCTOS AFECTADOS:**
   - API interna de gestión de suscriptores WIRED
   - Base de datos con registros de usuarios y plataformas de identidad compartida
2. **RESUMEN:**

A fines de diciembre de 2025 apareció en foros clandestinos una base de datos con 2,366,576 registros de usuarios de WIRED, incluyendo correos, nombres, direcciones y fechas de nacimiento. El atacante conocido como "Lovely" afirmó haber descubierto vulnerabilidades IDOR en el sistema central de cuentas de Condé Nast y aprovechó esto para extraer datos desde abril de 1996 hasta septiembre de 2025. Aunque Condé Nast no confirmó oficialmente el incidente, analistas como Hudson Rock y Bleeping Computer verificaron la legitimidad de los datos. El hacker amenaza con exponer hasta 40 millones de registros adicionales de otras publicaciones, incluyendo Vogue y The New Yorker.

3. **DETALLE**

El delincuente utilizó fallos de tipo IDOR en el endpoint de la API para iterar identificadores de usuario y extraer información en formato JSON sin autenticación adecuada. El volcado filtrado contenía 2.3 millones de correos, 285.936 nombres, 102.479 direcciones y 32.426 números telefónicos. Los datos abarcan registros de suscripción desde 2011 y activos hasta septiembre 2025. La autenticidad fue corroborada comparando con registros de Robo-InfoStealer (RedLine y Raccoon). Tras acusar a Condé Nast de ignorar reportes de seguridad, el atacante filtró los archivos el 20 de diciembre en foros como Breach Stars y ofreció los datos por ~2.30 créditos del foro. Además, amenazas indican que planea filtrar hasta 40 millones más de registros de otras marcas del grupo editorial.

4. **RECOMENDACIONES:**
   - Corregir fallos de control de acceso en API (validar IDOR y autenticación)
   - Implementar autenticación fuerte y autorizaciones por frontend y backend
   - Implementar monitoreo de API con alertas de actividad inusual (rate-limiting, anomalias)
   - Segmentar bases de datos y usar servidores de validación separados y registrar logs de auditoría extendidos para detección forense
   - Capacitar equipo de desarrollo en seguridad API y control de acceso
   - Notificar a usuarios afectados e integrar el incidente a registro de brechas legales (GDPR, CCPA)

5. **REFERENCIAS:**
   - https://www.bleepingcomputer.com/news/security/hacker-claims-to-leak-wired-database-with-23-million-records/

Aeropuertos de India sufren ataques de GPS spoofing que afectan navegación aérea

Tipo de Ataque: GPS Spoofing (falsificación de señales GNSS)

Medio de Propagación: Interferencia en señales de navegación satelital

1. **PRODUCTOS AFECTADOS:**
   - Sistemas de navegación GNSS en aeronaves
   - Equipos de aterrizaje y aproximación basados en GPS
   - Infraestructura de gestión de tráfico aéreo en tierra

2. **RESUMEN:**

El 1 de diciembre del 2025 se informó en el Parlamento de la India que, en aeropuertos como Kolkata, Amritsar, Mumbai, Hyderabad, Bengaluru y Chennai, varias aeronaves experimentaron señales GNSS falsificadas. El ataque consistió en GPS spoofing, que alteró posiciones e incluso generó advertencias de terreno falsas. Tras reportes de vuelos afectados, la Airports Authority of India (AAI) solicitó al Wireless Monitoring Organisation (WMO) identificar las fuentes de interferencia

3. **DETALLE:**

Los ataques consistieron en la emisión de señales GNSS falsas que suplantaron las legítimas, afectando la precisión de navegación en aeronaves durante aproximaciones críticas. Esto provocó advertencias de terreno sin fundamento y errores en la posición reportada por los sistemas de vuelo. Aunque no se registraron accidentes, el incidente incrementó la carga operativa en controladores y pilotos, quienes debieron recurrir a procedimientos manuales y sistemas alternativos para garantizar la seguridad.

La Airports Authority of India confirmó que los eventos ocurrieron en aeropuertos estratégicos y solicitó al WMO reforzar recursos para rastrear transmisores maliciosos. El informe oficial menciona que incidentes similares se habían reportado previamente en zonas fronterizas, lo que sugiere un patrón de actividad que ahora afecta hubs interiores. La falta de mecanismos anti-spoofing en algunos equipos y la dependencia de GNSS para aproximaciones aumentaron el impacto del ataque, evidenciando vulnerabilidades críticas en la infraestructura OT aeronáutica.

4. **RECOMENDACIONES:**
   - Implementar sistemas anti-spoofing GNSS y alertas de integridad en aeronaves y ATC
   - Activar redundancia mediante sistemas terrestres (ILS, VOR/DME) para aproximaciones críticas
   - Solicitar monitoreo activo y captura de señales sospechosas por parte del WMO
   - Entrenar a pilotos y controladores en protocolos manuales ante pérdida de señal GNSS válida
   - Establecer alertas NOTAM inmediatas y SOPs para interferencias detectadas

5. **REFERENCIAS:**

- https://www.thehindu.com/news/national/chennai-bengaluru-among-airports-where-aircraft-encountered-gps-spoofing/article70346453.ece

Ciberataque disruptivo en PDVSA, empresa estatal petrolera venezolana (sector hidrocarburos)

Tipo de Ataque: Intrusión con impacto operativo (disrupción de operaciones OT)

Medio de Propagación: Compromiso en capa perimetral IT/OT

1. **PRODUCTOS AFECTADOS:**
   - Sistemas de control industrial SCADA
   - Sistemas DCS (Distributed Control Systems)
2. **RESUMEN:**

PDVSA sufrió un ciberataque que, según el análisis de Enigma Security, interrumpió operaciones de exportación, afectando su cadena logística de despacho de crudo. Aunque comunicados oficiales minimizaron el impacto, el análisis técnico revela una afectación directa a infraestructura OT, debido a la dependencia de la empresa en sistemas SCADA y DCS vulnerables por protocolos antiguos como Modbus y DNP3. La caída de sistemas y los retrasos en los envíos sugieren un ataque que comprometió la convergencia IT/OT. El evento se enmarca en un patrón regional de ataques contra infraestructura energética en Latinoamérica.

3. **DETALLE:**

El análisis identifica que PDVSA opera redes industriales basadas en tecnologías SCADA y DCS, muchas de ellas construidas sobre protocolos legacy sin autenticación ni cifrado, como Modbus y DNP3, lo que facilita intrusiones remotas. El ataque, descrito como disruptivo, indica un compromiso en la capa perimetral de red donde convergen los sistemas IT y OT, un vector especialmente vulnerable en infraestructuras petroleras. Debido a la interconexión entre aplicaciones administrativas y sistemas operativos, el ingreso inicial podría haber ocurrido en entornos IT y haber escalado hacia OT. La interrupción reportada en las exportaciones de crudo apunta a un impacto en terminales y sistemas de control asociados al despacho y monitoreo. Enigma Security señala que este tipo de ataque sigue un patrón donde actores maliciosos realizan reconocimiento, comprometen accesos perimetrales, manipulan tráfico ICS y ejecutan disrupciones programadas. Además, recalca que la dependencia de PDVSA en sistemas antiguos aumenta la superficie de ataque, mientras la tensión geopolítica incrementa la probabilidad de ataques dirigidos.

4. **RECOMENDACIONES:**
   - Segregar y blindar la convergencia IT/OT, aplicando firewalls industriales y controlando estrictamente los accesos remotos en la capa perimetral.
   - Modernizar o proteger protocolos industriales legacy (Modbus, DNP3) mediante gateways seguros, cifrado y autenticación robusta para evitar manipulaciones remotas.
   - Implementar monitoreo continuo especializado para ICS, con IDS/IPS industriales que detecten anomalías en SCADA/DCS y tráfico OT.
5. **REFERENCIAS:**

- https://enigmasecurity.cl/ataques-1398/

Ciberataque a la Red Eléctrica de Polonia (infraestructura energética)

Tipo de Ataque: Sabotaje cibernético dirigido a infraestructura crítica (interrupción operativa)

Medio de Propagación: Sistemas de control y comunicación de la red eléctrica (OT/SCADA

1. **PRODUCTOS AFECTADOS:**
   - Sistemas de comunicación entre parques solares y eólicos y la red nacional
   - Plataformas OT para gestión y monitoreo de generación distribuida
   - Infraestructura SCADA vinculada a producción y distribución eléctrica
2. **RESUMEN:**

A finales de diciembre de 2025, Polonia enfrentó un ciberataque coordinado que apuntó a interrumpir comunicaciones entre instalaciones de energía renovable y el operador nacional del sistema, poniendo en riesgo la estabilidad de la red eléctrica durante un período de alta demanda invernal. El objetivo principal fue desestabilizar la infraestructura energética e inducir un apagón nacional. El ataque se ejecutó de forma simultánea contra múltiples instalaciones energéticas. Las autoridades lograron contener el incidente antes de que se produjera un corte masivo de energía.

3. **DETALLE:**

El ataque representó una evolución notable en tácticas de guerra híbrida dirigidas a infraestructura energética. A diferencia de ataques históricos que se centraban en grandes plantas o redes de transmisión, el vector elegido fue la capa de comunicaciones OT entre fuentes descentralizadas de energía renovable y el operador nacional. Los atacantes intentaron interrumpir los enlaces entre turbinas eólicas, parques solares y la red, buscando desestabilizar la operación agregada del sistema.

Reportes adicionales indican la posible utilización de malware como BlackEnergy y KillDisk, empleados previamente contra entornos SCADA, para tomar control remoto, deshabilitar subestaciones y afectar centros de servicio. Este intento fue coordinado en múltiples ubicaciones simultáneamente, demostrando un conocimiento profundo de la arquitectura energética polaca. Aunque la intrusión logró degradar temporalmente servicios locales, los mecanismos de defensa impidieron un impacto mayor. El ataque se produjo durante una ola de frío extremo, lo que habría amplificado los efectos de un apagón. Las autoridades confirmaron que este fue el ataque más severo a la infraestructura energética del país en años y reforzaron la hipótesis de participación de actores estatales rusos.

4. **RECOMENDACIONES:**
   - Implementar segmentación estricta entre redes OT e IT para limitar el movimiento lateral.
   - Fortalecer la seguridad de comunicaciones entre fuentes de generación distribuida y centros de control, actualizar sistemas SCADA y aplicar parches en equipos de control industrial.
   - Desplegar IDS/IPS específicos para entornos OT con detección de patrones orientados a energía.

5. **REFERENCIAS:**

- https://shieldworkz.com/blogs/decoding-the-december-cyber-assault-on-polands-power-grid