Boletín de Ciberseguridad

Riesgo de vulnerabilidades IT y OT

Febrero - 2026

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 Febrero.

Alertas de Seguridad IT:

- Odido, operador de telecomunicaciones neerlandés, sufre exposición masiva de datos de más de 6 millones de clientes
- Advantest, corporación japonesa líder en equipos de prueba para semiconductores, sufre ataque de ransomware contra su red corporativa
- UFP Technologies, empresa fabricante de dispositivos médicos, sufre ataque de ransomware con exfiltración de datos

Alertas de Seguridad OT/ICS:

- Sector energético de Polonia, proveedor de energía (utilities), ataque destructivo contra OT/ICS con pérdida de control y visibilidad
- Ataque al sector energético polaco, CISA alerta OT, empresa de energía renovable

Odido, operador de telecomunicaciones neerlandés, sufre exposición masiva de datos de más de 6 millones de clientes

Tipo de Ataque: **Exposición de Información**

Medio de Propagación: **Acceso no autorizado al sistema interno de contacto con clientes**

1. **PRODUCTOS AFECTADOS:**
   - Sistema de gestión y contacto con clientes (Customer Contact System)
   - Infraestructura asociada al almacenamiento de datos personales

2. **RESUMEN:**

Entre el 7 y 8 de febrero, Odido detectó un acceso no autorizado a su sistema de contacto con clientes, comprometiendo información personal de más de 6 millones de usuarios. El incidente afectó tanto a clientes de Odido como de su subsidiaria Ben. Los datos expuestos incluyen nombres, direcciones, teléfonos, correos, fechas de nacimiento, números de cliente, cuentas bancarias y documentos de identidad. La compañía asegura que los servicios de telecomunicaciones no fueron interrumpidos y que no se comprometieron contraseñas, registros de llamadas ni facturación. Tras identificar el acceso malicioso, Odido bloqueó la intrusión, notificó a autoridades y comenzó a alertar directamente a los clientes afectados

3. **DETALLE:**

El ataque se originó mediante un acceso no autorizado al sistema interno utilizado para gestionar la comunicación con clientes. La intrusión permitió la exfiltración de múltiples categorías de datos personales almacenados en dicho sistema. El actor no identificado explotó una debilidad o punto de acceso dentro de la infraestructura IT de Odido, aunque la empresa no ha divulgado el vector exacto utilizado. La brecha permitió extraer información sensible como datos de identidad, contacto, bancarios y documentos oficiales, lo que eleva el riesgo de fraudes posteriores, ingeniería social y suplantación de identidad. Los sistemas críticos de servicio (telefonía, internet, TV) permanecieron intactos, lo que indica que la intrusión estuvo focalizada únicamente en el entorno IT administrativo. Odido actuó rápidamente cerrando el acceso, reforzando medidas de seguridad y notificando a las autoridades regulatorias. No se ha detectado publicación de los datos robados, pero la compañía advierte que podrían aparecer en línea más adelante y recomienda monitoreo constante. Tampoco existe evidencia de que un grupo específico esté detrás del ataque o que haya existido extorsión vinculada al incidente.

4. **RECOMENDACIONES:**
   - Implementar monitoreo continuo de sistemas de contacto y bases de datos sensibles.
   - Restringir el acceso a sistemas internos mediante MFA y segmentación estricta.
   - Actualizar políticas de retención y cifrado de datos personales almacenados.
   - Capacitar a los usuarios para identificar posibles campañas de phishing derivadas del incidente.

5. **REFERENCIAS:**
   - https://www.securityweek.com/dutch-carrier-odido-discloses-data-breach-impacting-6-million/

Advantest, corporación japonesa líder en equipos de prueba para semiconductores, sufre ataque de ransomware contra su red corporativa

Tipo de Ataque: Ransomware

Medio de Propagación: Intrusión externa en la red corporativa (método aún en investigación)

1. **PRODUCTOS AFECTADOS:**
   - Infraestructura IT utilizada para operaciones administrativas y de soporte
2. **RESUMEN:**

El 15 de febrero, Advantest detectó actividad inusual dentro de su entorno IT, lo que llevó a activar sus protocolos de respuesta a incidentes. La investigación preliminar determinó que un actor no autorizado accedió a partes de la red interna y desplegó ransomware. Hasta el momento no se ha confirmado la exfiltración de datos de clientes o empleados, pero la empresa continúa evaluando el impacto e indicó que notificará directamente a quienes pudieran verse afectados. Ningún grupo criminal ha reivindicado el ataque y la investigación sigue activa con apoyo de especialistas externos.

3. **DETALLE:**

El incidente comenzó con la detección de comportamiento anómalo en los sistemas IT de la empresa, lo que indica un posible compromiso inicial mediante acceso no autorizado a la red corporativa. Tras activar sus protocolos de respuesta, Advantest aisló los sistemas afectados para contener la propagación del ransomware. La investigación preliminar determinó que el atacante logró acceder a porciones específicas de la red e inició la ejecución de malware de cifrado, aunque no existen aún indicios concluyentes sobre robo de datos. La empresa no ha detallado públicamente el vector inicial, pero el impacto se centró en la infraestructura administrativa, sin evidencia de afectación a sistemas operativos industriales o equipos de prueba. Advantest está colaborando con expertos externos para identificar la ruta de entrada, evaluar el alcance exacto del ataque y reforzar sus controles. Actualmente, no se ha observado filtración de datos, pero la situación podría evolucionar en función del progreso de la investigación y de las tácticas del actor que permanece sin identificar.

4. **RECOMENDACIONES:**
   - Implementar monitoreo reforzado de actividad inusual en la red corporativa y servidores críticos.
   - Aislar y segmentar los sistemas más sensibles para reducir el impacto potencial de futuras intrusiones.
   - Fortalecer los mecanismos de autenticación, especialmente mediante MFA en accesos administrativos.
   - Capacitar al personal en detección temprana de indicadores de compromiso y manejo de incidentes.

5. **REFERENCIAS:**
   - https://www.bleepingcomputer.com/news/security/japanese-tech-giant-advantest-hit-by-ransomware-attack/

UFP Technologies, empresa fabricante de dispositivos médicos, sufre ataque de ransomware con exfiltración de datos

Tipo de Ataque: Ransomware con Doble Extorsión (Data Exfiltration + Cifrado)

Medio de Propagación: Red Corporativa

1. **PRODUCTOS AFECTADOS:**
   - Sistemas de facturación corporativa
   - Sistemas de generación de etiquetas de entrega
   - Infraestructura de red IT corporativa
2. **RESUMEN:**

El 14 de febrero de 2025, UFP Technologies detectó un ataque de ransomware sofisticado que comprometió múltiples sistemas de su infraestructura IT. Los atacantes lograron infiltrarse en la red corporativa, exfiltraron datos sensibles y posteriormente desplegaron malware de cifrado. El CFO de la compañía, Ronald Lataille, confirmó que se trata de un ataque ransomware clásico donde "los datos fueron robados y luego destruidos". El incidente afectó principalmente los sistemas de facturación y la capacidad de crear etiquetas de entrega para clientes. La compañía activó inmediatamente sus protocolos de respuesta a incidentes, implementó medidas de aislamiento y contrató asesores externos de ciberseguridad. Gracias a sistemas de respaldo y planes de contingencia preexistentes, las operaciones comerciales continuaron sin impacto material significativo. Hasta la fecha, ningún grupo de ransomware ha reclamado públicamente la responsabilidad del ataque.

3. **DETALLE**

Los atacantes obtuvieron acceso inicial mediante explotación de servidor perimetral mal configurado, pivotando hacia la red corporativa interna de UFP Technologies. Desplegaron ransomware que se propagó horizontalmente, cifrando servidores ERP de facturación, sistemas logísticos y bases de datos empresariales críticas. El malware interrumpió operaciones financieras y generación de etiquetas de envío, forzando desconexión de servicios clave. Análisis forense preliminar confirma robo previo de información corporativa sensible y potencial PII, empleando táctica de extorsión dual. La empresa ejecutó contención inmediata aislando subredes infectadas, eliminando persistencia maliciosa y restaurando desde copias seguras desconectadas. Continúan evaluaciones para medir volumen exfiltrado y rastrear publicación en foros clandestinos.

4. **RECOMENDACIONES:**
   - Implementar EDR/XDR en endpoints y servidores para detectar movimiento lateral y exfiltración temprana
   - Activar MFA obligatoria en VPN, OWA y accesos administrativos con políticas de geobloqueo
   - Desarrollar IRP detallado con playbooks ransomware, notificación regulatoria y contratos forenses preestablecidos

5. **REFERENCIAS:**
   - https://www.securityweek.com/medical-device-maker-ufp-technologies-hit-by-cyberattack/

Compromiso de sistemas OT en el Sector Energético de Polonia

Tipo de Ataque: Sabotaje/destrucción de OT (wiper en ICS; no es ransomware)

Medio de Propagación: Compromiso de edge devices expuestos a Internet (VPN/routers/gateways)

1. **PRODUCTOS AFECTADOS:**
   - RTUs (Remote Terminal Units) y PLCs de subestaciones de conexión de parques renovables.
   - HMIs, servidores OT, dispositivos de comunicación industrial y firmware de equipos OT.
2. **RESUMEN:**

Actores maliciosos ejecutaron ataques coordinados contra el sector energético en Polonia: más de 30 plantas renovables (eólica/fotovoltaica), una planta de cogeneración y una empresa manufacturera. Los atacantes ingresaron vía edge devices vulnerables, se movieron a la red OT y desplegaron wiper malware, causando pérdida de visibilidad/control entre instalaciones y el operador de distribución, borrado de datos en HMI y corrupción de firmware en OT. Aunque la generación continuó, los operadores no pudieron supervisar ni telecontrolar las instalaciones. El incidente fue documentado por CERT Polska (30-ene-2026) y amplificado por CISA (10-feb-2026) con mitigaciones prioritarias para el sector.

3. **DETALLE:**

El vector inicial se basó en dispositivos perimetrales expuestos a Internet, algunos sin soporte vigente y sin MFA, lo que permitió acceso remoto. Desde allí, los atacantes pivotaron hacia segmentos OT, aprovechando credenciales por defecto para llegar a HMI y RTUs. Una vez dentro, realizaron reconocimiento de la topología de las subestaciones de conexión (puntos que enlazan generación renovable con la red), identificando dispositivos de automatización críticos (RTUs, relés de protección, serial servers, modems y switches). El payload principal consistió en wiper/destructores diseñados para corromper firmware, borrar ficheros de sistema y degradar HMIs, ocasionando loss of view/ loss of control hacia el operador. El patrón observado no corresponde a extorsión financiera (no hubo demandas), sino a sabotaje deliberado. A pesar de los daños, la producción eléctrica no se detuvo; sin embargo, los operadores perdieron capacidad de supervisión/telecontrol, elevando el riesgo operacional. CISA subrayó los riesgos de edge devices end-of-support, la urgencia de verificación de firmware en OT y la eliminación de contraseñas por defecto; CERT Polska publicó IOCs, análisis forense y cronologías del ataque.

4. **RECOMENDACIONES:**
   - Ejecutar pruebas de acceso y tabletops conjuntos IT/OT con escenarios de loss of view/control, usando los IOCs y tácticas del informe de CERT Polska
   - Implementar monitoreo OT (telemetría de RTUs/HMIs, detección de wipers/firmware tampering) y playbooks de respuesta que contemplen pérdida de dispositivos.
5. **REFERENCIAS:**

- https://www.cisa.gov/news-events/alerts/2026/02/10/poland-energy-sector-cyber-incident-highlights-ot-and-ics-security-gaps

Ataque al sector energético polaco, CISA alerta OT, empresa de energía renovable

Tipo de Ataque: Intrusión destructiva OT/ICS (daño físico a hardware/control)

Medio de Propagación: Credenciales por defecto expuestas + explotación remota

1. **PRODUCTOS AFECTADOS:**
   - RTUs (Remote Terminal Units)
   - Sistemas HMI (Human-Machine Interface)
   - Firmware OT en plantas renovables/CHP/manufacturing
   - Sistemas de control distribuido en energía
2. **RESUMEN:**

Un actor malicioso lanzó ataques coordinados contra ~30 instalaciones del sector energético polaco (plantas renovables, CHP y manufacturing), dañando RTUs, borrando datos de HMI y corrompiendo firmware OT. No hubo apagones, pero se perdió control y monitorización. CERT Polska y CISA emitieron alertas en febrero de 2026 tras análisis post-incidente. El ataque explotó credenciales por defecto en dispositivos edge OT expuestos, destacando gaps en segmentación IT/OT. Publicado el 10 febrero 2026 tras investigación.

3. **DETALLE:**

Los atacantes explotaron credenciales por defecto en dispositivos edge OT (RTUs, HMI) expuestos en Internet, ganando acceso remoto sin autenticación fuerte. Una vez dentro, ejecutaron comandos destructivos: borrado selectivo de datos críticos en HMI (logs operativos, configuraciones), corrupción de firmware en RTUs (alterando parámetros de control/telemetría) y disrupción de comunicaciones Modbus/DNP3.

En algunos casos, se vio manipulación de UPS y telefonía de centros de control, pero el foco fue edge OT. No hubo escalada a PLC centrales ni cambios en procesos físicos (sin blackout), pero la pérdida de RTUs/HMI impidió monitorización remota y respuesta rápida.

CISA vincula esto a campañas rusas (Electrum/KAMACITE), con tácticas living-off-the-land (usando herramientas legítimas OT para persistir). La exposición vino de misconfigs comunes: puertos abiertos (502 Modbus, 20000 DNP3), credenciales fábrica sin cambio, falta de segmentación Purdue.

4. **RECOMENDACIONES:**
   - Cambiar inmediatamente credenciales por defecto en todos dispositivos OT.
   - Activar monitoreo de anomalías en protocolos OT (Modbus/DNP3).
   - Realizar inventario completo de dispositivos edge OT con credenciales débiles.

5. **REFERENCIAS:**

- https://industrialcyber.co/industrial-cyber-attacks/cisa-alerts-on-ot-vulnerabilities-after-poland-energy-attack-damaged-rtus-and-wiped-hmi-data/