# Boletín de Ciberseguridad

## Riesgo de vulnerabilidades IT y OT

Marzo - 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 Marzo.

**Alertas de Seguridad IT:**

- Filtración de datos en LexisNexis, empresa de servicios legales y gestión de riesgos
- Filtración de datos en Mazda Motor Corporation, empresa automotriz
- Ciberataque y filtración de datos en AkzoNobel, empresa fabricante de pinturas y recubrimientos

**Alertas de Seguridad OT/ICS:**

- Campaña de 149 ataques DDoS hacktivist contra infraestructura crítica, sectores gubernamentales y financieros
- Ataque cibernético a Stryker Corporation, compromete entorno Microsoft y afecta manufactura global
- Ataque ransomware a planta de tratamiento de agua de Minot, ciudad de infraestructura crítica de Dakota del Norte

# Filtración de datos en LexisNexis, empresa de servicios legales y gestión de riesgos

**Tipo de Ataque:** **Exposición de Información**

**Medio de Propagación:** **Aplicación web y servicios en la nube (AWS)**

1. **PRODUCTOS AFECTADOS:**
   - Servidores corporativos de LexisNexis
   - Instancias en la nube de Amazon Web Services (AWS)
   - Sistemas de soporte y encuestas de clientes
   - Plataformas internas de gestión de cuentas corporativas

2. **RESUMEN:**

LexisNexis confirmó una filtración de datos luego de que actores maliciosos publicaran información presuntamente robada de sus sistemas en un foro de ciberdelincuencia. El incidente fue dado a conocer tras un intento fallido de extorsión, cuyo rechazo motivó a los atacantes a divulgar parte de la información comprometida. Según la investigación interna de la compañía, los atacantes lograron acceder a ciertos servidores que almacenaban principalmente datos antiguos, anteriores al año 2020. Como resultado de la intrusión, se expusieron aproximadamente 2 GB de información, incluyendo alrededor de 400.000 registros con datos personales y corporativos.

3. **DETALLE:**

De acuerdo con las declaraciones de los atacantes, la intrusión se habría producido mediante la explotación de la vulnerabilidad conocida como React2Shell, la cual afecta a aplicaciones web desarrolladas con el framework React y permite la ejecución remota de comandos bajo determinadas condiciones. Esta debilidad, combinada con configuraciones de seguridad insuficientes en algunas instancias de AWS, habría facilitado el acceso no autorizado a los servidores corporativos. La falta de controles adecuados de segmentación y protección en la infraestructura en la nube permitió la extracción de más de 2 GB de datos, incluyendo información de cuentas corporativas, credenciales internas, secretos de desarrollo de software y datos personales. Entre la información expuesta se identificaron nombres, direcciones de correo electrónico, números telefónicos y cargos laborales, incluso direcciones pertenecientes a dominios gubernamentales. Si bien la empresa descartó el compromiso de contraseñas activas, datos financieros o bases de clientes vigentes, el incidente evidencia debilidades en la gestión de vulnerabilidades y en la protección de entornos cloud, sumándose además a antecedentes de filtraciones previas sufridas por el grupo.

4. **RECOMENDACIONES:**
   - Implementar controles de acceso estrictos y principio de mínimo privilegio en entornos cloud.
   - Aplicar parches de seguridad inmediatos a frameworks y librerías web vulnerables.
   - Fortalecer la supervisión continua y los mecanismos de detección temprana de intrusiones.

5. **REFERENCIAS:**
   - https://www.securityweek.com/new-lexisnexis-data-breach-confirmed-after-hackers-leak-files/

# Filtración de datos en Mazda Motor Corporation, empresa automotriz

**Tipo de Ataque:** **Acceso no autorizado / Exposición de Información**

**Medio de Propagación:** **Aplicación interna de gestión empresarial**

1. **PRODUCTOS AFECTADOS:**
   - Sistema de gestión interno para operaciones de almacén
   - Plataforma administrativa relacionada con piezas adquiridas
   - Base de datos de empleados y socios comerciales
2. **RESUMEN:**

Mazda Motor Corporation confirmó una filtración de datos personales que afectó a empleados y socios comerciales tras detectarse un acceso no autorizado a uno de sus sistemas internos. El incidente fue identificado a mediados de diciembre y estuvo relacionado con un sistema de gestión utilizado para las operaciones de almacén vinculadas a piezas adquiridas en Tailandia. Como resultado del ataque, se vieron comprometidos un total de 692 registros correspondientes a empleados de Mazda, empresas del grupo y socios comerciales. La compañía aclaró que no se almacenaba información de clientes en el sistema afectado, por lo que descartó cualquier impacto sobre datos de este tipo. Mazda indicó que el incidente fue contenido, notificado a las autoridades y que, hasta el momento, no se han identificado daños secundarios derivados del ataque.

3. **DETALLE:**

De acuerdo con la información proporcionada por la compañía, el incidente se produjo cuando un tercero no autorizado logró acceder al sistema de gestión interno mediante la explotación de vulnerabilidades de seguridad presentes en la aplicación. Aunque Mazda no reveló el nombre del software afectado ni los fallos específicos explotados, confirmó que las debilidades permitieron el acceso indebido a información administrativa almacenada en el sistema. Los datos expuestos incluyeron identificadores de usuario emitidos por la empresa, nombres completos, direcciones de correo electrónico, nombres de compañías asociadas e identificadores de socios comerciales. No se obtuvieron datos de clientes ni información financiera, ya que dichos registros no se encontraban en la plataforma comprometida. Tras detectar la intrusión, Mazda aplicó parches de seguridad, revisó las políticas de control de acceso, fortaleció la monitorización del sistema y restringió el acceso a Internet. La empresa señaló que existe el riesgo de que la información expuesta sea utilizada en campañas de phishing u otros fraudes, aunque aclaró que la investigación sigue en curso y que no se ha establecido relación con incidentes previos, como la campaña dirigida contra Oracle E-Business Suite.

4. **RECOMENDACIONES:**
   - Implementar procesos de gestión de vulnerabilidades y parches de seguridad continuos.
   - Fortalecer los mecanismos de monitoreo y detección de accesos no autorizados.
   - Revisar y actualizar las políticas de seguridad de aplicaciones internas.
   - Capacitar a empleados y socios sobre riesgos de phishing y uso indebido de información expuesta.

5. **REFERENCIAS:**
   - https://www.securityweek.com/mazda-says-employee-partner-information-stolen-in-cyberattack/

# Ciberataque y filtración de datos en AkzoNobel, empresa fabricante de pinturas y recubrimientos

**Tipo de Ataque:** **Ransomware con exfiltración de información**

**Medio de Propagación:** **Red corporativa y sistemas web expuestos a Internet**

1. **PRODUCTOS AFECTADOS:**
   - Red corporativa de una sede de AkzoNobel en Estados Unidos
   - Sitio web estadounidense de AkzoNobel y sistemas internos de almacenamiento documental
   - Plataformas de correo electrónico corporativo
2. **RESUMEN:**

AkzoNobel confirmó haber sufrido un ciberataque luego de que el grupo de ransomware Anubis publicara información presuntamente robada de sus sistemas. La compañía indicó que los atacantes lograron vulnerar la red de una de sus instalaciones en Estados Unidos, aunque aseguró que el incidente fue detectado y contenido oportunamente. Según la empresa, el impacto del ataque es limitado y se encuentra circunscrito únicamente a la sede afectada. No obstante, los ciberdelincuentes afirman haber exfiltrado una gran cantidad de datos corporativos y ya han comenzado a divulgar muestras de la información sustraída. AkzoNobel señaló que está notificando y brindando apoyo a las partes potencialmente impactadas, además de colaborar con las autoridades pertinentes mientras continúa la investigación.

3. **DETALLE**

El incidente fue atribuido al grupo de ransomware Anubis, una operación de ransomware como servicio activa desde finales de 2024 y reconocida por emplear tácticas de doble extorsión. Según información publicada por los atacantes, estos habrían obtenido acceso a la red corporativa de AkzoNobel y exfiltrado aproximadamente 170 GB de datos, equivalentes a cerca de 170.000 archivos. Como evidencia del ataque, Anubis filtró muestras que incluyen capturas de documentos internos y listados de los archivos robados. Entre la información expuesta se identificaron acuerdos confidenciales con clientes estratégicos, direcciones de correo electrónico, números de teléfono, correspondencia privada, escaneos de pasaportes, documentos de pruebas de materiales y hojas de especificaciones técnicas internas. El grupo Anubis cuenta además con capacidades destructivas adicionales, incluyendo herramientas para el borrado de datos, lo que incrementa el nivel de riesgo asociado a este tipo de ataques.

4. **RECOMENDACIONES:**
   - Reforzar la segmentación de red para limitar el impacto de accesos no autorizados.
   - Restringir y monitorear activamente los sistemas y servicios expuestos a Internet.
   - Fortalecer la protección de información sensible mediante controles de acceso y cifrado.

5. **REFERENCIAS:**
   - https://www.bleepingcomputer.com/news/security/paint-maker-giant-akzonobel-confirms-cyberattack-on-us-site/

# Campaña de 149 ataques DDoS hacktivist contra infraestructura crítica, sectores gubernamentales y financieros

**Tipo de Ataque:** DDoS (Denial of Service Distribuido) + Hack-and-Leak

**Medio de Propagación:** Redes externas / Internet / Botnet

1. **PRODUCTOS AFECTADOS:**
   - Sistemas SCADA y PLCs en infraestructura energética
   - Infraestructura gubernamental (110 organizaciones)
2. **RESUMEN:**

Entre el 28 de febrero y 2 de marzo de 2026, 12 grupos hacktivist lanzaron 149 ataques DDoS coordinados contra 110 organizaciones en 16 países, como respuesta a la operación militar Epic Fury/Roaring Lion de EE.UU.-Israel contra Irán. Los ataques se concentraron en Medio Oriente (107 casos), afectando desproporcionadamente infraestructura pública y objetivos estatales. Los grupos Keymous+, DieNet y NoName057(16) representaron el 74.6% de la actividad total. El 47.8% de las organizaciones atacadas pertenecen al sector gubernamental, seguido por finanzas (11.9%) y telecomunicaciones (6.7%). Grupos pro-rusos (Russian Legion, Cardinal) afirmaron haber comprometido redes militares israelíes incluyendo sistemas de defensa críticos..

3. **DETALLE:**

La campaña DDoS fue ejecutada mediante botnets distribuidas orquestadas por múltiples grupos hacktivist con alineación geopolítica (pro-iraní, pro-ruso). Los vectores de ataque incluyeron saturación de ancho de banda (volumétrico), agotamiento de recursos de servidor y ataques de protocolo contra infraestructura DNS/NTP. Grupos como Handala Hack y FAD Team reclamaron acceso no autorizado a sistemas SCADA y PLCs en infraestructura energética israelí, aunque sin confirmación independiente. Paralelamente, se detectó campaña de phishing SMS con réplica maliciosa de la aplicación Red Alert del Comando del Frente Interior israelí, distribuyendo malware de vigilancia móvil mediante sideloading de APK malicioso. La Guardia Revolucionaria iraní (IRGC) atacó sectores de energía digital en Medio Oriente, incluyendo Saudi Aramco y centro de datos AWS en EAU, con intención de infligir dolor económico global. El grupo UNC1549/GalaxyGato (estado-nación iraní) intensificó operaciones contra sectores de defensa, aeroespacial y telecomunicaciones regionales. El UK NCSC y SentinelOne alertaron sobre riesgo elevado de targeting ICS específico contra infraestructura crítica, energía, gobierno, finanzas, academia y medios en Israel, EE.UU. y aliados.

4. **RECOMENDACIONES:**
   - Activar monitoreo continuo de tráfico red para detectar patrones anómalos de DDoS y exfiltración
   - Validar aislamiento adecuado de dispositivos IoT/ICS y reducir superficie de ataque externa
5. **REFERENCIAS:**

- https://thehackernews.com/2026/03/149-hacktivist-ddos-attacks-hit-110.html

# Ataque cibernético a Stryker Corporation, compromete entorno Microsoft y afecta manufactura global

**Tipo de Ataque:** Wiper attack con archivo malicioso / Compromiso de dispositivos empresariales

**Medio de Propagación:** Entorno Microsoft corporativo / Microsoft Intune (MDM)

1. **PRODUCTOS AFECTADOS:**
   - Entorno Microsoft corporativo de Stryker (Microsoft Intune/MDM)
   - Sistemas de procesamiento de pedidos, manufactura y envíos
2. **RESUMEN:**

El 11 de marzo de 2026, Stryker experimentó un ciberataque que causó disrupción de su entorno Microsoft corporativo. Los atacantes comprometieron Microsoft Intune y ejecutaron comandos de borrado remoto (wipe) en decenas de miles de dispositivos de empleados. El incidente fue atribuido a grupo Handala (vinculado a MOIS iraní) en contexto de conflicto Medio Oriente. El ataque causó disrupción de manufactura global, procesamiento de pedidos y envíos durante semanas, obligando a operaciones manuales y reprogramación de procedimientos quirúrgicos personalizados. Investigación posterior con Palo Alto Unit 42 identificó archivo malicioso usado para ejecutar comandos y ocultar actividad del atacante. Para el 1 de abril, la red de manufactura global volvió a operación completa, con producción moviéndose hacia capacidad máxima.

3. **DETALLE:**

Los atacantes obtuvieron acceso a credenciales administrativas de Microsoft Intune mediante ingeniería social (phishing), permitiendo emitir comandos de borrado remoto a dispositivos gestionados. Análisis forense posterior identificó archivo malicioso capaz de ejecutar comandos para ocultar presencia del atacante, sin capacidad de propagación autónoma. El archivo fue usado para mantener persistencia y ejecutar comandos de wipe selectivo en dispositivos corporativos. La disrupción de manufactura fue consecuencia indirecta: pérdida de sistemas de gestión de pedidos, comunicación interna y coordinación logística obligó a transición manual de operaciones en plantas globales. Sistemas de productos médicos conectados permanecieron aislados del entorno Microsoft comprometido. Stryker implementó monitoreo intensificado de seguridad cloud, revisión de controles de acceso y escaneos más frecuentes como medida precautoria. Unit 42 confirmó mediante General Assurance Letter que no se identificó actividad maliciosa dirigida hacia sistemas de clientes, proveedores o partners externos.

4. **RECOMENDACIONES:**
   - Implementar autenticación resistente a phishing para acceso a plataformas MDM críticas
   - Segmentar gestión de dispositivos corporativos (IT) de sistemas de control industrial/manufactura (OT) mediante firewalls dedicados
   - Realizar auditorías regulares de accesos privilegiados a plataformas de gestión empresarial y validar separación arquitectónica OT/IT
5. **REFERENCIAS:**

- https://www.stryker.com/us/en/about/news/2026/a-message-to-our-customers-03-2026.html

# Ataque ransomware a planta de tratamiento de agua de Minot, ciudad de infraestructura crítica de Dakota del Norte

**Tipo de Ataque:** Ransomware

**Medio de Propagación:** Red interna / Servidor de control de planta

1. **PRODUCTOS AFECTADOS:**
   - Servidor de control de planta de tratamiento de agua municipal
   - Infraestructura SCADA de gestión de suministro de agua
2. **RESUMEN:**

El 14 de marzo de 2026, el personal de la planta de tratamiento de agua de Minot (Dakota del Norte) descubrió una carta de ransomware en servidor de control afectado. El servidor fue inmediatamente desconectado mientras personal IT trabajaba en resolución del incidente. El personal de tratamiento de agua condujo procedimientos manuales durante 16 horas, requiriendo verificaciones de calibradores in situ con mayor frecuencia para mantener estándares de presión y seguridad. La planta de tratamiento y todas las instalaciones municipales relacionadas al sistema de agua permanecieron operativas en todo momento, y el suministro de agua fue seguro según documentos oficiales. La ciudad reportó el incidente a todas las autoridades locales, estatales y federales necesarias. El FBI investiga la carta digital de extorsión, aunque no hubo demanda directa de pago según funcionarios.

3. **DETALLE:**

El ransomware comprometió un servidor de control dentro de la infraestructura OT de la planta de tratamiento de agua municipal de Minot (~50,000 habitantes). El ataque afectó sistemas automatizados de monitoreo y control de procesos, obligando a desconexión inmediata del servidor para contener propagación. Durante 16 horas de operaciones manuales, técnicos realizaron inspecciones presenciales frecuentes de medidores de presión, flujo y calidad de agua para compensar pérdida de telemetría automatizada y garantizar estándares de seguridad. La nota de ransomware apareció sin demanda explícita de pago, sugiriendo posible ataque oportunista contra infraestructura crítica. El City Manager Tom Joyce confirmó que el evento ha sido revisado para identificar oportunidades de entrenamiento y diseño preventivo. Expertos advierten que este incidente evidencia vulnerabilidad creciente del sector de agua estadounidense (50,000+ municipalidades pequeñas) ante ataques de organizaciones criminales y actores estado-nación (Irán, China), agravado por falta de financiamiento y regulaciones inconsistentes.

4. **RECOMENDACIONES:**
   - Implementar segmentación de red entre sistemas SCADA de agua y redes corporativas IT
   - Establecer protocolos de respaldo manual documentados y entrenar personal en operación de emergencia sin sistemas automatizados
   - Desplegar soluciones de detección de intrusiones específicas para protocolos OT (Modbus, DNP3) en infraestructura crítica de agua
5. **REFERENCIAS:**

- https://www.kxnet.com/news/top-stories/minot-water-plant-ransomware-attack/