Boletín de Ciberseguridad

Riesgo de vulnerabilidades IT y OT

Septiembre - 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 Septiembre.

Alertas de Seguridad IT:

- Hackeo a la Dirección de Inteligencia de la PNP, entidad estatal de seguridad nacional
- Harrods, tienda de lujo británica, expone datos de 430,000 clientes por brecha en proveedor externo
- Plex, empresa de software y servicios tecnológicos, sufre brecha de datos que expone credenciales de usuarios
- Hackeo al diario oficial El Peruano, medio estatal de publicación legal en Perú

Alertas de Seguridad OT/ICS:

- Collins Aerospace, empresa líder en tecnología de defensa y aviación, provoca caos en aeropuertos europeos tras ataque de Ransomware
- Asahi, cervecera japonesa, paraliza producción tras ataque de Ransomware
- Bridgestone, fabricante japonés de neumáticos, detiene producción en Norteamérica por ciberataque

Hackeo a la Dirección de Inteligencia de la PNP, entidad estatal de seguridad nacional

Tipo de Ataque: **Exfiltración de información**

Medio de Propagación: **Red interna**

1. **PRODUCTOS AFECTADOS:**
   - Base de datos de la Dirección de Inteligencia (DIRIN) de la PNP
   - Servidores administrados por la Dirección de Tecnologías de la Información y Comunicaciones
   - Aplicaciones de mensajería utilizadas por personal de inteligencia
   - Documentación clasificada y registros de agentes encubiertos
2. **RESUMEN:**

El 4 de septiembre de 2025, la División de Seguridad Digital de la Dirección de Inteligencia de la PNP detectó una posible vulneración de sus servidores. Posteriormente, el grupo hacktivista Deface Perú publicó en Telegram documentos confidenciales bajo el nombre “Dirin Leaks”. La filtración expuso información sensible sobre agentes encubiertos, planes de seguridad presidencial y seguimientos a periodistas. La PNP activó un plan de contingencia, suspendió servicios y comenzó investigaciones con apoyo nacional e internacional.

3. **DETALLE:**

El ataque fue atribuido al colectivo Deface Perú, que logró acceder a los servidores de la Dirección de Inteligencia de la PNP. La vulneración permitió la exfiltración de más de 2 GB de documentos confidenciales, los cuales fueron difundidos en el canal de Telegram “DefacePeru Chat”. Entre los archivos filtrados se encuentran datos personales de agentes encubiertos, planes de protección para la presidenta Dina Boluarte y expresidentes, así como reportes de vigilancia a periodistas considerados “amenazas a la gobernabilidad”. El grupo denunció la debilidad de la infraestructura estatal, criticando la inversión en un datacenter que calificaron de “inútil”. La PNP confirmó el incidente y activó medidas de contención, incluyendo la suspensión de servicios y la coordinación con la Dirección de Ciberdelincuencia para identificar a los responsables. El caso ha generado preocupación por el riesgo a la vida de los agentes expuestos y por la vulnerabilidad de los sistemas críticos del Estado.

4. **RECOMENDACIONES:**
   - Realizar auditoría forense completa de los servidores comprometidos
   - Fortalecer la seguridad perimetral y segmentación de redes críticas
   - Implementar cifrado de extremo a extremo en comunicaciones internas
   - Activar autenticación multifactor (MFA) para todo el personal de inteligencia
   - Establecer protocolos de respuesta rápida ante filtraciones de datos
   - Revisar y reforzar políticas de acceso y almacenamiento de datos sensibles
   - Monitorear canales de comunicación alternativos para detectar amenazas emergentes
5. **REFERENCIAS:**

- https://www.gob.pe/institucion/pnp/noticias/1240629-comunicado-n-14-2025

Harrods, tienda de lujo británica, expone datos de 430,000 clientes por brecha en proveedor externo

Tipo de Ataque: **Exposición de Información (Data Breach)**

Medio de Propagación: **Plataforma Web**

6. **PRODUCTOS AFECTADOS:**
   - Sistema de gestión de clientes operado por proveedor externo
   - Datos de clientes afiliados a programas de fidelización y tarjetas co-brandeadas
7. **RESUMEN:**

El 26 de septiembre de 2025, Harrods, reconocida tienda de lujo con sede en Londres, notificó a 430,000 clientes sobre una brecha de datos ocasionada por un incidente en uno de sus proveedores externos. La información comprometida incluye nombres, correos electrónicos, teléfonos y direcciones postales, además de etiquetas internas relacionadas con marketing y programas de fidelización. Harrods aseguró que sus propios sistemas no fueron comprometidos y que no se expusieron contraseñas ni datos financieros. La empresa ha informado a las autoridades pertinentes y continúa colaborando en la investigación.

8. **DETALLE:**

El incidente fue causado por una intrusión en los sistemas de un proveedor externo no identificado, que almacenaba datos de clientes de Harrods. La brecha permitió el acceso a **identificadores personales básicos**, como nombre, correo electrónico, número de teléfono y dirección. También se expusieron **etiquetas internas** utilizadas para marketing, como niveles de membresía y afiliación a tarjetas co-brandeadas (por ejemplo, Harrods-Amex o Harrods-Visa), aunque Harrods considera que esta información es difícil de interpretar por terceros no autorizados.

El atacante se comunicó directamente con Harrods, lo que sugiere un intento de extorsión, pero la empresa se negó a negociar. No se ha confirmado si el incidente está relacionado con el ataque anterior de mayo, atribuido al grupo Scattered Spider, aunque Harrods afirma que se trata de eventos separados. La empresa ha activado protocolos de respuesta, ha informado a la ICO (Information Commissioner's Office) y ha comenzado a contactar a los clientes afectados.

9. **RECOMENDACIONES:**
   - Auditar la seguridad de proveedores externos que manejan datos sensibles
   - Implementar controles de acceso y cifrado en sistemas de terceros
   - Establecer cláusulas contractuales claras sobre gestión de incidentes y notificación
   - Activar monitoreo continuo de integridad en plataformas de e-commerce
   - Reforzar campañas de concientización sobre phishing y suplantación de identidad

10. **REFERENCIAS:**

- https://cybersecuritynews.com/harrods-data-breach/

Plex, empresa de *software* y servicios tecnológicos, sufre brecha de datos que expone credenciales de usuarios

Tipo de Ataque: **Exposición de Información**

Medio de Propagación: **Acceso no autorizado a base de datos mediante vulnerabilidad en el servidor**

1. **PRODUCTOS AFECTADOS:**
   - Plataforma de streaming Plex
   - Cuentas de usuario con autenticación tradicional y SSO

2. **RESUMEN:**

Plex ha confirmado una brecha de seguridad en una de sus bases de datos, donde un tercero no autorizado accedió a información sensible de usuarios, incluyendo correos electrónicos, nombres de usuario, contraseñas cifradas y datos de autenticación. Aunque la compañía contuvo rápidamente el incidente y asegura que las contraseñas estaban protegidas mediante hashing seguro, se ha solicitado a todos los usuarios que restablezcan sus credenciales como medida preventiva.

3. **DETALLE**

El ataque se originó por la explotación de una vulnerabilidad crítica identificada como CVE-2025-34158, relacionada con el manejo inseguro de solicitudes HTTP en Plex Media Server. Esta falla permitía la ejecución de código arbitrario en sistemas vulnerables mediante validación insuficiente de parámetros entrantes. Como consecuencia, el atacante logró acceder a una base de datos que contenía credenciales cifradas. Aunque Plex no ha revelado el algoritmo de hashing utilizado, existe el riesgo de que, con suficientes recursos, las contraseñas puedan ser descifradas. La empresa ha corregido la vulnerabilidad y está realizando auditorías internas para reforzar su infraestructura de seguridad.

4. **RECOMENDACIONES:**
   - Restablecer la contraseña de la cuenta Plex desde plex.tv/reset
   - Activar la opción “Cerrar sesión en dispositivos conectados” al cambiar la contraseña
   - Cerrar todas las sesiones activas si se usa SSO desde plex.tv/security
   - Habilitar la autenticación de dos factores (2FA)
   - Actualizar Plex Media Server a la última versión disponible
   - Aislar el servidor Plex o aplicar reglas estrictas de firewall para limitar su exposición
   - Realizar escaneos regulares en busca de actividad sospechosa
   - Evitar compartir contraseñas o datos personales por correo electrónico
   - Estar alerta ante posibles intentos de phishing relacionados con Plex

5. **REFERENCIAS:**

- https://www.bleepingcomputer.com/news/security/plex-tells-users-to-reset-passwords-after-new-data-breach/

Hackeo al diario oficial El Peruano, medio estatal de publicación legal en Perú

Tipo de Ataque: Exposic Defacement, interrupción de servicio y eliminación de contenido oficial
Medio de Propagación: Sitio web institucional (www.elperuano.pe)

1. PRODUCTOS AFECTADOS:

- Portal web oficial del diario El Peruano
- Infraestructura digital del medio estatal

2. RESUMEN:

El 28 de septiembre de 2025, el sitio web del diario oficial El Peruano fue hackeado por el colectivo digital Deface Perú, quienes reemplazaron la página principal con un mensaje político dirigido al Gobierno peruano. El ataque ocurrió en medio de protestas sociales y coincidió con la publicación del reglamento para el octavo retiro de fondos de las AFP. El acceso al portal fue bloqueado por más de dos horas, y se eliminaron temporalmente las normas legales publicadas ese día. Las autoridades iniciaron investigaciones para identificar a los responsables.

3. DETALLE:

El ataque fue ejecutado por el grupo de hacktivistas Deface Perú, quienes previamente habían vulnerado sistemas de la Dirección de Inteligencia de la Policía Nacional del Perú (PNP). En esta ocasión, lograron acceder al servidor del diario El Peruano, reemplazando su página principal con un fondo negro y letras verdes que contenían un mensaje de protesta. El mensaje denunciaba injusticias sociales, acusaba al Gobierno de ignorar al pueblo y advertía sobre futuras acciones. Además del defacement, se reportó la eliminación de las normas legales publicadas el mismo día, incluyendo el reglamento del octavo retiro de la AFP. El grupo utilizó canales como Telegram para difundir su mensaje y atribuirse el ataque. Expertos advierten que el uso de VPNs, encriptación y servidores extranjeros dificulta la identificación de los responsables. El diario redirigió sus publicaciones oficiales a enlaces externos mientras se restauraba el sitio. El incidente expone la fragilidad de los sistemas digitales estatales y plantea preocupaciones sobre la seguridad de la información pública.

4. RECOMENDACIONES:

- Fortalecer la infraestructura digital de medios estatales con sistemas de detección de intrusos
- Implementar autenticación multifactor (MFA) para administradores de sistemas críticos

5. REFERENCIAS:

- https://larepublica.pe/politica/2025/09/28/hackers-de-el-peruano-lanzan-mensaje-al-gobierno-cada-mentira-difundida-cada-muerto-sin-justicia-es-una-cuenta-pendiente-1634500

Collins Aerospace, empresa líder en tecnología de defensa y aviación, provoca caos en aeropuertos europeos tras ataque de Ransomware

Tipo de Ataque: Ransomware

Medio de Propagación: Red Interna / Acceso remoto no autorizado

1. PRODUCTOS AFECTADOS:

- Sistema MUSE (Multi-User System Environment) de Collins Aerospace
- Infraestructura de check-in, embarque y manejo de equipaje en aeropuertos
- Operaciones de vuelo en aeropuertos europeos (Heathrow, Berlín, Bruselas, Dublín, Cork)

2. RESUMEN:

El 19 de septiembre de 2025, un ataque de ransomware afectó el sistema MUSE de Collins Aerospace, proveedor de soluciones de procesamiento de pasajeros para aeropuertos. El incidente provocó interrupciones masivas en los servicios de check-in y embarque en múltiples aeropuertos europeos, incluyendo Heathrow, Berlín, Bruselas y Dublín. Más de 100 vuelos fueron cancelados o retrasados, y miles de pasajeros fueron procesados manualmente. RTX Corporation, empresa matriz de Collins Aerospace, confirmó el incidente en una declaración oficial ante la SEC. Un sospechoso fue arrestado en el Reino Unido, aunque la investigación sigue en curso.

3. DETALLE:

El ataque comprometió el sistema MUSE, que permite a múltiples aerolíneas compartir recursos de check-in y embarque. El ransomware utilizado podría pertenecer a variantes como HardBit o Loki, ambas ofrecidas como servicios (Ransomware-as-a-Service), lo que permite su uso por múltiples afiliados. El vector de ataque inicial fue probablemente una vulnerabilidad en la infraestructura de red o una campaña de phishing dirigida a empleados de Collins Aerospace. Una vez dentro, los atacantes cifraron archivos críticos en servidores que operaban fuera de la red principal de RTX, pero dentro de redes específicas de clientes (aeropuertos). Esto provocó la caída de sistemas automatizados, obligando a los aeropuertos a operar con procesos manuales, como el uso de iPads, laptops y pases de abordar escritos a mano. La Agencia de Ciberseguridad de la Unión Europea (ENISA) confirmó que se trató de un ataque de ransomware y que se está investigando si hubo robo de datos. La empresa está trabajando en restaurar los sistemas afectados y ha desplegado actualizaciones de seguridad para el software MUSE.

4. RECOMENDACIONES:

- Segmentar redes OT e IT para limitar la propagación de malware
- Implementar monitoreo continuo de tráfico y comportamiento anómalo
- Realizar simulacros de respuesta ante incidentes en entornos OT

5. REFERENCIAS:

- https://www.bleepingcomputer.com/news/security/airport-disruptions-in-europe-caused-by-a-ransomware-attack/

Asahi, cervecera japonesa, paraliza producción tras ataque de Ransomware

Tipo de Ataque: Ransomware

Medio de Propagación: Red Interna (servidores corporativos comprometidos)

1. PRODUCTOS AFECTADOS:

- Sistemas de gestión de pedidos y envíos
- Infraestructura de producción en 30 fábricas nacionales
- Centros de atención al cliente y call centers
- Sistemas ERP y MES (Manufacturing Execution Systems)

2. RESUMEN:

El 29 de septiembre de 2025, Asahi Group Holdings, principal cervecera de Japón, sufrió un ciberataque que provocó una falla masiva en sus sistemas. El incidente obligó a suspender la producción en la mayoría de sus 30 fábricas, interrumpiendo pedidos, envíos y atención al cliente. La empresa confirmó que se trató de un ataque de ransomware y que se detectaron indicios de transferencia no autorizada de datos. Aunque no se ha confirmado la filtración de información personal, la recuperación total aún no tiene fecha definida.

3. DETALLE:

El ataque comenzó con una intrusión en los servidores internos de Asahi, afectando sistemas críticos como ERP y MES, lo que obligó a detener líneas de producción y procesos logísticos. La empresa estableció un centro de respuesta de emergencia y aisló los sistemas comprometidos para contener el daño. Las investigaciones forenses revelaron rastros de exfiltración de datos, aunque no se ha confirmado el alcance total.

El ransomware afectó tanto sistemas administrativos como operativos, paralizando la cadena de suministro. Asahi recurrió a la toma manual de pedidos y entregas físicas para mantener el abastecimiento parcial. La falta de preparación ante este tipo de incidentes ha sido señalada como una debilidad estructural en la ciberseguridad industrial japonesa.

4. RECOMENDACIONES:

- Implementar segmentación de redes entre sistemas IT y OT
- Activar soluciones de respaldo offline y recuperación ante desastres y fortalecer la seguridad de servidores críticos (ERP, MES) con monitoreo continuo
- Actualizar y parchear sistemas operativos y aplicaciones vulnerables
- Establecer protocolos de comunicación y continuidad operativa ante crisis

5. REFERENCIAS:

- https://www.securityweek.com/cyberattack-on-beer-giant-asahi-disrupts-production/

Bridgestone, fabricante japonés de neumáticos, detiene producción en Norteamérica por ciberataque

Tipo de Ataque: Ciberataque con características de Ransomware

Medio de Propagación: Red Interna / Segmento SCADA

1. **PRODUCTOS AFECTADOS:**
   - Sistemas de control industrial (SCADA)
   - Infraestructura de producción en plantas de Aiken (EE.UU.) y Joliette (Canadá)
   - Sistemas de manufactura y logística interna
2. **RESUMEN:**

El 2 de septiembre de 2025, Bridgestone Americas confirmó un ciberataque que afectó sus operaciones en múltiples plantas de manufactura en Norteamérica. El incidente obligó a detener temporalmente la producción en instalaciones clave en Carolina del Sur y Quebec. Aunque la empresa lo calificó como un "incidente cibernético limitado", se activaron protocolos de emergencia y se inició una investigación forense. Bridgestone aseguró que no se comprometieron datos de clientes ni interfaces externas, y que la contención fue rápida y efectiva.

3. **DETALLE:**

El ataque fue detectado por el equipo de seguridad de Bridgestone a las 2:00 a.m., cuando se observó tráfico inusual y accesos no autorizados en el segmento SCADA de su red interna. Este segmento controla procesos industriales críticos. Gracias a una arquitectura de seguridad basada en **autenticación multifactor**, **segmentación de red** y **monitoreo continuo**, se logró contener el ataque en sus primeras fases.

Aunque no se ha confirmado públicamente el uso de ransomware, expertos señalan que el patrón del ataque —interrupción abrupta de operaciones, falta de atribución inmediata y afectación directa a sistemas OT— sugiere una intrusión con fines de extorsión. No se ha identificado al grupo responsable ni se ha reportado una demanda de rescate. Este es el segundo gran incidente de Bridgestone en tres años, tras el ataque de LockBit en 2022.

4. **RECOMENDACIONES:**
   - Fortalecer la seguridad de sistemas SCADA con monitoreo de tráfico y control de accesos
   - Activar protocolos de respuesta ante incidentes con simulacros regulares
   - Auditar la infraestructura OT para identificar vulnerabilidades en sistemas heredados
   - Aplicar políticas de respaldo y recuperación específicas para entornos industriales
   - Establecer comunicación directa con autoridades locales y nacionales ante incidentes
   - Evaluar el cumplimiento de estándares como NIST SP 800-82 e IEC 62443
5. **REFERENCIAS:**

- https://www.bleepingcomputer.com/news/security/tire-giant-bridgestone-confirms-cyberattack-impacts-manufacturing/