

Costa Rica. 20 de noviembre de 2025

Empresas en alerta: ciberataques y fraudes digitales se disparan en la temporada alta de ventas

- Costa Rica figura entre los 15 países con mayor índice de ciberdelitos a nivel mundial, impulsado por ataques de ransomware y fraudes digitales.
- Expertos advierten que un solo ciberataque puede comprometer semanas de ventas y dañar la confianza del cliente en plena temporada alta.

Costa Rica, 17 de noviembre, 2025. Con el inicio de la temporada alta de compras —que abarca el Viernes Negro, el pago de aguinaldos y la Navidad— las empresas, tanto grandes como pequeñas, enfrentan un incremento sostenido en ciberamenazas que ponen en riesgo sus operaciones, ingresos y reputación.

De acuerdo con el Radware Global Threat Analysis Report 2025, durante la temporada navideña de 2024 el tráfico de *bots* maliciosos superó por primera vez al de usuarios reales en plataformas de comercio electrónico. Paralelamente, el informe Cybercrime Trends 2025 de SoSafe advierte que las campañas de *phishing* aumentan significativamente en estas fechas, impulsadas ahora por el uso de inteligencia artificial (IA) generativa.

Riesgos más comunes en la temporada alta

José Ricardo López, Director de Consultoría y Ciberseguridad del Grupo EULEN, explica que las amenazas más frecuentes se agrupan en dos grandes categorías, en línea con marcos reconocidos como el NIST Cybersecurity Framework:

1. **Ataques dirigidos**, orientados al acceso no autorizado, cifrado de información o extorsión, como ocurre con el **ransomware**, el cual se apoya en técnicas de movimiento lateral, explotación de vulnerabilidades y robo de credenciales para maximizar el impacto.
2. **Ataques masivos y automatizados**, orientados a capitalizar el incidente de forma temprana sin conocimiento detallado del afectado.
 - **Phishing avanzado** y campañas de ingeniería social potenciadas por IA generativa.
 - **DDoS** que buscan saturar recursos críticos de negocio.
 - **Abuso de bots** contra plataformas de comercio electrónico, inventarios y pasarelas de pago.

Durante la temporada alta, estos bots realizan actividades como:

- **Account Takeover (ATO)** mediante prueba de credenciales filtradas.
- **Card testing**, con microtransacciones destinadas a validar tarjetas robadas, lo que afecta la disponibilidad del sistema de pagos y puede generar cargos desconocidos.
- **Denegación de inventario**, bloqueo de carritos y manipulación de precios o cupones.

En el ámbito financiero, estos ataques se vinculan con requisitos de cumplimiento establecidos en **PCI DSS v4.0** y directrices antifraude publicadas por organismos internacionales.

El Grupo EULEN es líder en el diseño de servicios a empresas, con el objetivo de ofrecer a la sociedad servicios innovadores que aportan soluciones útiles, de calidad y más eficientes. Está especializado en las actividades de limpieza, seguridad, servicios auxiliares (de logística, generales y de telemarketing), FSM (Facility Services & Management), servicios sociosanitarios, mantenimiento integral, soluciones globales de recursos humanos y empleo y medio ambiente. Fundada en 1962 en Bilbao, la compañía está presente en 11 países y el volumen de ventas consolidadas supera los 1.600 millones de euros, con una plantilla global de más de 75 000 personas.

El Grupo EULEN está adherido al Pacto Mundial y firmemente comprometido con la sociedad a través del desarrollo de políticas socialmente responsables: integración laboral de colectivos desfavorecidos, conciliación de la vida familiar y profesional para su personal

Para más información:

Natalia Carvajal Lorenzo
ncarvajal@themapcomm.com
<http://www.themapcomm.com>

Tfn. +506 6081-7777
The Map Communications

El impacto de la inteligencia artificial en la ciberseguridad

La inteligencia artificial se ha convertido en una herramienta de doble filo. Aunque impulsa la eficiencia operativa de las organizaciones, también potencia la capacidad de ataque de los ciberdelincuentes. Según el informe *Cybercrime Trends 2025* de SoSafe, los criminales están utilizando la IA para desarrollar *deepfakes* realistas y generar campañas masivas de *phishing* con un nivel de personalización sin precedentes.

Cómo pueden las empresas hacer frente a estos riesgos

José Ricardo subraya que la mitigación de estas amenazas requiere una estrategia de seguridad integral basada en controles como los recomendados por CIS Controls v8 y ISO/IEC 27001:2022, destacando:

- **Autenticación multifactor (MFA)** e implementación de un modelo **Zero Trust** para reducir riesgos de suplantación y accesos no autorizados.
- **Actualización y parcheo continuo (Vulnerability & Patch Management)** para evitar explotación de vulnerabilidades conocidas.
- **Copias de seguridad inmutables y probadas** regularmente, con un tiempo objetivo de recuperación (RTO) inferior a 24 horas
- **Protecciones específicas para comercio electrónico**, incluyendo **WAF (Web Application Firewall)**, **detección de fraude**, **tokenización** y monitoreo de transacciones.
- **Monitorización continua de seguridad (SOC, SIEM, EDR/XDR)** para reducir el tiempo de detección y respuesta ante incidentes.
- **Gestión de proveedores y cadena de suministro digital**, ya que terceros siguen siendo uno de los principales vectores de entrada.
- **Pruebas periódicas de respuesta ante incidentes**, simulación de escenarios de fraude y comunicación temprana a clientes y autoridades competentes, conforme a ISO 27035.

José Ricardo recalca que “la seguridad no puede considerarse únicamente como una función tecnológica, sino como un habilitador estratégico del negocio”. Esto implica invertir en soluciones de protección y desarrollar una cultura organizacional basada en la prevención y la resiliencia operativa.

Costa Rica: un país cada vez más expuesto al cibercrimen

En el ámbito nacional, Costa Rica se posiciona entre los países más vulnerables de la región ante las amenazas digitales. Según el Global Organized Crime Index (OCINDEX) 2025, el país obtuvo una puntuación de 7.50 en delitos cibernéticos, un aumento de 0.50 puntos respecto al informe anterior. Con esta cifra, Costa Rica ocupa el puesto 15 a nivel mundial y el cuarto en el continente americano, evidenciando la creciente sofisticación y frecuencia de los ataques digitales.

El mismo informe revela que la criminalidad organizada alcanzó una puntuación de 5.90, reflejando una expansión de los mercados ilícitos, entre ellos la ciberdelincuencia, impulsada principalmente por ataques de *ransomware* dirigidos a instituciones públicas.

Por otra parte, Fernando Gamboa, Asesor de Seguridad de Grupo EULEN Costa Rica explicó que: “Las empresas que logren anticiparse a estas amenazas, invertir en tecnología y fortalecer la cultura de prevención estarán mejor preparadas para enfrentar los desafíos del nuevo entorno digital.”

El Grupo EULEN es líder en el diseño de servicios a empresas, con el objetivo de ofrecer a la sociedad servicios innovadores que aportan soluciones útiles, de calidad y más eficientes. Está especializado en las actividades de limpieza, seguridad, servicios auxiliares (de logística, generales y de telemarketing), FSM (Facility Services & Management), servicios sociosanitarios, mantenimiento integral, soluciones globales de recursos humanos y empleo y medio ambiente. Fundada en 1962 en Bilbao, la compañía está presente en 11 países y el volumen de ventas consolidadas supera los 1.600 millones de euros, con una plantilla global de más de 75 000 personas.

El Grupo EULEN está adherido al Pacto Mundial y firmemente comprometido con la sociedad a través del desarrollo de políticas socialmente responsables: integración laboral de colectivos desfavorecidos, conciliación de la vida familiar y profesional para su personal

Para más información:

Natalia Carvajal Lorenzo
ncarvajal@themapcomm.com
<http://www.themapcomm.com>

Tfn. +506 6081-7777
The Map Communications

| Comunicado de Prensa

Proteger la infraestructura digital ya no es opcional, sino una exigencia estratégica. Las empresas que no logren anticiparse a las amenazas cibernéticas ponen en riesgo no solo la seguridad de sus clientes, sino su propia operatividad y permanencia en el mercado. Un ataque no gestionado a tiempo puede traducirse en pérdidas cuantiosas, interrupción del servicio e incluso el cierre definitivo de la compañía.

El Grupo EULEN es líder en el diseño de servicios a empresas, con el objetivo de ofrecer a la sociedad servicios innovadores que aportan soluciones útiles, de calidad y más eficientes. Está especializado en las actividades de limpieza, seguridad, servicios auxiliares (de logística, generales y de telemarketing), FSM (Facility Services & Management), servicios sociosanitarios, mantenimiento integral, soluciones globales de recursos humanos y empleo y medio ambiente. Fundada en 1962 en Bilbao, la compañía está presente en 11 países y el volumen de ventas consolidadas supera los 1.600 millones de euros, con una plantilla global de más de 75 000 personas.

El Grupo EULEN está adherido al Pacto Mundial y firmemente comprometido con la sociedad a través del desarrollo de políticas socialmente responsables: integración laboral de colectivos desfavorecidos, conciliación de la vida familiar y profesional para su personal

Para más información:

Natalia Carvajal Lorenzo
ncarvajal@themapcomm.com
<http://www.themapcomm.com>

Tfn. +506 6081-7777
The Map Communications