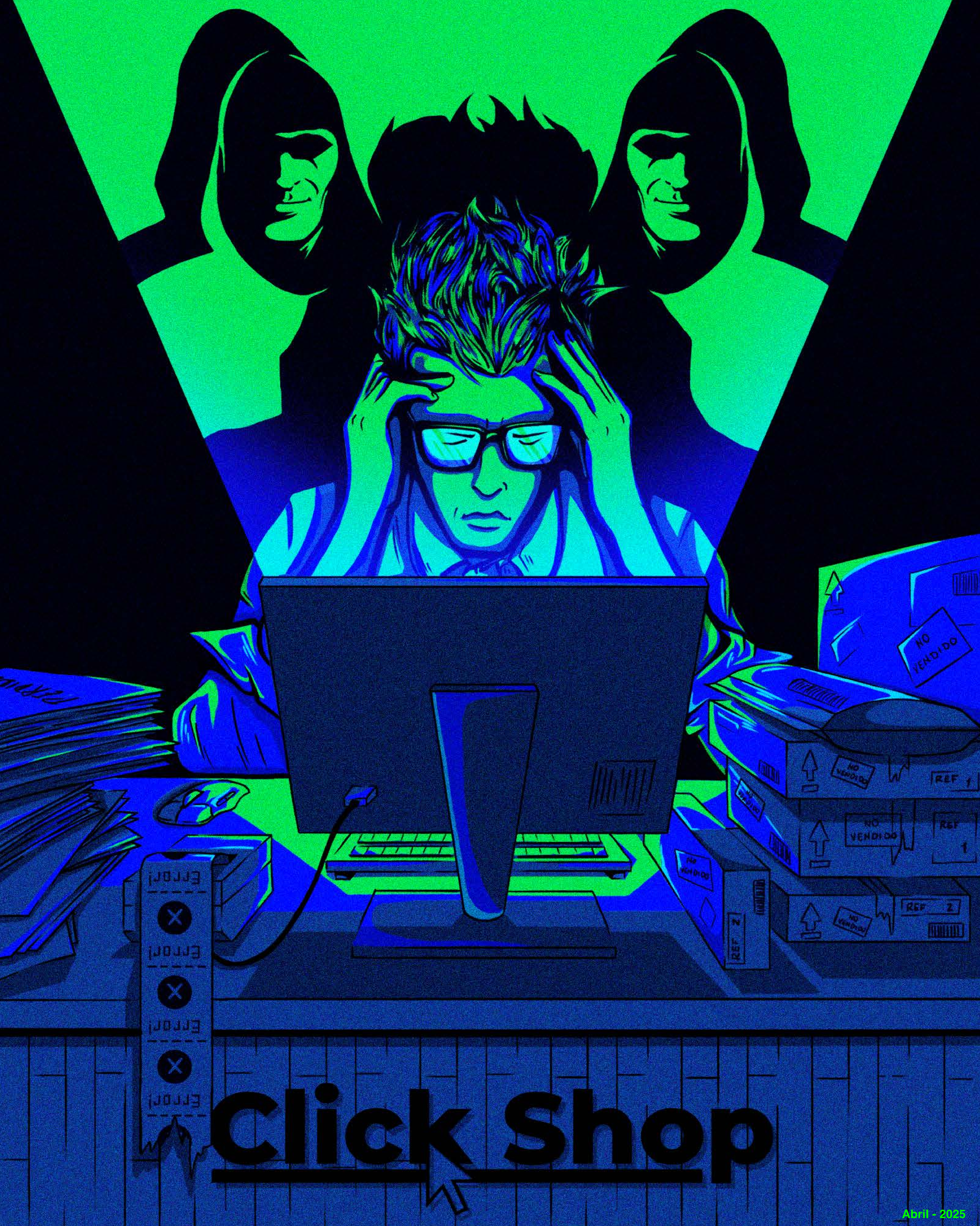
KERBEROS
MANAGING GENERAL AGENCY

Ciberseguridad
el nuevo eslabón del Retail



Abril - 2025

La ciberseguridad, el nuevo eslabón en la cadena productiva del sector Retail

Durante los últimos años hemos sido testigos de los grandes avances que la tecnología ha representado para las diferentes industrias, sin duda alguna, el sector retail ha sido un sector que ha tenido la oportunidad de potencializar la operación, teniendo en cuenta que los sistemas y las tecnologías han generado fortalezas en aspectos como la gestión de inventarios, atención al cliente, estrategias de mercadeo mediante el análisis de datos y sin lugar a duda la opción de poder generar transacciones en línea, permitiendo una escalabilidad sostenida y constate del negocio.

Sin embargo, este avance también ha traído consigo un aumento exponencial en los riesgos cibernéticos. Hoy, los retailers no solo gestionan productos, sino también grandes volúmenes de datos sensibles: información de tarjetas de crédito, direcciones, hábitos de compra y más. Esta riqueza de datos los convierte en blancos atractivos para los ciberdelincuentes ya que les permite obtener información que puede ser vendida por sumas considerables y usada para fines no éticos.

Ciberseguridad en el retail latinoamericano:

Cifras que alertan

- En 2023, el sector retail fue uno de los tres más atacados de Latinoamérica, concentrando el 25% de los incidentes cibernéticos en la región (IBM).
- Los ataques de phishing aumentaron un 617% en Latinoamérica durante el último año (Prey Project).
- El costo promedio de una filtración de datos en la región alcanzó los USD 2,76 millones, con un incremento del 12% respecto a 2023 (América Retail).
- En 2024, un ciberataque afectó a más de 1.800 tiendas físicas de una cadena de retail mexicana, generando pérdidas cercanas a USD 15 millones (WeLiveSecurity).
- El 50% de las empresas en la región ya invierten entre USD 10 y 49 millones en ciberseguridad (EY).

Factores que explican la alta exposición del retail a los ciberataques

Dependencia de terceros

Tiendas y marketplaces se apoyan en servicios externos (hosting, pagos, logística, publicidad, soporte, etc.) que pueden contener vulnerabilidades. Un error de un proveedor puede convertirse en una puerta de entrada para atacantes, afectando le continuidad de la operación y fugando data sensible de clientes.

Operaciones omnicanal

La combinación de tiendas físicas, e-commerce, apps móviles y otros canales crea un entorno con múltiples puntos de exposición. Una falla en uno de ellos (como un endpoint mal configurado) puede comprometer toda la red y ocasionar una afectación multiplataforma.

Riesgos en franquicias

Los franquiciados suelen operar con menos recursos y menor madurez tecnológica, convirtiéndose en eslabones débiles que pueden afectar la reputación del franquiciante si son comprometidos.

Temporadas pico y personal temporal

Épocas como Navidad o el Día sin IVA requieren refuerzo de personal, generando la vinculación de más colaboradores para satisfacer la demanda. Muchos de estos empleados temporales no están capacitados en ciberseguridad, lo que aumenta la probabilidad de errores, mal manejo de datos o incluso amenazas internas.

Popularidad de las tarjetas de regalo

Aunque impulsan ingresos y fidelización, también permiten anonimato a los delincuentes. Algunos atacantes usan tarjetas de crédito robadas para comprar gift cards, revenderlas y lavar dinero sin dejar rastro.

Principales amenazas cibernéticas en el sector retail

Explotación de vulnerabilidades

Desde fallas en software, IoT (POS, estanterías inteligentes), repositorios de código o configuraciones standard en la nube sin la debida “hardenización”. También se destacan ataques como DDoS, SQL Injection y Man-in-the-Middle.

Phishing

Sigue siendo una de las técnicas más utilizadas. Gracias a la IA generativa, los mensajes maliciosos son cada vez más convincentes y difíciles de detectar.

Ransomware

Este tipo de malware, que en muchos casos se origina vía phishing, cifra sistemas críticos y exige rescates millonarios, forzando de manera casi inmediata el pago por parte de la compañía afectada. Puede paralizar el canal online y físico.

Deepfakes

Los atacantes pueden usar videos o audios falsos para suplantar empleados o clientes y acceder a información confidencial o realizar fraudes.

Credential stuffing

Los criminales usan bots y credenciales filtradas para acceder a cuentas de clientes o empleados. La reutilización de contraseñas facilita este tipo de ataques.

Digital skimming

Se inyecta código malicioso en sitios de e-commerce para robar datos de tarjetas durante el checkout, sin que el usuario lo note.

Amenazas internas

Empleados o contratistas con acceso a sistemas sensibles pueden generar brechas, ya sea por negligencia o intencionalidad.

¿Cómo prepararse ante una cibercrisis?

1. **Diseñar un plan de respuesta a incidentes**

   Que permita a las organizaciones desarrollar un esquema rápido y eficiente para restablecer los procesos afectados y de esta manera minimizar la pérdida de ingresos por la detención de las operaciones.

2. **Contar con respaldo financiero**

   Como una póliza de ciberseguridad que cubra gastos legales, reputacionales, recuperación de datos y compensaciones.

3. **Evaluar constantemente la superficie de ataque**

   Incluyendo proveedores, canales digitales, dispositivos físicos y configuraciones en la nube.

4. **Capacitar a todo el personal**

   No solo al equipo de TI. La ciberseguridad es una responsabilidad compartida.

5. **Monitorear en tiempo real los sistemas**

   Para detectar comportamientos anómalos antes de que escalen.

6. **Asegurar los endpoints y el IoT**

   Incluyendo dispositivos POS, cámaras inteligentes, tablets, etc.

7. **Revisar la seguridad de los franquiciados**

   Especialmente en cadenas grandes con múltiples sedes.

8. **Contar con un aliado estratégico**

   Para mitigar el impacto reputacional ya que la pérdida de confianza por parte de los clientes puede constituir perdidas importaste a largo plazo

9. **Afectación de equipos que se utilicen dentro de la operación**

   Donde en algunos casos podrían quedar en estado de bricking, siendo la única solución la recompra de los mismos

La ciberseguridad en el retail ya no es una opción. Es un factor estratégico que determina la continuidad del negocio, la confianza del cliente y la competitividad a largo plazo. Invertir en protección hoy es evitar pérdidas irreparables mañana.

KERBEROS

MANAGING GENERAL AGENCY

www.kerberosre.io