EDICIÓN # 6

ENERO / 2026

KERBEROS

MANAGING GENERAL AGENCY

# Predicciones 2026

## ¿QUÉ ESPERAMOS DEL RIESGO CIBERNÉTICO?

KERBEROS
MANAGING GENERAL AGENCY

# Predicciones 2026

## ¿QUÉ ESPERAMOS DEL RIESGO CIBERNÉTICO?

El horizonte del riesgo cibernético nunca es estático. Cada año surgen nuevas amenazas, nuevas regulaciones y nuevas tecnologías que alteran el statu quo.

Definir una estrategia frente a estos cambios constantes puede sentirse como navegar una tormenta sin instrumentos confiables: ¿cómo están evolucionando las tácticas de los atacantes?, ¿hacia dónde se dirige realmente el mercado del seguro cibernético?, ¿qué tecnologías son solo tendencias pasajeras y cuáles modificarán de manera estructural el equilibrio entre ataque y defensa?

# 1 Evolución del ransomware: De la innovación técnica a la monetización simplificada basada en datos

Una de las formas más claras de anticipar la evolución del ransomware es seguir el flujo del dinero. Durante el último año, hemos observado cómo grupos de amenazas especializados han dejado de enfocarse en la innovación técnica para concentrarse en simplificar la monetización de los ataques. En 2026, esta tendencia se acelerará, ya que muchos grupos abandonarán el proceso altamente demandante de cifrar sistemas, el cual requiere mantener malware, administrar claves y negociar con las víctimas. En su lugar, un mayor número de atacantes adoptará esquemas de extorsión basada en supresión de datos, robando información sensible y exigiendo un pago a cambio de no divulgarla, una táctica que implica una carga operativa mucho menor.

Este cambio ya está en curso. Estamos observando menos bloqueos completos de sistemas y un aumento de la extorsión basada en robo y filtración de información. Al mismo tiempo, cada vez menos organizaciones están pagando rescates. Dado que las filtraciones de datos se han vuelto tan comunes, muchas empresas se están volviendo cada vez más insensibles, lo que obliga a los actores de amenazas a atacar a un mayor número de organizaciones para obtener los mismos retornos. A medida que esta presión continúa, los atacantes favorecerán modelos de monetización más simples, baratos y rápidos, basados en el robo de datos en lugar del cifrado.

# 2 Automatización de intrusiones mediante IA y uso de herramientas nativas del sistema (Living-off-the-Land)

Los atacantes recurren cada vez más a la automatización impulsada por modelos de lenguaje de gran escala (LLM) para encadenar herramientas nativas de los sistemas operativos y ejecutar intrusiones completas sin utilizar malware tradicional. Las técnicas living-off-the-land existen desde hace años, pero están siendo amplificadas radicalmente por agentes de inteligencia artificial que pueden generar dinámicamente comandos de PowerShell, orquestar reconocimiento, moverse lateralmente, escalar privilegios y exfiltrar información, todo utilizando herramientas que intentan mezclarse perfectamente con la actividad normal del sistema.

Para los defensores que no están preparados, esto hace que la detección sea un desafío. Las herramientas nativas parecen legítimas y las secuencias de comandos generadas por LLM pueden variar cada vez, evadiendo los sistemas tradicionales de detección basados en firmas. Los ataques living-off-the-land dejan muy pocos rastros forenses, pero lo que los delata es la velocidad, fluidez y eficiencia de la actividad. A medida que los adversarios continúen perfeccionando estos flujos de trabajo impulsados por IA, los defensores deberían esperar más ataques que aparenten ser comportamiento administrativo rutinario, pero que se desarrollen a una velocidad imposible para un ser humano.

# 3 Riesgo estructural de las VPN SSL y transición hacia arquitecturas Zero Trust

Uno de los problemas de seguridad más comunes que observamos es el uso de VPN SSL. Si bien proporcionan acceso remoto esencial, las VPN SSL siguen siendo objetivos persistentes para los actores de amenazas, con vulnerabilidades y compromisos repetidos en productos de proveedores como SonicWall, Cisco y Fortinet. Estas brechas relacionadas con VPN generan una proporción desproporcionada de reclamaciones y pérdidas en seguros cibernéticos.

En 2026, las VPN SSL se volverán una solución de acceso cada vez menos viable, a medida que los atacantes continúen explotándolas y el modelo de confianza cero se vuelva más accesible. Para las pequeñas y medianas empresas (PYMES), migrar de VPN SSL a acceso a la red de confianza cero (ZTNA) representaría una de las mejoras más impactantes en su postura de seguridad, reduciendo drásticamente la superficie de ataque y limitando el movimiento lateral. No todas las PYMES pueden migrar de inmediato, pero incluso pasos incrementales hacia arquitecturas Zero Trust pueden reducir significativamente el riesgo de compromiso y la probabilidad de futuras reclamaciones.

# 4 Traslado de las amenazas cibernéticas al mundo físico y riesgos de coerción directa

Las amenazas cibernéticas están trasladándose cada vez más al mundo físico. A medida que más grupos reclutan miembros en países occidentales —incluidos Estados Unidos, Canadá y el Reino Unido—, la probabilidad de amenazas físicas creíbles aumentará. La participación doméstica en grupos de alto perfil como Scattered Spider, donde de miembros con base en EE. UU. atacaron organizaciones como Caesars y MGM, demuestra que la distancia geográfica ya no protege a las víctimas.

De cara a 2026, esta proximidad hace que las amenazas físicas sean más realistas, señalando la peligrosa posibilidad de combinar compromisos digitales con coerción en el mundo real. Las empresas pueden enfrentar una nueva era en la que los ciberataques no solo representen riesgos financieros y operativos, sino también riesgos para la seguridad personal. La extorsión cibernética podría incluso evolucionar hacia un modelo de economía de trabajos temporales, utilizando acoso, persecución y amenazas físicas para presionar a las víctimas a pagar.

# 5 Riesgo de agregación por fallas técnicas y dependencia de infraestructuras cloud

Después de un año de interrupciones significativas, los aseguradores cibernéticos se enfocarán cada vez más en reducir el riesgo de agregación cuando miles de sitios web y servidores se vean afectados simultáneamente. Eventos como las caídas de CrowdStrike y AWS, causadas por fallos técnicos y no por ataques, ponen de manifiesto que las empresas siguen expuestas si carecen de estrategias multirregión o multicloud, las cuales muchas no adoptan por limitaciones de recursos.

Estas interrupciones exponen una brecha más amplia en la forma en que el mercado evalúa, modela y asegura las dependencias cibernéticas; la deuda técnica y las vulnerabilidades de infraestructura a menudo son pasadas por alto tanto por las empresas como por los aseguradores durante la suscripción. Para seguir siendo rentables, los aseguradores necesitarán una comprensión más profunda de las interconexiones tecnológicas, las dependencias críticas y cómo estas se traducen en potencial de pérdidas correlacionadas. Este conocimiento permitirá que la suscripción aborde directamente los riesgos de interrupción del negocio vinculados a software en la nube y otros fallos técnicos sistémicos.

# 6 Persistencia del mercado blando y presión competitiva sobre el underwriting

Es probable que el mercado blando del seguro cibernético persista hasta 2026, con reducciones de tarifas y estrategias de precios agresivas que intensifican la competencia. Incluso mientras las aseguradoras persiguen el crecimiento, los suscriptores deberán mantenerse atentos a la exposición persistente a la agregación y al riesgo sistémico de cola larga que las primas descontadas pueden ocultar. A medida que los términos centrales de las pólizas convergen, el precio y la cobertura por sí solos dejarán de definir la ventaja competitiva.

En su lugar, la diferenciación se desplazará hacia capacidades de valor agregado: mejoras de seguridad más sólidas, inteligencia más rica y servicios de respuesta a incidentes más sofisticados que ayuden directamente a los asegurados a reducir el riesgo.

En 2026, el mercado blando revelará qué aseguradoras cuentan con el rigor de suscripción necesario para crecer de forma sostenible sin sacrificar la rentabilidad. Aquellas que dependan excesivamente de tendencias temporales de siniestros enfrentarán una mayor volatilidad si los eventos cibernéticos aumentan o cambia la severidad. La estabilidad a largo plazo del mercado dependerá de evaluaciones disciplinadas y modelos bien calibrados, más que de recortes de tarifas a corto plazo.

# 7 Incremento de reclamaciones vinculadas a chatbots de IA y grabación automatizada de llamadas

Veremos un aumento en las reclamaciones relacionadas con chatbots de inteligencia artificial y herramientas de grabación de llamadas. Las organizaciones enfrentan acusaciones de que los chatbots instalados en sus sitios web comparten de manera indebida el contenido de las conversaciones con terceros. Este tipo de reclamaciones representa aproximadamente el 5 % de las reclamaciones por privacidad web, una proporción elevada considerando el nivel aún limitado de adopción, pero que se espera crezca a medida que más empresas incorporen chatbots de IA.

Este crecimiento se verá acompañado por nuevas reclamaciones relacionadas que alegan el uso de herramientas ilegales de grabación de llamadas impulsadas por IA. Estas herramientas se han proliferado a medida que los empleados buscan automatizar la toma de notas, pero algunas graban las voces de los participantes sin su conocimiento. Este aumento en el uso impulsará un incremento de reclamaciones, ya que constituye una analogía directa con una interceptación ilegal de comunicaciones.

# 8 Mayor escrutinio sobre el riesgo cibernético sistémico y la acumulación

El riesgo cibernético sistémico será objeto de un mayor escrutinio, ya que la acumulación creciente ejerce una fuerza desestabilizadora cada vez mayor sobre el sistema financiero global. A medida que la exposición del mercado continúa expandiéndose, los métodos actuales de agregación —a menudo limitados a industria, ingresos o geografía— serán cada vez más insuficientes para seguir el ritmo de la escala y complejidad de la interdependencia digital.

Los mini-cats sectoriales expondrán aún más estas deficiencias, empujando a los reaseguradores hacia visiones más transparentes y ricas en datos de sus carteras digitales.

# 9 Riesgo de agregación por dependencia de clientes críticos en la cadena de suministro

La fijación de la industria del seguro cibernético con las interrupciones de un solo proveedor ha oscurecido una amenaza sistémica mayor: el riesgo de agregación por clientes. Eventos como el ataque a Jaguar Land Rover han demostrado cuán expuestos están los proveedores aguas abajo; pequeños fabricantes sufren daños económicos desproporcionados cuando su principal comprador se ve gravemente afectado.

Las pólizas actuales rara vez abordan la pérdida financiera que experimenta un proveedor cuando un cliente crítico sufre un evento cibernético y los pedidos se detienen repentinamente. En 2026, la creciente preocupación por esta exposición empujará a los aseguradores a ampliar los límites de las pólizas e introducir protecciones explícitas frente a interrupciones de clientes dependientes.

10

# Velocidad de los ataques frente a la limitada capacidad de respuesta defensiva

Los atacantes están entrando y saliendo de las redes empresariales cada vez más rápido. Los datos muestran que, una vez que los atacantes obtienen acceso inicial, pueden tardar tan solo 47 segundos en moverse lateralmente. Mientras tanto, la mayoría de los proveedores de detección y respuesta gestionada anuncian tiempos de respuesta de 15 a 20 minutos, cuando para ese momento el ataque ya puede haber escalado de forma significativa.

La realidad actual es que los atacantes tienen meses para prepararse, pero los defensores con recursos limitados solo cuentan con segundos para responder. La solución pasa por respuestas automatizadas que funcionen como un reflejo, no como una decisión lenta y deliberada. El futuro del ataque y la defensa en ciberseguridad dependerá de quién cuente con el mejor software y los mejores algoritmos.

# 11 Aumento sostenido de reclamaciones por privacidad y recolección indebida de datos

La frecuencia de reclamaciones por recolección indebida de datos ya está aumentando, impulsada por el conocimiento de las leyes de privacidad y normas de interceptación que permiten a los individuos reclamar daños estatutarios. Mientras que históricamente las cartas de reclamación y demandas provenían de estudios jurídicos bien financiados que apuntaban a sitios web de alto tráfico o complejos, está surgiendo una nueva ola de reclamantes oportunistas que identifican en las cartas automatizadas una oportunidad rentable.

En 2026, a medida que el cumplimiento normativo en materia de privacidad se fragmenta y las tecnologías de rastreo se vuelven más sofisticadas, las organizaciones sin divulgaciones claras, mecanismos adecuados de consentimiento o supervisión de herramientas de marketing y analítica de terceros estarán especialmente expuestas. Sin medidas proactivas, es probable que experimenten un aumento significativo de reclamaciones de terceros relacionadas con privacidad.

www.kerberosre.io

KERBEROS

MANAGING GENERAL AGENCY