¡Sus datos serán robados!

(Afirman los expertos en ciberseguridad)

Por **Julian Murguia** , CTO
Omega Krypto
16 de marzo de 2026

Los principales expertos mundiales en ciberseguridad coinciden en que las brechas de seguridad son inevitables y afirman que la pregunta ya no es **si** su organización será vulnerada, sino **cuándo** sucederá y **con qué frecuencia**.

A esto se suma que el Informe de Defensa Digital de Microsoft de 2025 afirma claramente que la recopilación de datos fue el objetivo principal en el 80% de todos los ciberataques de 2025; y tu peor pesadilla se hace realidad cuando te das cuenta de que el robo de datos también es inevitable.

El informe de IBM sobre el coste de las filtraciones de datos de 2025 confirma que *estas ocurren a pesar de los sólidos controles preventivos* . A medida que crece la dependencia digital, los ataques se vuelven más frecuentes, más sofisticados y más costosos. ¡Y el uso de la inteligencia artificial por parte de los atacantes no hace más que empeorar las cosas!

Según TotalAssure, el *tiempo medio para detectar una brecha de seguridad en 2025 fue de 181 días* , mientras que, según el Informe Global de Respuesta

Julian Murguía, CTO
julian.murguia@omegakrypto.com
https://omegakrypto.com

a Incidentes de la Unidad 42 de Palo Alto Networks de 2025 , *a los atacantes les bastaron tan solo 72 minutos para extraer datos* .

La sensación de que tu organización ya está condenada a muerte, esperando el inevitable día en que será vulnerada y sus datos confidenciales serán robados, te corroe el corazón y la mente, temiendo que pueda provocar el colapso de tu organización y su desaparición.

Con esta mentalidad, el daño causado por el robo de datos nunca se solucionará, porque la derrota ya ha sido aceptada.

¿Qué otra cosa que no sea admitir la derrota es cuando te dicen que las filtraciones (y el robo de datos) son inevitables?

Como resultado, la estrategia de ciberseguridad ha pasado de la prevención pura a la resiliencia: detectar más rápido, responder con mayor rapidez, recuperarse antes y mitigar al máximo.

Pero la resiliencia tiene un punto ciego crítico:

¡Algunos daños simplemente no se pueden mitigar!

Si un ciberataque inutiliza dispositivos médicos críticos en un hospital y, como consecuencia, mueren pacientes, ninguna estrategia de mitigación puede revertir tal pérdida.

La muerte es irreversible, al igual que el robo de datos.

Una vez que terceros tienen acceso a sus datos confidenciales, el daño ya está hecho. Los datos se copian, se conservan y pueden ser explotados indefinidamente.

Da igual la rapidez con la que se detecte una brecha de seguridad; si la detección se produce después de la exfiltración de datos, ya es demasiado tarde.

La recuperación puede restaurar los sistemas, pero no puede borrar la información robada que está en posesión del atacante.

Los sistemas pueden reconstruirse, las operaciones pueden reanudarse, el ransomware a veces puede evitarse, pero los datos robados conservan el 100% de su valor y siguen siendo totalmente utilizables.

Aunque se pague el rescate y se restablezcan los sistemas, los atacantes conservan los datos robados. El coste a largo plazo de las filtraciones suele perdurar durante años, paralizando a las organizaciones o incluso obligándolas a cerrar definitivamente.

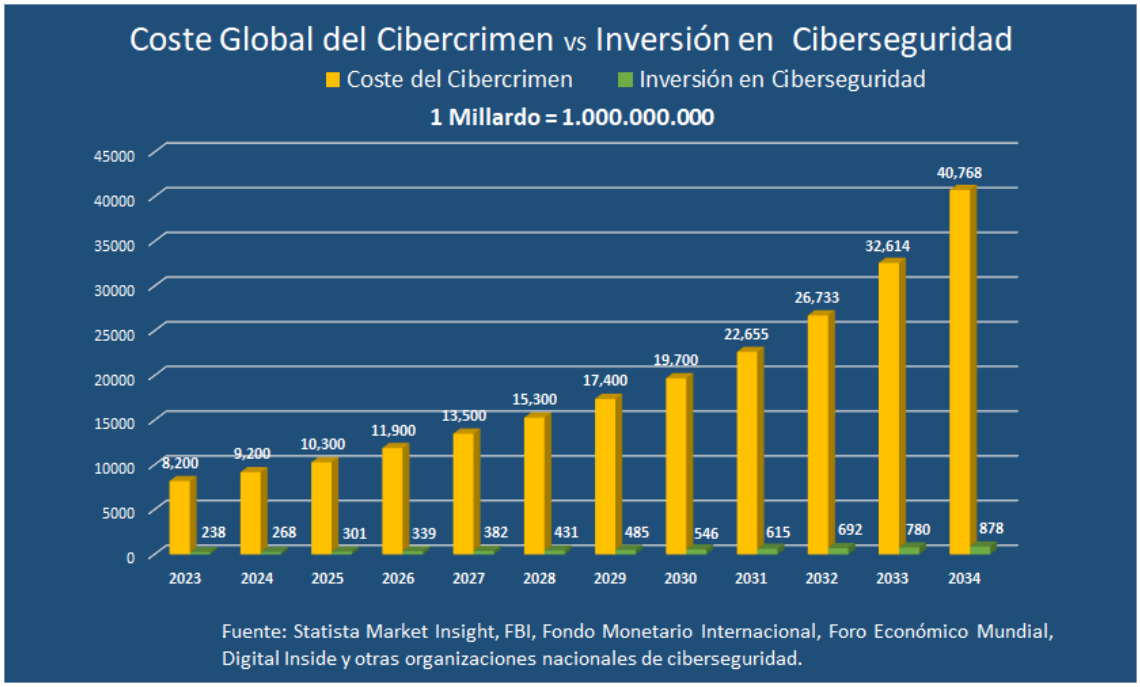
La ciberseguridad opera en un campo de batalla asimétrico. Los atacantes solo necesitan una vulnerabilidad: error humano, robo de credenciales,

acceso interno o compromiso de la cadena de suministro. Los defensores deben protegerlo todo, en todo momento.

Esto no es un fallo de la ciberseguridad, sino la naturaleza del panorama de amenazas.

La cruda realidad: la inversión mundial en ciberseguridad en 2025 fue de aproximadamente 301 mil millones de dólares estadounidenses, mientras que el coste mundial del cibercrimen en el mismo año fue de aproximadamente 10,3 billones de dólares estadounidenses (más de 34 veces mayor), lo que sitúa al cibercrimen como la tercera economía mundial más grande (detrás de Estados Unidos y China).

Y las proyecciones sobre cómo evolucionará esta batalla son ominosas:



Coste anual global del cibercrimen frente a la inversión anual global en ciberseguridad (Años 2023 a 2034)

Es un hecho que la ciberseguridad no logra detener el robo de datos porque se centra en el control de acceso, no en la protección del contenido. Cortafuegos, VPN, autenticación, arquitecturas de confianza cero: todo ello busca prevenir el acceso no autorizado. Pero una vez que se obtiene acceso, los datos son legibles.

En algún momento, repetir las mismas defensas esperando resultados diferentes deja de ser optimismo y se convierte en locura.

Julian Murguía, CTO
julian.murguia@omegakrypto.com
https://omegakrypto.com

Si no es posible prevenir por completo las filtraciones de datos y revertir el robo de información, detener los daños relacionados con dichas filtraciones requiere un enfoque fundamentalmente diferente.

En lugar de cambiar la pregunta de si su organización sufrirá o no una brecha de seguridad, cuándo y con qué frecuencia, simplemente nos hicimos una pregunta totalmente diferente:

¿Y si los datos robados no tuvieran ningún valor?

Los atacantes no entran por los sistemas, sino por los datos. Y si los datos robados no se pueden usar, monetizar ni explotar, entonces la brecha de seguridad pierde su propósito.

Permítanme darles un ejemplo:

Un banco sufre una brecha de seguridad y los atacantes obtienen acceso a todos sus sistemas y bases de datos.

Pueden ver el saldo de cada cuenta, pero cuando intentan obtener la información personal del titular de la cuenta, esta información específica en la base de datos está protegida de tal manera que no pueden leerla.

Acaban de descubrir que todo su esfuerzo, tiempo y dinero invertidos en asaltar el banco fueron en vano, una pérdida total.

Los datos a los que accedieron son inútiles; robaron el banco y se llevaron papel higiénico usado.

Para el banco, el incidente equivale a un fallo de hardware: se sustituye el equipamiento afectado, se restablecen las copias de seguridad y se reanudan rápidamente las operaciones.

No se ha filtrado ningún dato confidencial y no ha habido ningún impacto en la reputación ni en las finanzas del banco.

Para los clientes, no ha pasado nada: su dinero sigue en sus cuentas y su información personal permanece confidencial.

Si sus datos confidenciales son robados, quedarán completamente inservibles. Esto no solo evitará cualquier daño que dichos datos puedan causar, sino que también disuadirá a futuros ciberataques que intenten robarlos.

¿Cómo proteger el contenido de sus datos y neutralizar su valor en caso de robo?

El cifrado es el único mecanismo capaz de neutralizar el valor de los datos robados.

Julian Murguía, CTO
julian.murguia@omegakrypto.com
https://omegakrypto.com

Pero no se trata de cualquier cifrado. Los algoritmos de cifrado modernos, simétricos o asimétricos, no son inquebrantables. Simplemente son computacionalmente difíciles de descifrar. Con el tiempo y la potencia suficientes, fallan. Los datos cifrados robados hoy en día acabarán siendo legibles.

Esto no es teórico. La amenaza de "recolectar ahora, descifrar después", documentada por Palo Alto Networks, significa que los atacantes ya están recopilando datos cifrados, esperando la capacidad cuántica para descifrarlos.

Si el cifrado va a ser la solución, tiene que ser diferente; se requiere un cifrado alternativo.

Como afirmó el CEO de IBM, Arvind Krishna, en 2018: " *Si alguien dice que quiere que algo esté protegido durante al menos 10 años, debería considerar seriamente si debería empezar a utilizar técnicas de cifrado alternativas ahora mismo* ".

Lo dijo hace casi 8 años y su afirmación es más válida que nunca.

Para detener de forma permanente los daños relacionados con las filtraciones de datos, el cifrado debe cumplir requisitos que los enfoques actuales no pueden:
• Proteger el contenido de los datos, no solo el acceso.
• Proteger de forma segura los datos estructurados sin dañar los sistemas.
• Trabajar con bases de datos y almacenamiento estructurado.
• Conservar el formato y la longitud de los datos.
• Seguir siendo utilizable por las aplicaciones existentes
• Ser resistente a la computación cuántica por diseño
• Neutralizar indefinidamente los datos robados.

Para lograrlo, es necesaria una técnica de cifrado completamente nueva.

No una extensión.
No un modo.
No una solución alternativa.

Un nuevo enfoque.

Hemos creado una tecnología para proteger de forma segura el contenido de sus datos confidenciales, que puede hacerlos inútiles para cualquier atacante en caso de robo.

Tras casi una década de investigación y desarrollo, hemos creado y patentado una novedosa tecnología de cifrado diseñada específicamente para resolver el problema que la ciberseguridad moderna no puede: prevenir y eliminar el daño que puede causar el robo de datos.

Julian Murguía, CTO
julian.murguia@omegakrypto.com
https://omegakrypto.com

Nuestra tecnología supera los requisitos de seguridad más estrictos, como GDPR, DORA, NIS2, HIPAA, NIST Cybersecurity Framework, etc.; ocupa poco espacio, requiere pocos recursos, tiene un impacto mínimo en el rendimiento de los sistemas y se integra perfectamente en cualquier sistema o dispositivo existente.

No sustituye a la ciberseguridad, sino que la complementa al resolver el problema más costoso —y aún sin resolver— en este ámbito: ***el daño causado por el robo de datos.***

Como mostramos en nuestro ejemplo, no es necesario cifrar todos los datos, solo aquellos que dan sentido a todo lo demás.

Al cifrar selectivamente los campos críticos y sensibles, los datos restantes se vuelven sin contexto , sin sentido e inútiles para los atacantes.

Incluso si se roban los datos , incluso si se realizan intentos de descifrado, incluso años después.

Si bien, al incorporar nuestra tecnología a su estrategia de seguridad, aún pueden producirse brechas de seguridad, aún se puede acceder a los sistemas y aún se pueden robar datos, ¡ **el daño termina aquí!**

Porque los datos robados, sin significado, estructura ni valor, no son más que ruido.

La pregunta que les hacemos es:

¿Aceptará la derrota y esperará pasivamente a que su organización sea vulnerada y sus datos confidenciales sean robados, o actuará ahora para garantizar que una brecha de seguridad no acabe con su organización?

¡La supervivencia de su organización depende de su respuesta!

Actúa ahora, antes de que sea demasiado tarde.

Podemos ayudar.

Julian Murguía, CTO
julian.murguia@omegakrypto.com
https://omegakrypto.com

Referencias:

Informe de Defensa Digital de Microsoft 2025 :
https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Digital-Defense-Report-2025.pdf#page=29

Informe de IBM sobre el coste de una filtración de datos en 2025:
https://webobjects2.cdw.com/is/content/CDW/cdw/on-domain-cdw/brands/ibm/cost-of-a-data-breach-2025-full-report.pdf#page=27

TotalAssure - Tiempo promedio para detectar un ciberataque en 2025:
https://www.totalassure.com/blog/average-time-to-detect-cyber-attack-2025#global-detection-time-benchmarks

Informe global de respuesta a incidentes de la Unidad 42 de Palo Alto Networks de 2025:
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/unit42/Unit42-Global-Incident-Response-Report.pdf#page=25

Palo Alto Networks - Coseche ahora, descifre después:
https://www.paloaltonetworks.com/cyberpedia/harvest-now-decrypt-later-hndl

Grupo Thales - Proteja su privacidad - Seminario web:
https://cpl.thalesgroup.com/es/node/17376

Palo Alto Networks:
https://www.paloaltonetworks.com/perspectives/mastering-the-basics-cyber-hygiene-and-risk-management/

Cloudflare : La confianza del cliente es el mejor indicador de seguridad.
https://www.cloudflare.com/the-net/illuminate/security-customer-trust/

Seclore – Las filtraciones son inevitables, la pérdida de datos no lo es - Seminario web:
https://www.seclore.com/resources/videos/breach-is-inevitable-data-loss-isnt/

Julian Murguía, CTO
julian.murguia@omegakrypto.com
https://omegakrypto.com