Publicado en Ciudad de México el 22/11/2024

# [Contratar un ciberseguro: lo que toda organización debe saber, según Minsait](http://www.notasdeprensa.es)

## En un entorno en el que la tecnología es el pilar de las operaciones empresariales, los riesgos cibernéticos están en aumento constante. Los ciberataques, como el ransomware, las filtraciones de datos y el malware, pueden paralizar una organización en cuestión de minutos, afectando sus finanzas, reputación y operaciones. Erik Moreno, director de Ciberseguridad de Minsait en México, comparte sus reflexiones

 Ante esta coyuntura, surge una pregunta crucial: ¿es necesario contar con un ciberseguro? Si bien este recurso no puede prevenir un ataque, es fundamental para ayudar a las empresas a recuperarse y mitigar los daños provocados por un incidente de seguridad. Un ciberseguro funciona de manera similar a otros tipos de seguros, como los de automóvil o salud, ya que busca reducir el impacto financiero en caso de un evento adverso. Su propósito es ofrecer cobertura frente a los costos derivados de un ataque cibernético, que pueden incluir desde la pérdida de ingresos por la interrupción del negocio, la destrucción de activos digitales, hasta la recuperación de datos y la restauración de sistemas. Así, el ciberseguro le permite a la empresa afectada recuperarse en el menor tiempo posible De igual forma, contribuyen a acelerar la respuesta a los incidentes, a gestionar crisis y cubrir los gastos legales que puedan surgir tras un evento de ciberseguridad. Si bien el ciberseguro ofrece beneficios, también es esencial conocer las exclusiones y limitaciones que pueden aplicar. Por ejemplo, las pólizas no cubren las multas impuestas por regulaciones como el GDPR, que pueden representar una carga económica considerable para las organizaciones víctimas de un ataque.  Para algunas organizaciones, la prima de un ciberseguro puede parecer alta, pero cuando se compara con las posibles pérdidas por un ciberataque, el costo-beneficio de la póliza puede justificar la inversión. Sin embargo, antes de tomar una decisión, se recomienda que las empresas evalúen el nivel de riesgo al que están expuestas.  Evolución de la demandaEl mercado de ciberseguros ha pasado por varias olas en los últimos años. Inicialmente, la demanda de este tipo de pólizas aumentó de manera significativa, impulsada por el crecimiento de los ciberataques. Sin embargo, disminuyó brevemente cuando los costos de las pólizas comenzaron a subir debido a la alta demanda. En la actualidad, la demanda ha vuelto a repuntar, lo que está llevando a una mayor competencia entre las aseguradoras y, a largo plazo, podría hacer que los precios disminuyan. A pesar de este nuevo aumento, no todo ha sido sencillo para las aseguradoras. Los ataques de ransomware han puesto en aprietos a muchas de ellas, ya que hasta un 70% de las pólizas se ha utilizado para cubrir los daños causados por estos incidentes. En consecuencia, las aseguradoras elevan sus estándares de evaluación, exigiendo a las empresas que demuestren tener controles de seguridad adecuados antes de emitir una póliza. El proceso de obtención de un ciberseguro, por tanto, incluye ahora una evaluación rigurosa de las medidas de seguridad de la organización.  Este cambio ha tenido un efecto positivo, ya que está empujando a las empresas a mejorar su nivel de madurez en ciberseguridad. Ya no es sólo la presión de las normativas y regulaciones lo que impulsa a las empresas a invertir en ciberseguridad, sino también las exigencias de las aseguradoras, si es que se está evaluando su contratación.  Sin embargo, contratar un ciberseguro no es garantía de que todos los problemas se resolverán de manera sencilla. Una de las exclusiones más comunes en las pólizas, hasta en un 90% de ellas, es que no cubren los ataques patrocinados por estados o naciones. Este tipo de ataques, también conocidos como ciberguerra, pueden ser difíciles de identificar, lo que complica aún más el proceso de reclamación. Las aseguradoras pueden argumentar que un ataque proviene de una nación y, por lo tanto, no estarían obligadas a pagar. Otra exclusión que se debe tener en cuenta es el error humano. Si una empresa no implementa correctamente los controles de seguridad o no responde de manera adecuada a un incidente, la aseguradora podría negar la cobertura. Esto resalta la importancia de que las organizaciones no sólo adquieran un ciberseguro, sino que también desarrollen una estrategia de ciberseguridad robusta que incluya capacitación para sus empleados y un plan de respuesta a incidentes. "¿Necesita su negocio un ciberseguro?"Ahora bien, antes de proceder a contratar un ciberseguro, hay varias preguntas que deben formularse:  ¿Qué impacto tendría en la empresa una interrupción prolongada de sus operaciones?  ¿Qué tan rápido puede responder a un ataque y evitar que se propague en su entorno tecnológico?  ¿Está dispuesta a asumir el riesgo financiero de no tener un seguro?  ¿Qué tan preparada está para responder a un incidente de ciberseguridad? ¿Qué condiciones ofrece la aseguradora para el pago de la póliza? ¿Entiende las preocupaciones y los riesgos del negocio?  Estas preguntas son fundamentales para determinar si un ciberseguro es necesario y cuál sería su papel dentro de una estrategia de ciberseguridad más amplia. Evaluar el costo-beneficio de una póliza de ciberseguro también implica analizar las diferentes opciones disponibles en el mercado. No todas las pólizas son iguales, y algunas pueden ofrecer mejores condiciones o una cobertura más amplia que otras. Comparar los términos de las pólizas, las exclusiones y el servicio que ofrece cada aseguradora es fundamental para tomar una decisión informada. Un diferenciador clave es contratar una empresa de consultoría especializada en ciberseguridad como Minsait. Minsait destaca la importancia de los ciberseguros como responsabilidad para proteger la información de los clientes, dado que la cadena de suministro es uno de los principales vectores de ataque en las organizaciones. Finalmente, es esencial no ver a los ciberseguros como una solución aislada, sino como parte de una estrategia integral de ciberseguridad que incluya controles preventivos, una respuesta rápida a incidentes y un análisis continuo de los riesgos. En última instancia, la decisión de contratar o no un ciberseguro dependerá del apetito de riesgo de cada organización y de su capacidad para gestionar las amenazas cibernéticas de manera efectiva. Minsait es la compañía de Indra líder en transformación digital y Tecnologías de la Información. Minsait presenta un alto grado de especialización y conocimiento sectorial, que complementa con su alta capacidad para integrar el mundo core con el mundo digital, su liderazgo en innovación y en transformación digital y su flexibilidad. Con ello, enfoca su oferta en propuestas de valor de alto impacto, basadas en soluciones end-to-end, con una notable segmentación, lo que le permite alcanzar impactos tangibles para sus clientes en cada industria bajo un enfoque transformacional.

**Datos de contacto:**

Gabriela Medina Guerrero

AB Estudio de Comunicación, Directora Asociada

5539663493

Nota de prensa publicada en: [https://www.mexicopress.com.mx/contratar-un-ciberseguro-lo-que-toda](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Nacional Ciberseguridad Seguros Innovación Tecnológica



[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)