VALUATIVE SAS NIT 830.121.091-0 Oficinas a nivel Nacional
info@valuative.co - www.valuative.co

EL CYBER SEGURO LOS RIEGOS CIBERNETICOS

UN ENFOQUE PARA SUSCRIPCION Y ATENCION DE RECLAMO CRITERIOS Y CONCEPTOS

COBERTURA OFRECIDA POR EL MERCADO Y TRATAMIENTO DE LA SUSCRIPCION Y EL INICIO DEL RECLAMO

2

VALUATIVE
LIDERES EN INVESTIGACIÓN Y PROTECCIÓN PATRIMONIAL

Cra. 7 No.156 - 10 Of.1607 /Torre Krystal
Centro Empresarial North Point
Bogotá D.C., Colombia
PBX.: +57(1) 390 2846
info@valuative.co

VALUATIVE
LÍDERES EN INVESTIGACIÓN Y PROTECCIÓN PATRIMONIAL

Cra. 7 No. 156 – 10 Of. 1607 / Edificio Torre Krystal
Bogotá D.C., Colombia
Pbx: +57 (1) 3902846
info@valuative.co

EL CYBER SEGURO
LOS RIEGOS CIBERNETICOS

UN ENFOQUE PARA SUSCRIPCION Y ATENCION DE RECLAMO
CRITERIOS Y CONCEPTOS
PARTE 2

COBERTURA OFRECIDA POR EL MERCADO
Y TRATAMIENTO DE LA SUSCRIPCION Y EL INICIO DEL RECLAMO.

INTRODUCCION

Con el aumento constante de los delitos cibernéticos, muchas organizaciones en una variedad de industrias son susceptibles a los ataques cibernéticos. Los ciberataques recientes indican que las infracciones son inevitables y pueden ser extremadamente dañinos. Las infracciones cibernéticas pueden conducir a costos tangibles, degradación de la marca y cambios en el comportamiento del consumidor.

En este contexto, muchas organizaciones han llegado a la conclusión de que un cyber ataque es inevitable, no es una cuestión de "si" sucederá, sino de "cuándo".

Aunque es imposible estar al 100% seguro, se desarrollan un sólidos enfoques de gestión contra ciberriesgo; las organizaciones pueden implementar una serie de tratamientos de riesgo a través de medidas de prevención, detección y actividades de respuesta para mantener las amenazas o riesgos cibernéticos, a un nivel aceptable.

Además, el panorama del riesgo cibernético en constante evolución ha impulsado el interés en el seguro cibernético como un elemento complementario del cyber enfoque de gestión de riesgos, que permite a las organizaciones transferir algunos de los riesgos asociados con incidentes cibernéticos a sus aseguradores.

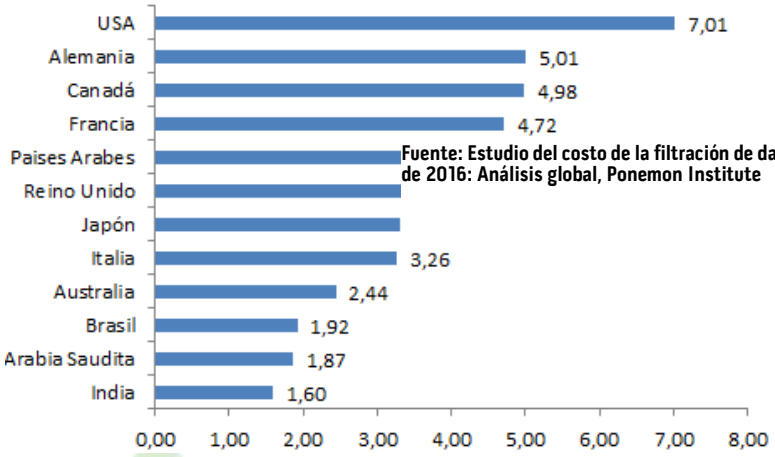
EL COSTO DEL CIBERDELITO

Cra. 7 No. 156 – 10 Of. 1607 / Edificio Torre Krystal
Bogotá D.C., Colombia
Pbx: +57 (1) 3902846
info@valuative.co

Las mayores filtraciones de datos de las últimas décadas han costado a cada uno de las empresas afectadas cientos de millones de dólares.

▪▪ En 2016, el costo de la violación de datos varió de US $ 2,1 millones por una pérdida de menos de 10.000 registros, a US $ 6,7 millones por más de 50.000 registros perdidos o robados (según el diario El País; Ver Figura)

▪▪ En el mismo estudio, un costo promedio para una organización si uno de estos registros se pierde o es robado puede acercarse a US$158 Mio.



Fuente: Estudio del costo de la filtración de datos de 2016: Análisis global, Ponemon Institute

Los costos son atribuibles a la investigación de la infracción, actividades de remediación, notificación de clientes, seguimiento, gestión de la reputación, honorarios legales y liquidaciones, y/o multas reglamentarias.

EL MERCADO DE CIBER SEGUROS HOY

El ciberseguro puede complementar las medidas de seguridad activas de una organización proporcionando cobertura de protección en tres áreas:

1. **Responsabilidad por una violación o pérdida de datos**
2. **Costos de remediación (por ejemplo, para investigar el incumplimiento, notificando a los afectados, etc.)**
3. **Multas / sanciones reglamentarias y costos de liquidación**

La demanda de ciberseguro, junto con el número de proveedores de seguros, ha ido aumentando a medida que el uso de la tecnología se ha vuelto más frecuente.

La Pólizas del mercado de seguros cibernéticos de EE. UU. ampara aproximadamente el **90% del mercado**, con primas anuales brutas emitidas del orden de **US$ 3.250** millones en 2016.

Es importante resaltar que los primeros en adoptar dicha protección fueron los servicios financieros, empresas, minoristas y organizaciones de salud, con grandes cantidades de **información de identificación personal** (PII por sus siglas en inglés).

El mercado de seguros de ciberseguridad se ha desarrollado mucho más rápidamente en Estados Unidos que en la Unión Europea debido a que las leyes de violación de datos y su notificación, la hace obligatoria en el primero. Sin embargo, en el mercado europeo se puede esperar que se ponga al día en el medio o largo plazo, en razón del establecimiento del Reglamento General de Protección de Datos (GDPR) en la comunidad y probablemente requerirá una notificación inmediata de violaciones de datos personales a las autoridades de supervisión.

*Es de tener en cuenta que **Ley 1581 de 2012** constituye el marco general de la **protección** de los **datos** personales en **Colombia**. … El Decreto 1313 de 2013 tiene como objeto reglamentar parcialmente la Ley 1581 de 2012, dictando disposiciones generales para la **protección de datos** personales.* Para el efecto, sugerimos la lectura disponible en los hipervínculos:

Ley Estatutaria 1581 de 2012:
http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html
Diario Oficial No. 48.587 de 18 de octubre de 2012 – Congreso de la República

Decreto 1377 de 2013:
https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

Es claro que el Seguro Cibernético es solo un elemento de Gestión de Riesgo y nunca podrá eliminar la amenaza por completo.

A pesar del aumento de los incidentes cibernéticos, la adopción del seguro cibernético entre Organizaciones se mantiene en un nivel bajo: según la "Encuesta de Riesgos Empresariales de 2012", el 65% de las empresas que cotizan en bolsa no

Cra. 7 No. 156 – 10 Of. 1607 / Edificio Torre Krystal
Bogotá D.C., Colombia
Pbx: +57 (1) 3902846
info@valuative.co

compra un seguro cibernético, pero el 63% de los responsable de la toma de decisiones están preocupados por el efecto de las amenazas latentes.

La anterior preocupación, se debe principalmente a:

- **Falta de conciencia** - muchos ejecutivos subestiman los costos asociados con incidentes cibernéticos y/o de forma inexacta creen que ya están asegurados bajo la póliza de responsabilidad general de la empresa.

- **Complejidad en la suscripción**: el número creciente de violaciones de datos ha llevado a varias aseguradoras a ser más cautelosas y por ello, consideran que los potenciales clientes podrían sentirse intimidados por la complejidad asociada con el proceso de suscripción (por ejemplo, nivel de detalle de encuestas de riesgo, uso potencial de evaluaciones de riesgos por parte de terceros, etc.)

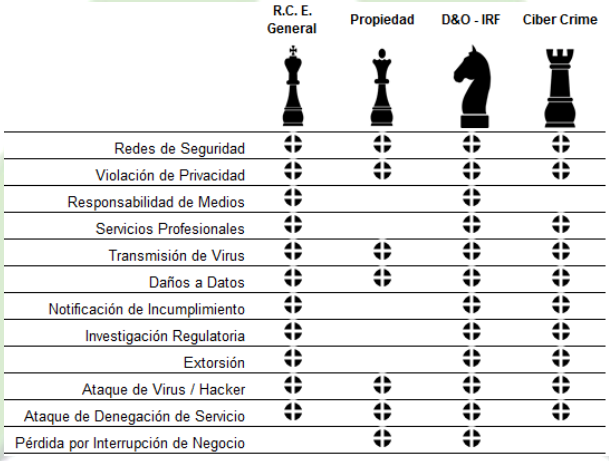
- El desafío de alinear **cobertura de seguro** con la **exposición al riesgo**, requiere de amplia experiencia en suscripción y gestión de riesgos para tener una comprensión adecuada del **costo total del riesgo cibernético** para una organización y determinar si los términos y políticas propuestos satisfacen las necesidades del asegurado.

En general, el mercado de seguros cibernéticos permanece inmaduro, con espacio para mejorar:

a. Ofrecer una gama amplia de cobertura y considerando que las políticas en este sentido varían significativamente de un cliente a otro.

b. Hay datos actuariales limitados disponibles para que las aseguradoras ajusten las primas según qué productos y controles de seguridad son más efectivos.

c. La cobertura es inadecuada en algunas áreas, por ejemplo, el seguro cibernético no es bueno para cobertura de propiedad intelectual, robo o daño a la reputación, y la de caída en el negocio que puede resultar.



Comparativo entre Seguros Tradicionales y Pólizas de Riesgo Cibernético

Las pólizas de seguro cibernético brindan una variedad de opciones de cobertura y condiciones previas que necesitan ser considerados al comprar un seguro cibernético:

1. La primera parte protege contra pérdidas incurridas directamente por la Empresa en respuesta a un incidente cibernético (**Gastos Directos**), y normalmente incluye robo y fraude, investigación forense, interrupción del negocio, extorsión y pérdida y restauración de datos informáticos.

2. **Cobertura de terceros:** protege contra pérdidas sufridas por terceros en respuesta a un incidente cibernético, y normalmente incluye litigios, acuerdos con reguladores, costos de notificación, gestión de crisis y seguimiento crediticio El seguro cibernético está previsto y tasado para adaptarse a los clientes individuales. Como tal, las pólizas de seguro cibernético pueden estipular exclusiones, imponer límites o añadir cláusulas para proteger a la aseguradora de mayores riesgos

Cra. 7 No. 156 – 10 Of. 1607 / Edificio Torre Krystal
Bogotá D.C., Colombia
Pbx: +57 (1) 3902846
info@valuative.co

A manera de ejemplo, incumplimiento de una computadora de un proveedor en la nube, o dispositivos sin cifrar que contienen información personal o sensible, datos, o mal funcionamiento del software de computadora debido a errores de programación.

Tamaño de la Compañía (Basado en Ingresos)	Compañías pequeñas (Menos de US $ 100 Mio)	Compañías Medianas US $100 Mio a US $1.000 Mio	Compañías Grandes Mas de US $1.000 Mio
Cobertura	$1 - 5 Millones US	$5 - 20 Millones US	$15 - 25+ Millones US
Prima Anual (Costo de Cobertura)	$7.000 - $15.000 US por millón de Cobertura	$10.000 - $30.000 US por millón de Cobertura	$20.000 - $50.000 US por millón de Cobertura
Sublímites de Cobertura Típica (Restricciones de Pago)			
Los sublímites pueden restringir los pagos en un solo aspecto de la cobertura del 10% al 50% de la Cobertura total			
Costos de Notificación	Límite $100.000 - $ 500.000	Límite $500.000 - $ 2 Millones	Límite $1,5 - $2,5 Millones
Costos de Manejo de Crisis	Límite $250.000 - $ 1,25 millones	Límite $ 1,25 millones - 5 millones	Límite $ 3,75 millones - 6,25 millones
Gastos de defensa Legal y regulatorio	Límite $500.000 - $ 2,5 millones	Límite $ 2,5 - $ 10 millones	Límite $ 7,5 - $ 12,5+ millones

Fuente: Deloitte research on insurance provider Web sites

En general, los Cyber Seguros no proveen:

A. Protección contra el riesgo de reputación, mientras se puede otorgar un reclamo monetario por violación de la seguridad de la información; el daño hecho a la marca de una organización no puede ser reparado con la misma facilidad o transferido a una compañía de seguros.

B. La eliminación del riesgo: el seguro, ya sea cibernético o de otro tipo, proporciona a la organización la oportunidad de transferir, o no eliminar el riesgo.

C. Un reemplazo para un programa de seguridad de la información requiere de fuertes controles de seguridad y una información completa de tal programa de seguridad como requisitos previos para comprar un seguro cibernético.

Como ejemplo, considérese un gran procesador de tarjetas de crédito que compró una cyber póliza de seguro con **cobertura de US $ 30 millones** contra un incidente cibernético.

Desafortunadamente, una violación de datos que involucra varios millones de tarjetas de crédito dio como resultado que la empresa pagó más de US $145 millones en compensación por pagos fraudulentos. En esta situación, el **asegurado** tuvo que **desembolsar US $115 millones** y no fue adecuadamente cubierto.

Para medir la cobertura cibernética las organizaciones necesitan de mayor efectividad, y en consecuencia las aseguradoras han comenzado a implementar procedimientos rigurosos para la suscripción de pólizas de seguro Cibernético.

Tales procedimientos incluyen un número de pasos bien definidos:

A. **Solicitud Inicial.** El Intermediario o Broker del Seguro pide al cliente completar un formulario de auto evaluación sobre su información de tecnología (TI), así como de su entorno de seguridad.

B. **Evaluación.** El proveedor de seguros cibernéticos revisa la evaluación, luego organiza una evaluación in situ del cliente.

Para los clientes de mayor riesgo, el proveedor de seguros solicita **a un tercero** la evaluación de riesgos a realizar en la sede del cliente, con el costo a cargo de dicho cliente.

C. **Revisión:** la evaluación de riesgos del tercero proporciona los resultados al proveedor de seguro cibernético basado en TI de referencia y prácticas de seguridad principales.

D. **Informe:** El Intermediario utiliza el informe recibido y produce el suyo propio con recomendaciones sobre las sugerencias recibidas del tercero.

E. **Suscripción:** El proveedor del seguro (Asegurador) estructura la cobertura, adecua las exclusiones y calcula las primas basado en su informe de evaluación.

Consideraciones clave para seleccionar un Seguro Cibernético:

Cra. 7 No. 156 – 10 Of. 1607 / Edificio Torre Krystal
Bogotá D.C., Colombia
Pbx: +57 (1) 3902846
info@valuative.co

Cuando se selecciona un seguro Cibernético o de Cyber Seguridad, es recomendable prestar atención a ciertas consideraciones, como:

Comprender la exposición al riesgo del Asegurado:

a. Evaluar la exposición actual a riesgo cibernético para comprender el tipo y cantidad de cobertura requerida.
b. Es posible que no se requiera cobertura en áreas donde los controles están bien establecidos y en las que se ha probado de forma rutinaria.

Comprender las complejidades de la póliza:

a. Dado que existe una amplia variedad de seguros, a menudo se requieren un riguroso proceso de suscripción – gastar tiempo por adelantado para comprender las condiciones previas que deben cumplirse para obtenerlo.

b. También es importante comprender las coberturas y exclusiones de la póliza para asegurarse de que las circunstancias de una pérdida se enmarcan en ellas. Este paso es importante al momento de afrontar la atención de un siniestro, pues deberá procurarse dicho análisis, de tal forma que las circunstancias en que se ha presentado el evento reclamado en verdad se encuadren dentro de las previsiones indemnizatorias de la póliza.

c. Si bien las pólizas de seguro pueden ayudar en la transferencia de riesgos, el asegurado debió realizar un análisis de costo – beneficio para determinar la idoneidad de invertir en cobertura de seguro cibernético.

d. Es claro que éste tipo de producto está destinado a cubrir riesgos que no pueden ser atendidos o previstos internamente.

Cubrimiento y Peligros Excluidos

Las póliza existentes en el mercado, normalmente importada de mercados de amplia experiencia como el Americano, el Británico o el Continental europeo, detallan que riesgos o peligros se encuentran excluidos. **Lo anterior nos lleva a condiciones de Cubrimiento de todos los riesgos que no se encuentren específicamente excluidos.**

Si bien las computadoras y los datos pueden resultar dañados por una amplia gama de peligros, son muy vulnerables a los tipos de peligros que se enumeran a continuación. Estos peligros están excluidos en las causas especiales de pérdida.

Sin embargo, a nivel local, los productos existentes otorgan protección sobre la responsabilidad del asegurado frente a sus clientes.

- **La cobertura** en general responde por la restauración de páginas web o estructuras de comunicaciones con el fin de procurar la pronta retoma de actividades, minimizando las pérdidas financieras y de mercado.

- **Adicionalmente,** es común el ofrecer amparo por la asunción de **costos de recuperación de archivos digitales** o pérdidas por interrupción del negocio a causa de actos maliciosos (p. ej. Malware, hacking, acceso no autorizado o ataques que restringen el acceso a Web Page.

- Complementariamente, es posible la contratación, por parte del asegurado, de servicios de respuesta a incidentes, inmediatamente de acaecido un hecho cubierto.

- **Sobrecarga de energía.** No incluye los daños causados por una **interrupción del servicio público**, incluida cualquier sobrecarga de energía asociada, si la falla se origina fuera de sus instalaciones. Las fallas (y las sobrecargas asociadas) que se originan en sus instalaciones también se excluyen si son el resultado de equipos de servicios públicos ubicados en sus instalaciones. Sin embargo, si una falla de energía o una sobretensión resultan en un peligro cubierto (como un incendio), cualquier **pérdida resultante** de ese peligro está cubierta.

- **Perturbación eléctrica.** Excluye los daños causados por energía eléctrica, magnética o electromagnética. Esto incluye arcos eléctricos, cortocircuitos y electricidad estática.

Cra. 7 No. 156 – 10 Of. 1607 / Edificio Torre Krystal
Bogotá D.C., Colombia
Pbx: +57 (1) 3902846
info@valuative.co

1.

- **Cambio de temperatura.** Excluye los daños causados por cambios de temperatura o humedad.

- **Avería mecánica.** Excluye el daño causado por avería mecánica , incluido el daño causado por la fuerza centrífuga

EL PROCESO DE RECLAMACION

No todas las reclamaciones cibernéticas se tratan por igual en consecuencia, la Aseguradora y su Ajustador deben conocer qué se necesita exactamente para presentar una reclamación y verificar que se puede satisfacer la reclamación que se le presenta.

Cuando se presenta una reclamación, las aseguradoras requieren que los asegurados ejecuten un proceso formal de reclamo, así como a respuesta a incidentes incluyendo almacenamiento de registros, correos electrónicos, investigaciones forenses y otras evidencias usando métodos que preservan la integridad de la evidencia.

Aquí es claro recalcar que una póliza de Cyber Seguridad NO REEMPLAZA la estructura sólida de un programa de seguridad.

En consecuencia, debe considerarse que el Asegurado reclamante ha de haber desarrollado primero sus Programas de Seguridad y que el Seguro es solo un elemento de Gestión del Riesgo (Transferencia).

Juan Carlos Lancheros Rueda
Cert CILA, BC´s Mech Eng, BC´s B.A, M.I.A, P.M.S, F.M.S.
C.E.O.