

Inspecciones | Valuaciones | Prevención | Ingeniería | Ajustes y peritajes | Capacitación | www.lea-global.com

Circular 03.19

¿QUIÉN NECESITA UN SEGURO CIBERNÉTICO?

EL RIESGO CIBERNÉTICO Y LOS SEGUROS

El riesgo cibernético (“cyberisk”) puede definirse como las pérdidas derivadas del uso de la tecnología de la información y la comunicación, cuando la tecnología está comprometida en su confidencialidad, integridad o en la disponibilidad de los datos, sistemas o servicios.

La industria aseguradora se ha preocupado por el riesgo de cobertura cibernética “oculta o silenciosa”, también llamada “no afirmativa, que podría estar contemplada en los seguros tradicionales (Propiedad, Responsabilidad, marítimos, etc.), que no fueron diseñados especialmente para cubrir estos riesgos, pero en muchos casos si lo hacen por falta de exclusiones. La opinión mayoritaria en el mercado es que cualquier tipo de riesgo cibernético debería ser trasladado a pólizas específicas denominadas de “cobertura afirmativa” dando lugar al nacimiento de un nuevo ramo de seguros.

Esta circular está destinada a analizar el estado actual de este debate, a partir de un análisis de los seguros para riesgos cibernéticos ofrecidos por el mercado, denominados “POLIZAS MULTIRRIESGOS CIBERNÉTICOS”

ANTES QUE NADA, ANALIZAR MIS PÓLIZAS VIGENTES

Hasta hace algunos años, ninguno de los seguros excluía los riesgos cibernéticos; esta situación comenzó a cambiar en Y2K, cuando se comenzaron a introducir exclusiones. El riesgo cibernético no afirmativo, también llamado “silencioso” o “no intencionado” se refiere a las exposiciones desconocidas o no cuantificadas (para las aseguradoras) que se originan a partir de los peligros cibernéticos que pueden disparar distinto tipo de pólizas no específicas para el riesgo cibernético.

Las cláusulas más habituales para la exclusión de riesgos cibernéticos son las cláusulas CL380 y NMA2914 y NMA 2915, las cuales tienen distintos alcances:

	NMA 2914	NMA 2915	CL380
Nombre	Electronic Data Endorsement A	Electronic Data Endorsement B	Institute Cyber Attack Exclusion Clause
¿Distingue daño malicioso y/o no malicioso?	No distingue	No distingue	Se refiere solo a daños maliciosos
Responde por	Consecuencias de incendio / explosión y puede extenderse a otros peligros adicionales (como rotura de máquinas)	Consecuencias de incendio / explosión y puede extenderse a otros peligros adicionales (como rotura de máquinas)	Excluye todos los daños maliciosos excepto que el seguro brinde cobertura de guerra
¿El riesgo cibernético es un riesgo o un disparador de la póliza?	Es un disparador, pero debe registrarse un daño material súbito	Es un disparador, pero debe registrarse un daño material súbito	Es un disparador
¿Cubre la restauración del daño en el sistema cibernético afectado?	Cubre la restauración hasta el estado original.	Cubre el valor del medio afectado y el tiempo para restaurar la información en back up	No cubre
Se usa mayoritariamente en riesgos de	Propiedad (Todo Riesgo) Manufactura y Energía	Propiedad (Todo Riesgo) Manufactura y Energía	Responsabilidad Civil, Construcción

La cláusula LSW 238 se utiliza para amparar las pérdidas provocadas por robos de valores y crímenes realizados por equipos de computación, especialmente en las pólizas integrales bancarias.

Los riesgos silenciosos, o no afirmativos, se pueden ilustrar, por ejemplo, como un malware que infecta un GPS, que podría causar accidentes de aviación, marinos o de automóviles; como un incidente cibernético que provoca un incendio, por ejemplo, a través de un dispositivo conectado a las casas, o como una práctica inadecuada en la gestión de la seguridad informática de una corporación que lleva a un reclamo en una póliza D&O.

Hay pocos ejemplos de ataques cibernéticos que se han materializado como daño físico, ya que el ciber se suele manifestar en forma de pérdidas más intangibles, y no tanto en daños físicos; sin embargo, en 2014 el gobierno alemán informó que un ataque cibernético había provocado daños materiales en una acería cuando un horno fue apagado en forma sorpresiva por hackers que se introdujeron en el sistema de control.

Otro caso de daños materiales fue el ocurrido en centrales nucleares de Irán, en 2010, con el virus Stuxnet. En este caso se produjo el daño varias máquinas centrífugas para enriquecimiento de uranio y fue atribuido al ejército israelí en el contexto del enfrentamiento entre ambos países.

EL ANALISIS DEL RIESGO CIBERNÉTICO


Un análisis de riesgos cibernéticos debe ser realizado en forma previa a la contratación de una póliza de seguros, incluyendo la siguiente metodología de análisis:

- Desarrollo de un perfil de riesgos ¿Cuál de los riesgos (1 al 7) afecta mi actividad?
- Revisión del “wording” de los contratos” existentes (posible cobertura de riesgos silenciosos) y de las pólizas de riesgos afirmativos, ya que hay diferentes pólizas en el mercado.
- Análisis de eventos ocurridos en la propia empresa y en el sector.
- Elaboración de escenarios de pérdidas realistas
- Análisis de las medidas preventivas
- Nivel de encriptación
- Análisis de los planes de contingencia, de recuperación, plan de crisis y de continuidad del negocio

Una de las preocupaciones principales deber ser que la industria cuente con personal preparado para enfrentar contingencias. Algunos “cyber attacks” han provocado caída del sistema de energía o caídas de los sistemas de control; estas contingencias tienen que enfrentarse con planes pre elaborados, ensayados y capacitando al personal (especialmente a partir de simulaciones).

Muchos operadores de salas de control (especialmente en procesos continuos) se han mostrado incapaces de controlar eventos relativamente sencillos como roturas de tuberías, escapes e incluso inundaciones de partes de la planta; preocupa pensar que puede pasar frente a un “general outage” de energía o del propio sistema de control.

Enfrentar el riesgo cibernético implica pensar en el software y hardware (sistemas de control robustos a prueba de “cyber attack”), pero también en la preparación humana frente a toda contingencia y porque además estaremos mejorando la cultura de seguridad en forma integral.

<p>La mañana del 12 de mayo de 2017 nos despertábamos con la noticia de un ciberataque masivo realizado con un ransomware llamado WannaCry que afectó según las estimaciones a más de 300.000 máquinas en 150 países.</p>	<p>Los primeros días tras el ataque fueron de actividad frenética, y pronto aparecerían algunas soluciones parciales al problema, como el célebre mecanismo 'kill switch' descubierto casi por accidente. Marcus Hutchins, el responsable de aquel descubrimiento, acabaría siendo detenido por el FBI meses después por haber realizado ataques de hacking entre 2014 y 2015. Wannacry encriptaba todos los datos del equipo de forma que el usuario no pudiera acceder a ellos salvo con una clave que solo podrían obtener previo pago de un rescate de 300 dólares en criptomonedas ('ransom', de ahí el nombre de esta familia de ataques).</p>
	

¿QUIEN NECESITA UN SEGURO CIBERNÉTICO?

Un buen análisis de riesgos derivará, seguramente, en las siguientes recomendaciones:

Empresas para las cuales se recomienda **en gran medida** la contratación (en forma inmediata) de un Seguro de Riesgos Cibernéticos:

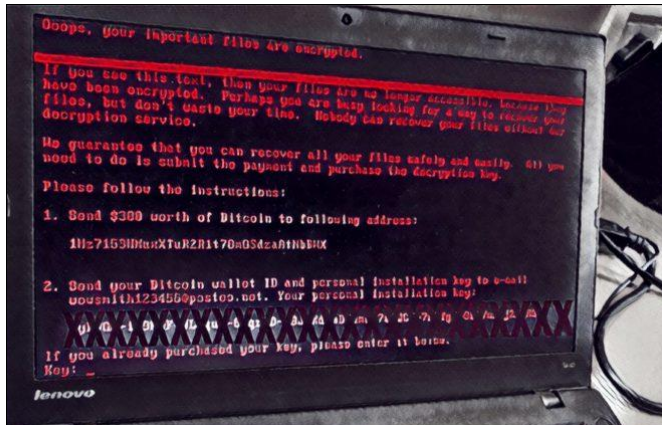
- Las empresas que brindan un servicio “on line”: **Comunicaciones, Servicios de Internet, Retailers, recreación on line, pagos.**
- Empresas con bases de datos personales con registros de valores referidas a cuentas monetarias o no monetarias, como valores (dinero, acciones, o cualquier otro tipo de valor): **Bancos, casas de cambio, Fintech, operadores bursátiles on line y otras**
- Las organizaciones que recopilan información personal sensible (de personas) referidas a su salud, estado civil, domicilio, relaciones y actividades: **Sistemas de salud, hospitales, incluso instituciones educativas.**
- Empresas responsables del funcionamiento de redes de datos o comunicaciones: **Empresas telefónicas, de comunicaciones, programadores, asistencia técnica on-line, sistemas de monitoreo a distancia de alarmas o dispositivos.**

Empresas para las cuales **en ciertos** casos se recomienda la contratación (en forma inmediata) de un Seguro de Riesgos Cibernéticos:

- Las organizaciones que procesan datos confidenciales de otras empresas: **Logística, Tercerización de actividades, servicios profesionales legales y contables.**
- Aquellas que sustentan el negocio en propiedad intelectual exclusiva almacenada en medios electrónicos: **Cine, Patentes, Licencias.**
- Las empresas de servicios públicos que controlan sus operaciones (operación y/o facturación) con internet de las cosas (IOT) o con sistemas industriales de control (ICS): **Suministro de agua, electricidad, transporte de electricidad, municipalidades**
- Posiblemente su empresa tiene varias plantas industriales y su riesgo de daño físico se encuentra diversificado, pero sus empleados utilizan los sistemas centralizados de control de la producción o distribución y no sabrían que hacer si los sistemas fallan: **Manufactura, Industria Pesada.**
- Las empresas que almacenan información en la nube, especialmente si es información confiada por terceros.

Empresas para las cuales se recomienda **en baja proporción** la contratación (en forma inmediata) de un Seguro de Riesgos Cibernéticos:

- Las empresas con servicio “on line” de relativa importancia en el negocio.
- Empresas con bases de datos personales o corporativas de escasa relevancia.
- Las organizaciones que recopilan información personal o corporativa de escasas sensibilidad.
- Empresas en las cuales el análisis de riesgos muestra niveles de restauración del servicio que no ponen en riesgo la integridad financiera de la organización.



Menos de dos meses después de la aparición de WannaCry, atacaba **NotPetya**, un nuevo ransomware que en 2017 causó el caos en diversas organizaciones, entre ellas la alimenticia Mondelez, la naviera Maersk y la farmacéutica Merck & Co.

Mondelez, la empresa de alimentos de USA fue afectada en 1.700 servidores y 24.000 notebooks, hizo una reclamación por los costos de su póliza de seguro de riesgo cibernético que, según dijo, proporcionaba cobertura para “pérdidas físicas o daños a datos electrónicos, programas o software, incluida la pérdida física o daños causados por la introducción maliciosa de un código o instrucción de máquina”. De acuerdo con los documentos judiciales de Mondelez, Zurich inicialmente trabajó para ajustar la reclamación de la manera habitual y en un momento incluso prometió hacer un pago provisional de \$ 10 millones. Pero más tarde se negó a pagar, confiando en una exclusión en la política de "una acción hostil o bélica" por parte de un gobierno o poder soberano o personas que actúen por ellos. La dificultad se debía a que los gobiernos occidentales estaban acusando a Rusia de planificar el ataque de **NotPetya** contra empresas de Ucrania.

NotPetya; tenía la intención de destruir, sabotear e interrumpir los negocios, en lugar de extorsionarlos para obtener ganancias financieras.

En una conferencia, el Director de Finanzas de Merck, Robert Davis, dijo que **NotPetya** había "impactado negativamente los resultados del tercer trimestre, incluido un impacto desfavorable en los ingresos de aproximadamente USD 135 millones por pérdidas de ventas y aproximadamente USD 175 millones en costos, distribuidos entre el costo de los productos vendidos y los gastos operativos anticipamos un impacto similar a los ingresos y gastos en el cuarto trimestre, que se refleja en nuestra guía actualizada".

El informe del segundo trimestre de 2014 de Merck destaca la siguiente cuestión;

“La Compañía tiene cobertura de seguro que asegura los costos resultantes de los ataques cibernéticos. Sin embargo, puede haber disputas con los aseguradores sobre la disponibilidad de la cobertura de seguro para reclamos relacionados con este incidente”.

En marzo de 2019, el ransomware LockerGoga atacó la planta principal de Norsk Hydro en Noruega provocando interrupciones de fabricación con daños de USD 40.000.000.-

COBERTURAS DISPONIBLES

Las diversas pólizas que amparan “riesgos afirmativos” cubren los costos que surgen del impacto en la propia empresa de una vulneración o falta de disponibilidad de datos o un ataque a la red (falta de disponibilidad del sistema), ya sean estas consecuencias a la propia empresa y una responsabilidad frente a terceros.

Entre los daños a la propia empresa, los más importantes son los siguientes:

1. Costos de investigación, de notificación a los afectados y de control de créditos o deudas económicas derivadas de una vulneración de datos
2. Pérdidas por interrupción del negocio/ extra costos para continuar la operación
3. Extorsión cibernética y ransomware.
4. Costos de reemplazar, restaurar y recrear datos dañados o perdidos

En relación con la responsabilidad frente a terceros las coberturas habituales son las siguientes:

1. Responsabilidades por daños personales, responsabilidad por uso de claves para transacciones financieras y costos de defensa y prevención.
2. Responsabilidades asumidas por la seguridad de redes.
3. Responsabilidades frente a autoridades por la privacidad de datos personales, multas y costos de defensa.

En el año 2013 la empresa Target sufrió la violación de datos personales de más de 100 millones de clientes.

Los costos totales de atender la contingencia, incluyendo el incumplimiento de las políticas de privacidad, honorarios legales, las comunicaciones de crisis y los costos forenses alcanzaron a USD 300 Millones.

Target contaba con un seguro de sólo USD 100 millones, con un deducible de USD 10 millones y un sublímite de USD 50 millones para acuerdos con redes de tarjetas de pago. Aunque Target ha resuelto más de 100 demandas presentadas por clientes y socios comerciales, aún enfrenta varias demandas colectivas de accionistas y la pérdida de valor de la empresa.



Los costos "duros" cubiertos por el seguro cibernético muchas veces son solo la punta del iceberg. Las políticas cibernéticas no suelen cubrir daños intangibles como la pérdida de ventas, la caída de la buena voluntad del cliente y la confianza o el daño a la marca.

Hay diferentes tipos de pólizas, con diferentes alcances y wordings. Todas contienen gran cantidad de exclusiones, para las cuales se pueden desarrollar planes "a medida". Algunas de las exclusiones relativas que se identifican en las coberturas, son las siguientes:

- Juego on line, Remates on line, Empresas de provisión de servicios de internet, Sitios de pagos, sitios de entretenimiento para adultos, sitios de monedas virtuales
- Riesgos cibernéticos no maliciosos / falta de fidelidad de empleados
- Peligros naturales
- D&O – Responsabilidades de gerentes y directores
- Valor económico de los datos
- Transferencia ilegal de fondos
- Daños materiales o lesiones, falla de infraestructura, robo de telecomunicaciones
- Huelgas o Guerra

CONCLUSIONES

Al instante de iniciar un Análisis de los Riesgos Cibernéticos en una empresa, las siguientes evidencias empíricas recabadas de la experiencia del mercado de seguros, deben ser tenidas en cuenta:

- 1) Los daños “no intencionales” han sido (en general) de fácil recuperación, en general los planes de contingencia y recuperación ante desastres logran reponer el servicio en tiempos suficientes sin afectar la salud financiera de los afectados.
- 2) Los “ataques” (daños intencionales), logran en cierta proporción sus comprometiendo la salud financiera de largo plazo de las empresas. Una gran proporción de casos (pero de menor cuantía) se relacionan con la transferencia de información confidencial a terceros, los casos más graves son aquellos en los cuales los datos han permitido transferencias ilícitas de valores o de propiedad intelectual, como en el caso de Sony Pictures.
- 3) En menor cantidad de casos, (pero con pérdidas más importantes), se produce la interrupción del negocio (como el caso Playstation,) también ilustrado en el caso Sony.

El caso **SONY**

El 24 de noviembre de 2014, un grupo de hackers, que se identificó con el nombre de "Guardianes de la Paz" (GOP) filtró un lanzamiento de datos confidenciales del estudio de cine **Sony Pictures**. Los perpetradores emplearon una variante del malware del limpiador Shamoon para borrar la infraestructura informática de Sony.

El grupo GOP exigió que Sony retirara su próxima película, *The Interview*, una comedia sobre un complot para asesinar al líder norcoreano Kim Jong-un, y amenazó con ataques terroristas en cines que proyectan la película. Luego de que cadenas de cine de los EE. UU. Optaron por no seleccionar “*The Interview*” en respuesta a las amenazas, Sony eligió cancelar el estreno formal y saltar directamente a un lanzamiento digital.

Los funcionarios de inteligencia de los Estados Unidos, después de evaluar el software, las técnicas y las fuentes de red utilizadas en el hackeo, alegaron que el ataque fue patrocinado por el gobierno de Corea del Norte, quien desde entonces ha negado toda responsabilidad.



Una serie de ataques masivos coordinados durante el fin de semana de 2011 ha tumbado la red PlayStation Network, y ha causado cortes y problemas en Xbox Live, Battle.net, y otras redes de videojuegos online.

Lo que empezó siendo un inocente ataque hacker para reivindicar un mejor servicio en la red de ocio de **Sony**, se ha convertido en un delito federal que ha puesto al FBI en máxima alerta.

Incluso una amenaza de bomba dirigida al avión en el que viajaba el Presidente de Sony Online Entertainment, John Smedley, obligó a desviar el vuelo a un aeropuerto cercano para revisar el aparato.

- 4) Los daños directos en la infraestructura (como incendios o roturas de máquinas) han sido (hasta ahora) de menor importancia y se refieren especialmente a ataques intencionales e ideológicos. La protección de los daños se relaciona con la capacidad de los operadores de detener las instalaciones en forma segura cuando el control automático deja de funcionar. (una serie de casos puede ser recabada en la página www.risidata.com/index.php?/Database/event_date/desc).

- 5) No deben dejarse de lado los casos en los cuales un daño cibernético es consecuencia de un ataque o accidente analógico, como una falta de fidelidad de un empleado o un incendio afecta el servicio on line, como en el caso de UOL adjunto.



El incendio registrado en las oficinas de UOL en el edificio de la calle Florida 537 (Buenos Aires – Argentina), interrumpió los servicios por varios días, influyó de manera decisiva en la decisión de presentar la solicitud del concurso preventivo.

Además de dos víctimas mortales, hubo otras víctimas, los clientes de UOL, entre ellos empresas que tenían albergados sus sitios en los servidores de UOL, como el diario La Gaceta de San Miguel de Tucumán., editorial Perfil, America TV y otras.