Ciberriesgos sistémicos/ Actualización del producto:

Preguntas frecuentes de los corredores

CHUBB®

Octubre de 2021

Chubb se compromete a seguir liderando el sector de los ciberseguros al proporcionar dirección y estructura para ayudar a situarlo en la senda de la sostenibilidad a largo plazo.

Actualmente, la frecuencia y gravedad de los incidentes cibernéticos está llevando a muchas aseguradoras, Chubb entre ellas, a replantearse sus precios y condiciones. En los últimos meses, múltiples ciberataques generalizados han puesto en peligro objetivos que van desde la cadena de suministro de software y los proveedores de seguridad de correo electrónico hasta los servidores de datos y la infraestructura. Los acontecimientos conllevaron varios tipos de ciberataques con el potencial de convertirse en sucesos catastróficos.

Por consiguiente, Chubb está desarrollando soluciones nuevas e innovadoras para gestionar estas exposiciones. Chubb seguirá ofreciendo las principales coberturas cibernéticas que nuestros asegurados y socios de distribución conocen y comprenden; sin embargo, también estamos reestructurando nuestros términos y condiciones en torno a Eventos de impacto generalizado y colaborando con las asociaciones sectoriales y Gobiernos en diferentes formas que podrían brindar una certeza de cobertura más informada para todas las partes.

Impacto en los corredores y en los tomadores cibernéticos

Chubb prevé que nuestras nuevas soluciones proporcionarán a los socios distribuidores más estabilidad a largo plazo y crecimiento en el mercado de los ciberseguros. Los corredores tendrán una nueva oportunidad para demostrar su experiencia a los clientes, incluida la capacidad de ilustrar más claramente el grado de cobertura disponible para exposiciones sistémicas, personalizar los términos y condiciones de las exposiciones específicas del cliente y aumentar las diferentes coberturas con servicios de valor añadido como la mitigación de pérdidas y el asesoramiento sobre riesgos. El nuevo enfoque de Chubb recurrirá a conceptos conocidos por la mayoría de corredores y clientes con experiencia en seguros de propiedad y de daños por catástrofes. Con el tiempo, un enfoque estructurado para cuantificar el ciberriesgo catastrófico debería dar lugar a una mayor capacidad de seguro cibernético en el mercado.

Mercado de ciberriesgos

¿Qué está impulsando los cambios en la estrategia actual de los ciberseguros?

Las amenazas e incidentes cibernéticos están aumentando y evolucionando. En 2020, se publicaron más de 18 000 nuevas vulnerabilidades de software, casi el triple que en 2015, y siguen aumentando sin parar.[1] Entretanto, en 2020 se identificaron cerca de 1,2 millones de nuevas amenazas de malware, más del doble que en 2015.[2] Mientras que tácticas como el ransomware se han vuelto más habituales y costosas, los ataques a los correos electrónicos profesionales y las filtraciones de datos siguen aumentando la frecuencia de los incidentes cibernéticos a niveles máximos, especialmente con el aumento de los programas de teletrabajo. La mayor frecuencia y gravedad de estos ciberataques está ejerciendo presión sobre las ratios de pérdidas por deterioro de las aseguradoras, mientras que las exposiciones sistémicas con potencial catastrófico son cada vez más generalizadas.

¿Comparten otras organizaciones el punto de vista de Chubb sobre el tema del ciberrriesgo sistémico?

Sí, creemos que otras organizaciones, Gobiernos, reguladores y agencias de calificación han observado también la magnitud y la urgencia de este tema. En 2020, el Congreso estadounidense formó la Comisión del Solarium del Ciberespacio, presidida por el senador Angus King (I-ME) y el representante Mike Gallagher (R-WI). Tras un estudio de un año de duración, la Comisión concluyó que Estados Unidos corre el riesgo de sufrir un ciberataque catastrófico y está en una situación «peligrosamente insegura en el ámbito cibernético.[3]

En Europa, la Agencia de Ciberseguridad de la Unión Europea (ENISA) se creó hace más de 15 años para hacer frente al creciente número de incidentes cibernéticos graves que afectan al sector público y privado. Su nuevo informe, publicado en abril de 2021, destaca que, a la luz de las amenazas actuales para la ciberseguridad, la plantilla mundial de ciberseguridad tendría que crecer un 89 % para que las organizaciones puedan defender eficazmente sus activos críticos de tecnologías de la información y comunicaciones (TIC). Para hacer frente a esta situación crítica, los Gobiernos nacionales comenzaron a aplicar una serie de programas y políticas.

En el Reino Unido, el Secretario de Defensa, Ben Wallace, anunció en octubre que el país estaba construyendo un nuevo centro de guerra digital para reforzar la resistencia del Reino Unido a los ciberataques. Además, la agencia de calificación de seguros AM Best informó en junio de 2021 de que «las perspectivas del mercado de los ciberseguros son poco halagüeñas», al apuntar a «las implicaciones de gran alcance de los efectos en cascada de los ciberriesgos y la falta de límites geográficos o comerciales» y concluyó que las aseguradoras «cuyo enfoque de gestión de riesgos es deficiente en lo que respecta a la cibernética pueden encontrarse expuestas a un riesgo de acumulación más allá de [su] tolerancia al riesgo y podrían enfrentarse a presiones en términos de calificación.[4]

Visite los siguientes enlaces para acceder a las observaciones de otras organizaciones:

- Executive Order on Improving the Nation's Cybersecurity (US Government): www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
- Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market (US Government Accountability Office): www.gao.gov/products/gao-21-477
- Cyber Insurance Rates Could Rise 50% in 2021 (MarshMcLennan Agency): www.marshmma.com/blog/cyber-insurance-rates-could-rise-50-in-2021
- Balancing Risk and Opportunity Through Better Decisions (Aon): www.aon.com/2021-cyber-security-risk-report/

¿En qué se diferencia la estrategia de Chubb de la del sector?

La mayor parte del sector de los ciberseguros se centra solo en las cuestiones de ransomware y la adecuación de las tarifas, y está abordando estas cuestiones reduciendo la capacidad, aumentando las tarifas y haciendo ajustes en la suscripción de coberturas específicas o sectoriales. Aunque Chubb está adoptando medidas similares, también aprovechamos décadas de experiencia y nuestra dimensión considerablemente mayor para centrarnos en el problema mucho más amplio de las exposiciones sistémicas. Otras empresas han hablado sobre esta necesidad en nuestro sector, pero hasta la fecha se han adoptado escasas medidas. Es probable que Chubb lidere el movimiento en este ámbito.

¿Pueden las técnicas avanzadas de sucripción cibernética mitigar el riesgo de cibercatástrofes?

Chubb cuenta con un equipo específico de ingenieros y suscriptores de riesgos cibernéticos, y estamos introduciendo nuevas herramientas de análisis de amenazas y de IA en nuestros procesos de suscripción. Además, proporcionamos a nuestros tomadores de seguros cibernéticos acceso a un paquete completo de servicios de prevención y mitigación de pérdidas. Nuestra inversión proactiva en estas áreas ha propiciado que los resultados de los seguros cibernéticos de Chubb superen a los del sector de los ciberseguros en general.[5] A pesar de estas importantes inversiones, muchas amenazas cibernéticas están diseñadas específicamente para evadir los controles internos y las mejores prácticas. Ningún control de suscripción o de prevención de pérdidas puede descartar por completo el riesgo de cibercatástrofes.

¿Qué es la ciberexposición sistémica? ¿Cómo define Chubb este término?

En nuestra opinión, «sistémica» se refiere a una exposición que tiene el potencial de afectar a muchos clientes debido a las coincidencias o elementos comunes de la exposición, mientras que «catastrófico» se refiere a un riesgo sistémico que se manifiesta en forma de pérdidas importantes o graves para muchos asegurados.

¿Qué ciberriesgos catastróficos han surgido en los últimos años?

La dependencia cada vez mayor de la tecnología por parte de empresas y consumidores, así como la interconectividad de las tecnologías y los socios, han creado un entorno en el que los ciberriesgos pueden crecer exponencialmente. Los eventos cibernéticos también están teniendo un impacto más generalizado. En un periodo de 100 días, de diciembre de 2020 a marzo de 2021, varios ataques masivos pusieron en peligro distintos objetivos, desde cadenas de suministro de software y proveedores de seguridad de correo electrónico hasta servidores de datos e infraestructuras municipales. En total, más de 100 000 organizaciones de todo el mundo se vieron afectadas por estos eventos, lo que provocó alteraciones para millones de clientes y ciudadanos y también pérdidas económicas sustanciales. A modo de ejemplo, el ataque a una cadena de suministro de software, conocido como Solorigate, en el que se insertó un código malicioso en una actualización de un software de análisis de redes de confianza, afectó a 20 000 empresas y agencias gubernamentales. Este acontecimiento habría podido ser mucho peor si la intención hubiera sido robar o destruir datos críticos u otra información.

Los siguientes tipos de riesgos, especialmente combinados, tienen el potencial de convertirse en sucesos catastróficos.

Ataque de Vulnerabilidad Grave Generalizado:
Algunas vulnerabilidades de software conocidas que carecen de parches pueden ser graves, ya que son fáciles de aprovechar, se pueden desplegar remotamente con privilegios de acceso limitados y causan un impacto adverso considerable.[6]

Ataque Grave de Día Cero:
Algunas vulnerabilidades de software que son conocidas por los ciberdelincuentes, pero todavía no por el resto, se pueden aprovechar fácilmente, son potencialmente graves y a menudo carecen de protección.

Ataque a la Cadena de Suministro de Software:
Estos ataques son troyanos que permiten que los ciberdelincuentes entren en los sistemas a través de un software certificado y fiable.

Interrupciones en las infraestructuras:
Las infraestructuras críticas de la sociedad, como las redes eléctricas y los servicios de telecomunicaciones, se enfrentan a un riesgo potencial de fallo de dimensiones enormes, ya sea debido a un ciberataque o a incidentes cibernéticos no maliciosos, incluyendo fallos en el sistema, errores humanos o errores de programación. El ataque a principios de este año a Colonial Pipeline, la empresa de suministro de combustible a la costa este de Estados Unidos, aprovechó una interrupción de la infraestructura a través de un ataque de ransomware que provocó escasez de combustible para millones de ciudadanos y empresas en varios estados.

Resto de Eventos Generalizados:
Existen algunos tipos de ciberataques que pueden llevarse a cabo simultánea y automáticamente contra un gran número de víctimas, provocando en última instancia un suceso cibernético catastrófico. Internet y algunos servicios de telecomunicaciones han alcanzado el nivel de infraestructura crítica para la sociedad, y algunas empresas grandes de computación en la nube son tan utilizadas que una interrupción generalizada afectaría a las operaciones comerciales de miles o millones de empresas.

Casos de ransomware:
Aunque no son necesariamente sistémicos en sí, los ataques de ransomware, que secuestran información o archivos electrónicos de empresas o personas específicas hasta que se paga un rescate, se están llevando a cabo actualmente con una eficiencia industrializada, con un aumento constante de los rescates solicitados. Algunos ataques destructivos pueden disfrazarse de ransomware, como NotPetya y WannaCry.

El mercado de los ciberseguros lleva años debatiendo sobre el ransomware. ¿Ha cambiado la visión de Chubb ahora?

Llevamos varios años analizando las tendencias de ransomware y, a medida que estas tendencias han ido evolucionando, también lo han hecho nuestras estrategias de suscrip-ción. Para ayudar a gestionar los riesgos, hemos respondido con cambios en la estrategia de suscripción (por ejemplo, evitando determinadas clases o negocios que carecen de ciertos controles), retenciones, límites y coaseguros. Chubb también está aplicando la suscripción basada en señales para estos riesgos, que analiza los factores ponderados y las señales de riesgo obtenidas de diversas fuentes internas y externas para ayudarnos a identificar los factores de riesgo de los clientes actuales y potenciales. La nueva oferta de ciberproductos de Chubb tendrá todavía más formas de configurar sublímites, coaseguros y retenciones para casos de ransomware en múltiples acuerdos de seguro.

¿Cuántos siniestros por ciberriesgos sitémicos ha recibido Chubb hasta ahora?

En los últimos nueve meses, Chubb ha recibido cientos de avisos cibernéticos asociados a grandes eventos de impacto generalizado.

¿Por qué seguimos viendo tantos cambios en el mercado de cyber? ¿Ha experimientado el sector de los seguros cambios similares en otras líneas de negocio?

Los seguros cibernéticos realmente alcanzaron la madurez hace pocos años e incluso hoy son una línea de seguros en plena transformación. En paralelo, los riesgos cibernéticos son dinámicos y aumentan rápidamente en complejidad y gravedad. Históricamente, el mercado de los seguros de propiedad ha sufrido turbulencias debido a eventos repentinos de una magnitud sin precedentes, como el terremoto de San Francisco de 1906 y los ataques terroristas del 11 de septiembre. Las soluciones se desarrollaron tras registrarse estos eventos y proporcionaron mayor claridad en torno a los peligros inminentes, favoreciendo así el desarrollo de coberturas separadas para riesgos catastróficos.
Con los seguros cibernéticos, tenemos la oportunidad de actuar ahora para mejorar el diseño de los productos, así como la posibilidad de crear soluciones con los Gobiernos con vistas a proporcionar estabilidad al mercado de los seguros y seguridad de cobertura para los clientes.

Oferta de productos de Cyber de Chubb

¿Seguirá Chubb ofreciendo las mismas coberturas cibernéticas que ofrece ahora?

Seguirán estando disponibles las mismas coberturas principales que ofrecemos actual-mente: gastos de respuesta a incidentes, ciberriesgo de primera parte, responsabilidad cibernética de terceros y responsabilidad profesional. Además, Chubb distingue entre Eventos de impacto limitado y Eventos de impacto generalizado. Prevemos que nuestros productos principales se ajustarán a una estimación del 90 % de las pérdidas históricas en las coberturas estándar de Eventos de impacto limitado.

Chubb cubrirá los riesgos por deterioro significativos, y también ofrecerá coberturas adicionales para exposiciones sistémicas con potencial catastrófico y generalizado como ampliaciones del ciberseguro principal, lo que nos permite ofrecer estas coberturas de una manera más estructurada y sostenible. Se denominarán colectivamente coberturas de Eventos de impacto generalizado, e incluirán los distintos subelementos descritos en la póliza. Los Eventos de impacto generalizado y cada subcomponente estarán sujetos a un límite, una retención y un importe de coaseguro específicos. Funciona de manera similar a la gestión llevada a cabo por los seguros de propiedad en caso de riesgos catastróficos como inundaciones y terremotos durante más de un siglo.

¿Qué tipos de ampliaciones de cobertura podemos esperar?

Chubb incorporará varias mejoras en la cobertura dentro del producto principal de seguro de cyber que anteriormente solo se ampliaba mediante suplemento. Entre ellas se encuentran las ampliaciones secundarias, como las multas reglamentarias, las multas e inspecciones del sector de las tarjetas de pago (PCI), el daño a la reputación, el fraude por transferencia engañosa, el cierre preventivo, etc. Chubb también ofrecerá ampliaciones de cobertura separadas para dar cabida a los Eventos de impacto generalizado, como los Ataques a la Cadena de Suministro de Software, los Ataques Graves de Día Cero y los Ataques de Vulnerabilidad Grave Generalizado. El gráfico de la izquierda ofrece una visión general de este desglose. Los clientes existentes y potenciales tendrán que trabajar con su corredor para determinar los ciberriesgos únicos a los que se enfrentan en sus operaciones y entorno informático, y después seleccionar las ampliaciones de cobertura más adecuadas para ellos.

¿Va Chubb a cambiar los precios para las cobeturas de ciberseguros?

Los precios seguirán reflejando las necesidades específicas de cobertura y el perfil de riesgo de cada cliente. Cuando se requiera la aprobación jurisdiccional para expedir un seguro sobre una base aceptada, se hará una presentación de tarifas actualizada, y suscribiremos y acordaremos el precio según estas tarifas actualizadas.

¿Cuándo entrarán en vigos estos cambios en los productos?

Chubb ya ha utilizado este nuevo enfoque en Major Accounts, y lo ampliaremos a otros segmentos del mercado en los próximos meses. Es fundamental empezar a trabajar con los gestores de riesgos de sus clientes con bastante antelación a sus renovaciones para identificar sus riesgos específicos y explorar las ampliaciones de cobertura que les proporcionarán la protección adecuada. El lanzamiento del nuevo enfoque sobre una base aceptada dependerá de las tramitaciones específicas para cada zona geográfica y estado, que se espera que empiecen a hacerse efectivas a partir de enero de 2022.

¿Habrá un documento de ventas que podamos adjuntar al formulario para explicar las ventajas?

Sí, se puede descargar un resumen del producto.

Proceso de suscripción

¿Qué puedo hacer para prepararme para estos cambios? ¿Podré disponer de recursos que me ayuden en mis negociaciones con clientes exitentes y potenciales?

Además de leer y comprender estas preguntas frecuentes, le animamos a que aproveche la formación y los seminarios web que Chubb organizará. A lo largo del año se facilitarán materiales como informes, seminarios web y vídeos que podrá compartir con sus asegurados. Visite chubb.com/es/cyber o póngase en contacto con su suscriptor de cyber de Chubb para obtener más información.

Cotización

¿Existen determinadas consideraciones de suscripción sobre las que se basan la cobertura sistémica y los precios que ofrece Chubb?

Sí. Diversos factores determinarán la cobertura sistémica y el precio ofrecido por Chubb, como las dependencias críticas de la organización, las garantías contractuales con los proveedores de servicios, la higiene y los controles de ciberseguridad, y la planificación y las pruebas de respuesta ante incidentes/resiliencia.

¿En qué consiste el cambio de la estructura de precios de la cobertura de Eventos de impacto generalizado?

Chubb se compromete a ofrecer transparencia a todos los clientes y brindará opciones separadas de precios, límites y retención para la cobertura sistémica.

Formato de póliza

¿Qué cobertura se excluye en los nuevos productos de Cyber de Chubb?

No se excluye la cobertura de los Eventos de impacto generalizado. Se está estructurando de manera que se ofrezca de forma transparente capacidad para los eventos cubiertos. Los asegurados tienen la opción de contratar la cobertura de Eventos de impacto generalizado, pero no es obligatoria.

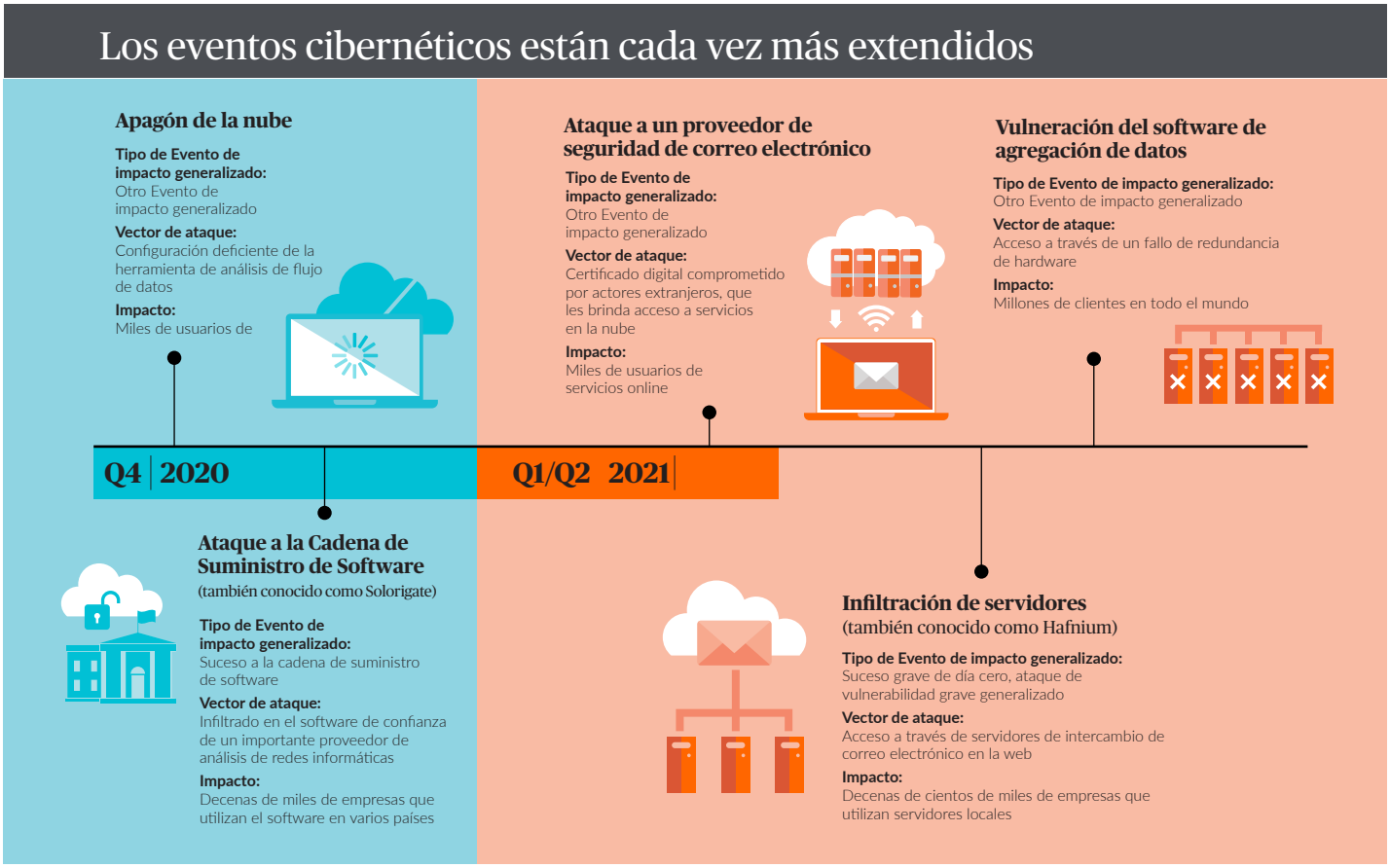
¿Dónde se describen en la póliza los concepros de Eventos de impacto limitado y Eventos de impacto generalizado?

En la primera página de la póliza se establece que los ciberincidentes se clasificarán como Eventos de impacto limitado o como Eventos de impacto generalizado; estas definiciones se describen en la sección II de la póliza. Otras definiciones clave utilizadas dentro de estos conceptos son las de Catalizador generalizado y Grupo de impacto limitado, entre otras.

En el caso de las pólizas que ofrecen los mismos límites, retenciones y coaseguros para todos los tipos de Eventos de impacto generalizado, no es importante diferenciar entre las cuatro subcategorías de Eventos. Sin embargo, si existen límites, retenciones o coaseguros diferenciados, se deben revisar las siguientes definiciones de la subcategoría de Eventos de impacto generalizado:

- Ataque de Vulnerabilidad Grave Generalizado
- Ataque Grave de Día Cero
- Ataque a la Cadena de Suministro de Software
- Resto de Eventos Generalizados

La sección X de la póliza aborda las «Obligaciones en caso de ciberincidente» y describe detalladamente cómo el asegurado y Chubb colaborarán en caso de un Ciberincidente. Esto incluye información sobre el calendario y los métodos para determinar si un Ciberincidente es un Evento de impacto limitado o un Evento de impacto generalizado. Como siempre, la póliza debe leerse en su totalidad.



¿Puede dar ejemplos de algún caso histórico real de Eventos de impacto generalizado?

En el gráfico anterior se muestran ejemplos de Eventos de impacto generalizado recientes.

¿Cómo funciona el coaseguro? ¿Puede exponer un ejemplo?

El coaseguro aplicable a los Eventos de Impacto Generalizado; Ataque Ransomware y Evento de software vulnerable es un coaseguro «minimizador de pérdidas», lo que implica que el coaseguro del tomador de la póliza no erosiona los límites del seguro. En cambio, la responsabilidad de cada pérdida se reparte entre el asegurado y la aseguradora, y la parte de la aseguradora está sujeta al límite aplicable para ese riesgo.

Por ejemplo, si la póliza tiene un sublímite general del 5 % del límite global de la póliza de 10 millones de dólares para eventos de impacto generalizado, la responsabilidad máxima de la aseguradora para cualquier pérdida por evento de impacto generalizado en virtud de ese sublímite de evento de impacto generalizado sería de 500.000 dólares (es decir, el 5 % de 10 millones de dólares).

Si la cobertura de un evento de impacto generalizado está sujeta a un coaseguro del 50%, entonces un evento de pérdida de 1 millón de dólares se repartiría entre el asegurado y la aseguradora al 50 %, y el sublímite de evento de impacto generalizadose agotaría entonces porque la aseguradora habría pagado la totalidad del sublímite disponible de 500.000 dólares.

Alternativamente, una pérdida de 500.000 dólares por evento de impacto generalizado también se repartiría al 50 %, pero como la aseguradora solo pagaría 250.000 dólares en esta situación, quedarían 250.000 dólares en virtud del sublímite de evento de impacto generalizado para futuros casos.

Notas finales

1. Base de datos National Vulnerability Database del National Institute of Standards and Technology. Consultada en https://nvd.nist.gov/vuln/search
2. Instituto AV-TEST (2021). Consultado en www.av-test.org/en/statistics/malware/
3. La Comisión Federal advierte de la situación peligrosamente insegura de Estados Unidos frente al Riesgo de ciberataques catastróficos (2020). Consultado en www.forbes.com/sites/daveywinder/2020/03/14/make-america-safe-again-federal-commission-warns-us-at-risk-of-catastrophic-cyber-attack/?sh=244402e34d27
4. Problemas de ransomware y agregación exigen nuevos enfoques al ciberriesgo (2021).
5. Consultado en www.insurancejournal.com/research/research/ransomware-and-aggregation-issues-call-for-new-approaches-to-cyber-risk/
6. Ibid.
7. Tendencias de las vulnerabilidades de seguridad en 2020 según NIST: Análisis (2021). Consultado en www.redscan.com/media/Redscan_NIST-Vulnerability-Analysis-2020_v1.0.pdf

Acerca de Chubb

Chubb es la mayor aseguradora de propiedad y responsabilidad civil que cotiza en bolsa. Con operaciones en 54 países y territorios, Chubb ofrece seguros de propiedad y responsabilidad civil comerciales y personales, seguros de accidentes personales y de salud complementarios, reaseguros y seguros de vida a un grupo diverso de clientes. Como compañía experta en suscripción, evaluamos, asumimos y gestionamos los riesgos con perspectiva y disciplina. Atendemos y gestionamos nuestros siniestros de forma equitativa y rápida. La empresa también se caracteriza por su extensa oferta de productos y servicios, su amplia capacidad de distribución, su excepcional solidez financiera y su presencia local en todo el mundo. La sociedad matriz, Chubb Limited, cotiza en la Bolsa de Nueva York (NYSE: CB) y forma parte del índice S&P 500. Chubb tiene oficinas ejecutivas en Zúrich, Nueva York, Londres, París y otros lugares, y una plantilla de aproximadamente 31 000 profesionales en todo el mundo. Puede obtener más información en www.chubb.com.

Para obtener más información sobre la experiencia y los conocimientos de Chubb en materia de gestión de riesgos cibernéticos, visite chubb.com/es/cyber

Chubb. Insured.℠

Chubb European Group SE, Sucursal en España, con domicilio en el Paseo de la Castellana 141, Planta 6, 28046 Madrid y C.I.F. W-0067389-G. Inscrita en el Registro Mercantil de Madrid, Tomo 19.701, Libro 0, Folio 1, Sección 8, Hoja M346611, Libro de Sociedades. Entidad Aseguradora, cuyo capital social es de 896.176.662€, con sede en Francia y regulada por el código de seguro francés, inscrita en el Registro Comercial de Nanterre con el número 450 327 374 y domicilio social en la Tour Carpe Diem, 31 Place des Corolles, Esplanade Nord, 92400 Courbevoie, France. Supervisada por la Autorité de Contrôle Prudentiel et de Résolution (ACPR), 4, Place de Budapest, CS 92459, 75436 PARIS CEDEX 09 y por la Dirección General de Seguros y Fondos de Pensiones, con código de inscripción E-0155.