Ciberriesgos catastróficos –
Una preocupación en aumento

CHUBB®

los incidentes cibernéticos pueden provocar pérdidas que no están limitadas en el espacio o el tiempo

Con la digitalización del mundo actual, se ha incrementado la frecuencia, gravedad y sofisticación de los incidentes cibernéticos, junto con la dependencia de la tecnología. Las vulnerabilidades y exposiciones se multiplican debido al aumento de la interconectividad, creando riesgos sistémicos que son enormes, crecientes y no son fáciles de detectar o controlar. Al combinar estas dimensiones sistémicas de los riesgos con unas consecuencias potencialmente graves y generalizadas, se dan las condiciones para una catástrofe cibernética.

Al igual que las pandemias, los incidentes cibernéticos pueden provocar pérdidas que no están limitadas en el espacio o el tiempo. Ya no es algo teórico, los ciberdelincuentes han demostrado su capacidad para alterar las cadenas de suministros de empresas de todo el mundo y paralizar infraestructuras críticas, como sucedió en el ataque reciente a Colonial Pipeline, que interrumpió el suministro de combustible a la costa este de Estados Unidos. Los incidentes cibernéticos recientes han causado miles de millones de dólares en pérdidas económicas, así que no es difícil imaginar un ataque catastrófico que pueda poner a prueba la capacidad de balance del sector de los seguros.

A diferencia de catástrofes imprevistas anteriores, estamos asistiendo a una intensificación rápida y continua de los ciberriesgos. Este aviso anticipado es una oportunidad para pasar a la acción ahora y contribuir a garantizar que existan las defensas cibernéticas y las protecciones económicas adecuadas cuando ocurran catástrofes inevitables.

Los seguros de cyber llegan a su mayoría de edad

El aumento constante en la adopción de seguros de cyber significa que cada vez más empresas están protegidas, pero el ciberriesgo agregado se está extendiendo entre el sector de los seguros.

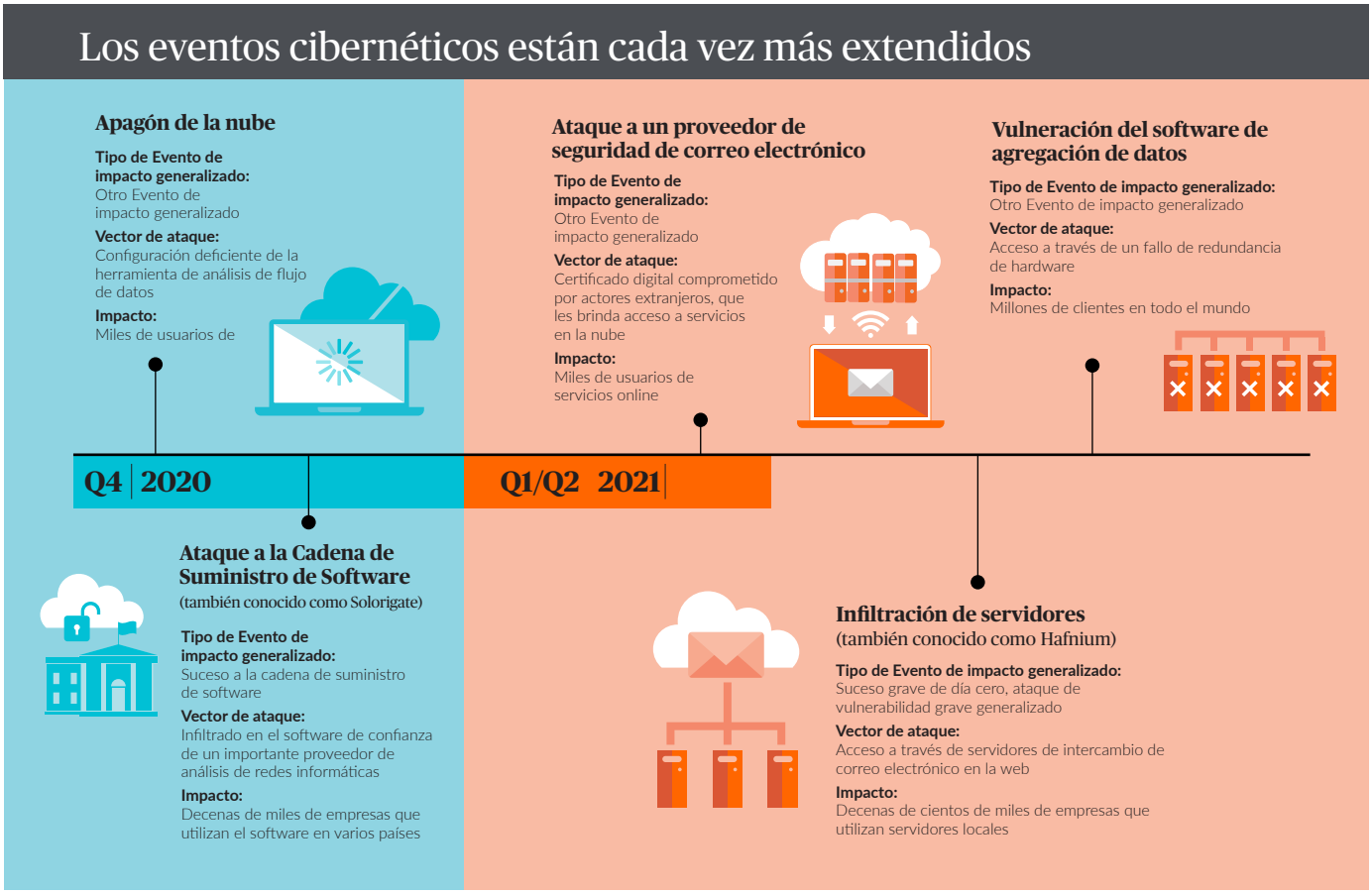
La promesa de un seguro de cyber se ha hecho plenamente efectiva en los últimos años. Las aseguradoras han pagado las pérdidas después de importantes ciberataques y han contribuido a proteger a numerosas organizaciones en todo el mundo.

Actualmente, las principales coberturas – costes de respuesta a incidentes, ciberriesgo de primera parte, responsabilidad cibernética de terceros, responsabilidad profesional/errores y omisiones – proporcionan soluciones y gestión del riesgo importantes a empresas de todos los tamaños y sectores. Además, los servicios de gestión del ciberriesgo ofrecidos por los operadores han resultado muy útiles para ayudar a las empresas a mitigar el riesgo y mejorar sus defensas tecnológicas en la interfaz de usuario, mientras que los equipos de respuesta a incidentes han demostrado su efectividad a la hora de restablecer rápidamente la conexión de las empresas tras un evento cibernético.

El aumento constante en la adopción de seguros de cyber - estimado ahora en unas 4 millones de pólizas para las aseguradoras de líneas adicionales domiciliadas en EE.UU. y fuera de este país, y con cerca del 50 % de las empresas estadounidenses cubiertas, según un informe de la Oficina "Government Accountability" de mayo de 2021[1] - significa que cada vez más empresas están protegidas, pero el ciberriesgo agregado se está extendiendo entre el sector de los seguros.

Al mismo tiempo, las empresas también han mejorado su resiliencia cibernética en los últimos años. En 2020, el 53 % de los profesionales informáticos y de seguridad declararon que sus empresas habían alcanzado un alto nivel de resiliencia cibernética, comparado con el 35 % en 2015.[2]

Aunque los seguros de cyber están desempeñando claramente un papel cada vez más importante a la hora de mitigar la ciberexposición de las empresas, la capacidad de las aseguradoras para absorber el potencial de pérdida total a largo plazo no está tan clara.



Intensificación de los riesgos y el impacto

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.

A pesar de que las empresas son más conscientes de los ciberriesgos y sus consecuencias, las amenazas e incidentes cibernéticos no han hecho más que aumentar y evolucionar.

En 2020, se publicaron más de 18 000 nuevas vulnerabilidades de software, casi el triple que en 2015, y siguen aumentando sin parar.[3] Entretanto, en 2020 se identificaron cerca de 1,2 millones de nuevas amenazas de malware, más del doble que en 2015.[4] Entre las violaciones de seguridad de surtieron efecto en 2020, el 85 % implicaron un elemento humano, como programas de ingeniería social.[5]

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 durante la pandemia de COVID-19 y los amplios sistemas de teletrabajo implantados como resultado.

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. Más de 100 000 organizaciones de todo el mundo se vieron afectadas por estos eventos.

En uno de estos eventos, conocido como Solorigate, se descubrió que un ataque masivo a cadenas de suministros, en el que se había insertado un código malicioso en una actualización de un software de análisis de redes de confianza, había pasado desapercibido durante casi ocho meses. El ataque afectó a 20 000 empresas y a gencias gubernamentales.

En otro evento, un grupo de supuestos actores del Estado-nación y mafias criminales conocido como Hafnium aprovechó una vulnerabilidad entonces desconocida («día cero») en un software común para acceder a servidores locales de potencialmente cientos de miles de empresas.

Los incidentes graves aumentan la tensión

¿Cuándo se producirá un evento de cyber realmente catastrófico que sea a la vez general y destructivo?

Aunque los eventos de Solorigate y Hafnium fueron generalizados y costosos, podría haber sido peor. Parece que el motivo principal en ambos ataques era el espionaje, pero si la finalidad hubiera sido robar o destruir datos críticos u otra información, las consecuencias económicas podrían haberse multiplicado fácilmente. Según dijo Kevin Mandia, Director General de la empresa de ciberseguridad FireEye, en su declaración ante la Comisión de Inteligencia del Senado, los actores del ataque de Solorigate tenían el acceso necesario y la capacidad necesaria si hubieran querido ser más perjudiciales.

Para ilustrar mejor la situación, en 2017 el ataque de NotPetya aprovechó un software de impuestos llamado M.E.Doc utilizado casi exclusivamente en Ucrania, pero después el malware se extendió indiscriminadamente y al final afectó a importantes empresas de Europa, Estados Unidos y otras partes, lo que provocó unas pérdidas estimadas de 10 000 millones de dólares. Algunas empresas que fueron víctimas del ataque de NotPetya sufrieron pérdidas superiores a los 100 millones de dólares. Si este tipo de malware destructivo se hubiera empleado en los ataques de Solorigate o Hafnium, los daños económicos combinados hubieran podido ser exponencialmente mayores que los del evento de NotPetya.

Ese mismo año, el ataque del ransomware WannaCry afectó a más de 200 000 ordenadores en todo el mundo. Afortunadamente, utilizó una vulnerabilidad conocida que ya contaba con un parche, por lo que la mayoría de usuarios resultaron inmunes. Sin embargo, como en el ejemplo de Hafnium expuesto anteriormente, el impacto podría haber sido mucho más generalizado y grave si hubiera empleado una vulnerabilidad de día cero.

Hasta la fecha, hemos visto eventos muy generalizados (Solorigate, Hafnium) y eventos destructivos (NotPetya, WannaCry), pero realmente no ha habido catástrofes cibernéticas a la vez generalizadas y graves. Ante la perspectiva de las enormes pérdidas potenciales, ¿Cuándo se producirá un evento de cyber realmente catastrófico que sea a la vez general y destructivo?

Ciberriesgos potencialmente catastróficos

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 siguientes tipos de eventos, especialmente combinados, tienen el potencial de convertirse en catastróficos.

Ataques de Vulnerabilidad Grave Generalizado:
Diariamente se publican de media unas 50 nuevas vulnerabilidades de software. Si no se aplicaran parches, podrían ser aprovechadas para atacar. Aproximadamente el 15 % son graves, es decir, son fáciles de explotar, se pueden desplegar remotamente con privilegios de acceso limitados y causan un impacto adverso considerable. Como las vulnerabilidades graves son generalizadas y se pueden identificar en las redes de víctimas potenciales a través de las técnicas habituales de escaneado por Internet, las empresas que no aborden las vulnerabilidades de software graves corren el riesgo de ser víctimas.

Ataques Graves de Día Cero:
Las vulnerabilidades de software de día cero son conocidas por los ciberdelincuentes, pero todavía no por el resto. Son especialmente preocupantes porque algunas son fácilmente explotables, potencialmente graves y a menudo carecen de protección. Dicho de otro modo, incluso las empresas con buenos programas de gestión de cyber pueden verse expuestas a los Ataques Graves de Día Cero.

Ataques a la cadena de Suministro de Software:
Los ataques a la cadena de suministro de software son troyanos que permiten que los ciberdelincuentes entren en los sistemas a través de un software certificado y fiable. La operación Solorigate demostró el alto grado de sofisticación de los adversarios al explotar prácticas de desarrollo de software comunes utilizadas en el sector tecnológico. Se espera que estos ataques, muchos de los cuales parecen ser dirigidos o patrocinados por actores estatales, continúen e incluso aumenten. Las fricciones geopolíticas, especialmente entre Occidente y sus adversarios, seguirán agravando esta amenaza.

Interrupciones en las infraestructuras:
Los ataques y otros incidentes de cyber que implican infraestructuras pueden tener consecuencias generalizadas. Por ejemplo, en el ataque de mayo de 2021 a Colonial Pipeline, la empresa de suministro de combustible a la costa este de Estados Unidos, los ciberdelincuentes extranjeros aprovecharon una interrupción de la infraestructura a través de un ataque de ransomware, lo que empeoró el impacto. Como resultado, el oleoducto tuvo que cerrar durante varios días, provocando una escasez de combustible que afectó al 45 % del suministro americano para millones de ciudadanos y empresas de varios estados. El riesgo de interrupción en las infraestructuras es único puesto que puede derivarse de un ciberataque, pero también de fallos en el sistema, errores humanos, errores de programación u otros tipos de incidentes cibernéticos no maliciosos.

Resto de Eventos Generalizados:
Existen algunos tipos de ciberataques que pueden llevarse a cabo simultáneamente y automáticamente contra un gran número de víctimas. Internet y algunos servicios de telecomunicaciones han alcanzado el nivel de infraestructura crítica para la sociedad, con lo que el riesgo potencial de fallo adquiere una magnitud enorme. En algunos casos, una empresa de telecomunicaciones puede ser la única proveedora de una ciudad grande o mediana. En otros casos, algunas empresas grandes de computación en la nube se utilizan tanto que una interrupción generalizada afectaría a las operaciones comerciales de miles o millones de empresas distintas al mismo tiempo. Cualquier ataque de este tipo capaz de un despliegue masivo podría provocar un evento cibernético catastrófico.

Ataques de ransomware:
Aunque no son necesariamente catastróficos 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. Las demandas típicas, que empezaron con unos miles de dólares, se han disparado hasta las decenas de millones, y todas las organizaciones, tengan el tamaño que tengan, pueden ser objetivo de los delincuentes.

Reforzar la ciberresiliencia

es más crítico que nunca que las empresas se preparen para una posible catástrofe cibernética.

Debido a la intensificación de los ciberriesgos – directamente, a través de la naturaleza de las operaciones y entornos informáticos, e indirectamente, a través del fallo de infraestructuras comunes o ciberdelincuentes que explotan las vulnerabilidades – es más crítico que nunca que las empresas se preparen para una posible catástrofe cibernética.

Una buena manera de empezar es entendiendo las exposiciones específicas a las que puede enfrentarse cada organización desde la perspectiva de los posibles eventos descritos en este informe, y después dedicando los recursos necesarios a mejorar las defensas y la resiliencia cibernética. Los proveedores de IT compartidos representan riesgos sistémicos importantes, por eso las organizaciones tienen que realizar procesos de diligencia debida exhaustivos sobre estos proveedores y generar redundancia y resiliencia en torno a ellos, además de administrar sus contratos de cerca y auditar y revisar anualmente su desempeño en materia de ciberriesgos.

Asimismo, las organizaciones deben aprovechar al máximo la experiencia que les brinda su corredor o agente de seguros y su compañía de seguros cyber. Aunque los equipos de TI, gestión de riesgos y continuidad del negocio pueden confiar en su protección cibernética y las medidas de respuesta a incidentes, ninguna organización puede estar nunca totalmente protegida de todos los incidentes potenciales, especialmente los catastróficos.

Muchas compañías de seguros ofrecen una variedad de servicios preincidentes para ayudar a las empresas a mejorar su posición de defensa cibernética, como evaluaciones de preparación para la respuesta, análisis comparativos de desempeño en seguridad, pruebas de vulnerabilidad de la red y simulaciones de ataques comunes. Las organizaciones también deberían estar bien preparadas para responder cuando se produzca un incidente cibernético. Un equipo de expertos en respuesta a incidentes de la aseguradora puede ayudar a limitar los daños de dichos eventos y restablecer la plena operatividad de la organización lo antes posible. Estos servicios pueden marcar la diferencia entre simplemente sobrevivir a un evento cibernético grave o avanzar con confianza.

Ofrecer soluciones

Los ciberseguros, al igual que los seguros de daños, están expuestos a eventos catastróficos.

Desde una perspectiva global, los ciberataques catastróficos tienen el potencial de paralizar los negocios y paralizar las infraestructuras críticas. Al igual que en el caso de la pandemia de coronavirus, esto requiere que el gobierno y el sector privado trabajen juntos en temas importantes, como la divulgación y notificación de incidentes cibernéticos para mejorar la coherencia de los datos y el establecimiento de marcos legales para disuadir y castigar a los ciberdelincuentes.

La frecuencia y gravedad de los incidentes cibernéticos está llevando a las aseguradoras a replantearse sus precios y condiciones. El desarrollo de un mercado estable para los seguros cibernéticos al tiempo que se responde al posible aumento de estos riesgos catastróficos exigirá nuevas soluciones a nivel macro y societal, y también en las ofertas de productos de las aseguradoras individuales. Para el sector de los seguros, el reto es cómo diseñar pólizas que proporcionen seguridad en la cobertura, protección efectiva, y ayuden a gestionar los ciberriesgos de desgaste y catastróficos para clientes y aseguradoras.

Tradicionalmente, las aseguradoras han cubierto los eventos catastróficos de la propiedad, como inundaciones y terremotos, con pólizas separadas para valorar de manera transparente y controlar estas exposiciones. Este proceso ha contribuido a mantener la estabilidad general del mercado y la disponibilidad de coberturas. Por ejemplo, aunque muchos de los principales fenómenos como terremotos, inundaciones y huracanes de los últimos cincuenta años han sido casos de ingresos materiales para el sector de los seguros de propiedad y responsabilidad civil, raramente han desembocado en insolvencias de las aseguradoras. Por ello, el sector de los seguros ha permanecido resiliente y estable para los asegurados, incluso después de acontecimientos catastróficos.

Los ciberseguros, al igual que los seguros de daños, están expuestos a eventos catastróficos, por lo que el sector de los ciberseguros debería responder de la misma manera que el sector de los seguros de daños. El sector debe ser proactivo a la hora de ofrecer cobertura para eventos catastróficos por separado de las coberturas principales. La cobertura para eventos catastróficos no se excluiría, sino que se delimitaría más claramente, asegurando que la cobertura separada se valore de forma transparente y esté sujeta a una suscripción adecuada, a límites de cobertura y a retenciones de clientes adecuadas. Este enfoque permitirá al sector de los ciberseguros seguir ofreciendo soluciones innovadoras a los asegurados, al tiempo que garantiza la sostenibilidad del mercado a largo plazo.

Acerca del autor

Michael Kessler,Vice President of Chubb Group and the Division President of Chubb's Global Cyber Risk , supervisa todas las facetas de la empresa incluyendo la estrategia, desarrollo comercial y de productos, operaciones de suscripción y servicios, y resultados de pérdidas y ganancias generales. Kessler tiene casi 30 años de experiencia en seguros y consultoría actuarial. Previamente había ejercido de responsable de reaseguro de Chubb (2016-2021) y director Actuario (2008-2016). Kessler es licenciado en matemáticas por la Cornell University. Es miembro de la American Academy of Actuaries y asociado de la Casualty Actuarial Society.

Nota final

1. Seguro cibernético: Las aseguradoras y los asegurados se enfrentan a retos en un mercado cambiante (2021). Extraído de www.gao.gov/products/gao-21-477
2. Informe de organizaciones ciberresilientes (2020). Extraído de www.ibm.com/security/digital-assets/soar/cyber-resilient-organization-report/#/
3. Base de datos National Vulnerability Database del National Institute of Standards and Technology. Consultada en https://nvd.nist.gov/vuln/search
4. Instituto AV-TEST (2021). www.av-test.org/en/statistics/malware/
5. Informe sobre investigaciones de filtración de datos de Verizon del 2021 (2021). Extraído de https://enterprise.verizon.com/resources/reports/2021/2021-data-breach-investigations-report.pdf
6. Comité de Inteligencia del Senado de Estados Unidos (2021). Consultado en www.intelligence.senate.gov/hearings/open-hearing-hearing-hack-us-networks-foreign-adversary
7. Tendencias de las vulnerabilidades de seguridad en 2020 según NIST: Análisis (2021). www.redscan.com/media/Redscan_NIST-Vulnerability-Analysis-2020_v1.0.pdf

Acerca de Chubb

Chubb es la mayor aseguradora de daños 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 cuenta con oficinas ejecutivas en Zúrich, Nueva York, Londres, París y otros lugares, y tiene una plantilla de aproximadamente 31 000 profesionales en todo el mundo. Puede obtener más información en www.chubb.com/es.

Para más información sobre los conocimientos y la experiencia del líder en el sector Chubb en gestión del ciberriesgo, visite chubb.com/es/cyber

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.

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.

ES8127-MD 02/22