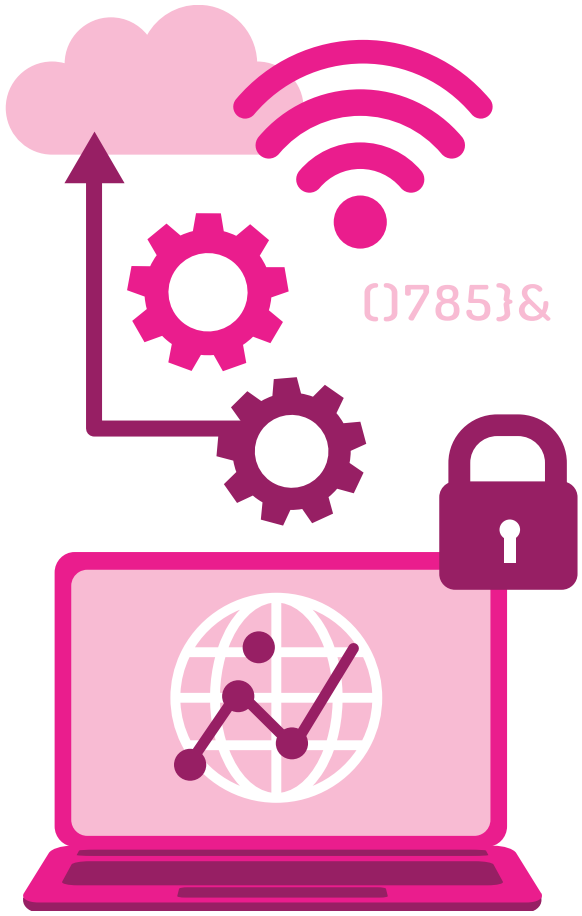
CHUBB®

Guía de Gestión de Riesgos Cibernéticos para Corredores

Esta guía incluye información sobre:

¿Por qué es importante la Ciberseguridad?



La era digital y de la información nos permite recopilar más datos, colaborar de forma más eficiente, agilizar los procesos empresariales y extraer información en todo el mundo las 24 horas del día.

El aumento de la dependencia a los sistemas informáticos y del acceso a la información puede incrementar considerablemente la exposición de una empresa a las amenazas para la ciberseguridad. Las interrupciones, los errores o los ataques de estos nuevos procesos pueden dar lugar a cuantiosos gastos que pueden arruinar los resultados de una empresa. Así pues, cuando esto ocurra, necesitará una amplia protección por parte de una aseguradora especializada en la gestión de los riesgos cibernéticos, que ofrezca una amplia gama de soluciones integradas de seguros para contribuir a minimizar las lagunas en la cobertura y que entienda cómo adaptar la cobertura a su empresa. **En Chubb, mantenemos el firme compromiso de proporcionar a nuestros asegurados soluciones para los riesgos cibernéticos desde 1998.**

Gaps de cobertura en los seguros tradicionales

Las empresas pueden operar con la convicción de que sus pólizas de seguro existentes son suficientes para cubrir la exposición tanto en materia de privacidad como de seguridad de sus datos. Lamentablemente, no siempre es así, y las pólizas de seguro tradicionales pueden ser inadecuadas para responder a los riesgos a los que las organizaciones se enfrentan hoy en día.

Responsabilidad Civil General	Daños	Infidelidad de Empleados
Las pólizas de responsabilidad civil general suelen activarse en respuesta a reclamaciones por lesiones corporales o daños a la propiedad. Un evento cibernético generalmente no conlleva lesiones corporales o daños a la propiedad, y las pólizas de responsabilidad general no suelen ofrecer cobertura para los costes del asegurado.	Las pólizas de daños generalmente responden a la destrucción o daño a la propiedad tangible resultantes de un peligro físico. Por lo tanto es la pérdida tangible la que permite activar la cobertura de interrupción del negocio y gastos adicionales. Un evento cibernético, por sí mismo, puede no dar lugar a daños físicos, pero puede provocar la interrupción de un negocio o que daría lugar a importantes gastos y a la pérdida de ingresos.	Las pólizas de infidelidad de empleados generalmente responden a las pérdidas directas provenientes del robo de dinero, valores o propiedad tangible por parte de los empleados Las extensiones para abarcar los delitos informáticos suelen excluir cualquier cobertura de responsabilidad frente a terceros y pueden no proporcionar una cobertura suficiente de la pérdida de información confidencial.

Exposiciones por Sectores

Instituciones financieras

Las instituciones financieras están altamente expuestas a riesgos cibernéticos debido a una combinación de factores.Los delitos cibernéticos, el hacktivismo y los ataques sofisticados con fines de espionaje en nombre de un beneficiario son solo algunos de los riesgos a tener en cuenta. La vulnerabilidad a los eventos cibernéticos puede ser alta, ya que muchas instituciones financieras dependen de redes altamente interconectadas e infraestructuras críticas. Debido a su elevada dependencia de la tecnología, la mayoría de las instituciones financieras seguirán sufriendo una exposición al riesgo cibernético cada vez mayor.

Reclamaciones comunes: ***Phishing* en redes sociales** y **Errores Humanos**

Atención sanitaria

La transición generalizada hacia la digitalización de los historiales médicos ha dado lugar a que las compañías médicas dependan cada vez más de los sistemas informáticos para recopilar y tramitar datos médicos y de salud personales altamente sensibles. Existe una gran exposición a errores administrativos, dado que los empleados deben introducir información precisa en los sistemas. Los sistemas informáticos heredados a menudo no son aislados, lo que aumenta la posibilidad de que un evento tenga un fuerte impacto en las operaciones.

Reclamaciones comunes: **Errores Humanos** y **Uso Indebido**

Venta minorista

Ya se trate de venta <Italic>online</Italic> o en las tiendas físicas, los datos de reclamaciones de Chubb muestran que el sector de distribución minorista está muy expuesto a las pérdidas ocasionadas por riesgos cibernéticos. Las empresas minoristas suelen tener muchas ubicaciones que pueden o no operar en sistemas de TI centralizados, una dependencia de una compleja red de proveedores de servicios de TI críticos, una posible dependencia de sitios web debido al auge de la venta en línea y una gran cantidad de información personal sensible debido a la alta frecuencia de las transacciones financieras y los programas de fidelización.

Reclamaciones comunes: ***Piratería*** y ***Phishing* en redes sociales**

Hostelería

El sector de la hotelería abarca una amplia gama de operaciones, desde hoteles hasta bares y restaurantes. En todo el sector, las exposiciones relacionadas con el ciberespacio incluyen grandes volúmenes de información tanto de consumidores como de empleados, a menudo una gran dependencia de los sitios web para las reservas de los clientes, así como la información relacionada con los programas de fidelización, estos riesgos pueden conllevar problemas de privacidad, al ser objeto de ataques de ingeniería social y de *phishing*.

Reclamaciones comunes: ***Phishing* en redes sociales** y ***Piratería***

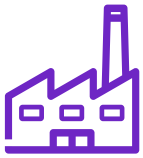
Servicios Profesionales

Debido a la gran cantidad de datos confidenciales recopilados, el sector de servicios profesionales es un blanco muy común en los ataques cibernéticos. Por ejemplo, la información y los fondos que posee un despacho de abogados o una asesoría contable pueden ser lucrativos para un atacante, y las consecuencias para la reputación de una empresa que sufre un ataque cibernético pueden ser perjudicial. La acumulación de información sensible de los clientes ha dado lugar a un aumento de eventos cibernéticos que afectan a empresas de servicios profesionales en los últimos años.

Reclamaciones comunes: **Errores Humanos** y ***Piratería***

*Los datos sobre las causas más comunes de las reclamaciones por incidentes cibernéticos provienen del Chubb Cyber Index®

Exposiciones por Sectores



Sector Manufacturero

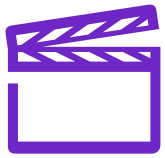
La industria manufacturera es uno de los sectores con mayor frecuencia de ataques cibernéticos. El notable uso e integración de la tecnología en este sector está cambiando la forma en que los fabricantes operan sus negocios. Con el fin de mejorar la productividad y la rentabilidad, muchos fabricantes están recurriendo al Internet de las Cosas (IoT), la digitalización y los servicios en la nube, lo que aumenta el impacto de ciertos incidentes cibernéticos. Eventos recientes que han afectado a los sistemas industriales de control (ICS, por sus siglas en inglés) y los sistemas de supervisión, control y adquisición de datos (SCADA, por sus siglas en inglés) han tenido efectos devastadores en las operaciones.

Reclamaciones comunes:
Malware y **en redes sociales** - ***Phishing***

Educación

Los centros educativos están en peligro debido a los datos sensibles que poseen sobre los estudiantes y el personal. Los colegios y las universidades suelen tener un presupuesto y unos recursos informáticos limitados. Las amenazas son tanto externas como internas, ya sea porque un estudiante introduzca *malware* en su red de forma maliciosa o involuntaria, o o de un miembro del personal que no sigue el protocolo y como consecuencia se produce una brecha de seguridad de los datos.

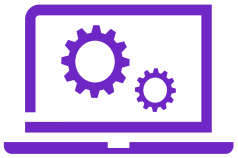
Reclamaciones comunes:
Phishing **en redes sociales** y ***Piratería***



Medios de Comunicación y Entretenimiento

Las empresas de medios de comunicación y entretenimiento suelen hacer frente a amenazas de extorsión cibernética que pueden tener como finalidad vulnerar material y contenido confidencial o sensible. Los ataques de denegación de servicio (DDoS, por sus siglas en inglés) o las interrupciones del sistema informático pueden afectar gravemente a las actividades de radiodifusión y a la transmisión de contenido en el momento programado. La posesión de información personal sensible de los suscriptores agrava esta exposición.

Reclamaciones comunes:
Errores Humanos y ***Phishing*** en redes sociales



Tecnología

Los clientes de las empresas de tecnología esperan de ellas una alta eficiencia en seguridad cibernética y protección de datos, lo que aumenta el daño a la reputación que podría causarse a raíz de un incidente cibernético. Los incidentes cibernéticos en los proveedores de servicios tecnológicos también pueden tener un impacto en la cobertura de Responsabilidad Civil Profesional. Póngase en contacto con el suscriptor de Chubb para obtener más información sobre nuestra oferta combinada de Riesgos Cibernéticos y Errores & Omisiones para empresas tecnológicas, la cual es líder del mercado.

Reclamaciones comunes:
Piratería y **Errores Humanos**

*Los datos sobre las causas más comunes de los siniestros cibernéticos proceden de Chubb Cyber Index®

Descubra lo que Chubb puede ofrecer a las pequeñas, medianas y grandes empresas para hacer frente a estos riesgos:

Pymes | **Medio Mercado** | **Grandes Empresas**

Pymes - Perspectiva

Si bien los medios se centran sobre todo en los incidentes cibernéticos sufridos por las grandes organizaciones, las pymes también suelen verse afectadas por amenazas y vulnerabilidades cibernéticas. Las Pymes a menudo son vistas como blancos más fáciles para los delincuentes cibernéticos debido a sus limitaciones en cuanto a recursos e inversión en TI.

Además, es más probable que descuiden medidas como la formación del personal en seguridad de la información, la orientación sobre el establecimiento de contraseñas y la autenticación de doble factor. Las Pymes suelen representar una oportunidad lucrativa para los delincuentes cibernéticos en comparación con las organizaciones más grandes, que pueden ser más difíciles de hackear. También deben tener en cuenta que si bien en algunos casos no sean el blanco principal, pueden verse afectadas por un ataque dirigido a un proveedor de TI subcontratado o un socio comercial.

Reclamaciones de Pymes - Chubb Cyber Index®

La mejor manera de ilustrar el riesgo cibernético al que se enfrentan las Pymes es con datos. Chubb lleva más de dos décadas gestionando siniestros cibernéticos. Como parte del proceso de siniestros, hacemos un seguimiento de los métricas clave, como las acciones que causan una pérdida cibernética, si un evento cibernético fue causado por un actor interno o externo, el número de registros afectados, el tamaño y el sector del asegurado afectado. A través del Chubb Cyber Index®, compartimos estos datos públicamente para ayudar a las empresas a comprender mejor los riesgos a los que se enfrentan.

El Chubb Cyber Index® proporciona a los usuarios un medio para identificar los principales riesgos cibernéticos a los que puede enfrentarse su empresa a partir de ejemplos reales de ciberataques y filtraciones de datos. Los usuarios pueden establecer parámetros y visualizar las tendencias históricas en función del tipo de amenaza, el tamaño de la empresa y el sector en el que opera.

Para obtener más información, visite Chubb Cyber Index® en:
https://chubbcyberindex.com

Pymes - Casos de Siniestros

Ransomware

Nuestro asegurado, una empresa de construcción, fue víctima de un ataque de *ransomware*. Los sistemas del asegurado fueron vulnerados después de que un empleado hiciera clic en un enlace malicioso en un correo electrónico. Los sistemas y servidores del asegurado fueron encriptados y, a continuación, se exigieron 800 000 EUR en bitcoin. El asegurado recurrió a los gestores de respuesta a incidentes de Chubb para que solicitaran al equipo de informática forense informáticos a fin de determinar el método y el alcance del ataque. A pesar de no haber pagado el rescate, todas las operaciones comerciales afectadas por más de seis meses.

Coberturas aplicables:

Recuperación de Datos y Sistemas, Interrupción de Negocio, Gastos de Respuesta a Incidentes y Extorsión Cibernética.

Mitigación

Revisión periódica de la seguridad informática, formación de los empleados, realización periódica de copias de seguridad de los datos y un plan de continuidad de negocio.

Empleado Descontento

Nuestro asegurado fue víctima de un empleado con malas intenciones que robó los registros de datos personales de más de 700 clientes, incluidos sus nombres, direcciones y datos de contacto. El empleado facilitó estos registros a su nuevo empleador para obtener beneficios. Dado que el evento tuvo lugar después de la entrada en vigor del RGPD, se tuvo que enviar un aviso a la AEDP y a los interesados afectados.

Coberturas aplicables:

Responsabilidad por Privacidad y Gastos de Respuesta a Incidentes.

Mitigación

Resulta increíblemente difícil evitar que empleados deshonestos busquen causar daño. La mayoría de las veces estos empleados cuentan con acceso al sistema, lo cual permite el robo de datos sensibles, ya sean personales o corporativos. En la jurisprudencia actual, en estos casos la empresa suele ser responsable ante sus clientes. La solución de seguro cibernético ofrecida por Chubb proporciona las herramientas necesarias para responder cuando esto ocurra.

Errores de Empleados

Nuestro asegurado, una gestora inmobiliaria, sufrió por accidente una vulneración de privacidad de datos como resultado de un error de un empleado. Al publicar un nuevo anuncio de un inmueble vacío, el empleado incluyó por error una imagen del historial clínico de otro cliente en el folleto *online* del inmueble.

Coberturas aplicables:

Responsabilidad por Privacidad y Gastos de Respuesta a Incidentes.

Mitigación

Es importante tener una política de privacidad para toda la empresa que detalle un protocolo para la gestión de información confidencial. Los empleados deben revisar, comprender y comprometerse a cumplir la política de privacidad al menos una vez al año.

Pymes - Supuestos de siniestros

Acceso No Autorizado - *Phishing*

Nuestro asegurado, una empresa de logística, fue víctima de un ataque de *phishing* con *malware*. A un empleado del equipo de Recursos Humanos le apareció una ventana emergente en su ordenador después de hacer clic en un enlace malicioso incluido en un correo electrónico. La ventana emergente decía que el ordenador estaba infectado y que llamara al número que se mostraba. A continuación, los estafadores obtuvieron acceso remoto al ordenador del empleado engañándolo durante la llamada.

Coberturas aplicables:
Responsabilidad por Privacidad y Seguridad de la Red y Gastos de Respuesta a Incidentes.

Mitigación

Incluso con la mejor tecnología y sistemas de seguridad, el activo más vulnerable de un asegurado suele ser su personal. Los empleados pueden ser engañados para revelar contraseñas o proporcionar acceso a sistemas. Se aconseja la formación periódica en materia de *phishing*, y resulta esencial contar con una póliza de seguro que proporcione los conocimientos pertinentes.

Pérdida de Datos almacenados en Registros Físicos

Nuestro asegurado, un bufete de abogados, se puso en contacto con la línea directa de respuesta a incidentes de Chubb tras descubrir que un empleado había incumplido el protocolo de la compañía al llevarse registros físicos de clientes de la oficina y guardarlos en su coche. Posteriormente, el coche fue robado y los registros de clientes se perdieron.

Coberturas aplicables:

Responsabilidad por Privacidad y Gastos de Respuesta a Incidentes

Mitigación

Es necesario contar con un proceso claro para el almacenamiento de datos, tanto digitales como físicos. Realizar copias de seguridad de los datos de forma regular es importante para poder recuperarse rápidamente de un incidente. Crear una política de privacidad para toda la empresa que los empleados deban aceptar y cumplir.

Pymes - Una solución cibernética a medida

1 Servicios de Mitigación de Pérdidas para PYMES

Chubb ofrece a las PYMES una serie de servicios complementarios a precios muy ventajosos para ayudarles a mitigar las reclamaciones más comunes por incidentes cibernéticos.

La soluciones de Gestión de Contraseñas para hasta 100 empleados de cada asegurado.

- Una gestión eficaz de las contraseñas puede ayudar a minimizar el uso no autorizado de credenciales robadas.

Las soluciones de Formación para Empleados ayudan a su equipo a prepararse para las amenazas del *phishing*, a identificar posibles amenazas cibernéticas, a proteger los datos confidenciales y a elevar los problemas a las personas adecuadas cuando sea necesario.

Haga clic aquí para obtener más información sobre nuestra gama completa de servicios cibernéticos, incluida la ciberseguridad y otras funciones.

2 Servicios de Respuesta a Incidentes para Pymes

Chubb entiende que no todos los incidentes pueden evitarse. Cuando ocurre un incidente cibernético, nuestras pólizas ponen a disposición a un equipo de expertos conformado por proveedores de servicios de respuesta a incidentes sin franquicia para nuestros clientes PYMES.

Estos especialistas están disponibles a cualquier hora de cualquier día del año y están preparados para guiarle en la recuperación ante cualquier incidente cibernético.

- Contamos con expertos en gestión de respuesta a incidentes, análisis informático forense, los recursos legales, las relaciones públicas y otros servicios.
- El acceso a la red de proveedores está incluido en la póliza.
- Disponibilidad las 24 horas del día y los 365 días del año a través de la aplicación Cyber Alert® o de la línea telefónica gratuita.
- Pueden proporcionar asistencia tras cualquier incidente cibernético, siempre dispuestos a ayudar en cualquier emergencia.

Haga clic aquí para obtener más información sobre cómo funciona la solución de Respuesta a Incidentes de Chubb.

3 Plataformas para Pymes

La plataforma <Italic>online</Italic> de Chubb (disponible en determinados países) se ha diseñado específicamente para que los corredores puedan presupuestar y contratar de forma *online los seguros para Pymes. Al combinar el diseño intuitivo con una experiencia centrada en el cliente, los corredores pueden preparar el seguro cibernético de sus clientes en cuestión de minutos antes de emitir la documentación de manera inmediata.*

Esta plataforma te permite contratar la cobertura de forma ágil y rapida e incluye los mismos beneficios de las pólizas contratadas por el camino *tradicional*:

- Cuestionario de preguntas sencillas
- Amplia disposición al riesgo para las Pymes
- El mismo condicionado que los negocios *tradicional*
- Acceso a los Servicios de Mitigación de Pérdidas cibernéticas de Chubb
- Edite las fechas de la póliza, los límites, la comisión y los datos de contacto sin la necesidad de contactar con un suscriptor
- Cotice y suscriba riesgos en cuestión de minutos

Póngase en contacto con su suscriptor de Chubb para obtener información de la plataforma *online u otras soluciones simplificadas para Pymes.*

Medio Mercado - Perspectiva

Las empresas de medio mercado se enfrentan a los mismos problemas de ciberseguridad que las grandes empresas, pero con menos presupuesto y menos personal especializado para gestionarlo. A menudo tienen la misma opinión que muchas PYMES, que solo las grandes empresas internacionales están expuestas a un riesgo significativo. Como las actividades maliciosas son ahora más sofisticadas, la lucha de las empresas de medio mercado para defenderse es ahora más compleja que nunca.

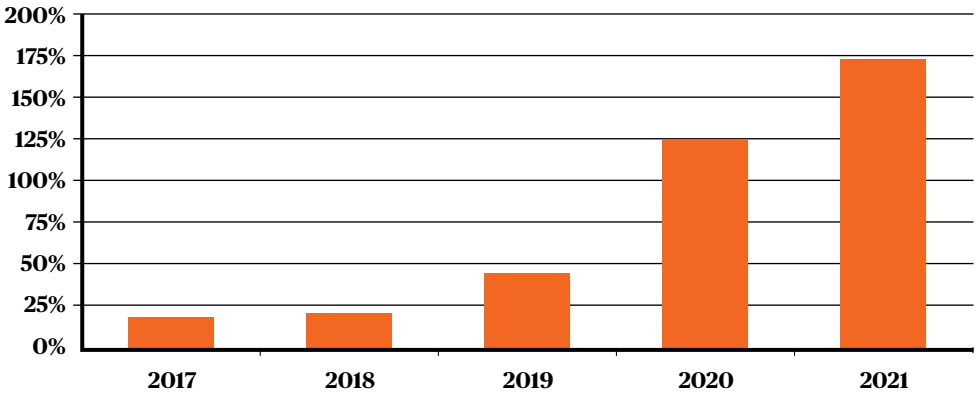
Chubb Cyber Index®

El Chubb Cyber Index® proporciona a los usuarios un medio para identificar los principales riesgos cibernéticos a los que puede enfrentarse su empresa a partir de ejemplos reales de ciberataques y filtraciones de datos. Los usuarios pueden establecer métricas y visualizar las tendencias históricas en función del tipo de amenaza, el tamaño de la empresa y el sector en el que opera.

Para obtener más información, visite Chubb Cyber Index® en https://chubbcyberindex.com

Reclamaciones de Chubb en comparación con 2016 (Crecimiento Porcentual)

Medio Mercado - Todos los sectores



Medio Mercado - Casos de Siniestros

Ransomware

Un geriátrico sufrió un ataque de *ransomware* de «fuerza bruta» y varios de sus archivos fueron cifrados. Al principio se exigió un rescate de unos 26 000 euros. Tras pagar una pequeña parte del rescate para obtener una muestra de la herramienta de descifrado, la empresa decidió confiar en sus copias de seguridad para restaurar sus sistemas.

Coberturas aplicables:

Recuperación de Datos y Sistemas, Interrupción de Negocio, Gastos de Respuesta a Incidentes y Extorsión Cibernética.

Mitigación

Aunque la inversión en tecnología de seguridad es esencial para ayudar a prevenir el acceso no autorizado, no es infalible. Los atacantes perfeccionan constantemente sus métodos de ataque, y cualquier empresa tiene que revisar su seguridad y sus procedimientos con regularidad para mantenerse al día en cuanto a las amenazas.

Errores de Empleados

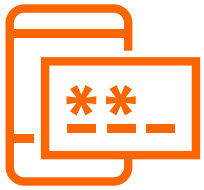
Un empleado de una empresa de distribución minorista de *hardware* ignoró las políticas y procedimientos internos y abrió un archivo aparentemente inofensivo adjunto a un correo electrónico. Al día siguiente, los registros de pedidos y las cajas registradoras empezaron a funcionar mal y el comercio se vio perjudicado debido al fallo de la red.

Coberturas aplicables:

DRecuperación de Datos y Sistemas, Responsabilidad por Seguridad de la Red, Interrupción de Negocio y Gastos de Respuesta a Incidentes.

Mitigación

Se debe prever una formación periódica para garantizar que el personal sea consciente de lo que debe buscar para identificar archivos adjuntos de correo electrónico sospechosos y del proceso que debe seguir en caso de tener sospechas. Además, el acceso inmediato a un gestor de incidentes y a una red de asistentes permitirá una rápida respuesta.



Vulneración de Seguridad de Datos

La red de un hotel fue hackeada, dejando potencialmente comprometidos todos los registros de empleados y clientes, incluida la información de las tarjetas de pago de los clientes.

Coberturas aplicables:

Gastos de Respuesta a Incidentes, Recuperación de Datos y Sistemas y Responsabilidad por Privacidad y Seguridad de la Red.

Mitigación

Las herramientas de seguridad sobre concienciación en torno a la detección son útiles para combatir a un *hacker* Esta permite detectar rápidamente cualquier actividad sospechosa. El cifrado de los datos también resulta fundamental para garantizar que los datos filtrados no puedan eliminarse y utilizarse fácilmente.

Medio Mercado - Casos de Siniestros

Minería de Criptomonedas

Una empresa manufacturera sufrió un ataque de *ransomware* que provocó el cifrado de varios de sus archivos. Después de que el asegurado contactara con Chubb a través de la línea directa de respuesta a incidentes 24/7, le pusimos en contacto con un gestor de respuesta a incidentes y expertos de informática forense de nuestro panel. Tras consultar a nuestros expertos, el asegurado optó por no pagar el rescate. Sin embargo, una vez la empresa forense comenzó a trabajar en la reparación del ataque de *ransomware*, descubrieron que el asegurado también fue víctima de minería de criptomonedas (cryptomining). Los atacantes habían instalado en el sistema del asegurado un *software* que estaba minando Bitcoins. La minería de criptomonedas ocurre cuando el sistema informático de una parte desprevenida se está utilizando para la minería de criptomonedas sin su conocimiento.

Coberturas aplicables:

Gastos de Respuesta a Incidentes, Interrupción de Negocio, Recuperación de Datos y Sistemas y Responsabilidad por Privacidad y Seguridad de la Red.

Mitigación

Es importante que las empresas de manufactura revisen periódicamente la seguridad de sus sistemas informáticos para garantizar que la producción no se vea afectada por un ataque. Deben plantearse la implementación de un plan de recuperación ante desastres y un plan de continuidad de las operaciones para que les permita minimizar la interrupción de negocio en caso de convertirse en el blanco de un ataque. Las herramientas contra el acceso no autorizado no son infalibles. Los atacantes están perfeccionando constantemente sus métodos de ataque, y todas las empresas deben revisar su seguridad y procedimientos regularmente para estar preparadas para cualquier amenaza.

Robo de Datos que da lugar a una Extorsión, Interrupción de Negocio y Gastos Adicionales

Una organización desconocida hackeó la red de un bufete de abogados y podría haber obtenido acceso a información confidencial de clientes, incluida información sobre la posible adquisición de una empresa con acciones negociadas en bolsa, el prospecto de una patente tecnológica de otra empresa cotizada, el borrador del folleto de un cliente de capital riesgo y un número significativo de listas de demandas colectivas que contienen Datos de Carácter Personal de demandantes. Un técnico forense contratado por el bufete de abogados determinó que se había introducido un *malware* en su red. Poco después, la empresa recibió una llamada del intruso en la que pedía 10 millones de dólares por no publicar la información robada en *internet* El bufete de abogados incurrió en 2 millones de euros en gastos relacionados con una investigación forense, negociaciones relacionadas con la extorsión, un pago de rescate, notificaciones, servicios de control de crédito e identidad, servicios de restauración de identidad y honorarios de abogados independientes.

Coberturas aplicables:

Extorsión Cibernética, Responsabilidad por Privacidad y Seguridad de la Red, Interrupción de Negocio y Gastos de Respuesta a Incidentes.

Mitigación

La formación del personal resulta importante para evitar la apertura de correos electrónicos maliciosos. Además, se deben implementar sistemas de seguridad informática para identificar el *malware* en caso de que llegue a la red.

Medio Mercado - Una solución cibernética a medida

1 Servicios de Mitigación de Pérdidas para Empresas del Mercado Medio

Con el fin de ayudar a nuestros asegurados de medio mercado a mitigar las reclamaciones cibernéticas más comunes, en Chubb ofrecemos una serie de servicios a nuestros asegurados.

Soluciones de Gestión de Contraseñas incluidas en la póliza para hasta 100 empleados de cada asegurado.

- Una gestión eficaz de las contraseñas puede ayudar a minimizar el uso no autorizado de credenciales robadas.

Existen Simulaciones de Formación sobre *Phishing* disponibles para los asegurados.

- El *phishing* o la suplantación de identidad es una de las causas de pérdidas cibernéticas de mayor crecimiento, y la simple formación de los empleados puede ser una herramienta eficaz para minimizar la posibilidad de que un ataque de *phishing* afecte a empresas de medio mercado.

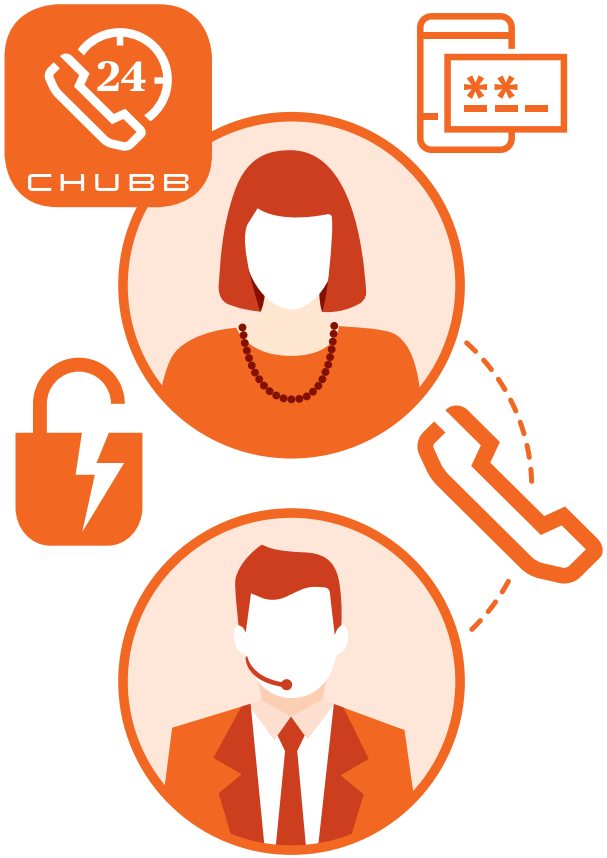
Haga clic aquí para obtener más información sobre nuestra gama completa de servicios cibernéticos, incluida la ciberseguridad y otras funciones.

2 Servicios de Respuesta a Incidentes para Empresas del Medio Mercado

Responder de manera rápida y efectiva a un incidente cibernético es clave para minimizar el impacto y las pérdidas. Cuando un cliente de Medio Mercado sufre un incidente de este tipo, nuestras pólizas cibernéticas ponen a disposición de este un equipo de expertos conformado por proveedores de servicios de respuesta a incidentes. Estos especialistas están disponibles a cualquier hora de cualquier día del año y están preparados para guiarle en la recuperación ante cualquier incidente cibernético.

- Contamos con expertos en gestión de respuesta a incidentes, informática forense, recursos legales, relaciones públicas y negociadores de extorsiones cibernéticas.
- Flexibilidad para utilizar nuestro panel de proveedores o cualquier proveedor que ya haya contratado en el marco de un plan de respuesta a incidentes cibernéticos.
- Disponibilidad las 24 horas del día a través de la aplicación Cyber Alert®.

Haga clic aquí para obtener más información sobre el funcionamiento de la solución de Respuesta a Incidentes de Chubb.



Medio Mercado - Una solución cibernética a medida

3 Servicios de Ingeniería

La forma de operar de los clientes y la tecnología que utilizan pueden variar según las circunstancias. Nuestros ingenieros de riesgos cibernéticos ayudan a los clientes a identificar y comprender sus vulnerabilidades tecnológicas y pueden ayudar a prevenir un incidente cibernético futuro incluso antes de que se inicie el periodo de vigencia de una póliza.

Beneficios Clave

- **Contacto directo con los clientes para obtener una comprensión profunda de su riesgo y exposición**
- **Flexibilidad para realizar la revisión del riesgo tanto antes de contratar la póliza como durante la vigencia de la misma**
- **Recomendaciones para el riesgo con orientación sobre cómo los clientes pueden mejorar su perfil de gestión de riesgos cibernéticos**
- **Ofrecemos formación técnica directa adicional para clientes y corredores**

Si bien este servicio está diseñado específicamente para clientes de medio mercado, puede considerarse para empresas de cualquier tamaño.

El proceso

¿Cómo funciona?

1 Programación previa a la visita

Objetivos de la visita, temas a tratar, quién debería participar y qué documentos necesitaremos antes de la reunión.

2 Visita (2-3 horas)

Evaluación de operaciones, instalaciones, redes e infraestructura, activos de seguridad de la información, procesos y políticas de protección procedimientos de seguridad específicos, detección de vulnerabilidades, respuesta a incidentes y pérdidas previas.

3 Recomendación

Una vez que se haya completado la visita o conferencia telefónica, proporcionaremos recomendaciones específicas, que pueden incluir una previsión de las posibles pérdidas y una sección detallada sobre mejoras aplicables al riesgo.

4 Reunión con el Cliente

Nos reuniremos con cada cliente para explicarles nuestros resultados, ofrecer asesoramiento sobre mejoras y trabajar con ellos para establecer mejores prácticas que ayuden a mitigar un posible incidente cibernético.

Grandes Empresas - Perspectiva

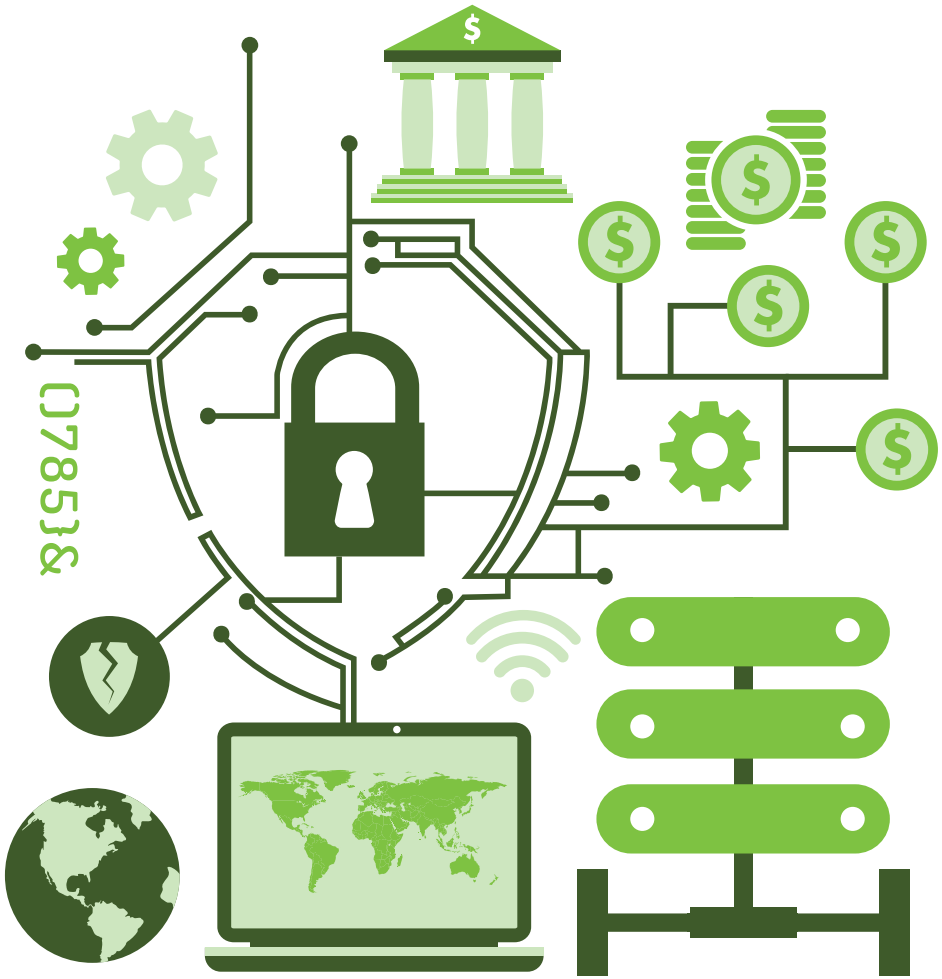
A medida que el número de ciberataques a grandes empresas y multinacionales, muy difundidos por la prensa, ha aumentado en los últimos años, también lo ha hecho la demanda de seguros cibernéticos a un ritmo muy veloz. La creciente demanda se ha visto impulsada por una acentuada presión en los consejos directivos para demostrar una evaluación adecuada de los riesgos cibernéticos, una mayor supervisión regulatoria y un aumento de la necesidad de compartir información entre compañeros y socios. Los consejos de administración y gerentes de riesgo reconocen que el seguro cibernético debería ser más que una simple transferencia de riesgo. La oferta de Chubb para Grandes Empresas proporciona una solución de respuesta a incidentes global pero flexible, una amplia variedad de opciones de programas multinacionales, servicios de reaseguro de cautivas y capacidad significativa a través de nuestro Servicio Cibernético Global (Global Cyber Facility).

Servicios de Respuesta a Incidentes para Grandes Empresas

Los planes de respuesta a incidentes cibernéticos suelen ser implementados y a menudo puestos a prueba por grandes empresas. Los servicios de respuesta a incidentes cibernéticos de Chubb están destinados a complementar las medidas ya implementadas. Nuestro equipo de gestores de respuesta a incidentes está preparado para trabajar con los proveedores especialistas que el asegurado prefiera, incluso si no forman parte del panel de expertos de Chubb.

- La póliza e el uso de proveedores a los que nuestros clientes ya han contratado como parte de un plan de respuesta a incidentes cibernéticos.
- Nuestra red mundial de equipos locales de respuesta a incidentes está diseñada para satisfacer las necesidades de los riesgos multinacionales.
- La aplicación Cyber Alert® de Chubb, diseñada para un gestor de riesgos o un responsable informático, se conecta con nuestro equipo de respuesta a incidentes y siniestros para agilizar la asistencia de expertos y la respuesta de la póliza

Haga clic aquí para obtener más información sobre el funcionamiento de la Solución de Respuesta a Incidentes de Chubb.



Grandes Empresas

1 Programas Multinacionales

La naturaleza global del riesgo cibernético requiere que las empresas entiendan cómo sus pólizas pueden responder a un incidente internacional y qué restricciones pueden aplicarse. Estructurar un programa de seguros multinacional eficiente y rentable requiere un conocimiento profundo del entorno normativo cibernético, siempre en evolución.

Algunas preguntas específicas que deben plantearse al considerar un programa de seguros multinacional:

- ¿Dónde se encuentran las entidades? Las restricciones pueden variar según el país.
- ¿Permiten los países que una aseguradora no autorizada (non-admmitted) pague las pérdidas directamente a la entidad local?
- ¿Desea el cliente proteger a los asegurados a nivel local? Los beneficios de una póliza local incluyen: pagos de siniestros a escala local, idioma local de la póliza y gestión local de los siniestros.

Capacidades de cobertura cibernética multinacional de Chubb:

Chubb puede ofrecer programas cibernéticos multinacionales de manera local y responsable a más de 35 países en todo el mundo, atendidos por el equipo de servicios globales de Chubb, que cuenta con experiencia y especialistas preparados para ayudar con las necesidades en materia de seguros multinacionales.

2 Global Cyber Facility

Una solución integral de gestión de riesgos cibernéticos para Grandes Empresas.

¿Con quién trabajamos?

- Organizaciones con más de 1.000 millones de dólares de ingresos anuales
- Todas tipo de sectores, incluidos los distribuidores minoristas, las instituciones financieras y los fabricantes.

Componentes de la oferta:

- Servicios preventivos de control de pérdidas prestados por organizaciones de defensa cibernética reconocidas a escala mundial para abordar las deficiencias en materia de seguridad cibernética identificadas durante la evaluación del riesgo.
- Política de transferencia de riesgos.
- Respuesta a incidentes y gestión de siniestros después de que se produzcan.

Cobertura principal de la póliza:

- **Límites primarios disponibles de 30 a 100 millones de euros de capital de Chubb** para respaldar las grandes torres.
- **Cláusulas DIC/DIL disponibles para evitar gaps de cobertura.** Entre las pólizas de ciberseguridad, responsabilidad civil y daños de una organización.
- Flexibilidad y personalización de la póliza.

¿En qué consiste el proceso?

- Iniciar proactivamente el proceso de venta tres meses antes de la solicitud se realice al mercado.
- Evaluación propia de Chubb para analizar el perfil de riesgo de la organización.
- Interacción directa entre el cliente y los suscriptores de Chubb.

Grandes Empresas

3 Cautivas

La gestión de riesgos cibernéticos mediante una cautiva resulta cada vez más crucial para las empresas multinacionales que consideran relevante una combinación de transferencia y retención de riesgo. Las cautivas se están convirtiendo en una solución común para mantener primas adecuadas y asequibles, o para alinear franquicias de pólizas locales dentro de una estructura consolidada.

Una cautiva también puede proporcionar una cobertura más completa que la disponible en el mercado de seguros para la empresa matriz. Esto permite a una compañía entender mejor las exposiciones y recoger información sobre pérdidas, de modo que su aseguradora o reaseguradora pueda asumir el riesgo con un límite y una prima adecuados.

¿Por qué?

- Optimizar la transferencia de riesgos
- Proporcionar diversificación
- Actuar como una incubadora
- Acceso a servicios complementarios

¿Cómo?

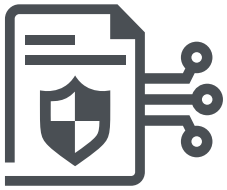
- Posibilidad de diseñar varias estructuras
- Capa primaria pequeña o capa de franquicia significativa
- Participación en grandes programas (Quota share)
- Adaptable a riesgos específicos

Retos

- Compresión de incertidumbre/ exposición
- Establecer el precio de la capa de retención
- Acumulación con otras líneas

Principales Argumentos de Venta

No todos sus clientes entenderán la importancia de una póliza de riesgos cibernéticos, o todos los beneficios que esta puede aportar. Hemos reunido algunos argumentos clave para ayudarle a explicar los principales beneficios a sus clientes.



Protección afirmativa

Las pólizas de seguro tradicionales pueden ser inadecuadas para responder a las exposiciones cibernéticas. Una póliza cibernética está específicamente diseñada para abordar estos vacios y ofrecerle una protección afirmativa frente a una exposición que puede ser difícil de comprender.

Usted puede verse afectado incluso sin ser el blanco del ataque

Los ataques cibernéticos se pueden propagar a través de sus proveedores o empresas de tecnología externalizadas, lo que genera un impacto significativo incluso cuando su empresa no es el objetivo. o. Chubb ha observado daños colaterales significativos derivados de incidentes cibernéticos originados en empresas externas. Por ejemplo, si su proveedor de servicios de almacenamiento de datos es el blanco del ataque, sus datos se podrían ver comprometidos en el proceso.

El seguro cubre los gastos de respuesta y recuperación, no solo la responsabilidad derivada de los datos comprometidos

La responsabilidad derivada de la pérdida o el uso indebido de datos sensibles es solo uno de los posibles resultados de un evento cibernético. La pérdida de beneficios, la respuesta a incidentes y los costes de recuperación constituyen una parte significativa de los pagos de siniestros atendidos por Chubb, incluso sin reclamaciones de terceros.

Complementamos a los equipos de informática

El seguro cibernético no merma la eficacia de los equipos de seguridad informática, sino que complementa sus competencias y protege a la empresa de lo desconocido.

Key Selling Points

Amenazas multinacionales

Las pérdidas cibernéticas no solo se producen a nivel local. Chubb ayuda a las empresas a recuperarse de los incidentes cibernéticos que tienen lugar en todo el mundo, incluidas las filtraciones de datos, los ataques de *ransomware* y otros incidentes.

Todas las empresas pueden verse afectadas

Los incidentes cibernéticos pueden afectar a cualquier empresa, independientemente de su tamaño y sector. Los incidentes pueden ser ataques dirigidos, errores cometicos por los empleados o pérdidas sufridas por daños colaterales a partir de un evento más amplio. Chubb tiene soluciones flexibles en función de sus necesidades, del nivel de madurez y el tamaño de su empresa.

Responder a la normativa cambiante

La nueva normativa sobre privacidad imponen normas y sanciones cada vez más estrictas, y el seguro cibernético puede ayudarle a adaptarse a estos cambios. Las pólizas de Chubb se ajustan a estos cambios.

Adaptación a los riesgos cibernéticos emergentes

Chubb informa trimestralmente sobre las nuevas tendencias en materia de siniestros cibernéticos emergentes, manteniéndolo al tanto de los nuevos riesgos a medida que los identificamos. El Chubb Cyber Index® también le ofrece información actualizada sobre las tendencias recientes e históricas.

Servicios Cibernéticos

Nuestra evaluación de tendencias de siniestros comunes ha evidenciado temas frecuentes en múltiples sectores y segmentos de clientes. Los errores humanos, el uso indebido y los ataques en redes sociales, como el *phishing*, son causas comunes de pérdidas cibernéticas, pero pueden evitarse o minimizarse con la concienciación y la formación adecuada.

Como parte de la solución aseguradora de Chubb, ofrecemos Servicios de Mitigación de Pérdidas diseñados específicamente para mitigar las causas comunes de las pérdidas cibernéticas. Los asegurados de Chubb tienen acceso a una serie de servicios que incluyen **seguridad de contraseñas, formación sobre *phishing*, concienciación de empleados** y mucho mas.

Nuestra filosofía de gestión de riesgos empresariales demuestra nuestro compromiso con la mejora de la gestión de riesgos cibernéticos de nuestros clientes. Nuestra asociación con expertos externos nos permite ofrecer a nuestros clientes acceso a servicios de mejora de riesgos cibernéticos fáciles de aplicar, muchos de los cuales son gratuitos.

Para acceder a los servicios y obtener más información, visite el sitio web de Chubb Cyber Services: a los servicios y obtener más información, visite el sitio web de Chubb Cyber Services: http://www.chubb.com/cyber-services

www.chubb.com/cyber-services

Servicios Cibernéticos

1. Gestión de contraseñas de Dashlane

Las contraseñas son la base de unas buenas prácticas de seguridad *online*. Los datos de siniestros de Chubb muestran que una gestión deficiente de las contraseñas puede provocar importantes pérdidas cibernéticas. La herramienta de gestión de contraseñas de Dashlane es gratuita para los asegurados de Chubb.

2. Prácticas y formación sobre *phishing* de Cofense

Este programa de formación sobre *phishing* está diseñado para identificar la susceptibilidad y el riesgo de ataques de *phishing*, un importante punto débil que ha provocado muchas pérdidas cibernéticas.

3. Aplicación Cyber Alert® de Chubb

Responder a un evento cibernético puede ser muy difícil, y no contar con el apoyo de expertos especializados puede aumentar las pérdidas derivadas de dicho evento. La aplicación gratuita de Chubb Cyber Alert® ofrece a los asegurados medios eficaces e inmediatos para notificar un siniestro y ponerse en contacto con nuestros especialistas en respuesta a incidentes cibernéticos

4. Otros servicios

En algunas regiones ofrecemos otros servicios a los asegurados, como formación sobre seguridad cibernética, evaluaciones de riesgo, ejercicios de planificación y otros servicios de mitigación de pérdidas cibernéticas. Descubra los servicios disponibles en su país aquí:

Obtener más información

www.chubb.com/uk-en/business/cyber-services-registration.aspx

Para obtener más información, póngase en contacto con nuestro equipo de asesoramiento sobre riesgos cibernéticos
cyber@chubb.com

Servicios de Respuesta a Incidentes - Perspectiva

Si bien los servicios de mitigación de pérdidas cibernéticas de Chubb pueden ayudar a disminuir las posibilidades de un evento cibernético, la realidad es que ningún nivel de protección es infalible contra las amenazas cibernéticas. Las pólizas cibernéticas de Chubb incluyen nuestra red de especialistas en respuesta a incidentes que están disponibles las 24 horas del día y los 365 días del año y están preparados para ayudar a nuestros asegurados a recuperarse de cualquier evento cibernético.

Puntos destacados

Chubb ayuda a las empresas a recuperarse de un incidente cibernético todos los días en todo el mundo.

>Cuando los asegurados notifican un incidente cibernético a través del centro de respuesta a incidentes cibernéticos de Chubb, reciben **asistencia inmediata** de un especialista en informes cibernéticos para recopilar detalles importantes con el fin de reunir a los expertos adecuados. El 90 % de estos asegurados, transcurridos aproximadamente 15 minutos, recibirán una llamada de un experto gestor de respuestas a incidentes.

Flexibilidad en cuanto a los proveedores - >: somos conscientes de que algunas empresas desean recurrir a proveedores que no forman parte de nuestra red. Chubb ofrece flexibilidad para que los asegurados recurran a los especialistas de su elección en muchos territorios, y estos pueden incluirse sin problemas en nuestra red de respuesta a incidentes.

Compruebe cómo funciona nuestro proceso de respuesta a incidentes aquí:

Siguiente

Servicios de Respuesta a Incidentes - Cómo Funciona

Esta guía explica cómo acceder al Equipo de Respuesta a Incidentes Cibernéticos de Chubb, cómo informar un siniestro y qué esperar de nuestra Plataforma de Respuesta a Incidentes.

1 El cliente es víctima de un incidente cibernético

La plataforma de respuesta a incidentes de Chubb está disponible las 24 horas del día, los 365 días del año. Proporciona acceso al Centro de Respuesta a Incidentes Cibernéticos de Chubb y a nuestro Equipo de Respuesta a Incidentes Cibernéticos y ofrece un enfoque integral para la gestión de eventos cibernéticos.

2 El cliente informa del incidente cibernético utilizando cualquiera de los siguientes métodos:

Aplicación móvil Chubb Cyber Alert®

Está disponible en la Apple Store y en la Google Play Store

Download on the App Store | ANDROID APP ON Google play

Online

Acceda a nuestra plataforma: www.chubbcyberalert.com

Línea telefónica directa

A continuación podrá encontrar el número de teléfono para su país:

Números Gratuitos por País:

Argentina	**800 666 1967**
Australia	**1 800 027428**
Austria	**0800 005 376**
Bélgica	**800 49 405**
Brasil	**0800 095 7346**
Canadá	**1 866 561 8612**
Chile	**1 230 020 1212**
China	**400 120 5310**
Colombia	**01 800 518 2642**
República Checa	**800 142 853**
Dinamarca	**80 250 571**
Finlandia	**0 800 1 12382**
Francia	**08 05 10 12 80**
Alemania	**0800 589 3743**
Hong Kong	**800 900 659**
Indonesia	**001 803 011 2974**
Irlanda	**1 80 093 7331**
Israel	**1 80 921 3812**
Italia	**80 019 4721**
Japón	**00531 1 21575**
Corea del Sur	**00798 14 800 6017**
Malasia	**1 800 8 12541**
México	**001 855 250 4580**
Países Bajos	**0800 020 3267**
Nueva Zelanda	**0800 441402**
Noruega	**800 12554**
Panamá	**001 800 507 3360**
Perú	**0800 56006**
Polonia	**00 800 121 4960**
Portugal	**800 8 14130**
Singapur	**800 120 6727**
Sudáfrica	**080 09 82340**
España	**800 810 089**
Suecia	**020 088 3181**
Suiza	**080 016 6223**
Taiwán	**00801 13 6828**
Turquía	**0811 213 0171 (landline)**
Turquía	**0812 213 0043 (mobile)**
EAU	**8000 444 4411**
Reino Unido	**0800 279 7004**
Estados Unidos	**1 844 740 9227**
Vietnam	**1203 2353 (VNPT)**
Vietnam	**1228 0688 (Viettel)**

Gestión de Respuesta a Incidentes - Cómo funciona

3 Contacto del Centro de Respuesta a Incidentes de Chubb

En el plazo de 1 minuto desde que se informa el incidente, el cliente será contactado por un asesor para recopilar la siguiente información:

- Nombre del asegurado
- Ubicación de la póliza
- Datos de contacto
- Ubicación del incidente

La información se enviará al equipo local de gestión de respuesta a incidentes y al Departamento de Siniestros de Chubb. Mantener a Chubb informado le permitirá obtener la respuesta más eficiente de la póliza.

4 Gestión de Respuesta a Incidentes

En el plazo de 1 hora de la comunicación, el cliente recibirá una llamada telefónica de un gestor local de respuesta a incidentes en el lugar donde se produzca el incidente.

- Realizar la investigación inicial
- Desarrollar un plan de acción de respuesta para contener el incidente
- Designar a especialistas que ayuden con el asesoramiento y la recuperación:

Informática forense | Asesoría Legal | Relaciones Públicas | Cumplimiento Regulatorio | Protección de Identidad | Control de Crédito | Contabilidad Forense

5 Recuperación

Mientras un equipo de proveedores expertos trabaja para contener el incidente, el Equipo de Respuesta a Incidentes Cibernéticos le ayudará en la recuperación de sus actividades comerciales.

6 Seguimiento

Los proveedores especializados de Chubb considerarán la prestación de servicios adicionales con el objeto de analizar el incidente y establecer reparaciones futuras, una revisión de las lecciones aprendidas y consejos de mitigación de riesgos.

Cobertura – Gestión de Riesgos Cibernéticos Empresariales

La cobertura

Daños Propios

- **Respuesta a Incidentes** - de un incidente cibernético real o presunto
- **Interrupción de Negocio** - pérdida de beneficios netos y gastos de continuación de la actividad
- **Recuperación de Datos y Sistemas** - aumento del coste del trabajo, costes de recuperación de datos, mitigación de interrupción adicional del negocio
- **Extorsión Cibernética** - pagos de extorsión y negociación

Daños a Terceros

- **Responsabilidad por Privacidad y Seguridad de la Red** - responsabilidad derivada de la vulneración de datos o el fallo de seguridad de la red:
  - **Pérdida de Tarjetas de Pago** responsabilidades contractuales frente a las empresas del sector de las tarjetas de pago como resultado de un incidente cibernético
  - **Fondo de compensación del consumidor**
  - **Multas** y sanciones (cuando sean legalmente asegurables) - RGPD
- **Responsabilidad por Actividad en Medios** - responsabilidad por difamación o infracción *online*

Puntos Destacados

- **Interrupción de Negocio Contingente** para proveedores tecnológicos subcontratados
- **Fallo del Sistema** incluye error humano, error de programación, y fallo eléctrico
- **Extensiones estándar:**
  - **Gastos de respuesta de emergencia a incidentes**: gastos en 48 horas para las pymes y clientes de medio mercadoinsureds
  - **Gastos de Mejora** -mejora de software y aplicaciones
  - **Delito cibernético** - pérdidas económicas directa tras un robo cibernético
  - **Gastos de recompensa**
  - **Fraude de telecomunicaciones**
- **Pagar en nombre del cliente** por los gastos de respuesta a incidentes
- **Flexibilidad con los proveedores de respuesta a incidentes**
- **Empleado deshonesto**
- **Notificación voluntaria**
- **Cierre voluntario**
- **Daños a la reputación***
- **Fraude de Ingeniería** Social (SEF)*
- Introducción de la cobertura de Eventos Generalizados

*mediante endoso

Endosos

Chubb aborda los crecientes riesgos cibernéticos con un enfoque flexible y sostenible. Los titulares de las pólizas pueden adaptar los niveles de cobertura del seguro cibernético para los eventos generalizados, los casos de *ransomware* y las vulnerabilidades de *software* vulnerables.

1 Eventos Generalizados

El mundo se va digitalizando e interconectando cada vez más año tras año. Los programas de software, las plataformas de comunicación y las plataformas tecnológicas ampliamente utilizados son aprovechados y, a menudo, miles o millones de empresas confían en ellos. Un solo ataque y/o fallo de una de estas plataformas o tecnologías ampliamente utilizadas podría crear un riesgo de agregación que exceda la capacidad de la industria de seguros para asegurar. Con el fin de ofrecer a los asegurados claridad en la cobertura y estabilidad en el mercado, Chubb proporciona límites, franquicias y coaseguros específicos para dichos Eventos Generalizados.

Los tipos de Eventos Generalizados cubiertos incluyen:

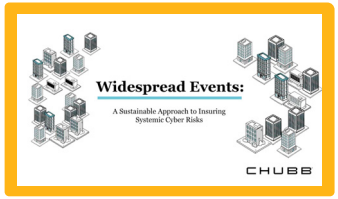
- Eventos Generalizados de la Cadena de Suministro de Software
  Se trata de ataques que permiten a los perpetradores entrar en los sistemas a través de *software* de confianza y certificado, y son, a efectos prácticos, un caballo de troyanos para un sistema.
- **Eventos Generalizados Graves de Día Cero**
  Estos ataques se derivan de determinadas vulnerabilidades de *software* conocidas por los ciberdelincuentes, pero aún no por el resto; se trata de vulnerabilidades que se pueden aprovechar fácilmente, son potencialmente graves y a menudo carecen de protección.
- **Eventos Generalizados de Vulnerabilidad Grave**
  Se trata de ataques derivados de graves vulnerabilidades de *software* conocidas y no parcheadas. Las vulnerabilidades se consideran graves, ya que son fáciles de aprovechar, se pueden desplegar remotamente con privilegios de acceso limitados y causar un efecto adverso considerable.[1]
- **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 evento cibernético catastrófico. Internet y algunos servicios de telecomunicaciones han alcanzado el nivel de infraestructura crítica para la sociedad, y algunas grandes empresas de computación en la nube son tan utilizadas que una interrupción generalizada podría afectar a las operaciones comerciales de miles o incluso millones de empresas.

Ejemplos prácticos de los peligros de los Eventos Generalizados:

- Eventos Generalizado de la Cadena de Suministro de *Software* Solorigate (2020), NotPetya (2017)
- Eventos Generalizado Grave de Día de Cero: Hafnio (2021)
- Eventos Generalizado de Vulnerabilidades Graves: Ataque MSSP (2021)
- Resto de Eventos Generalizados: Interrupción de la nube en Virginia (2020)

El endoso de Evento Generalizados de Chubb recoge normas de ajuste de pérdidas concisas y sensatas, por ejemplo:

- Los gastos de respuesta a incidentes no erosionan los límites de Eventos Generalizados hasta después de que se determine que un incidente es un Evento Generalizado, sin que se devuelvan los gastos originados antes de esa determinación.
- Los asegurados pueden optar por no compartir determinados tipos de datos de investigación cuando se acuerda mutuamente que un incidente es un Evento Generalizado.
- Todos los incidentes cibernéticos se clasifican como Eventos de Impacto Limitado (por ejemplo, un evento local con normas de pérdida habituales) o Evento Generalizado (por ejemplo, un evento sistemático con diferencias de ajuste de pérdida estructural como límites, franquicias y coaseguros), lo que permite a los asegurados adquirir la cobertura que mejor se adapte a las necesidades de su organización.



Eventos Generalizados

[1]Tendencias de Vulnerabilidades NIST Security en 2020: Un Análisis (2021). Disponible en https://www.redscan.com/media/Redscan_NIST-Vulnerability-Analysis-2020_v1.0.pdf

Otras secciones de cobertura

2 *Ransomware*

Los ataques de *ransomware* han crecido drásticamente tanto en frecuencia como en gravedad. Las implicaciones de pérdidas para los asegurados son mucho más amplias que el valor del importe del rescate. Tanto si se paga el rescate como si no, los asegurados suelen incurrir en costes legales, gastos de investigación forense, pérdidas por interrupción de negocio, gastos de recuperación de datos digitales y, en ocasiones, gastos de responsabilidad civil y defensa legal.

La sección de *ransomware* permite adaptar los límites de la cobertura, la franquicia y el coaseguro para las pérdidas originadas a resultas de un incidente de este tipo.

3 Eventos de *Software* Vulnerable

Mantener el *software* actualizado es un aspecto importante de una buena higiene de Ciberriesgos. Muchas pérdidas pueden evitarse parcheando el *software* vulnerable antes de que los ciberdelincuentes tengan la oportunidad de explotarlo, pero algunas organizaciones pueden no hacerlo de inmediato. A veces hay razones legítimas por las que las actualizaciones de *software* deben probarse antes de ser desplegadas, y la compatibilidad, la capacidad o simples problemas logísticos pueden impedir incluso a una organización de seguridad de la información bien gestionada desplegar los parches en el primer día o semana desde su lanzamiento. Por ese motivo, Chubb ofrece a los asegurados un periodo de gracia de 45 días para parchear las vulnerabilidades de *software* que se publican como Vulnerabilidades y Exposiciones Comunes (CVE) dentro de la Base de Datos Nacional de Vulnerabilidades operada por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST).

La sección de Eventos de *Software* Vulnerable ofrece cobertura tras el vencimiento del periodo de gracia de 45 días, y el reparto del riesgo entre el asegurado y la aseguradora se desplaza progresivamente hacia el asegurado, que asume un riesgo cada vez mayor si la vulnerabilidad no se parchea en 45, 90, 180 y 365 días.

***Software* Vulnerable**

Apetito

Para ayudarle a prestar un mejor servicio a sus clientes, hemos creado el siguiente resumen de nuestro apetito. No se trata de una lista exhaustiva, sino de una orientación general. Para riesgos únicos o sectores que no figuran en la lista, póngase en contacto con nuestro equipo de suscripción para discutir sus necesidades.

De preferencia

- Publicidad*
- Agricultura
- Arquitectos e ingenieros
- Galerías de arte y Museos
- Concesionarios de Automóviles y Estaciones de Servicio
- Productos Químicos y Similares
- Comunicaciones*
- Construcción
- Producción y Fabricación de Alimentos
- Contratistas Generales
- Consultores de Gestión
- Consultores de *Marketing*
- Organizaciones Sin Ánimo de Lucro
- Artes Escénicas y Teatro*
- Impresión y Publicación*
- Fabricación de Productos
- Sector Inmobiliario
- Consultoría Técnica
- Asociaciones Comerciales
- Producción de Televisión/ Radio/Cine*
- Comercio Mayorista

Aceptado

- Contabilidad
- Proveedores de Servicios Sanitarios
- Administradores de Activos
- *Hardware* y *Software* Informático
- Instituciones de Depósito
- Consultas de Médicos y Dentistas
- Agencia de Empleo/Agencia de Personal
- Ingeniería y Administración/ Servicios de Fabricación
- Instituciones Financieras (no indicadas en otra parte)
- Fabricación Industrial
- Gestoras de Inversiones/Fondos
- Bufetes de Abogados (Corporativos)
- Agentes Hipotecarios
- Servicios Personales
- Servicios Profesionales (no indicadas en otra parte)
- Restaurantes / Hostelería
- Minoristas
- Servicios de Transporte (no indicados en otra parte)

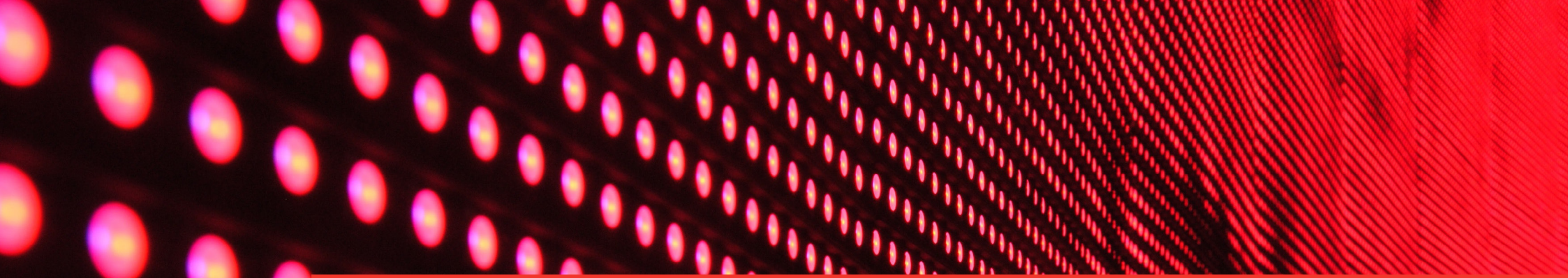
Selectivo

- Centro de Residencias Asistidas
- Servicios de Facturación
- Radiodifusión*
- Call Centers
- Agencias de Cobro
- Colegios y Universidades
- Comerciantes de Materias Primas
- Establecimientos de Cambio de Divisas
- Gobierno
- Hospitales
- Seguros (líneas no personales)
- Notarios
- Residencias de Ancianos / Retiro
- Administración Pública
- Autoridad Pública / Municipalidades
- Caja de Ahorros para Particulares
- Corredores de Valores y Materias Primas
- Colegios Pequeños / Consejo Escolar (preescolar a 12 años)
- Telecomunicaciones
- Servicios de *Telemarketing**
- Agentes de Títulos
- Servicios Públicos

Prohibido

- Contenido para Adultos
- Aerolíneas
- Intermediarios de Criptomonedas
- Ofertas Públicas de Moneda
- Agregadores de Datos
- Intercambios *Online*
- Sitios Web / Aplicaciones
- Plataformas de Negociación

*No se incluyen las coberturas de E&O de Medios de Comunicación



CHUBB®

Para obtener más información

Para obtener más información sobre nuestra oferta de seguros cibernéticos, póngase en contacto con nuestros suscriptores o visite **www.chubb.com/cyber**

Volver al inicio

SP-0279-MD