



COLECCIÓN PARTICULARES · BIBLIOTECA MOLINA LÓPEZ

Guía de Seguros para Ciberseguridad y Fraude Digital

*Qué cubre realmente un seguro de ciberseguridad, qué asistencia
puede prestar y qué protección ofrece ya su banco*

*Fraude bancario, robo de identidad, ciberextorsión y protección jurídica
digital explicados con criterio para particulares y familias.*

ML-GUIA-CIB-001 · Colección Particulares · v1.0

Mateo Molina · Molina López · 2026

CARTA AL LECTOR

Antes de empezar

Un cargo no reconocido en la tarjeta, un correo que suplanta a su banco, una cuenta de redes sociales a la que ya no puede acceder. Cada vez más familias españolas se relacionan con este tipo de incidentes sin tener claro qué protección tienen realmente, ni quién responde: el banco, la aseguradora o nadie.

El seguro de ciberseguridad y fraude digital para particulares es un producto relativamente reciente y, con frecuencia, mal entendido: parte de lo que promete ya está protegido por la normativa bancaria, y parte de lo que preocupa a las familias —el ciberacoso a un hijo, la ciberextorsión, la gestión de una brecha de datos personales— no siempre está cubierto por defecto.

Además, no todas las garantías funcionan mediante una indemnización económica. En algunos productos, una parte importante del valor está en la asistencia inmediata: recuperación de cuentas, limpieza de dispositivos, restauración de datos, retirada de contenidos, apoyo psicológico o acompañamiento jurídico.

Esta guía distingue lo que ya protege la ley de lo que aporta realmente una póliza, recorre las coberturas principales, las exclusiones más habituales y los errores frecuentes al contratar. Al final encontrará un checklist para revisar su propia póliza, o la que esté valorando contratar.

Mateo Molina

Molina López · Análisis y Optimización de Seguros

RESUMEN EJECUTIVO

Seguros, coberturas y garantías que conviene revisar

Antes de entrar en el detalle de cada cobertura, esta tabla identifica los seguros y garantías relevantes para un particular o una familia frente al fraude digital, con su nivel de criticidad orientativo y qué aspecto conviene verificar en cada caso. No todas las garantías existen en todas las pólizas: la disponibilidad depende de la aseguradora y de la modalidad contratada.

SEGURO / GARANTÍA	QUÉ DEBE REVISARSE
Fraude en banca online y medios de pago CRÍTICA	Puede cubrir determinados perjuicios económicos derivados de fraude bancario que no hayan sido reembolsados por la entidad, dentro de los límites, franquicias y supuestos contratados. Debe distinguirse entre operaciones de pago no autorizadas y pagos o transferencias que el asegurado realizó o confirmó como consecuencia de un engaño.
Robo de identidad digital ALTA	Puede cubrir los gastos de restitución de identidad, asistencia para recuperar cuentas suplantadas y gestión de la incidencia. Debe verificarse qué documentación se exige para acreditar la suplantación.
Ciberextorsión y ransomware ALTA	Puede incluir la gestión técnica del incidente, investigación, limpieza de sistemas, restauración de datos y asesoramiento especializado ante amenazas o secuestro de información. Debe comprobarse qué servicios se prestan, qué gastos se reembolsan y si el pago de rescates está excluido.
Protección jurídica digital ALTA	Puede cubrir defensa y reclamación en conflictos derivados del uso de internet: contrataciones fraudulentas, disputas con plataformas o proveedores digitales. Debe verificarse el ámbito de cobertura y el límite de gastos de defensa.
Gestión de reputación online SEGÚN PÓLIZA	Puede incluir asesoramiento o gestiones para la retirada de contenido difamatorio o no autorizado. Debe verificarse si es una gestión de asistencia o una indemnización económica.

RESUMEN EJECUTIVO · CONTINUACIÓN

SEGURO / GARANTÍA	QUÉ DEBE REVISARSE
Ciberacoso y protección de menores SEGÚN COMPOSICIÓN FAMILIAR	Puede incluir apoyo psicológico, asistencia legal, retirada de contenidos, recuperación reputacional y ayuda ante situaciones de ciberacoso, hostigamiento o suplantación sufridas por menores del hogar. Debe verificarse quiénes quedan asegurados, qué hechos activan la garantía y si solo está disponible en modalidades familiares.
Responsabilidad civil digital SEGÚN PÓLIZA	Puede cubrir, dentro de las condiciones de la póliza, daños causados a terceros derivados del uso indebido de dispositivos o redes propias, por ejemplo la propagación involuntaria de software malicioso. Debe verificarse el capital y las exclusiones aplicables.
Asistencia técnica, prevención y recuperación OPCIONAL	Puede incluir soporte remoto, revisión de vulnerabilidades, protección frente a malware o ransomware, recuperación de cuentas, limpieza de dispositivos y restauración de datos. Debe comprobarse qué servicios son preventivos, cuáles se prestan únicamente después de un incidente y si existen límites de uso.
Fraude en compras online OPCIONAL	Puede cubrir determinados perjuicios derivados de compras fraudulentas, comercios inexistentes o bienes no entregados, siempre que se cumplan las condiciones contratadas. Debe comprobarse su coordinación con la protección de la tarjeta, la plataforma de pago, el marketplace y los mecanismos ordinarios de reclamación.
Esta tabla tiene finalidad orientativa. La disponibilidad, el alcance y los límites de cada garantía dependen de la póliza concreta contratada y pueden variar entre aseguradoras. Se recomienda verificar siempre las condiciones particulares y generales del contrato.	

CAPÍTULO 1

Qué es —y qué no es— un seguro de ciberseguridad para particulares

Bajo la etiqueta genérica de «seguro de ciberseguridad» conviven productos con alcances muy distintos, y una parte importante de lo que muchas familias creen que necesitan asegurar ya está protegido por otras vías. Antes de comparar pólizas conviene distinguir tres planos.

Lo que ya protege la normativa bancaria

En España, las operaciones de pago no autorizadas están sujetas al régimen establecido por el Real Decreto-ley 19/2018, de servicios de pago. Con carácter general, la entidad debe restituir el importe en los términos previstos por esta normativa, salvo que concurren circunstancias como la actuación fraudulenta o la negligencia grave del usuario.

Este régimen no debe confundirse con los pagos o transferencias que el propio cliente realizó o confirmó bajo engaño. En estos casos, la recuperación del dinero puede requerir un análisis diferente de la operación, de las medidas de seguridad aplicadas y de la actuación de las partes. Un seguro de fraude digital no sustituye la protección bancaria: puede complementarla en los supuestos incluidos en la póliza y mediante servicios técnicos, jurídicos o de recuperación.

Lo que aporta realmente una póliza de ciberseguridad

El valor añadido de estas pólizas suele concentrarse en tres áreas: la asistencia inmediata ante un incidente (técnica, legal o psicológica), la cobertura de gastos que la vía bancaria o legal no cubre directamente, y las garantías que no tienen respaldo normativo previo, como el ciberacoso, la gestión de reputación o la ciberextorsión.

Cuatro formas distintas de protección

Una póliza de ciberseguridad puede responder de distintas maneras ante un incidente:

- Indemnización económica, por una pérdida cubierta.
- Reembolso de gastos, como restauración de datos, reposición de equipos o recuperación de identidad.
- Asistencia técnica o jurídica, prestada directamente por profesionales.
- Servicios preventivos, como análisis de vulnerabilidades, protección frente a malware, control parental o vigilancia digital.

Antes de comparar capitales, conviene identificar cuál de estas modalidades ofrece realmente cada garantía.

◆ EL CRITERIO DE MOLINA LÓPEZ

Antes de valorar el precio, conviene revisar tres elementos: qué protección ofrece ya el banco o el seguro de hogar, qué pérdidas económicas añade la póliza y qué servicios preventivos, técnicos, jurídicos o psicológicos presta antes y después del incidente.

Relación con el seguro de hogar

Algunas pólizas de hogar incluyen ya una garantía de ciberriesgos o fraude online como extensión, mientras que otras no la contemplan en absoluto. Conviene verificar primero las condiciones del seguro de hogar antes de contratar una póliza específica que podría duplicar cobertura ya existente.

CAPÍTULO 2

Fraude bancario y robo de identidad digital

Estas dos coberturas concentran buena parte del interés de las familias al contratar este tipo de seguro, y también buena parte de la confusión sobre qué protege realmente cada vía —bancaria, aseguradora o ambas—.

Situación	Qué suele verificarse
Operaciones no autorizadas en tarjeta o cuenta	Debe verificarse la franquicia aplicable y si la póliza actúa como complemento a la obligación de reembolso de la entidad bancaria o como cobertura independiente para los supuestos excluidos de esa obligación.
Phishing, smishing y vishing	Puede cubrir, según las condiciones de la póliza, determinadas pérdidas derivadas de la obtención fraudulenta de credenciales o de operaciones realizadas mediante engaño. Debe comprobarse si incluye pagos o transferencias confirmados por el asegurado, operaciones efectuadas tras llamadas, mensajes o páginas de suplantación y qué comunicaciones o denuncias exige para tramitar el siniestro.

Situación	Qué suele verificarse
Suplantación de identidad en redes o plataformas	Puede incluir asistencia para recuperar el acceso a cuentas y gestionar la incidencia ante la plataforma correspondiente.
Apertura fraudulenta de cuentas o contratos a su nombre	Puede cubrir gastos de gestión y documentación para acreditar la suplantación ante terceros.
Uso indebido de datos personales tras una brecha de terceros	Debe verificarse si la póliza cubre las consecuencias de una brecha sufrida por un tercero (una empresa, un servicio online) que afecte a sus datos, no solo los incidentes originados en sus propios dispositivos.

Restauración de datos y reposición de dispositivos

Algunas pólizas no se limitan a cubrir el fraude económico. También pueden incluir la recuperación de datos o la reposición de dispositivos dañados, alterados o inutilizados como consecuencia directa de un incidente cibernético. Debe comprobarse si se indemniza el valor del equipo, el coste de reparación o únicamente el servicio técnico de restauración.

CAPÍTULO 2 · CONTINUACIÓN

Franquicias y límites por incidente

Es habitual que estas garantías incluyan una franquicia por incidente y un límite máximo de indemnización anual o por suceso. Ambos elementos condicionan el alcance real de la cobertura y deben compararse junto con el precio de la prima, no de forma aislada.

También debe comprobarse si existe un único límite máximo compartido por todas las garantías o límites independientes para cada una. Una póliza puede ofrecer muchas coberturas, pero con un capital conjunto relativamente reducido.

“Ante un fraude bancario, comunique la incidencia de inmediato a la entidad y revise también el plazo de notificación de la póliza. Banco y aseguradora pueden intervenir por vías distintas, pero no cabe obtener una doble compensación por la misma pérdida.”

Documentación y plazos

Según el tipo de incidente, la póliza puede exigir denuncia, comunicación a la entidad afectada, bloqueo de cuentas o dispositivos y notificación a las autoridades competentes. También puede establecer un plazo concreto desde la detección del hecho. No seguir el procedimiento o los plazos contratados puede dificultar la tramitación del siniestro.

CAPÍTULO 3

Protección jurídica digital y ciberacoso

Más allá del fraude económico, buena parte del valor de estas pólizas para una familia está en la asistencia ante conflictos y situaciones que no tienen una vía de reclamación tan clara como el fraude bancario.

Protección jurídica digital

Puede cubrir, dentro de las condiciones de la póliza, la defensa y reclamación en conflictos derivados del uso de internet: contrataciones fraudulentas, disputas con plataformas de comercio electrónico o proveedores de servicios digitales, y reclamaciones frente a terceros por daños causados a través de medios digitales. Debe verificarse el límite de gastos de defensa y si incluye la vía judicial o solo gestiones extrajudiciales.

Ciberacoso y protección de menores

Algunas pólizas familiares incluyen asistencia psicológica o legal ante situaciones de acoso digital sufridas por un menor del hogar. Esta es una de las garantías menos estandarizadas del mercado: su existencia, alcance y condiciones de activación varían considerablemente entre aseguradoras, por lo que no debe darse por incluida sin verificarlo expresamente.

También debe comprobarse si la póliza presta ayuda para localizar, documentar y solicitar la retirada de contenidos perjudiciales, y si incluye captura o certificación de evidencias para su posible utilización en una reclamación.

◆ EL CRITERIO DE MOLINA LÓPEZ

Si en su hogar hay menores, la cobertura de ciberacoso merece una revisión específica: no todas las pólizas la incluyen, y entre las que la incluyen, el alcance de la asistencia varía mucho más que en otras garantías más estandarizadas como el fraude bancario.

Coordinación con la asistencia jurídica familiar

Una póliza de ciberriesgo puede ofrecer asistencia técnica, gestión del incidente y determinadas indemnizaciones, mientras que una cobertura de asistencia jurídica familiar puede reforzar la defensa, la reclamación frente a bancos, plataformas o comercios y el asesoramiento legal en conflictos digitales. Debe revisarse cómo se coordinan ambas pólizas para evitar duplicidades y lagunas de cobertura.

CAPÍTULO 3 · CONTINUACIÓN

Exclusiones habituales

1 Negligencia grave en la custodia de credenciales

El incumplimiento de las medidas de seguridad exigidas expresamente por la póliza —por ejemplo, compartir credenciales o no mantener activadas determinadas funciones de protección— puede afectar a la cobertura cuando guarde relación directa con el incidente.

2 Dispositivos sin actualizaciones de seguridad

Algunas pólizas condicionan la cobertura a mantener el sistema operativo y el antivirus razonablemente actualizados en el dispositivo afectado.

3 Actividad profesional o empresarial

Las pólizas de particulares suelen excluir incidentes derivados del uso profesional del dispositivo o de una actividad económica, que requieren un seguro de ciberriesgos empresarial distinto.

4 Criptoactivos y monederos digitales

Con frecuencia excluidos o sujetos a condiciones especiales, dada la dificultad de acreditar la titularidad y el valor de este tipo de activos.

CAPÍTULO 4

Matices que conviene conocer antes de un incidente

Más allá de las exclusiones, el condicionado de cada póliza contempla matices que conviene identificar antes de que se produzca un incidente, no después.

Dispositivos cubiertos

Debe verificarse si la póliza cubre todos los dispositivos del hogar —ordenadores, móviles, tablets— o solo un número determinado, y si es necesario declararlos expresamente para que queden incluidos.

Servicios preventivos incluidos

Algunas pólizas incluyen herramientas de protección, antivirus, control parental, vigilancia de credenciales comprometidas, copias de seguridad o asesoramiento para configurar dispositivos y contraseñas. Debe comprobarse si estos servicios están incluidos durante toda la vigencia, si requieren activación o registro y a cuántos dispositivos se extienden.

Composición del hogar asegurado

Algunas garantías, como la protección ante ciberacoso, dependen de la composición familiar declarada. Conviene verificar si la póliza cubre a todos los miembros del hogar o solo al tomador.

Ámbito territorial

La mayoría de garantías operan con independencia del lugar donde se produzca el acceso fraudulento, pero algunas prestaciones de asistencia —legal o técnica— pueden limitarse al territorio español. Conviene verificarlo si la familia reside parte del año fuera de España.

CASO PRÁCTICO · Coordinación entre banco y aseguradora

Un cliente detecta un cargo fraudulento en su tarjeta y comunica el incidente tanto a su entidad bancaria como a su aseguradora. El banco devuelve finalmente el importe al considerar que se trataba de una operación no autorizada. La póliza no indemniza de nuevo esa misma pérdida, aunque podría mantener otras prestaciones cubiertas, como asistencia jurídica, recuperación de cuentas o gastos de gestión. El caso muestra que ambas vías pueden coordinarse, pero no generar una doble compensación por el mismo perjuicio.

CAPÍTULO 5

Errores frecuentes al contratar un seguro de ciberseguridad

- 1 Contratar sin revisar antes la protección que ya ofrece el banco**

Las operaciones de pago no autorizadas cuentan con una protección bancaria específica. Los pagos o transferencias que el cliente realizó bajo engaño pueden recibir un tratamiento diferente. Conviene identificar qué vía puede responder y qué añade realmente la póliza.
- 2 Asumir que el seguro de hogar ya incluye ciberriesgos**

No siempre es así; debe verificarse expresamente en las condiciones del seguro de hogar si existe esta extensión.
- 3 No declarar todos los dispositivos del hogar**

Si la póliza exige declaración expresa, un dispositivo no declarado puede quedar fuera de cobertura.
- 4 No verificar la cobertura de ciberacoso si hay menores en el hogar**

Es una de las garantías menos estandarizadas del mercado y no debe darse por incluida sin comprobarlo.
- 5 Ignorar los plazos de notificación del incidente**

La mayoría de aseguradoras exige comunicar el incidente en un plazo determinado desde su detección; superarlo puede dificultar la tramitación.
- 6 No conservar capturas, correos y justificantes del incidente**

La documentación del incidente en el momento en que ocurre suele ser más difícil de reconstruir después y es habitualmente exigida para tramitar el siniestro.
- 7 Valorar la póliza únicamente por el capital de indemnización**

Una parte importante del valor puede encontrarse en la asistencia técnica, recuperación de cuentas, restauración de datos, retirada de contenidos, prevención y apoyo jurídico o psicológico. Deben compararse conjuntamente capitales y servicios.

CAPÍTULO 6

Preguntas clave antes de contratar o renovar

Estas son las preguntas que conviene resolver con la aseguradora o el asesor antes de firmar la póliza, o antes de renovarla sin revisarla.

- ¿Qué franquicia y qué límite máximo se aplican al fraude en banca online y medios de pago?
- ¿La póliza cubre supuestos ya protegidos por la obligación de reembolso de mi entidad bancaria, o solo los que quedan fuera de ella?
- ¿La póliza cubre únicamente operaciones no autorizadas o también pagos y transferencias que yo mismo confirmé bajo engaño?
- ¿Incluye asistencia ante ciberacoso a menores del hogar, y bajo qué condiciones se activa?
- ¿Qué dispositivos quedan cubiertos y es necesario declararlos expresamente?
- ¿Incluye protección jurídica digital, y con qué límite de gastos de defensa?
- ¿Qué plazo tengo para notificar un incidente y qué documentación se exige?
- ¿Debo comunicar el incidente simultáneamente al banco y a la aseguradora?
- ¿Qué requisitos de seguridad exige la póliza —actualizaciones, verificación en dos pasos— para que la cobertura sea aplicable?
- ¿Qué garantías indemnizan económicamente y cuáles prestan únicamente un servicio de asistencia?
- ¿Existe un límite único compartido por todas las coberturas o límites separados?
- ¿Incluye recuperación de datos y reposición o reparación de dispositivos?
- ¿Ofrece herramientas preventivas, antivirus, vigilancia digital o control parental?
- ¿Incluye recuperación de cuentas, retirada de contenidos y certificación de evidencias?
- ¿Cómo se coordina esta póliza con la asistencia jurídica familiar y el seguro de hogar?

CHECKLIST

Revisión de su póliza actual

Utilice este checklist para revisar la póliza que ya tiene contratada o la que esté valorando. No sustituye la lectura de las condiciones particulares y generales del contrato.

Fraude y dispositivos

- Franquicia y límite máximo de la cobertura de fraude bancario
- Coordinación con la reclamación y el posible reembolso de la entidad bancaria
- Cobertura de pagos y transferencias confirmados bajo engaño
- Dispositivos cubiertos y necesidad de declararlos
- Plazo de notificación del incidente y documentación exigida
- Requisitos de seguridad exigidos (actualizaciones, verificación en dos pasos)
- Límite general compartido y sublímites por cobertura
- Restauración de datos y reposición de hardware
- Número de dispositivos cubiertos y herramientas preventivas incluidas

Protección jurídica y asistencia

- Cobertura de ciberacoso si hay menores en el hogar
- Límite de gastos de la protección jurídica digital
- Alcance real de la asistencia ante ciberextorsión
- Ámbito territorial de las prestaciones de asistencia
- Solapamiento con la cobertura de ciberriesgos del seguro de hogar, si existe
- Recuperación de cuentas y retirada de contenidos
- Captura y certificación de evidencias digitales
- Coordinación con la asistencia jurídica familiar

Documentación que conviene reunir

- Justificantes bancarios de las operaciones afectadas por el fraude
- Capturas de pantalla, correos o mensajes relacionados con el incidente
- Denuncia o comunicación presentada ante las autoridades, si procede
- Relación de dispositivos del hogar y su estado de actualización
- Condiciones del seguro de hogar, para comprobar si ya incluye ciberriesgos

CIERRE

Ideas clave

- Las operaciones de pago no autorizadas cuentan con una protección bancaria específica, mientras que los pagos realizados bajo engaño pueden requerir un análisis diferente. Conviene identificar qué añade realmente la póliza antes de valorar su precio.
- La cobertura de ciberacoso a menores es una de las menos estandarizadas del mercado y no debe darse por incluida sin verificarlo expresamente.
- Las franquicias, los límites por incidente y los plazos de notificación determinan el alcance real de la cobertura tanto como el precio de la prima.
- Algunas pólizas de hogar o de asistencia jurídica ya incluyen protección frente a determinados conflictos digitales; conviene revisar cómo se coordinan con la póliza específica.
- El valor de una póliza de ciberriesgo no depende únicamente del capital indemnizable: la prevención, la asistencia técnica y la recuperación posterior pueden ser igual de importantes.

*Un seguro de ciberseguridad bien revisado no evita el intento de fraude.
Evita que ese intento se convierta en un problema económico y legal sin resolver.*

SOBRE MOLINA LÓPEZ

Molina López · Análisis y Optimización de Seguros trabaja con más de 95 aseguradoras para encontrar, en cada caso, el equilibrio entre garantía y coste que corresponde a la situación real del cliente. No somos un comparador: analizamos qué necesita realmente cada familia antes de recomendar una póliza. La revisión de sus seguros no tiene coste y no implica obligación de contratar. Es un servicio que ofrecemos siempre de forma gratuita.

AVISO LEGAL — Esta guía tiene finalidad exclusivamente informativa y divulgativa. No constituye asesoramiento jurídico ni una recomendación personalizada de contratación. Las coberturas, condiciones, límites, exclusiones y la normativa bancaria de referencia pueden variar; antes de contratar, mantener, cancelar o modificar cualquier seguro, debe revisarse la situación concreta y la documentación aplicable.