

LAS PRUEBAS **CUÁLES CONSERVAR Y CÓMO ORGANIZARLAS**

Concienciar. Prevenir. Formar.



Después de descubrir una estafa romántica, enfrentarse a meses o incluso años de mensajes, fotografías, llamadas y operaciones económicas puede resultar abrumador.

Quizá no sepas por dónde empezar. Algunos mensajes pueden producirte dolor o vergüenza y es posible que sientas el impulso de borrarlos. También puedes temer no conservar pruebas suficientes o que nadie comprenda cómo llegaste a confiar y a realizar determinados pagos.

No necesitas revisarlo ni ordenarlo todo en un solo día. Lo primero es evitar que la información desaparezca. Después podrás organizarla poco a poco, con ayuda de una persona de confianza si lo necesitas.

Conserva primero. Ordena después

Antes de bloquear perfiles, eliminar aplicaciones, cambiar de teléfono o borrar conversaciones, guarda todo lo relacionado con los hechos.

Siempre que puedas, realiza al menos dos copias y guárdalas en lugares diferentes. Protege con contraseña los archivos que contengan información personal, bancaria o íntima.

Siempre que sea posible:

- Conserva los archivos originales.
- Guarda una copia en un ordenador, memoria externa o espacio seguro.
- No recortes, escribas encima ni modifiques la única copia que tengas.
- Si quieres señalar algo importante, hazlo sobre una copia.

Las pruebas deben contar la historia completa

La estafa no comenzó con la primera transferencia. Antes hubo una identidad construida, un vínculo aparentemente auténtico y un proceso destinado a generar confianza. Después llegaron las dificultades, las urgencias, las promesas y las peticiones económicas.

Las pruebas deben ayudar a comprender:

Cómo se presentó → cómo construyó el vínculo → cómo consiguió el dinero o la información.

No se trata de justificar por qué confiaste, sino de mostrar cómo alguien creó deliberadamente las condiciones necesarias para conseguirlo.

IDENTIDAD Y PRIMER CONTACTO

Guarda la identidad utilizada

Reúne los datos con los que la persona se presentó:

- Nombre, apellidos, alias y nombres de usuario.
- Números de teléfono y correos electrónicos.
- Perfiles en aplicaciones de citas y redes sociales.
- Enlaces completos a esos perfiles.
- Fotografías, vídeos y documentos recibidos.
- Supuesta profesión, empresa, nacionalidad o lugar de residencia.
- Nombres de familiares, amistades, médicos, abogados u otras personas mencionadas en su historia.
- Copias de pasaportes, carnés, contratos, billetes, facturas o justificantes enviados.

Haz capturas en las que puedan verse el nombre del perfil, la plataforma y, cuando sea posible, la fecha. Guarda también el enlace: una fotografía aislada puede no permitir localizar posteriormente la cuenta.

Es importante distinguir entre la identidad utilizada para estafar y la persona real que aparece en las fotografías. Con frecuencia, las imágenes pertenecen a alguien completamente ajeno al delito cuya identidad también ha sido suplantada.

Conserva el inicio del contacto

Guarda el primer perfil, anuncio o mensaje y anota:

- La fecha aproximada del primer contacto.
- La aplicación, red social o página en la que os conocisteis.
- Quién inició la conversación y cómo se presentó.
- Cuándo propuso continuar por WhatsApp, Telegram, correo electrónico u otro canal.
- Qué motivo dio para abandonar la primera plataforma.

Si hubo varios perfiles, teléfonos o canales de comunicación, registra el orden en el que fueron apareciendo.

Guarda el perfil y su enlace antes de bloquearlo o denunciarlo en la plataforma.

CONVERSACIONES Y CONSTRUCCIÓN DEL VÍNCULO

Conserva las conversaciones completas

No guardes únicamente los mensajes en los que se pidió dinero. El periodo anterior permite comprender cómo se creó la relación y por qué las peticiones posteriores resultaron creíbles.

Si la aplicación lo permite, exporta o descarga la conversación completa. Conserva también:

- Correos electrónicos y mensajes de texto.
- Audios, notas de voz, fotografías y vídeos.
- Registros de llamadas y videollamadas.
- Archivos y documentos adjuntos.
- Amenazas, presiones o intentos de chantaje.
- Mensajes eliminados que todavía puedan recuperarse desde tus propias copias.



Si realizas capturas de pantalla, procura que aparezcan el nombre o número del remitente, la fecha y la hora. No elimines la conversación original después de hacerlas. Las capturas sirven para destacar momentos importantes, pero es preferible acompañarlas de la conversación completa.

Señala los momentos que explican la manipulación

No es necesario convertir cada mensaje cariñoso en una prueba independiente. Conserva la conversación completa y señala aquellos momentos que permitan comprender:

- Cómo se intensificó la relación.
- La frecuencia de las comunicaciones.
- Las declaraciones de amor o compromiso.
- Los planes de convivencia, matrimonio, viajes o proyectos compartidos.
- Las promesas de devolución del dinero.
- Las excusas para no acudir personalmente o no encontrarse contigo.
- Las peticiones de confidencialidad.
- Los intentos de alejarte de familiares o amistades.
- La presión para decidir o pagar con rapidez.
- Los reproches, silencios, amenazas o desapariciones cuando manifestabas dudas.

Estos mensajes ayudan a demostrar que no se trató de una petición económica aislada, sino de un proceso de captación y manipulación emocional.

PAGOS Y OPERACIONES ECONÓMICAS

Reúne los justificantes

Solicita a tu banco documentos oficiales siempre que sea posible. Una captura de la aplicación bancaria puede resultar útil inicialmente, pero un justificante completo suele contener más información.

Conserva:

- Extractos bancarios y justificantes de transferencias.
- Fecha, hora, importe, concepto, beneficiario y cuenta de destino.
- Pagos con tarjeta, Bizum u otras aplicaciones.
- Resguardos de empresas de envío de dinero.
- Facturas y códigos de tarjetas regalo.
- Préstamos solicitados para efectuar los pagos.
- Correos o mensajes de confirmación.
- Comunicaciones mantenidas con el banco.



Si entregaste dinero en efectivo, anota la fecha, la cantidad, el lugar, quién lo recogió y cualquier otro dato disponible. Guarda también los mensajes en los que se acordó la entrega.

Incluye todas las operaciones, aunque el dinero se enviara a diferentes personas, empresas, cuentas o países. Los destinatarios pueden haber sido presentados como familiares, médicos, abogados, agentes, proveedores o personas de confianza.

Si utilizaste criptomonedas

Guarda:

- El nombre de la plataforma utilizada.
- Los justificantes de compra.
- La dirección del monedero de origen y de destino.
- El identificador o hash de cada transacción.
- La red utilizada.
- La fecha, la hora y el importe.
- Los correos de confirmación.
- Las conversaciones con las instrucciones de envío.
- Los datos de quien te ayudó a realizar la operación.

Una imagen del saldo o la cantidad total enviada no es suficiente. El identificador de cada transacción permite localizar la operación dentro de la cadena de bloques.

OTRAS PRUEBAS IMPORTANTES

Gestiones con bancos y plataformas

Guarda constancia de las medidas adoptadas después de descubrir la estafa:

- Avisos y reclamaciones enviados al banco.
- Respuestas y números de incidencia o expediente.
- Solicitudes de cancelación o recuperación de transferencias.
- Comunicaciones con plataformas de pago o empresas de envío de dinero.
- Reportes realizados en aplicaciones de citas y redes sociales.
- Comunicaciones con empresas de telefonía o correo electrónico.
- Denuncias anteriores y posibles ampliaciones.

Anota la fecha, el medio utilizado y, cuando sea posible, el nombre o referencia de la persona que te atendió.

Documentos y acceso a tus dispositivos

Anota qué información personal compartiste: DNI o pasaporte, datos bancarios, fotografías de tarjetas, contraseñas, códigos de verificación, firmas, contratos, imágenes íntimas, dirección o información familiar y laboral.

Si instalaste una aplicación de acceso remoto o permitiste que alguien controlara tu pantalla, conserva el nombre del programa y las conversaciones en las que te indicaron instalarlo.

Si sospechas que el dispositivo continúa comprometido, evita manipularlo innecesariamente y busca ayuda técnica para protegerlo y conservar la información (**INCIBE 017**).

Amenazas, chantaje o suplantación

Conserva los mensajes intimidatorios, las amenazas, los intentos de chantaje y las advertencias sobre la difusión de fotografías.

No pagues para evitar la publicación de imágenes ni continúes enviando contenido. Si aparecen cuentas que utilizan tu nombre, tus fotografías o tus documentos, haz capturas y guarda los enlaces antes de solicitar su eliminación.

Mantén estas pruebas separadas del resto para poder localizarlas rápidamente.

CÓMO ORGANIZAR LA DOCUMENTACIÓN

No existe una única forma válida de hacerlo. Lo importante es que otra persona pueda localizar los documentos y comprender su relación con los hechos.

Crea una carpeta

Dentro de ella, puedes crear estas subcarpetas:

1. Resumen y cronología.
2. Perfiles e identidad utilizada.
3. Conversaciones y correos.
4. Fotografías, audios, vídeos y documentos.
5. Pagos y operaciones económicas.
6. Amenazas, chantaje o suplantación.
7. Comunicaciones con bancos y plataformas.
8. Denuncia y gestiones posteriores.



Pon nombres claros a los archivos

Dentro de cada carpeta, utiliza nombres sencillos que indiquen la fecha y el contenido. Por ejemplo:

- > 2026-03-15_Petición_transferencia_WhatsApp
- > 2026-03-16_Justificante_transferencia_2.000_euros
- > 2026-03-20_Promesa_devolución_mensaje

Utilizar primero el año, después el mes y finalmente el día permite que los archivos aparezcan automáticamente en orden cronológico.

No sustituye a los documentos originales. Es una forma de nombrar las copias que utilizarás para preparar la denuncia.

Numera las pruebas relevantes

- Documento 1. Captura del perfil utilizado.
- Documento 2. Enlace y nombre de usuario.
- Documento 3. Conversación inicial exportada.
- Documento 4. Mensaje en el que solicita continuar por WhatsApp.
- Documento 5. Justificante de la primera transferencia.

Después podrás utilizar estos números en la cronología y en la denuncia.



PREPARA DOS TABLAS SENCILLAS

1. Cronología de los hechos

La cronología relaciona la historia emocional, las peticiones y los movimientos económicos. No necesita estar redactada todavía como una denuncia.

FECHA	QUÉ OCURRIÓ	CANAL	PAGO	DOC.
15/1/2026	Primer contacto y presentación	Instagram	—	1
16/1/2026	Pide cambiar a WhatsApp	Instagram	—	4
17/3/2026	Explica supuesta emergencia	WhatsApp y audio	—	12 y 13
18/3/2026	Pide dinero con urgencia	WhatsApp	2.000€	14 y 15
5/4/2026	Pide más dinero para otra emergencia	Correo electrónico	1.500€	21 y 22

No tienes que recordar las fechas de memoria. Puedes reconstruirlas consultando las conversaciones, los correos y los movimientos bancarios.

Si no conoces el día exacto, indica que la fecha es aproximada en lugar de inventarla.

2. Relación de pagos

Cuando existen varias operaciones, reunir las en un único documento permite comprender el perjuicio económico y detectar cuentas o destinatarios diferentes.

FECHA	IMPORTE	MEDIO DE PAGO	DESTINATARIO	CUENTA/REF/MONEDERO	DOC
18/3/2026	2.000€	Transf.	Nombre	IBAN	15
5/4/2026	1.500€	Transf.	Nombre	IBAN	22
12/4/2026	500€	Tarjeta regalo		Códigos o referencias	27

Añade todas las operaciones relacionadas, aunque fueran destinadas a diferentes personas, países o medios de pago.

Al final, indica la cantidad total entregada. Si todavía falta alguna operación por confirmar, puedes señalar que el cálculo es provisional.

No es necesario imprimir miles de páginas sin explicación. Conserva las conversaciones completas y prepara una selección ordenada de los fragmentos más significativos, indicando siempre dónde puede encontrarse el contenido completo.

PROTÉGETE MIENTRAS CONSERVAS LAS PRUEBAS

Protege tu intimidad

No publiques en redes sociales nombres, fotografías, cuentas bancarias o detalles de la estrategia antes de denunciar. La exposición pública puede alertar a los responsables y perjudicar a personas cuya identidad haya sido suplantada.

Guarda las imágenes íntimas y la información especialmente sensible en un espacio seguro. No las reenvíes innecesariamente: puedes informar de su existencia y aportarlas cuando sean requeridas.

Si alguien te ayuda a organizar la documentación, elige a una persona de confianza. No necesitas darle tus contraseñas ni acceso a todas tus cuentas.

No tienes que investigar por tu cuenta

Tu tarea no consiste en descubrir la verdadera identidad del estafador, localizarlo físicamente ni demostrar todos los delitos cometidos.

No vuelvas a contactar para tenderle una trampa o conseguir una confesión. Tampoco pagues a desconocidos que aseguren poder recuperar el dinero o rastrear teléfonos, cuentas o monederos.

Conserva lo que tienes, ordénalo y entrégalo a las autoridades. La investigación corresponde a los organismos competentes.

Si otras personas presenciaron conversaciones, te acompañaron al banco o conocieron las peticiones económicas, anota sus datos. No difundas su información ni compartas conversaciones privadas sin su conocimiento.

Recuerda

No necesitas demostrarlo todo ni hacerlo en un solo día.

Guarda primero.
Ordena después.
Conserva los originales y
trabaja con copias.



No te limites a reunir justificantes de pago. Conserva también la historia que explica cómo se construyó la confianza y cómo fue utilizada para obtener dinero o información.

No retrases una denuncia, un aviso al banco o una medida urgente de protección por no haber terminado de ordenar toda la documentación. La información podrá completarse posteriormente.

Trabajemos juntos

Es fundamental trabajar juntos para prevenir las estafas emocionales y concienciar a la sociedad sobre sus mecanismos y consecuencias. Apoyar a las víctimas y ofrecer herramientas de prevención son pasos esenciales para combatir esta forma de violencia.

Si como profesional, empresa o institución quieres formar parte de este cambio, contáctanos en **observatorio@anceme.es**