

Modificación de un correo electrónico y de su documento adjunto

Fraude del cambio de cuenta bancaria en una provisión de fondos

Autor	Amador Cubino
Informe original	Noviembre de 2025
Versión pública	Octubre de 2026, con una revisión de las pruebas (apartado 9)
Publicada con	www.nantec.es/blog/fraude-del-cambio-de-cuenta-bancaria-auditoria-forense/

Esta versión está rehecha desde cero a partir del informe entregado. No lleva nombres de personas ni de empresas, direcciones de correo, dominios, servidores, cuentas bancarias, teléfonos, números de expediente, direcciones IP, identificadores de los mensajes ni la fecha exacta: se sustituyen por descripciones («la asesoría», «el cliente», «el día de los hechos»). Las horas son las reales, en hora peninsular española salvo cuando se indica UTC. Corrige dos erratas del original: el orden de los identificadores de los dos primeros correos y el alcance del doble factor (apartado 4).

1 Resumen

- El día de los hechos, un viernes del otoño de 2025, a las **12:30:32**, la asesoría envió desde su cuenta de Microsoft 365 a su cliente un correo con una provisión de fondos corregida en PDF.
- El servidor de correo del cliente lo recibió a las **12:31:17**, por una conexión cifrada, y lo dejó en el buzón.
- El correo que había en el buzón del cliente llevaba el PDF modificado, con otro número de cuenta, y la cabecera Date cambiada a las **12:55:45**. El PDF se modificó a las **12:55:27**. El resto del documento es idéntico.
- El cliente pagó más de 37.000 euros a la cuenta del PDF modificado.
- Los registros de Microsoft 365 no muestran ningún acceso ajeno a la cuenta de la asesoría.
- Conclusión:** el correo salió íntegro de la asesoría y se modificó después de entregarse, en el buzón o en el servidor de correo del destinatario, por alguien con acceso a ellos. La firma ARC de Microsoft lo confirma de forma criptográfica (apartado 9).

2 Objeto y alcance

Determinar si el correo de la provisión de fondos se modificó, en qué punto del camino y a qué hora, y si hubo un acceso no autorizado a la cuenta de correo de la asesoría.

Alcance: los registros de inicio de sesión de Microsoft 365 de la cuenta de la asesoría, el seguimiento de mensajes de Microsoft 365, las cabeceras de los correos enviados y recibidos, y los adjuntos y sus

metadatos. Quedan fuera los registros del servidor de correo del destinatario, que no estaban disponibles (apartado 10).

3 Pruebas examinadas y método

- **Correos enviados** (ENV01, ENV02 y ENV03): exportados de la carpeta Enviados de la cuenta de la asesoría.
- **Correos recibidos** (REC01, REC02 y REC03): exportados del buzón del cliente como ficheros .eml, con las cabeceras completas.
- **Adjuntos**: los PDF de la provisión de fondos de ENV03 y REC03.
- **Registros de inicio de sesión** de Microsoft Entra ID, interactivos y no interactivos, exportados en CSV.
- **Seguimiento de mensajes** del centro de administración de Exchange (capturas).

Herramientas: el centro de administración de Microsoft 365 y su seguimiento de mensajes, `pdfinfo` y `pdftotext` para los PDF, y la lectura de las cabeceras SMTP. En la revisión (apartado 9), la verificación de la firma ARC con la clave pública que Microsoft publica en su DNS.

4 Accesos a la cuenta de la asesoría

Registros del día de los hechos:

Tipo	Número	Aplicaciones	Origen
Interactivos (alguien entra con usuario y contraseña)	3	Outlook en la web	Conexión de la oficina
No interactivos (un programa ya autorizado renueva su acceso)	164	Outlook de escritorio, Outlook en el móvil y Outlook en la web	Conexión de la oficina y cuatro conexiones móviles de operadoras españolas

- **Orígenes**: todas las conexiones y dispositivos coinciden con los que usa habitualmente el personal de la asesoría, según la información facilitada. La ubicación que asigna Microsoft a una IP móvil no es fiable: la salida a Internet de las operadoras no está donde está el móvil.
- **Doble factor**: cada sesión nueva exige la aprobación en Microsoft Authenticator. De las 164 renovaciones, 132 constan con autenticación multifactor y 32 «de factor único», que son renovaciones de sesiones ya autorizadas. *El informe original decía que todos los accesos eran con doble factor; se corrige aquí.*
- **Errores**: 25 avisos de doble factor caducado, que obligan a repetirlo (código 50078), y una renovación pedida con la autorización de otra aplicación (700007). Ningún intento fallido de contraseña.
- Ningún país extranjero, ninguna aplicación desconocida y ningún acceso que no sea de la asesoría.

Conclusión: no hay indicios de acceso no autorizado a la cuenta de la asesoría.

5 Seguimiento de mensajes

El seguimiento de mensajes de Microsoft 365 muestra tres correos enviados ese día al cliente, los tres entregados. Las horas de la herramienta son UTC: en España, una hora más.

Fecha (UTC) ↓	Asunto	Estado
██████████ 11:30 AM	RE: Expediente ██████████ - COMPRAVENTA	Entregado
██████████ 10:59 AM	Expediente ██████████ - CARTA DE PAGO Y CANCELACIÓN DE HIPOTECA	Entregado
██████████ 10:52 AM	Expediente ██████████ - COMPRAVENTA	Entregado

Figura 1. Seguimiento de mensajes, recortado: sin remitente, destinatario ni identificadores; la fecha y los números de expediente, tapados.

El detalle del tercero: Microsoft lo recibió del Outlook de la asesoría, lo procesó a las 11:30 UTC y lo entregó al servidor del cliente a las 11:31 UTC, que lo aceptó sin errores. Tamaño: 262,76 KB.

Estado
Office 365 envió el mensaje correctamente a la siguiente dirección externa:
Dirección externa: ██████████

Eventos de mensaje ^

▼ Fecha (UTC)

Evento

Detalle

▼ ██████████ 11:30 AM

Receive

Message received...

Message received by: ██████████

▼ ██████████ 11:30 AM

Submit

The message was ...

The message was submitted.

▼ ██████████ 11:30 AM

TRANSFER

▼ ██████████ 11:31 AM

Send external

Message sent to ...

Message sent to ██████████

Más información ^

Id. del mensaje
██
██

Id. de MessageTrace
██

Tamaño del mensaje

De IP

A IP

262.76 KB

██████████

██████████

Figura 2. Detalle del tercer correo, recortado; dirección, servidores, identificadores, IP y fecha, tapados.

6 Comparación de los correos

Correo	Enviado	Recibido	Contenido	Resultado
ENV02 / REC02 · Compraventa	11:52:12	11:52:57	Provisión de fondos y modelo de representación	Idénticos
ENV01 / REC01 · Carta de pago y cancelación de hipoteca	11:59:21	12:00:05	Provisión de fondos	Idénticos
ENV03 / REC03 · «RE: ... Compraventa»	12:30:32	12:31:17	«Adjuntamos la provisión de fondos con la factura de la notaría corregida»	Distintos

Los dos primeros son idénticos en texto y adjuntos. *El informe original intercambiaba sus identificadores de mensaje; el correo de las 11:52 es el de la compraventa, al que responde el tercero.*

El tercero conserva el identificador de mensaje, el asunto, el remitente y el texto, pero:

- la cabecera **Delivery-date**, que añade el servidor del destinatario al dejar el correo en el buzón, y la línea **Received** de esa entrega marcan las **12:31:17**, 45 segundos después de que saliera de Microsoft (11:30:32 UTC);
- la cabecera **Date**, que indica cuándo se escribió el correo, marca las **12:55:45**. En la copia de Enviados, 12:30:32.

Un correo no puede entregarse 24 minutos antes de escribirse: la cabecera **Date** se cambió después de la entrega. Las líneas **Received** y **Delivery-date** no cambiaron.

CORREO QUE LLEGÓ · EXTRACTO DE LAS CABECERAS

El servidor lo entregó a las 12:31:17; el correo dice que se escribió a las 12:55:45

Delivery-date: Fri, [REDACTED] Oct 2025 **12:31:17** +0100
La pone el servidor del destinatario al entregar el correo en el buzón.

Received: from ...outbound.protection.outlook.com by [servidor del destinatario] with esmtps (TLS1.3) ...; **12:31:17** +0100
Llega desde Microsoft por una conexión cifrada.

Received: from [servidor de Microsoft] ... with mapi; Fri, [REDACTED] Oct 2025 **11:30:32** +0000
Sale de Microsoft: las 12:30:32 en España.

Date: Fri, [REDACTED] Oct 2025 **12:55:45** +0100 (CET)
La hora a la que dice haberse escrito: 24 minutos después de entregarse, y en otro formato. En la copia de Enviados: 12:30:32.

Content-Disposition: attachment; filename="PROVISION DE FONDOS [REDACTED].pdf"; size=**109968**
El PDF que acompaña a esta línea mide 106.211 bytes.

Unique-by-id00101: [REDACTED]
Al final de todo, debajo de las que puso el servidor. No la llevan los otros dos correos.

Figura 3. Extracto de las cabeceras de REC03, con los valores del original; nombres, servidores, fecha y valores que identifican, sustituidos o tapados. Las dos últimas líneas son de la revisión (apartado 9).

7 Comparación de los PDF

El texto de los dos PDF, extraído con `pdftotext` y comparado línea a línea, es idéntico salvo una línea: el número de cuenta en el que ingresar la provisión. El enviado lleva la cuenta de la asesoría; el recibido, otra.

Los metadatos muestran cuándo se cambió: los dos se crearon en Word a las 12:29:40; el enviado no se modificó después y el recibido se modificó a las **12:55:27**, 24 minutos después de la entrega y 18 segundos antes de la hora de la cabecera `Date` falsa. Tamaño: 109.968 bytes el enviado y 106.211 el recibido.

LOS DOS PDF • METADATOS Y ESTRUCTURA		
	Enviado	Recibido
Programa que dice haberlo creado	Microsoft Word 2021	Microsoft Word 2021
Creado	12:29:40	12:29:40
Modificado	12:29:40	12:55:27
Hora interna (XMP)	12:29:40+01:00	13:55:27+02:00
Objetos (sueltos / en bloque comprimido)	31 / 0	11 / 20
Tamaño	109.968 bytes	106.211 bytes
Texto	La cuenta de la asesoría ■■■	Otra cuenta ■■■; el resto, igual

Figura 4. Metadatos y estructura de los dos PDF; las cuentas, tapadas. 13:55:27+02:00 es el mismo instante que 12:55:27+01:00. La hora interna y los objetos son de la revisión (apartado 9).

8 Dónde y cuándo se modificó

Punto	Valoración	Motivo
Equipo o cuenta de la asesoría	Descartado	La copia de Enviados es la correcta; no hay accesos ajenos; Microsoft firmó el correo correcto al enviarlo (apartado 9).
Microsoft 365	Descartado	El seguimiento muestra un envío normal, entregado en 45 segundos; lo firmado coincide con lo enviado.
Tránsito entre servidores	Descartado	Conexión cifrada (TLS 1.3) y 45 segundos de tránsito; un cambio en tránsito no explica un PDF modificado 24 minutos después de la entrega.
Buzón o servidor del destinatario	Compatible con todas las pruebas	El correo llegó íntegro a las 12:31:17; el PDF se modificó a las 12:55:27 y la cabecera <code>Date</code> , a las 12:55:45.

Formas de hacerlo con acceso al buzón o al servidor del destinatario:

- con la contraseña del buzón, por IMAP o por el webmail: descargar el correo, cambiar el PDF y la fecha, guardar el nuevo en el buzón y borrar el original;
- desde el panel del alojamiento (cPanel), que da acceso al correo de la cuenta;
- con acceso al servidor, sobre los ficheros del buzón;
- con un filtro o una regla del buzón que intercepte los correos de la asesoría.

Quien lo hizo actuó en 24 minutos sobre un correo concreto y dejó los otros dos como estaban.

Línea temporal

Hora	Hecho
12:29:40	Se crea en Word el PDF corregido de la provisión de fondos, con la cuenta de la asesoría.
12:30:32	El correo sale de Microsoft 365 (11:30:32 UTC), firmado.
12:31:17	El servidor del destinatario lo recibe por TLS 1.3 y lo deja en el buzón, íntegro.
12:55:27	Se guarda una versión del PDF con otra cuenta, con un programa distinto de Word.
12:55:45	Un correo con ese PDF y la cabecera Date de esa hora ocupa el lugar del original en el buzón.
Después	El cliente paga a la cuenta del PDF modificado.

9 Revisión de octubre de 2026

Al preparar la versión pública volví a las pruebas originales. Estos hallazgos no estaban en el informe de noviembre de 2025 y confirman sus conclusiones.

9.1 La firma ARC de Microsoft

Microsoft 365 añade a los correos que envía una firma ARC (RFC 8617): la cabecera **ARC-Message-Signature** lleva una huella SHA-256 del cuerpo, adjuntos incluidos (**bh=**), y una firma RSA (**b=**) de esa huella y de varias cabeceras, entre ellas **From**, **Date**, **Subject** y **Message-ID**. La clave pública está en el DNS de Microsoft (selector **arcselector10001**, dominio **microsoft.com**).

- REC01 y REC02: la huella del cuerpo coincide y la firma es válida. Confirma además que las exportaciones de los correos son fieles.
- REC03: no coincide la huella del cuerpo ni es válida la firma.
- REC03 con **Date**: ... **11:30:32 +0000**, el formato en que la escribe Microsoft y la hora del envío: la firma de las cabeceras vuelve a ser válida. De lo firmado, solo cambiaron la fecha y el cuerpo, y la fecha original era esa.

FIRMA DE MICROSOFT (ARC) • COMPROBACIÓN		
Correo recibido	Cuerpo y adjuntos (bh=)	Cabeceras firmadas (b=)
REC02 · 11:52 · Compraventa	Coincide	Válida
REC01 · 11:59 · Carta de pago	Coincide	Válida
REC03 · 12:30 · Provisión «corregida»	No coincide	No válida
REC03 con su Date original, 11:30:32 +0000	No coincide	Válida

Figura 5. Comprobación de la firma ARC de Microsoft en los tres correos recibidos, con la clave pública del DNS de Microsoft.

9.2 El PDF recibido lo guardó otro programa

Los dos PDF dicen haber sido creados por Microsoft Word 2021 y comparten el identificador interno del documento, pero el recibido está reorganizado: los dos tienen 31 objetos, pero el enviado los guarda

sueltos, como Word, y el recibido mete 20 en un flujo de objetos comprimido. Otro programa lo abrió y lo volvió a guardar conservando los datos de Word. Su hora de modificación interna (XMP) es 13:55:27+02:00: el mismo instante que las 12:55:27 en España, pero escrito desde un equipo con el reloj en UTC+2. Ese día la España peninsular estaba en UTC+1, en horario de invierno. Es un indicio, no una prueba: el huso de un equipo se configura a voluntad.

9.3 Huellas en las cabeceras de REC03

- **Formato de la fecha:** Microsoft escribe `Date` en UTC (+0000), como en REC01 y REC02. La de REC03 va en +0100 (CET), el formato de otro programa.
- **Tamaño declarado del adjunto:** la cabecera del adjunto conserva `size=109968`, el tamaño del PDF original; el PDF que acompaña mide 106.211 bytes.
- **Cabecera no estándar:** al final de todas, por debajo de las que añadió el servidor del destinatario al recibir el correo, aparece `Unique-by-id00101` (su valor se omite). No figura en REC01 ni en REC02 ni la pone Microsoft.

10 Conclusiones y limitaciones

1. El correo de las 12:30:32 se envió legítimamente desde la cuenta de la asesoría, con el PDF con su cuenta.
2. No hay indicios de acceso no autorizado a la cuenta de la asesoría.
3. El correo llegó íntegro al servidor del destinatario a las 12:31:17.
4. El PDF se modificó a las 12:55:27 (solo cambia el número de cuenta) y la cabecera `Date` se cambió a las 12:55:45, después de la entrega.
5. La firma ARC de Microsoft demuestra que el cuerpo y la fecha del correo recibido no son los que salieron de Microsoft, y que el resto de las cabeceras firmadas sí lo son.
6. La modificación se hizo en el buzón o en el servidor de correo del destinatario, por alguien con acceso a ellos.

Limitaciones. Para saber por dónde se accedió y quién lo hizo hacen falta los registros del servidor de correo del destinatario, que son de su proveedor de alojamiento:

- accesos al buzón por IMAP, POP y webmail, con IP y hora, entre las 12:30 y las 13:00 del día de los hechos;
- accesos al panel de control (cPanel) y al servidor por SSH;
- registros del servidor de correo (Exim y Dovecot) de ese intervalo;
- filtros, reglas y reenvíos activos en el buzón;
- cambios en los ficheros del buzón.

Hay que pedirlos cuanto antes: en cPanel, el seguimiento de entregas guarda 10 días por defecto, y la rotación de los demás registros depende de cada servidor.

11 Recomendaciones

- **Al destinatario:** cambiar las contraseñas del correo y del panel, activar el doble factor donde se pueda, cerrar las sesiones abiertas, revisar filtros y reenvíos, pedir los registros a su proveedor y denunciar con el correo guardado como fichero.

- **A la asesoría:** mantener el doble factor, avisar a los clientes de que nunca cambiará su cuenta por correo y confirmar por teléfono cualquier cambio de cuenta que reciba.
- **A quien paga:** confirmar por teléfono, con un número conocido, cualquier cuenta nueva o «corregida», y atender el aviso de la verificación del beneficiario del banco, obligatoria en la zona euro desde el 9 de octubre de 2025.

12 Glosario

Cabeceras	Datos técnicos que acompañan a un correo: remitente, destinatario, fecha y los servidores por los que pasa, cada uno con su hora.
Metadatos	Datos que un programa guarda dentro de un fichero: con qué se hizo, cuándo se creó y cuándo se modificó.
ARC	Authenticated Received Chain (RFC 8617): firma criptográfica que añade un servidor de correo, como Microsoft 365, sobre el contenido y algunas cabeceras.
Doble factor	Además de la contraseña, una aprobación en un dispositivo del usuario (aquí, Microsoft Authenticator en el móvil).
TLS	Cifrado de la conexión entre dos servidores, como el de las páginas https.
IMAP, webmail	Formas de leer y gestionar un buzón: desde un programa de correo o desde el navegador.
cPanel	Panel de control de muchos alojamientos web, desde el que se gestionan las cuentas de correo.
UTC	Hora universal coordinada. La España peninsular está en UTC+1 en invierno y UTC+2 en verano.

Amador Cubino

Informe original: noviembre de 2025 · Versión pública: octubre de 2026