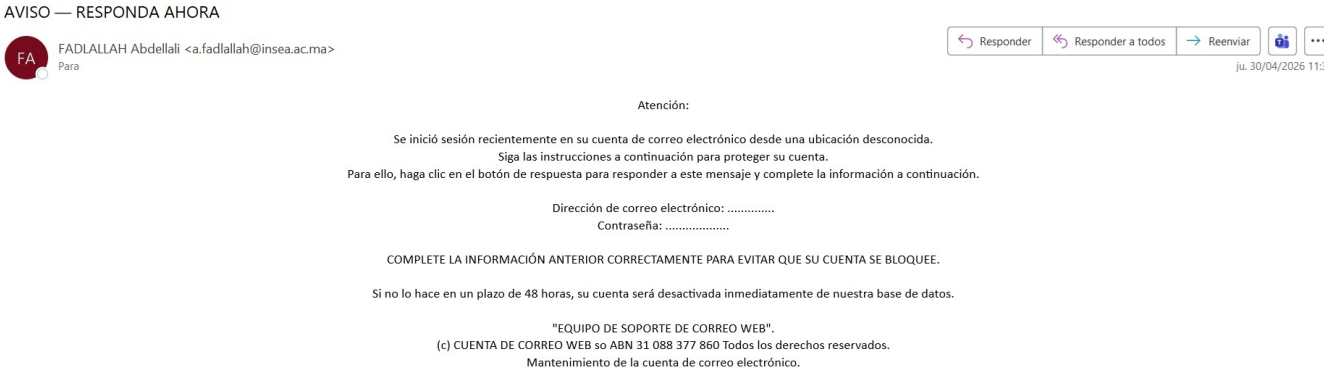
Campañas activas de correos fraudulentos: Extrema la precaución

Estimados compañeros,

Os informamos que en los últimos días se están detectando varias **campañas de correos electrónicos maliciosos de tipo *phishing* dirigidas a los profesionales del SAS**, **cuyo objetivo es obtener de forma fraudulenta datos personales y credenciales de acceso** (usuario y contraseña) a los sistemas informáticos.

Estos correos **pueden presentarse bajo distintas apariencias**. En algunos casos, suplantan la identidad de organismos oficiales e invitan a escanear un código QR para acceder a supuestos documentos urgentes (como notificaciones judiciales o requerimientos). En otros, incluyen falsas solicitudes de información personal.

A continuación, podéis ver algunos ejemplos de los correos recibidos:



AVISO — RESPONDA AHORA

FA FADLALLAH Abdellali <a.fadlallah@insea.ac.ma>
Para

Responder | Responder a todos | Reenviar

ju. 30/04/2026 11:

Atención:

Se inició sesión recientemente en su cuenta de correo electrónico desde una ubicación desconocida.
Siga las instrucciones a continuación para proteger su cuenta.
Para ello, haga clic en el botón de respuesta para responder a este mensaje y complete la información a continuación.

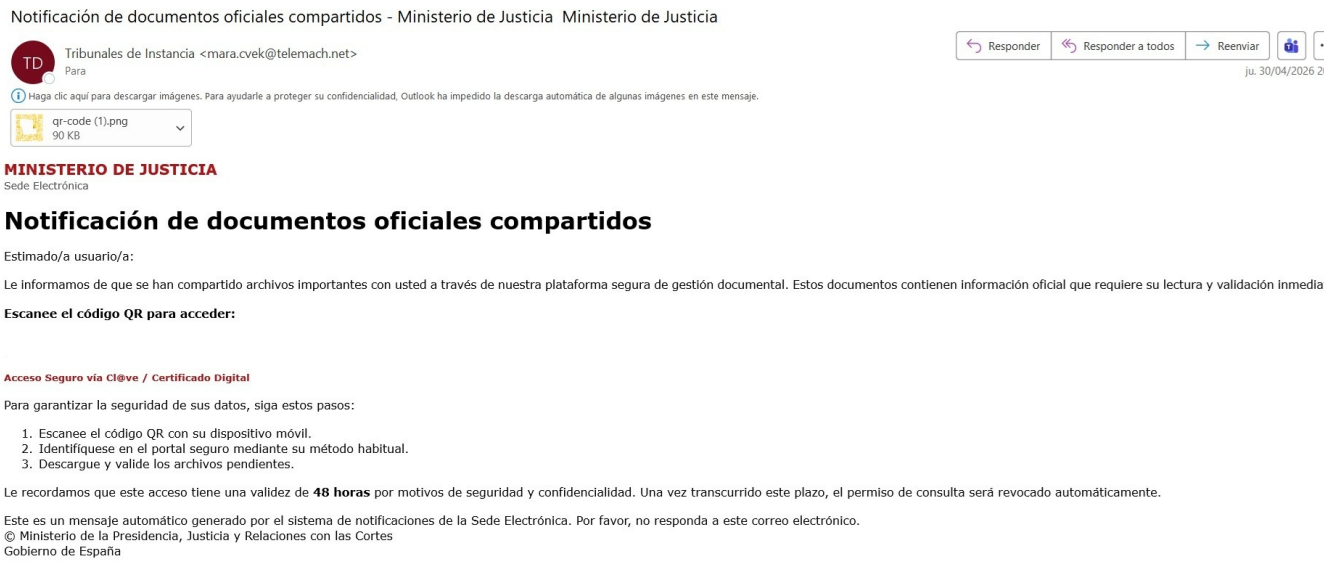
Dirección de correo electrónico: .....
Contraseña: .....

COMPLETE LA INFORMACIÓN ANTERIOR CORRECTAMENTE PARA EVITAR QUE SU CUENTA SE BLOQUEE.

Si no lo hace en un plazo de 48 horas, su cuenta será desactivada inmediatamente de nuestra base de datos.

"EQUIPO DE SOPORTE DE CORREO WEB".
(c) CUENTA DE CORREO WEB so ABN 31 088 377 860 Todos los derechos reservados.
Mantenimiento de la cuenta de correo electrónico.

Imagen 1. Correo malicioso solicitando información personal



Notificación de documentos oficiales compartidos - Ministerio de Justicia Ministerio de Justicia

TD Tribunales de Instancia <mara.cvek@telemach.net>
Para

Responder | Responder a todos | Reenviar

ju. 30/04/2026 2

Haga clic aquí para descargar imágenes. Para ayudarle a proteger su confidencialidad, Outlook ha impedido la descarga automática de algunas imágenes en este mensaje.

qr-code (1).png
90 KB

MINISTERIO DE JUSTICIA
Sede Electrónica

Notificación de documentos oficiales compartidos

Estimado/a usuario/a:

Le informamos de que se han compartido archivos importantes con usted a través de nuestra plataforma segura de gestión documental. Estos documentos contienen información oficial que requiere su lectura y validación inmedia

Escanee el código QR para acceder:

Acceso Seguro vía Cl@ve / Certificado Digital

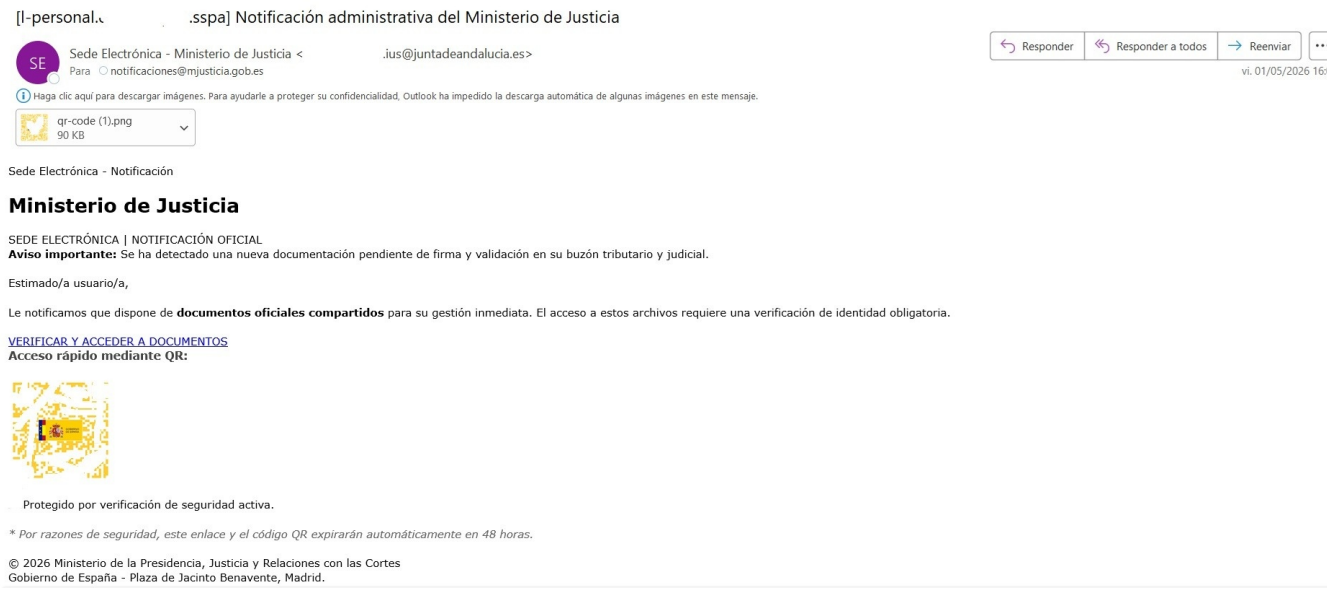
Para garantizar la seguridad de sus datos, siga estos pasos:

1. Escanee el código QR con su dispositivo móvil.
2. Identifíquese en el portal seguro mediante su método habitual.
3. Descargue y valide los archivos pendientes.

Le recordamos que este acceso tiene una validez de **48 horas** por motivos de seguridad y confidencialidad. Una vez transcurrido este plazo, el permiso de consulta será revocado automáticamente.

Este es un mensaje automático generado por el sistema de notificaciones de la Sede Electrónica. Por favor, no responda a este correo electrónico.
© Ministerio de la Presidencia, Justicia y Relaciones con las Cortes
Gobierno de España

Imagen 2. Correo electrónico fraudulento con QR


[l-personal.. .sspa] Notificación administrativa del Ministerio de Justicia

SE Sede Electrónica - Ministerio de Justicia < .ius@juntadeandalucia.es>
Para notificaciones@mjusticia.gob.es

Responder | Responder a todos | Reenviar
vi. 01/05/2026 16

Haga clic aquí para descargar imágenes. Para ayudarle a proteger su confidencialidad, Outlook ha impedido la descarga automática de algunas imágenes en este mensaje.

qr-code (1).png
90 KB

Sede Electrónica - Notificación

Ministerio de Justicia

SEDE ELECTRÓNICA | NOTIFICACIÓN OFICIAL
Aviso importante: Se ha detectado una nueva documentación pendiente de firma y validación en su buzón tributario y judicial.

Estimado/a usuario/a,

Le notificamos que dispone de **documentos oficiales compartidos** para su gestión inmediata. El acceso a estos archivos requiere una verificación de identidad obligatoria.

VERIFICAR Y ACCEDER A DOCUMENTOS
Acceso rápido mediante QR:

Protegido por verificación de seguridad activa.

** Por razones de seguridad, este enlace y el código QR expirarán automáticamente en 48 horas.*

© 2026 Ministerio de la Presidencia, Justicia y Relaciones con las Cortes
Gobierno de España - Plaza de Jacinto Benavente, Madrid.

Imagen 3. Otro correo de phishing con QR recibido

Es previsible que **este tipo de intentos continúen** en los próximos días, por lo que os pedimos que **extreméis las precauciones**. Para ello, os recordamos algunas **recomendaciones básicas de seguridad** ante estos casos:

1. **Analiza el contexto del mensaje**. Sospecha de solicitudes urgentes o poco habituales sin contrastarlo por otras vías.
2. **Revisa siempre la dirección del remitente**. Desconfía de mensajes que provengan de cuentas no corporativas o con dominios inusuales.
3. **No respondas jamás** a mensajes sospechosos.

4. **No escanees códigos QR ni abras enlaces ni archivos adjuntos** de remitentes desconocidos o que te generen dudas.
5. **No introduzcas tus credenciales** corporativas **desde enlaces o QR**.
6. Recuerda que **el SAS nunca solicita contraseñas por correo ni** mediante códigos **QR**.
7. **Accede siempre a las aplicaciones y sistemas corporativos** exclusivamente **desde** los **enlaces y sitios oficiales habituales**.
8. **Avisa inmediatamente**. Notifica estos mensajes fraudulentos. Consulta cómo hacerlo aquí: Consulta ayudaDIGITAL-AvisarPhishing

Muchas gracias por vuestra colaboración.

Comunicación

Dirección General de Tecnologías de la Información y Comunicaciones

Servicio Andaluz de Salud