BoleSTIC
Boletín de concienciación en ciberseguridad
Abril de 2026
Nº 23
Elaborado por el SOC de la Junta de Andalucía.

CONTENIDOS



# Alerta prioritaria

## ¡Cuidado con el cebo de la Renta! Los ciberdelincuentes también hacen la declaración

La declaración de la renta desata una de las oleadas de fraude más intensas del año. Los ciberdelincuentes aprovechan las comunicaciones de la Agencia Tributaria para lanzar ataques de phishing, smishing y vishing. Estas son las amenazas activas este mes.

- **El correo de "nueva notificación electrónica".** Mensajes que imitan con total fidelidad las comunicaciones electrónicas a de la AEAT. El asunto suele ser del tipo "Aviso: puesta a disposición de notificación electrónica REF-XXXX" e incluye el logo oficial y un tono administrativo impecable. El enlace, sin embargo, redirige a una web clonada diseñada para robar tus credenciales. Gracias a la inteligencia artificial, estos correos ya no contienen errores ortográficos ni diseños toscos que los delaten.
- **El SMS del "reembolso pendiente"**. Un mensaje breve, con un importe concreto y un enlace acortado para "tramitar la devolución". El gancho funciona porque la víctima ya espera ese dinero. La Agencia Tributaria nunca comunica devoluciones mediante SMS con enlaces: si recibes uno, es una trampa.
- **La llamada del "agente de Hacienda"**. Supuestos funcionarios que alertan de incidencias en tu declaración o solicitan confirmar datos personales. Con herramientas de clonación de voz por IA, estas llamadas son cada vez más difíciles de distinguir de las reales. Recuerda: la AEAT solo contacta telefónicamente si tú has solicitado cita previa. Si no la pediste, cuelga.
- **Webs clonadas y quishing tributario.** Páginas prácticamente idénticas a sede.agenciatributaria.gob.es con dominios ligeramente alterados (agencia-tributaria.net, hacienda-online.es...) y, cada vez más, códigos QR en cartas físicas con membrete oficial que redirigen a formularios de captura de credenciales. Un QR no muestra su destino real hasta que lo escaneas. ¡Asegúrate antes de que es verídico!

### ¡Recuerda!

- La Agencia Tributaria nunca solicita datos bancarios, contraseñas ni códigos de verificación por correo electrónico ni por SMS.
- Si recibes una comunicación de Hacienda y tienes dudas sobre su legitimidad, accede directamente a tu área personal en sede.agenciatributaria.gob.es para comprobar si existe realmente.
- La urgencia es la herramienta favorita del fraude. Si el mensaje mete prisa, para y verifica.

### ¿Qué debes hacer?

1. Accede a la AEAT escribiendo siempre la URL en el navegador. Nunca desde un enlace recibido por correo, SMS o QR.
2. Comprueba el dominio del remitente antes de actuar. El nombre visible puede ser "Agencia Tributaria", pero la dirección real nunca termina en @agenciatributaria.gob.es si es fraudulenta.
3. Si has introducido tus datos en una página falsa, cambia tus credenciales de inmediato y contacta con tu banco sin demora.
4. Reporta al SOC cualquier correo o SMS sospechoso recibido en tu cuenta corporativa, aunque no hayas hecho clic.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía · Agencia Digital de Andalucía

BoleSTIC
Boletín de concienciación en ciberseguridad
Abril de 2026
Nº 23
Elaborado por el SOC de la Junta de Andalucía.

CONTENIDOS



# Ciberataques mediante códigos QR

Queremos informarte de la detección de un nuevo caso de quishing dirigido a todo el personal de la Junta de Andalucía, mediante correos electrónicos que incluyen códigos QR con fines fraudulentos.

**Información relevante:**

- No se ha establecido ningún protocolo de seguridad que obligue a validar la identidad para evitar bloqueos temporales de tu cuenta.
- Nunca se solicita, por correo electrónico, la verificación de usuario y contraseña escaneando un código QR con tu dispositivo móvil. Cualquier correo con estas características no es legítimo.

**Cómo actuar ante este tipo de correos:**

- No escanees el código QR.
- No facilites tus credenciales.
- Reenvía el correo como fichero adjunto a la dirección abuse@juntadeandalucia.es.

[AVISO DE SEGURIDAD] Actualización obligatoria de credenciales - Diraya

Seguridad Informática - Junta de Andalucía < @juntadeandalucia.es>
Para

Responder | Responder a todos | Reenviar

lu. 13/04/2026 4:56

qr-code(2).png
145 KB

**Cuerpo del mensaje:**

Estimado/a usuario/a,

Le informamos que se ha detectado un intento de acceso inusual en su cuenta vinculada al portal **Diraya Producción**.

Por motivos de seguridad y siguiendo los nuevos protocolos de la **Consejería de Salud y Familias**, es obligatorio validar su identidad para evitar el bloqueo temporal de su acceso remoto.

Por favor, escanee el siguiente **código QR** con su dispositivo móvil para acceder al portal de autenticación y verificar su usuario y contraseña:

*Si no puede escanear el código, asegúrese de completar la validación antes de que finalice su jornada laboral para evitar la suspensión de su cuenta.*

Una vez completado, su acceso será restablecido automáticamente.

Atentamente, **Soporte Técnico - Servicio Andaluz de Salud Junta de Andalucía**

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

BoleSTIC
Boletín de concienciación en ciberseguridad
Abril de 2026
Nº 23
Elaborado por el SOC de la Junta de Andalucía.

CONTENIDOS



# Tema del mes

## Phishing: el anzuelo que puede pillar hasta al más atento

El phishing lleva años siendo el ciberataque más frecuente en España y en el mundo. No porque los usuarios sean descuidados, sino porque los atacantes son cada vez mejores. Según el INCIBE, en 2025 el phishing lideró los fraudes online con más de 25.000 casos, y en lo que va de 2026 la cifra sigue al alza. Entender cómo funciona es la primera línea de defensa.

## Ya no puedes detectarlo por los errores: qué ha cambiado

Durante años, la regla era sencilla: los correos de phishing tenían faltas de ortografía, diseños pobres y saludos genéricos. Esa regla ha muerto. La inteligencia artificial permite hoy generar mensajes perfectamente redactados, con el tono y el vocabulario exacto de la entidad imitada, y personalizados con datos reales del destinatario obtenidos de brechas anteriores. Un correo puede llegar con tu nombre, tu NIF y una referencia que parece sacada de tus propios expedientes, y ser completamente falso.

Esto no significa que no puedas detectarlo. Significa que ya no puedes fiarte del contenido para hacerlo. Los indicadores que siguen siendo válidos son otros: el dominio real del remitente —no el nombre visible, sino la dirección completa—, la URL a la que apunta el enlace antes de hacer clic, y sobre todo, el canal: ¿es este realmente el medio por el que esta entidad te contacta para este tipo de gestión?

## La trampa tiene cuatro pasos, y solo necesita que falles en uno

- Todo ataque de phishing, independientemente de su sofisticación, sigue la misma lógica: crear una situación creíble que te lleve a hacer algo que no deberías. El disfraz cambia; el proceso, no.
- Primero llega el anzuelo: un correo, un SMS o una llamada que imita a una entidad de confianza. Puede ser la Agencia Tributaria con una notificación pendiente, tu banco alertando de un acceso sospechoso, o Correos avisando de un paquete retenido. El mensaje está diseñado para parecer urgente y completamente legítimo.
- Después, la urgencia: "tienes 24 horas", "tu cuenta será bloqueada", "actúa antes de que caduque el plazo". La presión temporal no es accidental: busca que actúes antes de que tu criterio tenga tiempo de intervenir. Un segundo de duda es suficiente para detectar la trampa; el phishing intenta eliminar ese segundo.
- El tercer paso es el clic: un enlace que lleva a una web falsa, un adjunto que instala malware al abrirse.
- A partir de ahí, la captura: introduces tus credenciales creyendo que estás en el sitio correcto, o el archivo descargado extrae en segundo plano todo lo que tiene tu equipo. El daño puede tardar días en hacerse visible, pero ya está hecho.

SIGUE >>

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

BoleSTIC
Boletín de concienciación en ciberseguridad
Abril de 2026
Nº 23
Elaborado por el SOC de la Junta de Andalucía.

CONTENIDOS



<< VIENE DE LA ANTERIOR

## Cuatro formas de llegar al mismo destino

El phishing no es un único tipo de ataque, sino una familia de técnicas que comparten objetivo pero usan canales distintos. Conocerlas todas es importante porque cada una activa mecanismos de confianza diferentes.

- El email phishing es el más extendido. Su variante más peligrosa, el spear phishing, usa información real sobre la víctima para parecer legítimo.
- El smishing llega por SMS con enlaces que ocultan su destino real.
- El vishing usa llamadas de voz —cada vez más convincentes gracias a la clonación por IA— para solicitar datos o acciones urgentes.
- El quishing usa códigos QR que ocultan la URL maliciosa hasta que ya es demasiado tarde para rectificar.

## Hábitos de oro para no picar

- Verifica el dominio real, no el nombre visible. Haz clic en el remitente y comprueba la dirección completa para asegurarte de que el dominio (después de la @) es el auténtico de la entidad que te escribe
- Pasa el cursor por el enlace antes de hacer clic. Así puedes comprobar que la URL que aparece en la barra inferior del navegador es la real. Si no coincide con lo esperado, no hagas clic.
- Ante la urgencia, más calma. Cuanto más te metan prisa, más despacio debes ir.
- Ante la duda, escribe tú la URL. Abre el navegador y accede directamente al sitio oficial. Nunca desde el enlace del mensaje.
- Reporta aunque no hayas caído. Un correo sospechoso reportado al SOC puede bloquear la campaña y proteger a toda la organización.

## Checklist: "¿Detectarías el anzuelo?

Si tu respuesta a alguna de estas preguntas es "no", tu exposición al phishing es mayor de lo que crees:

- ¿Compruebas siempre el dominio real del remitente antes de actuar sobre un correo?
- ¿Sabes cómo ver la URL de destino de un enlace antes de hacer clic en él?
- ¿Accedes a los sitios web escribiendo siempre la dirección o mediante acceso en Favoritos?
- ¿Sabrías qué hacer si hubieses hecho clic en un enlace sospechoso sin darte cuenta?
- ¿Reportarías al SOC un correo sospechoso aunque no hubieras interactuado con él?
- ¿Conoces la diferencia entre phishing, smishing, vishing y quishing?

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
INSTITUTO NACIONAL DE CIBERSEGURIDAD

BoleSTIC
Boletín de concienciación en ciberseguridad
Abril de 2026
Nº 23
Elaborado por el SOC de la Junta de Andalucía.

CONTENIDOS



# Guía rápida

## Ciberseguridad en el día a día: preguntas frecuentes

**→ ¿Puedo usar ChatGPT u otras herramientas de IA para redactar documentos de trabajo?**

Depende. Comprueba antes si está autorizada por tu organización. Muchas envían los textos a servidores externos; con datos sensibles, puede ser una filtración

**→ ¿Puedo introducir en una IA externa datos personales o confidenciales de terceros, proyectos, etc.?**

No. Como norma general, si no lo publicarías en abierto tampoco debes introducirlo en una herramienta de IA no controlada por la organización.

**→ ¿Son siempre fiables las respuestas que genera una IA?**

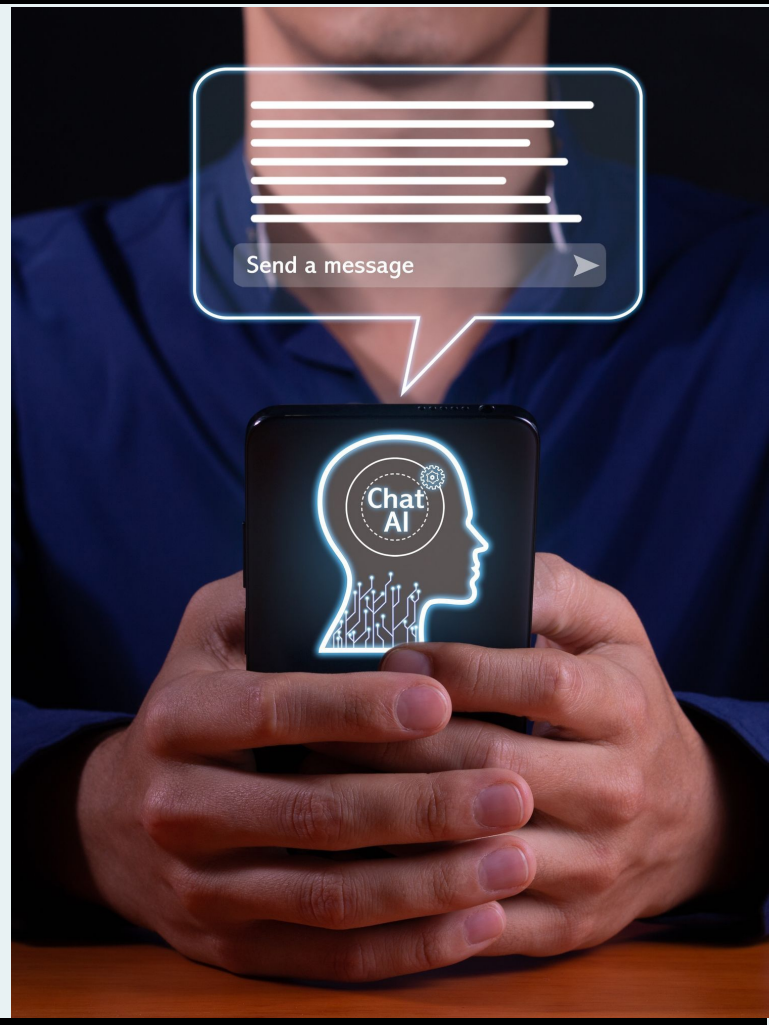
No. Los modelos cometen errores e inventan referencias con total convicción. Verifica siempre en fuentes oficiales, y comprueba lo generado, antes de usar el resultado en un documento de trabajo.

**→ ¿Puede la IA ser usada para atacarme a mí o a mi organización?**

Si. Los atacantes ya la usan para generar phishing sin errores, clonar voces de directivos y personalizar fraudes a escala. No es solo una herramienta de productividad.

**→ ¿Debo avisar si he usado una herramienta de IA no autorizada por error?**

Sí. Especialmente si introdujiste información sensible. Notifícalo al SOC cuanto antes para evaluar el riesgo.




Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

BoleSTIC
Boletín de concienciación en ciberseguridad
Abril de 2026
Nº 23
Elaborado por el SOC de la Junta de Andalucía.

CONTENIDOS



# Radar de amenazas

El panorama de la ciberseguridad evoluciona rápido y debemos estar informados. Compartimos algunas noticias destacadas de este mes.

### Campaña de la Renta 2026: cuidado con correos y SMS que suplantan a la Agencia Tributaria

Con el inicio de la campaña del IRPF, ESET alerta de un repunte de fraudes que imitan comunicaciones oficiales de la AEAT. Los mensajes incluyen enlaces a webs falsas donde se solicitan credenciales o datos bancarios con el pretexto de gestionar la declaración. La Agencia Tributaria no solicita datos personales ni bancarios por correo electrónico o SMS.

**> Enlace a la noticia**

### Vulnerabilidad zero-day en Adobe Acrobat Reader explotada mediante PDFs maliciosos

Se ha detectado una campaña activa que aprovecha un fallo de seguridad crítico en Adobe Acrobat Reader para infectar equipos con la simple apertura de un PDF manipulado. La vulnerabilidad permitiría el robo de información y la ejecución remota de código. Mantén el programa actualizado a la última versión disponible.

**> Enlace a la noticia**

### El troyano bancario Casbaneiro usa falsas notificaciones judiciales para atacar a víctimas en España

Este malware llega disfrazado de citaciones o requerimientos judiciales enviados por correo. Una vez ejecutado, roba credenciales de acceso a banca online y servicios digitales. Ante cualquier comunicación judicial inesperada, verifícala a través de los canales oficiales antes de abrir ningún archivo adjunto.

**> Enlace a la noticia**

### Qué ocurrió realmente en la brecha de Booking.com

Un análisis detalla cómo atacantes comprometieron cuentas de establecimientos asociados a la plataforma para contactar directamente con huéspedes y robar sus datos de pago. El vector de entrada fue el engaño a empleados de los hoteles, no un fallo técnico de Booking. Desconfía de mensajes de reservas que te pidan introducir datos bancarios fuera de la plataforma oficial.

**> Enlace a la noticia**

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
INSTITUTO NACIONAL DE CIBERSEGURIDAD

BoleSTIC
Boletín de concienciación en ciberseguridad
Abril de 2026
Nº 23
Elaborado por el SOC de la Junta de Andalucía.

CONTENIDOS



# Normativa al día

Debemos hacer un buen uso de las tecnologías de la información y la comunicación en nuestros puestos de trabajo. Te recordamos varios puntos importantes.

**Protege los documentos en papel igual que los digitales**

**Si usas IA o participas en proyectos de datos masivos, aplica códigos éticos**

**El correo corporativo es solo para uso profesional**

**Antes de enviar, comprueba bien los destinatarios**

**Evita almacenar información de trabajo en USBs o discos portátiles**

**Cierra la sesión al terminar, no solo la ventana**

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

CONTENIDOS



# Zona interactiva

## Quiz del mes

**Recibes email de un compañero con enlace a un documento en una plataforma desconocida que solicita tus credenciales. ¿Qué haces?**

- Meto mis credenciales si el correo parece legítimo
- Verifico con mi compañero por otro canal
- Meto mis credenciales pero las cambio después

**Un correo aparentemente de tu responsable te pide que realices una transferencia urgente fuera de los canales habituales y añade: "No lo comentes hasta que esté cerrado". ¿Cuál es la señal de alerta más clara?**

- La combinación de urgencia y petición de confidencialidad
- Que el importe de la transferencia sea elevado
- Que el correo llegue fuera del horario laboral

**Recibes una llamada de alguien que dice ser del servicio técnico de tu organización y te pide tu contraseña para "resolver una incidencia urgente". ¿Qué haces?**

- No la facilito: ningún servicio técnico legítimo necesita tu contraseña para trabajar
- La facilito si la incidencia parece real y el tono es profesional
- Pido que me llamen en otro momento y entonces sí la doy

**Recibes un correo de tu Consejería con un enlace para activar una nueva herramienta corporativa. ¿Qué haces?**

- Accedo al enlace porque el correo parece oficial
- Reenvío el correo a mis compañeros para que también se registren
- Verifico con el área de informática si existe realmente esa herramienta antes de hacer nada

**Usas una herramienta de IA externa para redactar un informe. Copias y pegas datos personales de ciudadanos. ¿Qué riesgo principal asumes?**

- Que el informe salga con errores de formato
- Que esos datos puedan quedar expuestos
- Que la herramienta tarde más tiempo en responder

**Encuentras un código QR en un documento impreso con membrete oficial que te invita a acceder a un trámite. ¿Qué riesgo debes tener en cuenta?**

- Que el QR pueda dañar la cámara de tu dispositivo
- Que el QR oculta la URL de destino hasta que ya lo has escaneado
- Que el documento pueda estar desactualizado

SIGUE >>

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía · Agencia Digital de Andalucía

BoleSTIC
Boletín de concienciación en ciberseguridad
Abril de 2026
Nº 23
Elaborado por el SOC de la Junta de Andalucía.

CONTENIDOS



<< VIENE DE LA ANTERIOR

## Caso práctico

Son las 9:15 de la mañana. Tienes que preparar una presentación para una reunión a las 12:00 y el tiempo es justo. Un compañero del departamento de al lado te escribe por el chat interno: «Oye, yo uso ChatGPT para esto y en diez minutos lo tienes. Solo tienes que pegarle el borrador del informe con los datos del expediente y te lo estructura solo. Funciona genial».

El informe que tienes que preparar incluye datos personales de varios ciudadanos: nombre, NIF, datos de salud y situación económica. La presión del tiempo es real. La herramienta parece una solución rápida y tu compañero la usa habitualmente.

¿Qué harías en esta situación?

Ver la respuesta

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
INSTITUTO NACIONAL DE CIBERSEGURIDAD

BoleSTIC
Boletín de concienciación en ciberseguridad
Abril de 2026
Nº 23
Elaborado por el SOC de la Junta de Andalucía.

CONTENIDOS



# Canal directo

**La seguridad es una tarea compartida. Si tienes cualquier duda o sospechas de un incidente, ¡contacta con nosotros!**

**Email:**
incidentes.soc@juntadeandalucia.es

**Teléfono:**
955 060 974
360974 (corporativo)

**Alertas de seguridad y campañas activas**
**> Consúltalas aquí**

**Síguenos en:**

X: @CentroCiberAND

LinkedIn: Centro de Ciberseguridad de Andalucía

Financiado por la Unión Europea NextGenerationEU