BoleSTIC
Boletín de concienciación en ciberseguridad
Febrero de 2026
Nº 21
Elaborado por el SOC de la Junta de Andalucía.

CONTENIDOS

Alerta prioritaria

Suplantaciones a instituciones, empresas y los riesgos de la IA en nuestras vidas

Si pensabas que las campañas de fraude iban a quedarse en cosa de enero, estabas muy equivocado. Los ciberdelincuentes continúan haciéndose pasar por entidades públicas y privadas, a la vez que compartimos cada vez más datos con los "chatbots". Estas son las amenazas activas de este mes.

- **Detectada una peligrosa campaña de ciberataques que utiliza mensajes en LinkedIn para engañar a profesionales.** Los atacantes envían archivos comprimidos que, supuestamente, contienen herramientas útiles como lectores de PDF o aplicaciones de trabajo legítimas. Sin embargo, al abrir estos archivos, el sistema ejecuta de forma oculta un programa malicioso (troyano) que se disfraza utilizando software real para no ser detectado por los antivirus.

- **Se dispara el uso (inseguro) de agentes de IA.** Esta nueva tecnología, capaz de controlar el ordenador y hacer tareas como si fuera el usuario humano, ha puesto en el ojo del huracán a Moltbot (también conocido como OpenClaw, o anteriormente Clawdbot). Miles de usuarios están usándolo sin las medidas de seguridad adecuadas, dejando expuestas interfaces de administración sin contraseña en internet. Al tener permisos para leer archivos y acceder a aplicaciones de mensajería, ha transformado una prometedora herramienta de productividad en un "caballo de Troya" para el espionaje y el robo de datos a gran escala.

- **Notificaciones que suplantan a la Agencia Tributaria y a la Dirección Electrónica Habilitada Única.** El INCIBE alerta sobre el fraude que consiste en el envío de notificaciones a través de correo electrónico, en el que informan de una nueva notificación electrónica sobre una supuesta reclamación. Esta va acompañada de un enlace para acceder a la plataforma y descargar la notificación, pero dicho enlace redirecciona a una web fraudulenta para robar las credenciales de acceso.

- **Crece el uso de deepfakes asociado a intentos de estafa.** El uso de los deepfakes —vídeos o audios creados con inteligencia artificial— ha experimentado un crecimiento alarmante del 900%, convirtiéndose en una de las herramientas favoritas de los ciberdelincuentes. El peligro radica en su gran realismo, lo que hace que para una persona sin conocimientos técnicos sea cada vez más difícil distinguir qué es real y qué es una manipulación diseñada para robar su dinero o sus datos.

¡Recuerda!

- Las compañías o instituciones no te solicitarán datos bancarios telemáticamente, mucho menos con urgencia.
- Las modas con nuevas herramientas y tecnologías suelen traer el desastre con las primeras adopciones, sobre todo cuándo son masivas.
- Cualquier contenido audiovisual en Internet puede estar fabricado con inteligencia artificial.
- No descargues ni abras ficheros inesperados, mucho menos de desconocidos.

¿Qué debes hacer?

1. Entra a la web de empresas o administraciones públicas manualmente y comprueba si existe el supuesto problema, nunca desde el mensaje urgente.
2. Si vas a usar herramientas nuevas de inteligencia artificial, consulta antes con personal técnico cualificado y con profesionales de protección de datos.
3. Trata cualquier fichero sospechoso como peligroso y analízalo con tu software antivirus o plataformas como VirusTotal.

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

BoleSTIC
Boletín de concienciación en ciberseguridad
Febrero de 2026
Nº 21
Elaborado por el SOC de la Junta de Andalucía.

CONTENIDOS

5º Congreso de Ciberseguridad de Andalucía

Llega la quinta edición del evento que consolida a Andalucía como el epicentro de la confianza digital y la resiliencia tecnológica. Bajo el lema "Secure Territories, Connected Future", nuestro congreso evoluciona para abordar la ciberseguridad no sólo como un desafío técnico, sino como una prioridad estratégica, institucional y ciudadana.

Organizado por la Agencia Digital de Andalucía (ADA), a través del Centro de Ciberseguridad de Andalucía (CIAN), Málaga volverá a ser el punto de encuentro ineludible donde especialistas y líderes globales compartirán los avances más disruptivos en seguridad digital.

El 5º Congreso de Ciberseguridad de Andalucía tendrá lugar en FYCMA, el Palacio de Ferias y Congresos de Málaga, los días 24 y 25 de marzo. Las inscripciones ya se encuentran abiertas.

Más información

BoleSTIC
Boletín de concienciación en ciberseguridad
Febrero de 2026
Nº 21
Elaborado por el SOC de la Junta de Andalucía.

CONTENIDOS

Tema del mes

La desinformación, ¿qué es y por qué nos afecta?

La desinformación no es solo un "error" en una noticia; es contenido creado deliberadamente para engañar, inducir a error o manipular a las personas. Su objetivo suele ser influir en la opinión pública, causar caos o beneficio económico.

Nos afecta porque apela a nuestras emociones (miedo, indignación o alegría extrema), lo que nos impulsa a compartir el contenido sin pensar, ayudando a que la mentira se propague.

¿Y a mí quién quiere engañarme? Mucha gente

A veces pensamos que los bulos son solo "noticias locas" de Internet, pero la realidad es que existen campañas profesionales diseñadas por gobiernos y grandes corporaciones para moldear lo que pensamos y cómo consumimos.

Países extranjeros pueden difundir noticias falsas sobre la economía o la sanidad de otro país para generar caos y desconfianza en sus instituciones, creando "granjas de troles" (miles de cuentas falsas manejadas por bots o personas) que entran en debates públicos para pelearse con usuarios reales, radicalizando las posturas y rompiendo la convivencia.

Las empresas tampoco se quedan atrás con lavados de imagen, guerra sucia contra la competencia y estudios sesgados “patrocinados”, que dejan sus productos y servicios por las nubes o crean necesidad de comprarlos.

Cómo identificar noticias falsas en redes sociales

Las redes sociales son el caldo de cultivo ideal para los bulos.
Para no caer en la trampa, el INCIBE recomienda seguir estos pasos de contraste:

- Duda de los titulares sensacionalistas: si el titular es demasiado increíble o busca una reacción emocional fuerte, sospecha.
- Verifica la fuente y el autor: ¿Quién publica la noticia? Busca si es un medio reconocido o una cuenta recién creada sin seguidores reales.
- Contrasta con otros medios: si una noticia es real e importante, aparecerá en varios medios de comunicación fiables, no solo en un post de Facebook, Tiktok o un mensaje de WhatsApp.
- Analiza las imágenes: a veces se usan fotos antiguas o manipuladas. Puedes usar buscadores de imágenes para ver si esa foto pertenece realmente a ese evento.

Cuidado con la publicidad engañosa y los anuncios falsos

No toda la desinformación es política; mucha es comercial. Los ciberdelincuentes crean anuncios falsos para estafarte o instalar virus en tu dispositivo. Fíjate en estos detalles:

- Ofertas demasiado buenas para ser verdad: un iPhone de última generación por 2 euros es, sin duda, un fraude.
- Errores de escritura: las marcas serias cuidan su ortografía. Si ves fallos gramaticales o traducciones extrañas, huye.
- La URL del sitio web: antes de hacer clic, mira la dirección. Si dice algo como tienda-oficial-gangas123.com en lugar de la web real de la marca, es falso.
- Presión temporal: frases como "¡Solo quedan 5 minutos!" buscan que actúes rápido sin pensar.

SIGUE >>

Financiado por la Unión Europea NextGenerationEU

BoleSTIC
Boletín de concienciación en ciberseguridad
Febrero de 2026
Nº 21
Elaborado por el SOC de la Junta de Andalucía.

CONTENIDOS

<< VIENE DE LA ANTERIOR

El impacto de la desinformación en la Administración Pública

En el ámbito público, la desinformación no solo busca engañar al individuo, sino socavar la confianza en las instituciones. Como servidor público, te conviertes en un intermediario crítico para la transmisión de información veraz.

- Preservar la confianza institucional: la difusión accidental de un bulo por parte de un funcionario puede interpretarse como una postura oficial. Esto daña la credibilidad del organismo y genera confusión en el ciudadano que busca guía en la Administración.
- Seguridad de la información y ciberseguridad: muchos anuncios o noticias falsas son la puerta de entrada para ataques de phishing. Un clic en una oferta falsa, o en un enlace de una noticia sensacionalista dentro de la red corporativa, puede comprometer bases de datos y la privacidad de miles de ciudadanos.

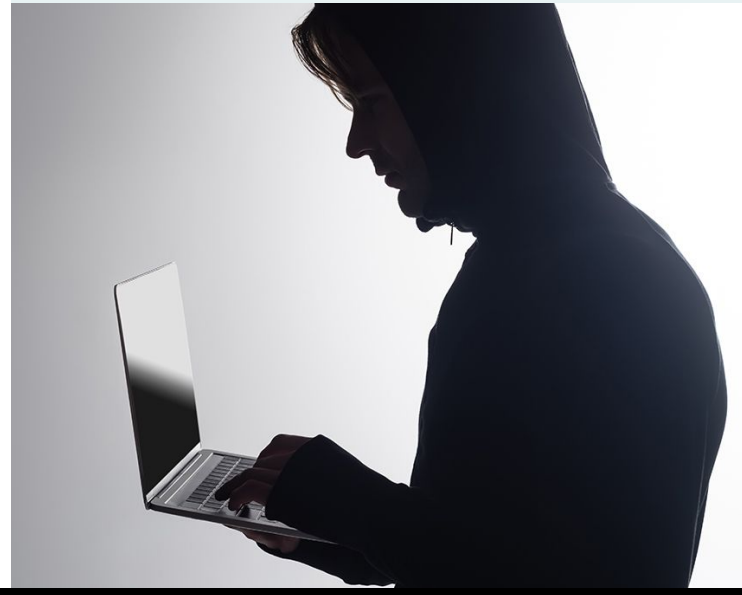
Hábitos de oro para tu día a día

- La “Regla de los 60 segundos”: nunca compartas algo inmediatamente después de leerlo.
  Deja pasar un minuto. Ese tiempo extra permite que tu cerebro racional tome el mando sobre el emocional.
- Diversifica tus fuentes: no te informes solo a través de lo que te sugiere el algoritmo de tu red social favorita.
  Visita directamente las portadas de diferentes periódicos o medios oficiales.
- Desconfía del "Me lo ha enviado un amigo": tu amigo o familiar no tiene por qué ser un experto en ciberseguridad. A menudo, las personas con mejores intenciones son las que más bulos propagan.
- Cero clics en publicidad sospechosa: si ves un anuncio de una marca que te interesa, no pinches en el anuncio.
  Ve tú mismo a la web oficial escribiendo la dirección en el navegador.
- Practica el "escepticismo saludable": en internet, parte de la base de que cualquier cosa que no esté verificada podría ser falsa. Es mejor ser precavido que ser el próximo en caer en la estafa.

Checklist: "Antes de compartir, verifica"

Si tu respuesta a alguna de las siguientes preguntas es “sí”, desconfía.

- ¿La información es sensacionalista o busca enfadarme?
- ¿Es una oferta "demasiado buena"?
- ¿Pide que lo comparta "urgentemente"?
- ¿Tiene errores de ortografía o un diseño pobre?
- ¿Desconozco la fuente original?



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
Febrero de 2026
Nº 21
Elaborado por el SOC de la Junta de Andalucía.

CONTENIDOS

Guía rápida

Ciberseguridad en el día a día: preguntas frecuentes

→ **¿El phishing solo llega por email?**
No. También puede llegar por SMS, llamadas, redes sociales o mensajes falsos en apps.

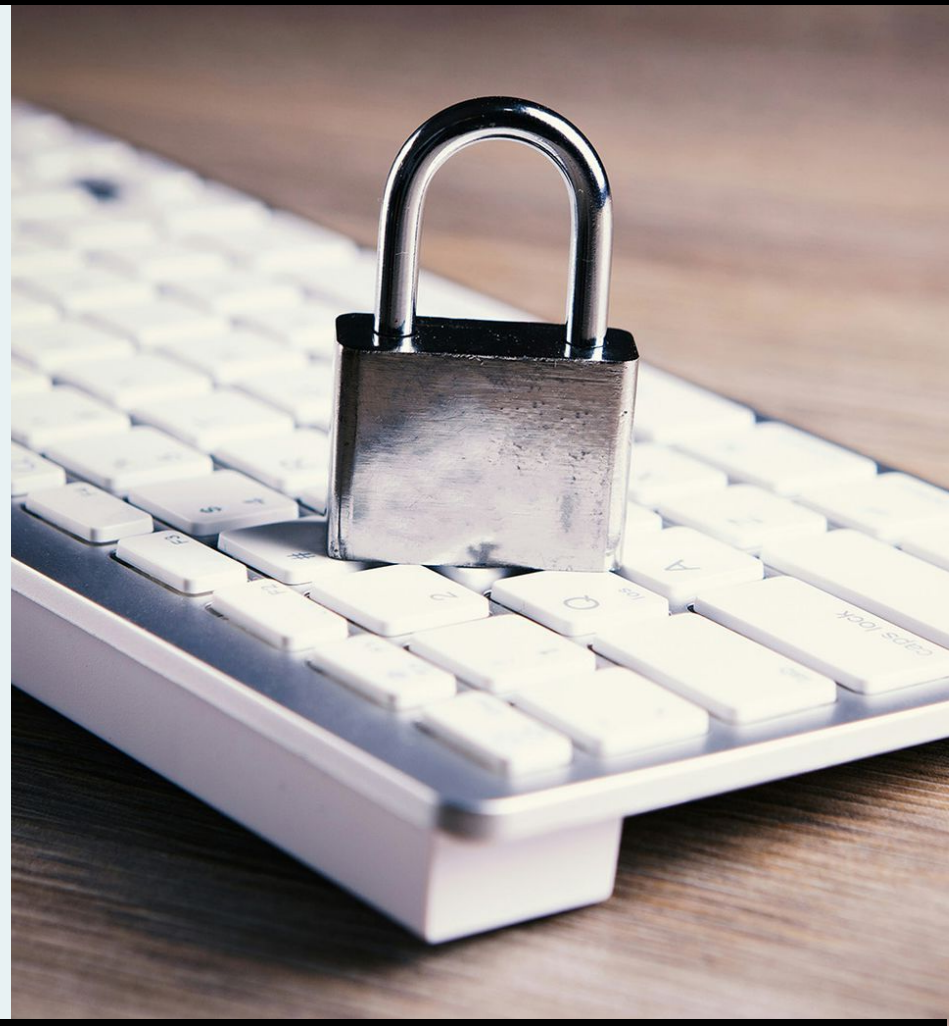
→ **¿Las redes WiFi públicas son seguras?**
No. Suelen carecer de medidas de seguridad y cualquiera se puede conectar a ellas.

→ **¿Un deepfake sólo afecta a famosos?**
No. Cualquiera puede ser víctima de suplantaciones con voz o imagen generadas con IA.

→ **¿Un archivo PDF puede tener virus?**
Sí. Puede incluir código malicioso si proviene de una fuente no confiable.

→ **¿Los enlaces acortados son siempre sospechosos?**
Depende. Se usan legítimamente, pero también para ocultar enlaces maliciosos.

→ **¿Activar la verificación en dos pasos mejora la seguridad?**
Sí. Añade una capa extra aunque roben tu contraseña.



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

BoleSTIC
Boletín de concienciación en ciberseguridad
Febrero de 2026
Nº 21
Elaborado por el SOC de la Junta de Andalucía.

CONTENIDOS

Radar de amenazas

El panorama de la ciberseguridad evoluciona rápido y debemos estar informados:

Los ciberataques se disparan un 26% en España en 2025 con la banca en la diana.

El crimen en línea no descansa. Los ciberataques han subido un 26% en España y la banca fue el sector más perjudicado, con un 34% de asaltos a través de la red. Así lo asegura el último informe anual del Instituto Nacional de Ciberseguridad (Incibe) que ha intervenido en 122.223 ataques online en nuestro país durante 2025.

> Enlace a la noticia

149 millones de credenciales expuestas de plataformas como Instagram, Facebook, Roblox, TikTok y Gmail, entre otras

Se ha reportado una brecha masiva de credenciales de acceso a diferentes servicios en línea. Esta filtración fue causada por un malware de tipo "infostealer", que recopiló los datos y los almacenó de forma pública. La información, que contenía datos como nombres de usuario y contraseñas de usuarios registrados, fue accesible a cualquier persona con acceso a la URL.

> Enlace a la noticia

Las contraseñas más hackeadas en España y en el mundo en 2026

A pesar de las constantes advertencias de seguridad, millones de personas en España y en el mundo siguen utilizando contraseñas extremadamente débiles que pueden ser descifradas en segundos. El ranking de 2026 revela que combinaciones predecibles como "123456", "password" o "admin" siguen siendo las más comunes, lo que facilita enormemente el trabajo de los ciberdelincuentes.

> Enlace a la noticia

Las cinco estafas más habituales que suplantan a Apple Pay

Apple Pay se ha convertido en un método de pago muy popular, pero esa misma popularidad ha atraído a estafadores que utilizan diversos engaños para robar dinero. Entre las tácticas más comunes se encuentran el envío de mensajes falsos (phishing) que alertan sobre supuestos problemas con la cuenta para que el usuario entregue sus datos, o fraudes en los que el delincuente simula haber pagado de más por un producto y pide la devolución de la diferencia.

> 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
Febrero de 2026
Nº 21
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.

El Código también se aplica en teletrabajo

Sigue siempre los protocolos de incidencias y permisos

Conoce al Delegado/a de Protección de Datos

Cuidado con dónde accedes en Internet

Ten el control siempre de tu certificado digital

No publiques contenido sin autorización

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

CONTENIDOS

Zona interactiva

Quiz del mes

Te llega un correo que dice: "¡Has ganado un iPhone!" y tú no recuerdas haber participado en nada. ¿Qué haces?

- Lo borro o lo marco como sospechoso y reporto.
- Reenvío el correo a mi familia por si ellos sí participaron.
- Hago clic rápido antes de que caduque.

Si tratando de acceder a una web tu navegador muestra un aviso de "sitio no seguro", ¿qué haces?

- Continúo, seguro que no pasa nada.
- Me detengo y reviso la dirección web.
- Cierro el navegador y reinicio el equipo.

Recibes una llamada diciendo ser del banco y te piden códigos de verificación. ¿Qué haces?

- Se los doy, suenan amables y parece urgente.
- Cuelgo y llamo al banco por el número oficial.
- Les pregunto si conocen mi DNI para saber si son el banco de

¿Qué es el phishing?

- Un virus que bloquea el equipo.
- Un trend de redes sociales que consiste en hacerse pasar por otro.
- Un intento de engaño para robar información.

¿Qué deberías hacer antes de tirar documentos con información sensible?

- Romperlos a mano o usar destructora de papel.
- No tirar nada y almacenarlo todo en mi escritorio.
- Tirarlos tal cual, total nadie mira la basura.

Tu pantalla está desbloqueada y te levantas a por agua. ¿Qué deberías hacer antes?

- Bloquear la sesión.
- Nada, vuelvo en un minuto.
- Apagar el ordenador.

SIGUE >>

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

BoleSTIC
Boletín de concienciación en ciberseguridad
Febrero de 2026
Nº 21
Elaborado por el SOC de la Junta de Andalucía.

CONTENIDOS

<< VIENE DE LA ANTERIOR

Caso práctico

Recibes por WhatsApp, desde un número desconocido, un vídeo en el que aparece el responsable de tu área. En el vídeo, explica que se ha quedado sin conexión y te escribe desde el teléfono de un familiar, que aparece con él en la foto de perfil. Parece estar hablando directamente a los empleados y solicita que, de manera urgente y confidencial, se realice una transferencia bancaria para cerrar una operación de un pliego importante con el que ha habido un retraso.

La imagen y la voz parecen completamente reales. Incluso utiliza expresiones que suele decir habitualmente. El mensaje transmite urgencia y pide que no se comente con otros compañeros “para no generar rumores” sobre el despiste del pago.

Minutos después, recibes también un correo electrónico reforzando la misma petición y con los datos bancarios para hacer el ingreso.

La situación parece muy convincente. Pero algo te genera duda: normalmente este tipo de decisiones no se comunican de esa manera.

Te invitamos a reflexionar sobre esta situación, y después revelar la respuesta.

Ver la respuesta

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
Febrero de 2026
Nº 21
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

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