BoleSTIC
Boletín de concienciación en ciberseguridad
Marzo de 2026
Nº 22
Elaborado por el SOC de la Junta de Andalucía.

CONTENIDOS

Alerta prioritaria
Congreso Ciber
Campaña "Mucho Ojo"
Tema del mes
Guía rápida
Radar de amenazas
Normativa al día
Zona interactiva
Canal directo

Alerta prioritaria

Tu móvil en el punto de mira: el dispositivo más atacado de 2026

En 2026, el móvil ya no es solo para comunicarse; es nuestra identidad digital, cartera y acceso al trabajo. Por eso es el objetivo prioritario de los ciberdelincuentes. Detallamos las amenazas más críticas de este mes para tu dispositivo personal y corporativo.

- **SIM swapping: el robo invisible de tu línea móvil.** Una técnica en peligroso auge documentada activamente en España. Los atacantes consiguen un duplicado fraudulento de tu tarjeta SIM tras engañar a tu operadora. El objetivo: interceptar los códigos de verificación (SMS de doble factor) que tu banco envía para autorizar operaciones. Un caso reciente ante el Tribunal Supremo acredita el robo de más de 83.000€ mediante 15 transferencias no autorizadas en una sola noche.
- **Smishing y falsas notificaciones push.** Se multiplican los SMS y mensajes de apps que imitan alertas urgentes y legítimas de tu banco, Correos o la Seguridad Social para robar credenciales. El INCIBE alerta de que el 40% de todos los incidentes reportados en España tienen origen en este canal, demostrando su alta efectividad y alcance masivo. Un solo clic puede comprometer toda tu información.
- **Vishing: la trampa de tu propia voz.** Las llamadas fraudulentas evolucionan. Los delincuentes buscan grabar una respuesta afirmativa (el famoso "¿Sí?") para validarla mediante IA como consentimiento en transacciones no autorizadas. Otra variante crítica es la solicitud telefónica urgente del código de verificación de WhatsApp recibido por SMS, con el fin de secuestrar tu cuenta y suplantar tu identidad ante todos tus contactos.
- **Apps maliciosas fuera de tiendas oficiales.** Existe una alerta activa sobre aplicaciones (juegos, utilidades) que circulan por canales no oficiales (WhatsApp, Telegram, webs de descarga directa) y que instalan spyware en segundo plano. Esto representa un riesgo extremo en dispositivos utilizados para acceder a sistemas corporativos de la Administración.

¡Recuerda!

- Las operadoras de telefonía nunca te llamarán solicitando el código de una SIM nueva, ni tu DNI, para una gestión urgente de tu línea que tú no hayas iniciado.
- Si tu móvil se queda repentinamente sin cobertura en una zona donde siempre la tienes, desconfía de inmediato y contacta con tu operadora desde otro terminal para descartar un SIM Swapping.
- El 40% de los ataques reportados al INCIBE son Smishing; sé extremadamente desconfiado con cualquier SMS o notificación de urgencia no esperada.

¿Qué debes hacer?

1. Usa tiendas oficiales: no instales apps descargadas de internet (.apk) o recibidas por mensajes. Limítate a Google Play o App Store.
2. Protege tu voz: al responder llamadas de números desconocidos, evita la palabra "¿Sí?". Si te piden datos o códigos, cuelga y llama a la entidad oficial.
3. No compartas códigos: jamás facilites códigos de verificación recibidos por SMS (WhatsApp, banca) a nadie.
4. Reporta: si sospechas de una infección, cambia tus contraseñas clave, avisa a tu banco y repórtalo al SOC si es un dispositivo laboral.

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

BoleSTIC
Boletín de concienciación en ciberseguridad
Marzo de 2026
Nº 22
Elaborado por el SOC de la Junta de Andalucía.

CONTENIDOS

Alerta prioritaria
Congreso Ciber
Campaña "Mucho Ojo"
Tema del mes
Guía rápida
Radar de amenazas
Normativa al día
Zona interactiva
Canal directo

Así fue el 5º Congreso de Ciberseguridad de Andalucía

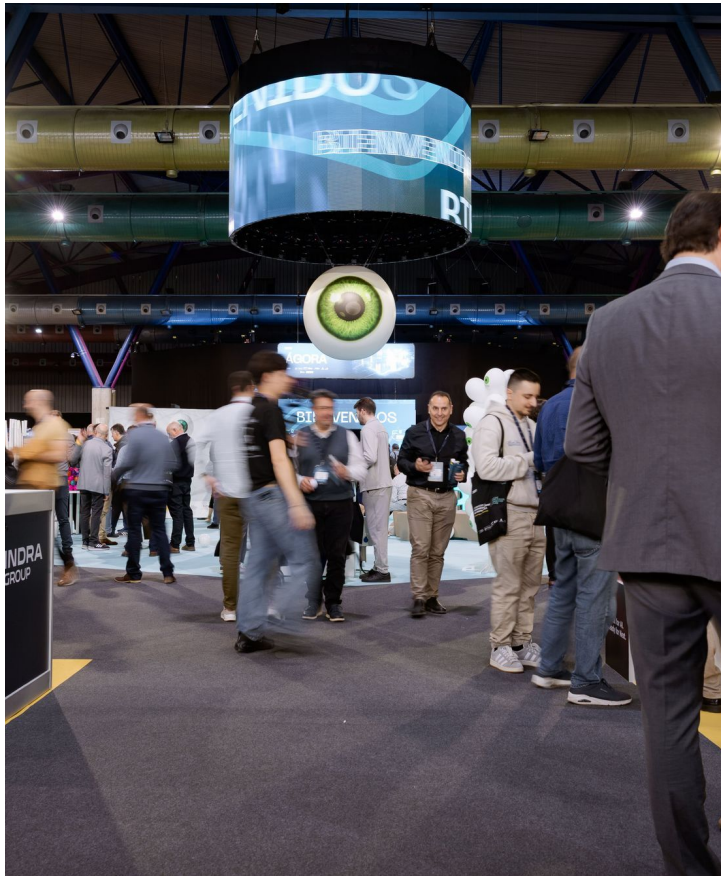
Bajo el lema “Secure territories, connected future”, la última edición del Congreso de Ciberseguridad de Andalucía puso el foco en la ciberseguridad no solo como un desafío técnico, sino como una prioridad estratégica, institucional y ciudadana.

Organizado por la Agencia Digital de Andalucía (ADA), a través del Centro de Ciberseguridad de Andalucía (CIAN), el evento reunió los días 24 y 25 de marzo en FYCMA (Málaga) a expertos, empresas e instituciones, para reflexionar sobre los retos actuales de la ciberseguridad, los cambios tecnológicos más disruptivos y los mecanismos que nos permitan construir un futuro digital más resiliente.

La apertura del Congreso corrió a cargo del Consejero de Industria, Energía y Minas de la Junta de Andalucía, Jorge Paradela, y del Alcalde de Málaga, Francisco de la Torre. Durante los dos días del evento se celebraron medio centenar de ponencias, mesas de debate y talleres, impartidos por reconocidos profesionales especialistas en normativa y desarrollo tecnológico en el ámbito de la ciberseguridad.

Resumen del primer día

Resumen del segundo día



BoleSTIC
Boletín de concienciación en ciberseguridad
Marzo de 2026
Nº 22
Elaborado por el SOC de la Junta de Andalucía.

CONTENIDOS

Alerta prioritaria
Congreso Ciber
Campaña "Mucho Ojo"
Tema del mes
Guía rápida
Radar de amenazas
Normativa al día
Zona interactiva
Canal directo

La ADA lanza “Mucho ojo”: una campaña para acercar la ciberseguridad a la ciudadanía

La Agencia Digital de Andalucía (ADA), a través del Centro de Ciberseguridad de Andalucía (CIAN), ha puesto en marcha recientemente la campaña “Mucho ojo”. Se trata de una iniciativa diseñada para reforzar la concienciación ciudadana en la adopción de hábitos digitales seguros, mediante un enfoque cercano, visual y accesible.

La campaña, que ha estado muy presente durante el 5º Congreso de Ciberseguridad de Andalucía, forma parte de las actividades que la ADA y el CIAN están desarrollando como parte del Proyecto Red Argos, integrado en la iniciativa INCIBE RETECH, en el marco del Plan de Recuperación, Transformación y Resiliencia, con la financiación de los Fondos Next Generation-EU.

Con "Mucho ojo" la ADA da un paso más en su compromiso con la protección digital de la sociedad, trasladando a la calle y a los canales digitales un mensaje claro: la ciberseguridad forma parte del día a día de las personas, y es clave para desenvolverse con confianza en un mundo cada vez más conectado.

Más información

BoleSTIC
Boletín de concienciación en ciberseguridad
Marzo de 2026
Nº 22
Elaborado por el SOC de la Junta de Andalucía.

CONTENIDOS

Alerta prioritaria
Congreso Ciber
Campaña "Mucho Ojo"
Tema del mes
Guía rápida
Radar de amenazas
Normativa al día
Zona interactiva
Canal directo

Tema del mes

Contraseñas: el problema que creías resuelto y no lo está

En un ecosistema donde las filtraciones de datos son cada vez más frecuentes, seguir utilizando la misma contraseña para todo se ha convertido en el eslabón más débil de nuestra seguridad digital. A menudo pensamos que nuestras cuentas están aisladas, pero si reutilizas tus claves, un único par de credenciales expuestas puede abrirle la puerta a los ciberdelincuentes hacia tu correo, tus redes sociales o tu banca online, incluso si esos servicios no tienen ninguna relación entre sí.

Cómo funcionan realmente los ataques que roban tus credenciales sin que lo notes

Los ciberdelincuentes ya no pierden el tiempo intentando adivinar tu contraseña letra a letra. En su lugar, utilizan tácticas mucho más rentables y silenciosas. La más popular es el credential stuffing (o relleno de credenciales). Consiste en coger listas inmensas de correos y contraseñas que ya se han filtrado en internet y usar programas automáticos para probarlas a toda velocidad en miles de webs distintas.

Como usan combinaciones que son reales, los sistemas de seguridad no siempre hacen saltar las alarmas. Para lograrlo a gran escala, se apoyan en inteligencia artificial y redes de bots. Otra técnica en auge es infectar los dispositivos con programas invisibles (infostealers) diseñados para robar las contraseñas que tienes guardadas en el navegador.

Gestores y doble factor: tus mejores aliados

Para frenar estos ataques, la regla de oro es innegociable: cada cuenta necesita una clave diferente. ¿Cómo gestionar esto sin volverse loco?

- Gestores de contraseñas: funcionan como una caja fuerte digital. Tú solo memorizas una única clave principal (la maestra), y el programa se encarga de inventar y recordar contraseñas larguísimas e indescifrables para cada web. Lejos de ser complicados, te ahorran tener que teclear cada vez que inicias sesión.
- El doble factor de autenticación (2FA): es un escudo extra. Aunque un atacante consiga tu clave, se topará con una pared si no tiene este segundo código temporal. Eso sí, en seguridad profesional se recomienda evitar los SMS (ya que te pueden duplicar la tarjeta SIM mediante SIM Swapping) y usar aplicaciones generadoras de códigos en tu móvil, que son mucho más robustas

Tus contraseñas, paso a paso

- Investiga: usa buscadores fiables de brechas de seguridad para comprobar si tu email corporativo o personal se ha filtrado alguna vez.
- Haz limpieza: si confirmas que una clave ha quedado expuesta, cámbiala al instante.
- Da el salto: instala un gestor de contraseñas y empieza a guardar ahí tus accesos más críticos.
- Pon el cerrojo: ve a los ajustes de tus apps principales y activa el doble factor (2FA) mediante aplicación.

SIGUE >>

Financiado por la Unión Europea NextGenerationEU

BoleSTIC
Boletín de concienciación en ciberseguridad
Marzo de 2026
Nº 22
Elaborado por el SOC de la Junta de Andalucía.

CONTENIDOS

Alerta prioritaria
Congreso Ciber
Campaña "Mucho Ojo"
Tema del mes
Guía rápida
Radar de amenazas
Normativa al día
Zona interactiva
Canal directo

<< VIENE DE LA ANTERIOR

Gestores de contraseñas: desmontando el mito de la complejidad

Muchas personas evitan usar gestores de contraseñas porque creen que añadirán pasos extra a su rutina o por el miedo de "poner todas las llaves en la misma cesta". Sin embargo, a nivel práctico, son la herramienta de ciberseguridad que más tiempo te va a ahorrar en el día a día.

- Autocompletado automático: una vez instalado en tu navegador o dispositivo móvil, el gestor detecta en qué página web estás y rellena tu usuario y contraseña con un solo clic o usando tu huella dactilar. Se acabó teclear o buscar libretas.
- Sincronización total: como muchos de ellos funcionan en la nube, si generas y guardas una contraseña nueva en tu ordenador, la tendrás disponible al instante en tu teléfono móvil.
- Seguridad blindada: ni siquiera la empresa desarrolladora del gestor puede leer tus claves. Todo el "cofre" se cifra matemáticamente y solo se puede abrir con tu única contraseña maestra.

La letra pequeña del doble factor: no todos son iguales

Ya vimos que el 2FA (doble factor) es imprescindible como escudo extra frente a robos de credenciales. Pero el método que elijas para recibir ese segundo código marca una gran diferencia en tu nivel de seguridad real.

- El peligro oculto de los SMS: recibir un código numérico por SMS es mejor que nada, pero hoy en día es un método vulnerable. Si eres víctima de SIM Swapping (un duplicado fraudulento de tu tarjeta SIM por parte de un atacante), el ciberdelincuente recibirá tus códigos bancarios directamente en su teléfono.
- La alternativa infalible (apps autenticadoras): es el método recomendado por los profesionales. Aplicaciones gratuitas como Google Authenticator o Microsoft Authenticator generan códigos temporales (que cambian cada 30 segundos) directamente en tu dispositivo físico.

Checklist: "Audita tus contraseñas en 5 minutos"

Si tu respuesta a alguna de las siguientes preguntas es "no", tu identidad digital podría estar en riesgo

- ¿Tienes una contraseña completamente diferente y única para tu correo corporativo?
- ¿Has comprobado recientemente si tu email se ha filtrado en alguna brecha de datos pública?
- ¿Utilizas un gestor de contraseñas para no tener que memorizar decenas de claves complejas?
- ¿Tienes activado el doble factor de autenticación (2FA) en tus cuentas principales (banco, correo, redes)?
- ¿Usas una aplicación autenticadora (como Google o Microsoft Authenticator) en lugar de recibir los códigos por SMS?
- ¿La clave principal de tu equipo es una "frase de contraseña" (larga pero fácil de recordar para ti)?

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

BoleSTIC
Boletín de concienciación en ciberseguridad
Marzo de 2026
Nº 22
Elaborado por el SOC de la Junta de Andalucía.

CONTENIDOS

Alerta prioritaria
Congreso Ciber
Campaña "Mucho Ojo"
Tema del mes
Guía rápida
Radar de amenazas
Normativa al día
Zona interactiva
Canal directo

Guía rápida

Ciberseguridad en el día a día: preguntas frecuentes

→ **¿Es seguro hacer una videollamada de trabajo desde un lugar público?**

Depende. Alguien puede escuchar información sensible. Usa auriculares y evita compartir pantalla con documentos confidenciales a la vista.

→ **¿El router de casa necesita alguna configuración especial si teletrabajas?**

Sí. Cambia la contraseña que viene de fábrica y asegúrate de que usa cifrado WPA2 o WPA3. Un router mal configurado es una puerta abierta.

→ **¿Imprimir documentos de trabajo en una impresora doméstica o pública es seguro?**

Depende. Muchas impresoras guardan copias de los documentos. Evita imprimir información sensible fuera del entorno corporativo.

→ **Si pierdo el móvil de trabajo debo esperar a llegar a la oficina para avisar?**

No. Notifica de inmediato. Cuanto antes se pueda bloquear o borrar el dispositivo en remoto, menor es el riesgo de exposición de datos.

→ **¿Conectar un dispositivo USB encontrado o prestado puede ser peligroso?**

Sí. Un USB desconocido puede ejecutar código malicioso en cuanto lo conectas, aunque parezca vacío. Nunca lo uses en un equipo de trabajo.

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
Marzo de 2026
Nº 22
Elaborado por el SOC de la Junta de Andalucía.

CONTENIDOS

Alerta prioritaria
Congreso Ciber
Campaña "Mucho Ojo"
Tema del mes
Guía rápida
Radar de amenazas
Normativa al día
Zona interactiva
Canal directo

Radar de amenazas

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

Cuidado con este correo de “Mi Carpeta Ciudadana”: así te engañan con un falso abono para robar tu cuenta bancaria

Correos fraudulentos imitan la plataforma oficial para informar de un supuesto abono pendiente. La web falsa, que copia con detalle el diseño oficial, solicita el IBAN y las credenciales bancarias de la víctima. Recuerda: la Administración nunca pide datos bancarios por correo.

> Enlace a la noticia

Desconfía de supuestas notificaciones de la Guardia Civil y Europol sobre la "Operación Endgame"

El INCIBE alerta de una campaña de phishing con un PDF adjunto que acusa al destinatario de estar implicado en ciberdelitos internacionales y le presiona para facilitar datos o realizar pagos. Las fuerzas de seguridad nunca notifican cargos penales por correo electrónico genérico.

> Enlace a la noticia

Dos extensiones de Chrome ‘legítimas’ se vuelven maliciosas tras cambiar de dueño y habilitan inyección de código y robo de datos

Dos extensiones con miles de usuarios pasaron a robar datos de navegación tras ser vendidas a nuevos propietarios que introdujeron código malicioso oculto. Revisa periódicamente las extensiones de tu navegador y elimina las que no uses.

> Enlace a la noticia

Troyano para Android que se hace pasar por servicios gubernamentales y aplicaciones de Starlink

Kaspersky detecta un malware que se distribuye imitando aplicaciones legítimas de servicios gubernamentales. Una vez instalado, accede a contactos, mensajes y credenciales en segundo plano. Descarga apps solo desde tiendas oficiales.

> Enlace a la noticia

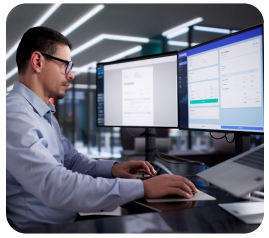
BoleSTIC
Boletín de concienciación en ciberseguridad
Marzo de 2026
Nº 22
Elaborado por el SOC de la Junta de Andalucía.

CONTENIDOS

Alerta prioritaria
Congreso Ciber
Campaña "Mucho Ojo"
Tema del mes
Guía rápida
Radar de amenazas
Normativa al día
Zona interactiva
Canal directo

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.



Usa la información de tu trabajo solo para lo que te corresponde

Evita usar tu nube personal para datos del trabajo

Nunca reveles tu contraseña, por ningún medio ni a ninguna persona

Elimina tus credenciales y certificados de los equipos viejos

Reporta inmediatamente la pérdida de equipos o accesos sospechosos

Ten precaución al abrir el correo laboral en equipos externos

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

CONTENIDOS

Alerta prioritaria
Congreso Ciber
Campaña "Mucho Ojo"
Tema del mes
Guía rápida
Radar de amenazas
Normativa al día
Zona interactiva
Canal directo

Zona interactiva

Quiz del mes

Un SMS incluye un enlace para reprogramar la entrega de tu paquete. ¿Qué señal indica que puede ser un fraude?

- El mensaje llega un lunes
- El enlace no coincide con el dominio oficial
- El mensaje no tiene errores de ortografía

Un compañero publica en LinkedIn: "Arrancamos migración a la nube con [nombre del proveedor] 💪". ¿Qué riesgo supone?

- Ninguno, es información genérica
- Revela datos técnicos útiles para ataques dirigidos
- Solo es un riesgo si menciona datos personales

Un artículo te invita a introducir tu correo para comprobar si tus datos han sido filtrados. ¿Qué haces?

- Introduzco un correo falso
- Lo introduzco, es la única forma de saberlo
- Cierro la página y uso haveibeenpwned.com

Tu operadora te comunica que alguien ha pedido un duplicado de tu SIM sin que tú lo hayas solicitado. ¿Qué puede ser?

- Una campaña de marketing
- Un error administrativo
- Un intento de SIM swapping para interceptar tus códigos

Necesitas consultar un documento de trabajo y te conectas a la WiFi de una cafetería. ¿Cuál es el mayor riesgo?

- Que la conexión sea lenta
- Que alguien intercepte tu tráfico
- Que el documento quede guardado en la red

Un compañero te pasa por WhatsApp un enlace para descargar una app fuera de la tienda oficial. ¿Qué haces?

- La instalo, si la recomienda un compañero es segura
- No la instalo y consulto con IT
- La instalo pero sin usarla con el correo corporativo

SIGUE >>

BoleSTIC
Boletín de concienciación en ciberseguridad
Marzo de 2026
Nº 22
Elaborado por el SOC de la Junta de Andalucía.

CONTENIDOS

Alerta prioritaria
Congreso Ciber
Campaña "Mucho Ojo"
Tema del mes
Guía rápida
Radar de amenazas
Normativa al día
Zona interactiva
Canal directo

<< VIENE DE LA ANTERIOR

Caso práctico

Son las 11 de la mañana. Abres LinkedIn y ves que una persona que no conoces te ha enviado una solicitud de conexión. Su perfil tiene foto, experiencia detallada y varios contactos en común contigo, entre ellos tu responsable directo.

Al aceptar, te llega de inmediato un mensaje: "Hola, soy consultora externa colaborando con vuestro equipo en el nuevo proyecto. Me ha pasado tu contacto [nombre de tu responsable]. ¿Podrías confirmarme qué herramientas de gestión documental usáis actualmente y quién es el responsable técnico? Lo necesito para preparar la reunión de esta semana."

El perfil parece legítimo. El nombre del proyecto que menciona coincide con uno real en el que estás trabajando. La solicitud parece razonable y no pide nada confidencial en apariencia.

¿Qué haces?

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
Marzo de 2026
Nº 22
Elaborado por el SOC de la Junta de Andalucía.

CONTENIDOS

Alerta prioritaria
Congreso Ciber
Campaña "Mucho Ojo"
Tema del mes
Guía rápida
Radar de amenazas
Normativa al día
Zona interactiva
Canal directo

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