BOLESTIC

Nº 16 septiembre 2025

Boletín de concienciación en ciberseguridad

Esta comunicación está destinada a los profesionales públicos de la Administración.
Algunos de los enlaces mostrados pueden requerir de la aceptación de cookies.

incidentes.soc@juntadeandalucia.es

TITULARES

Conexiones seguras: un básico en ciberseguridad

Nuestra actividad online pasa indudablemente por conectarnos: a Internet, con otros dispositivos, al coche, etc. Conocer los tipos de conexiones existentes y saber utilizarlas no es suficiente, es imperativo aprender los riesgos que conllevan y cómo evitarlos. Pág. 2

Phishing: no muerdas el anzuelo

El término phishing viene del inglés fishing, que se pronuncia igual, y que significa pescar. En este caso no se pescan peces, sino datos personales como nombres de usuario, contraseñas o datos de cuentas bancarias.

Pág. 3

¿Harto de que te llamen a todas horas con publicidad?

Pocas cosas hay tan molestas como recibir una llamada en tu teléfono personal a las 16:30 horas de un sábado cualquiera, y descubrir al descolgar, que se trata de una llamada publicitaria para pretender cambiarte de compañía telefónica o venderte una tarjeta de crédito.

Pág. 4

No todo es phishing... ¡cuidado con el smishing!

Los ciberdelincuentes lanzan sus redes cada vez por más medios, así que toca ser más precavidos que nunca. ¡No todas las amenazas llegan por correo electrónico! Ten cuidado también con los SMS y con los mensajes que recibes en WhatsApp, Telegram y otras aplicaciones de mensajería.

El smishing (combinación de SMS y phishing) es un ataque que utiliza mensajes de texto engañosos, con el objetivo de que compartas información personal o financiera realizando alguna acción (clic en un enlace, una llamada, un SMS...). Los mensajes pueden proceder de fuentes que parecen fiables, e intentan crear sensación de urgencia o miedo para que la víctima caiga en el engaño.

Te dejamos más información aquí. ¡Mucho ojo!

El POST-IT

Uso del equipamiento TIC del puesto de trabajo

LA PELÍCULA

CONTRAPORTADA

- Por una vuelta al cole más cibersegura
- No, la DGT no te envía emails ni mensajes para notificar multas de tráfico
- Expertos descubren la mejor arma contra los "deepfakes" de la IA: "Solo dile que dibuje una carita sonriente"
- Ocho de cada diez fraudes bancarios ocurren en el móvil

Comprueba si tu cuenta de correo está comprometida, https://haveibeenpwned.com/. Si es así, **cambia la contraseña**.

BOLESTIC
Nº 16 septiembre 2025
Boletín de concienciación en ciberseguridad

incidentes.soc@juntadeandalucia.es

TITULARES

Conexiones seguras: un básico en ciberseguridad

Cada día en nuestros dispositivos, utilizamos diferentes tipos de conexiones para navegar por Internet o compartir información entre otras múltiples acciones. Establecer conexiones seguras es un paso básico para evitar riesgos y sacar partido a todas las funcionalidades de estas tecnologías.

¿Qué son las conexiones seguras? Aprende a identificar los tipos de conexiones existentes

Son aquellas que se establecen sin entrañar riesgos de seguridad para usuarios y dispositivos. Wi-Fi, Ethernet, Bluetooth, NFC y VPN son los distintos tipos de conexiones que puedes establecer en tus dispositivos. ¿Sabes en qué consiste cada una de ellas?

- Wi-Fi: su función es conectarte a la Red de forma inalámbrica.
- *Ethernet*: te conecta a Internet mediante cable, es decir, de forma más estable y rápida por lo general.
- *Bluetooth*: conecta de forma inalámbrica pero de corto alcance, para comunicar dispositivos como altavoces, teclados o auriculares.
- NFC (*Near Field Communication*): comunica inalámbricamente dispositivos cercanos físicamente. Seguro que lo has usado para realizar pagos con el móvil.
- VPN *(Virtual Private Network*) establece una conexión cifrada entre tu dispositivo e Internet, añadiendo una capa de seguridad a redes públicas y protegiendo información confidencial.

Amenaza a la vista: los riesgos de las conexiones no seguras

- Robo de datos personales: si no te conectas mediante conexiones seguras te arriesgas a que tu información sea interceptada. Hablamos de contraseñas, datos personales o de pago. ¿A qué te expone esto? A que intenten hacerse pasar por ti para realizar acciones fraudulentas.
- *Malware*: otro riesgo al que te expones es que infecten tus dispositivos con programas maliciosos que podrían dañar tus archivos, robarte información o perder el control de tus propios dispositivos electrónicos.
- Suplantación de identidad: puede suceder cuando un ciberdelincuente intercepta la comunicación entre dos dispositivos, debido a una red insegura, lo que le podría permitir falsificar los mensajes que intercambias poniendo en riesgo la privacidad de tus comunicaciones.
- Espionaje y vigilancia: tu información es valiosa, por eso las conexiones no seguras pueden ser una vía de entrada a espías de tu comportamiento digital, lo que comprometería tu privacidad.
- Uso de la red para actividades ilegales: ¿te imaginas qué podría pasar si alguien hace pasar por tuya una actividad ilegal? Pues también puede pasar de forma digital. Algunos ejemplos son la descarga o distribución de contenido protegido con derechos de autor, divulgación de pornografía o el tráfico de armas, entre otros.

El primer paso es identificar las posibles amenazas, para así entender cómo actúa la ciberdelincuencia ante la posibilidad de acceder a nuestra información y datos personales. A partir de aquí es posible poner barreras, si sabemos cómo.

BOLESTIC
Nº 16 septiembre 2025
Boletín de concienciación en ciberseguridad
Esta comunicación está destinada a los profesionales públicos de la Administración.
Algunos de los enlaces mostrados pueden requerir de la aceptación de cookies.
incidentes.soc@juntadeandalucia.es

Phishing: no muerdas el anzuelo

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
protege tu empresa

Phishing más comunes

1	Emplear antivirus ***antiphishing*** específicos para mensajería y páginas web con sus correspondientes firmas actualizadas periódicamente.
2	Conocer la importancia de mantener actualizado el ***software*** de los sistemas y webs para evitar que los atacantes exploten vulnerabilidades.
3	Desconfiar cuando se transmite **sensación de urgencia, adulaciones, desconocimiento**... ¡Todo esto son tácticas de Ingeniería Social!
4	Ante dudas acerca del remitente siempre es recomendable **contactar** con este **por otro medio** para asegurar que la conversación sea segura.
5	Nunca hacer clic en una URL que solicita información sin antes **comprobar** que el sitio al que redirecciona es **legítimo**.
6	**URL acortada** es sinónimo de sospecha. Dado que deniegan la posibilidad de verificar la legitimidad, los sitios legales nunca las emplearán.
7	Nunca se debe iniciar sesión en un sitio sin antes haber verificado que opera con un **protocolo seguro HTTPS**. Esto se puede comprobar en la barra de navegación.
8	Se deben revisar las **políticas de privacidad y avisos legales** de los sitios web o formularios antes de introducir datos sensibles. De lo contrario se podría estar dando el consentimiento para que se cedan estos datos a terceros.
9	Si se descarga un fichero desde un ***email*** se debe confiar en la fuente de la que procede antes de hacer clic en la ventana de "habilitar contenido" que se despliega cuando lo hayamos descargado. Podría contener ***malware***.
10	Se debe desconfiar de cuerpos de correos electrónicos que realicen **comunicaciones personales**. Las entidades legítimas suelen referirse a su destinatario empleando nombres y apellidos.
11	Se debe desconfiar de cuerpos de correos electrónicos que contengan **errores ortográficos y gramaticales**. Una entidad seria no descuidará elementos tan importantes en la comunicación.
12	Ante la menor sospecha, mejor prevenir que curar: siempre se podrá borrar el mensaje (***phishing*** o ***smishing***) o colgar la llamada (si se puede tratar de un ***vishing***).

BOLESTIC
Nº 16 septiembre 2025
Boletín de concienciación en ciberseguridad
Esta comunicación está destinada a los profesionales públicos de la Administración.
Algunos de los enlaces mostrados pueden requerir de la aceptación de cookies.
incidentes.soc@juntadeandalucia.es

¿Harto de que te llamen a todas horas con publicidad?

DERECHO A NO RECIBIR LLAMADAS COMERCIALES NO SOLICITADAS

La Ley 11/2022 General de Telecomunicaciones en su artículo 66.1 refuerza las garantías de los usuarios en relación con su derecho a no recibir llamadas comerciales no solicitadas. Hasta la entrada en vigor de estos cambios, podías recibir estas llamadas si no te habías opuesto a ellas.

Estos cambios se aplican a las llamadas comerciales realizadas por una persona y no a las que se realicen con sistemas de marcación automática sin intervención humana (por ejemplo, con un mensaje pregrabado).

1. Si has dado previamente tu **consentimiento** podrás recibir llamadas comerciales.

2. Para que la empresa pueda justificar su interés legítimo en hacerte llamadas comerciales debes haber tenido **una relación previa con ella** habiendo adquirido sus productos o servicios y, además, los que quiera ofrecerte **deben ser similares** a los que hubieras contratado anteriormente.

3. Esta posibilidad sólo se refiere a las llamadas de la empresa con la que hayas tenido esa relación y no a otras entidades, aunque pertenezcan a su mismo grupo empresarial.

4. Si la relación contractual ya no está en vigor y no has realizado ninguna otra solicitud o interacción con la empresa **durante el último año**, no podrán llamarte.

5. Sólo pueden realizarse llamadas comerciales a **números generados de forma aleatoria** con el consentimiento previo del usuario. No pueden realizarse llamadas a estos números aleatorios basándose en el interés legítimo de la empresa, ya que no prevalece sobre el derecho de los usuarios a no recibir llamadas comerciales.

6. Si tu número de teléfono figura en una **guía de abonados** sólo podrán utilizarlo para llamadas comerciales si has dado previamente tu consentimiento expreso, que debe constar con carácter general en las correspondientes guías.

7. Si te has registrado previamente en un **sistema de exclusión publicitaria** sólo podrán hacerte llamadas comerciales si has dado tu consentimiento específico a la empresa que te llama. Si no tienen tu consentimiento, todas las empresas que realizan campañas comerciales están obligadas a consultar dichos sistemas. Si diste tu consentimiento y no quieres que te sigan llamando debes revocarlo.

8. Si eres una persona de contacto de la **entidad en la que trabajas** podrás recibir llamadas comerciales solo para relacionarse con la entidad y no contigo a título individual.

9. Si eres un empresario o profesional liberal sólo podrán hacerte llamadas comerciales referidas a productos y servicios relacionados con tu **actividad empresarial o profesional**, y no a título individual.

10. Al inicio de cada llamada **deberán informarte** de la identidad de la empresa o de la persona por cuenta de la cual te llaman, indicarte la finalidad comercial de la llamada y la posibilidad de revocar el consentimiento o ejercer el **derecho de oposición**. Ten en cuenta que todas las llamadas deberán grabarse.

Inscríbete en una lista de exclusión publicitaria

Al inscribirte en estas listas puedes elegir el medio o canal de comunicación a través del cual no deseas recibir publicidad (correo postal, llamadas telefónicas, correo electrónico u otro medio).

- Servicio Lista Robinson
- Lista Stop Publicidad

BOLESTIC

Nº 16 septiembre 2025

Boletín de concienciación en ciberseguridad

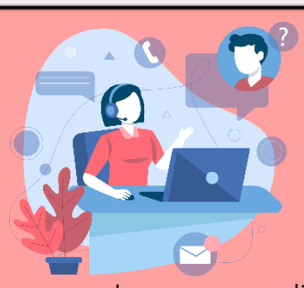
Esta comunicación está destinada a los profesionales públicos de la Administración.
Algunos de los enlaces mostrados pueden requerir de la aceptación de cookies.

incidentes.soc@juntadeandalucia.es

EL POST-IT

Uso del equipamiento TIC del puesto de trabajo

Código de conducta en el uso de las tecnologías de la información y la comunicación para profesionales públicos de la administración de la Junta de Andalucía.

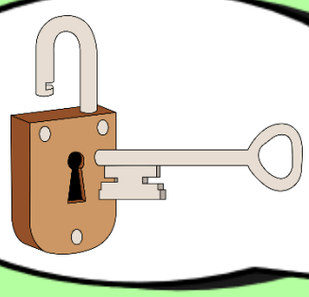


Seguiremos los procedimientos establecidos en cada Consejería o Agencia, para reportar incidencias, peticiones o permisos, sobre el equipamiento TIC y software.

Realizaremos un uso compatible con el desempeño de sus funciones. La puesta a disposición del equipamiento TIC no implica cesión de su propiedad.

No debemos modificar el equipamiento TIC, ni se realizarán reparaciones técnicas de mantenimiento o mejora del mismo. El software del equipo no podrá ser eliminado y no se instalarán nuevas aplicacioines, aunque estas sean de libre uso o gratuitas.

Utilizaremos los mecanismos de bloqueo que se hayan establecido en caso de desatención temporal del equipamiento TIC.



No permitiremos, ni facilitaremos, el uso del equipamiento TIC a terceros que no estén autorizados.

BOLESTIC
Nº 16 septiembre 2025
Boletín de concienciación en ciberseguridad

incidentes.soc@juntadeandalucia.es

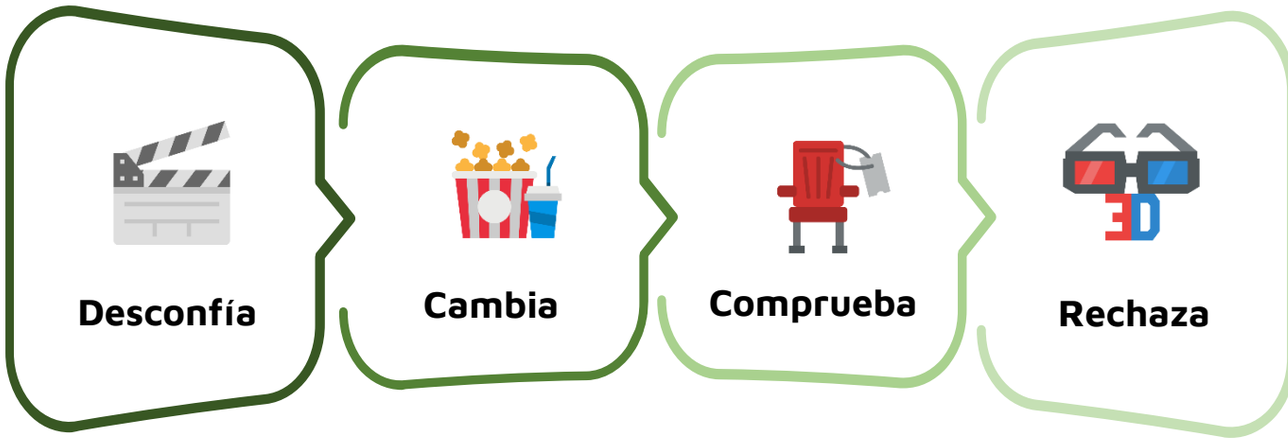
LA PELÍCULA

El cartero siempre te amenaza dos veces

Cada vez recibimos más correos maliciosos cuya intención es aprovecharse de nuestro desconocimiento, ingenuidad o buena voluntad.

Depende de nosotros saber cómo identificar un correo electrónico malicioso, para no ser víctimas de estafas, robo de claves, virus, etc.

Y sobre todo, utiliza el sentido común.



01. Desconfía

Desconfía, las entidades bancarias nunca solicitan datos personales por correo electrónico, sms o WhatsApp.

02. Cambia

No utilices el enlace adjunto al correo. Si quieres acceder a esa web, cambia de herramienta, utiliza el buscador o tus marcadores guardados.

03. Comprueba

Comprueba que la URL o dirección de la web que visitas es la que dice ser.

04. Rechaza

Rechaza de manera sistemática cualquier correo que solicite facilitar datos.

BOLESTIC
Nº 16 septiembre 2025
Boletín de concienciación en ciberseguridad
Esta comunicación está destinada a los profesionales públicos de la Administración.
Algunos de los enlaces mostrados pueden requerir de la aceptación de cookies.
incidentes.soc@juntadeandalucia.es

CONTRAPORTADA

Por una vuelta al cole más cibersegura

Hace tan sólo unos días las aulas se abrían de nuevo de par en par para acoger el curso escolar. En un sistema educativo cada vez más digital, es importante que nuestros hijos e hijas estén informados y preparados. ¡Échale un ojo a esta guía a modo de "mochila digital"! Para más información, pulsa aquí.

No, la DGT no te envía emails ni mensajes para notificar multas de tráfico

Si recibes un correo electrónico (o un mensaje de texto o WhatsApp), que parece provenir de la Dirección General de Tráfico para notificarte una multa... ¡no caigas! Se ha detectado una campaña que usa enlaces fraudulentos suplantando a la DGT con el objetivo de obtener tus datos. Para más información, pulsa aquí.

Expertos descubren la mejor arma contra los "deepfakes" de la IA: "Solo dile que dibuje una carita sonriente"

Cada vez resulta más complicado saber si aquello que se ve o escucha es real o ha sido creado mediante inteligencia artificial. Sobre todo en Internet, donde este tipo de estafas, denominadas como "deepfakes" están a la orden del día. Para más información, pulsa aquí.

Ocho de cada diez fraudes bancarios ocurren en el móvil

Los delincuentes se han adaptado: ya no necesitan vulnerar sistemas, les basta con convencer persuasivamente a sus víctimas para que autoricen los pagos por sí mismas. Para más información, pulsa aquí.