

## TITULARES

**¿Están tus datos personales en la Dark Web?**

Cuidado donde pones tu información personal en Internet o con los archivos que descargas de páginas desconocidas, los ciberdelincuentes están cada vez más presentes y cualquier ciberataque o malware podría afectarte de muchas maneras.

[Pág. 2](#)**Qué datos no debes compartir nunca en Internet**

Antes de compartir algo en Internet, debemos pararnos a pensar si realmente no nos importa que cualquier persona pueda acceder a ello, ya sea ahora o en el futuro.

[Pág. 3](#)**La inteligencia artificial (IA) y los ciberdelincuentes**

La IA es un tema fascinante, de gran relevancia en el mundo actual, y está revolucionando numerosos campos. Puede ser utilizada para fines muy útiles, pero también con objetivos maliciosos. ¡Todo depende de quién la use y para qué! Las amenazas basadas en IA son una realidad emergente que requieren atención.

[Pág. 4](#)**Hábitos digitales para evitar el phishing**

Octubre es el Mes Europeo de la Ciberseguridad, que en 2025 centra sus esfuerzos en combatir el phishing.

Siguiendo esta línea, queremos compartir contigo algunos consejos para que no caigas en una de las estafas online más frecuentes:

- Desconfía de mensajes que te pidan datos o verificar info de forma urgente.
- No cliques en enlaces que lleguen por correo: accede desde la URL oficial.
- Revisa cuidadosamente la cuenta del remitente para ver si el dominio es real.
- No descargues, y nunca abras/ejecutes, archivos que sean sospechosos.
- Mantén actualizado tu equipo y software de seguridad (antivirus, cortafuegos...).

Y recuerda, si has visto un comportamiento sospechoso o sufrido un incidente de seguridad, ¡notifícalo!

[incidentes.soc@juntadeandalucia.es](mailto:incidentes.soc@juntadeandalucia.es) / 955 060 974

**EI POST-IT****LA PELÍCULA****CONTRAPORTADA**

¿Te han pedido alguna votación por WhatsApp? ¡Mucho ojo!



Hackean a la Agencia Tributaria española



Campaña de phishing haciéndose pasar por Endesa



Magis TV, el 'Netflix pirata', podría espiar tus dispositivos y abrir la puerta al robo de datos



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

# TITULARES

## ¿Están tus datos personales en la Dark Web?

Se trata de la parte más oscura de Internet. Para acceder se requieren navegadores específicos. En este espacio se concentran servicios y páginas que ofrecen contenidos ilegales o poco recomendables. Esto no quiere decir que no podamos encontrarlos en otras zonas de Internet, pero aquí proliferan más y es más difícil controlarlos, ya que una de sus características de diseño es el anonimato.

Muchos piratas cibernéticos se centran en recopilar datos confidenciales (credenciales filtradas, números de tarjetas, documentos de identidad...) para compartirlos en la Dark Web. Una vez ahí, cualquiera podría adquirirlos y usarlos en otras acciones maliciosas.

Google dispone de una función que te permite saber si algunas de tus credenciales están comprometidas en este lado oscuro de Internet.

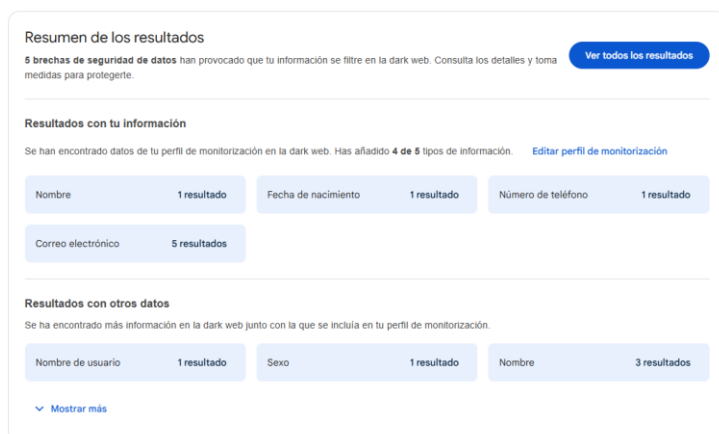
Si tienes una cuenta de Google, una vez que accedas a la misma pulsa en la foto de tu perfil y selecciona la opción "Seguridad".



### Google Cuenta

- Inicio
- Información personal
- Datos y privacidad
- Seguridad**
- Contactos y compartir
- Pagos y suscripciones
- Información general

Desplázate hacia abajo para acceder a "Informe de dark web" y actívalo. En ese momento, la herramienta empezará a rastrear para encontrar información personal.



Si presionas en la opción "Ver todos los resultados", en la parte inferior Google te mostrará recomendaciones de acuerdo a tu caso. De igual manera, la forma adecuada de reaccionar es cambiando tu contraseña regularmente a una que sea robusta, y mantenerte al tanto de las acciones sospechosas que se hagan desde tu cuenta.

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

Qué datos no debes compartir nunca en Internet

Aunque cada usuario es libre de hacer lo que quiera con sus datos personales, **compartir determinada información puede tener consecuencias muy graves para nuestra seguridad.**

**7 datos que nunca debes compartir en Internet**

- 1 Correo electrónico y número de teléfono**  
Aunque es habitual utilizarlos para registrarnos en sitios web...  
... si los compartimos libremente por Internet nos exponemos a ser víctimas de spam, phishing y todo tipo de ciberataques basados en ingeniería social.
- 2 Dirección y ubicación**  
Compartir nuestra ubicación en tiempo real o la dirección de nuestro hogar es muy peligroso.  
No sabemos las intenciones de alguien que pueda estar interesado en saber dónde vivimos, cuáles son los lugares que frecuentamos o cuándo no estamos en casa.
- 3 Fotos de menores**  
Todos nos morimos de ganas de mostrar al mundo a nuestro hijo, sobrino o nieto, especialmente en las redes sociales.  
Sin embargo, no sabemos dónde pueden acabar estas imágenes ni quién puede tener acceso a ellas. Lo mejor es taparle la cara de algún modo.
- 4 Fotos comprometedoras**  
El hecho de subir fotos a nuestras redes sociales e Internet ya tiene un impacto en nuestra identidad digital y debe hacerse con cabeza.  
Publicar fotos comprometedoras o de carácter íntimo o sexual pueden suponer una gran amenaza para nuestra seguridad y tener consecuencias muy graves, como la sextorsión o el ciberacoso.
- 5 Documentos personales**  
Nuestro DNI, carné de conducir, contrato de trabajo o datos bancarios son datos personales muy sensibles.  
Con su revelación nos exponemos, por ejemplo, a una suplantación de identidad y al uso de nuestros datos de forma fraudulenta.
- 6 Opiniones, quejas, comentarios comprometidos**  
Es habitual utilizar Internet para expresarse y compartir críticas y quejas.  
Sin embargo, un comentario subido de tono en la Red puede llegar a oídos de personas que puedan sentirse ofendidas o incluso atacadas, y que podrían no tomarse demasiado bien nuestros comentarios.
- 7 Conversaciones privadas**  
Del mismo modo que no debemos compartir fotos de terceros sin su aprobación...  
... las conversaciones privadas no son algo que debamos compartir en Internet, especialmente si contienen datos personales o información que podría considerarse como revelación de secretos y la otra persona preferiría no difundir.

OSI Oficina de Seguridad del Internauta

## La inteligencia artificial (IA) y los ciberdelincuentes

### Tipos de IA

Los Sistemas de IA se clasifican en función de su uso y propósito.

- ♦ Los **Sistemas de IA de propósito general** son versátiles y no están limitados a un sector específico.
  - ♦ Ejemplos: asistentes virtuales como Siri y Alexa, o herramientas web como ChatGPT y Copilot.
- ♦ Los **Sistemas de IA de alto riesgo** pueden influir en decisiones importantes sobre temas de salud, seguridad o los derechos fundamentales.
  - ♦ Ejemplos: dispositivos médicos, formación, selección de personal, procesos democráticos, etc.
- ♦ Los **Sistemas de IA prohibidos** son aquellos que pueden causar daño físico o psicológico modificando el comportamiento de una persona.
  - ♦ Ejemplo: cualquier vídeo, imagen o noticia falsa que distorsione el comportamiento de una persona o explote sus vulnerabilidades causándole daño.

### ¿Para qué usan la IA los ciberdelincuentes?

- ♦ **Mejora de código malicioso:** los creadores de *malware* utilizan plataformas IA, como puede ser ChatGPT para acelerar la creación de su código, solicitando funcionalidades específicas que luego integran en sus códigos maliciosos.
- ♦ **Generación de spam, phishing u otras amenazas:** los ciberdelincuentes la utilizan para generar correos electrónicos de *spam*, *phishing*, mensajes SMS de *smishing*, etc. aprovechando su capacidad para crear texto creíble en varios idiomas. La IA también puede generar anuncios que promocionan productos falsos o servicios fraudulentos.
- ♦ **Desinformación:** la facilidad para generar contenido de distinta tipología (texto, imagen, vídeos y audio) por parte de los sistemas IA es aprovechada para la creación de contenido falso para su posterior distribución.
  - ♦ **Fake news:** las noticias falsas son artículos o informes creados para engañar, a menudo diseñados para parecer que provienen de fuentes legítimas. Las IA pueden generar textos coherentes y persuasivos que imitan el estilo de los periodistas profesionales, lo que dificulta distinguir la verdad de la ficción.
  - ♦ **Deepfakes:** son un tipo avanzado de contenido falso que emplea técnicas complejas para crear vídeos y audios en los que personas reales parecen decir o hacer cosas que nunca ocurrieron. Esta tecnología puede ser utilizada tanto para entretenimiento como para actividades maliciosas, y su realismo puede hacer que sea extremadamente difícil identificar la falsificación sin herramientas especializadas. Los *deepfakes* se dividen principalmente en dos categorías:
    - ♦ **Deepfaces:** son vídeos en los que los rostros de las personas han sido alterados digitalmente para que parezcan otros. Esta tecnología puede ser usada para crear vídeos falsos de políticos, celebridades, o cualquier individuo, haciendo que parezca que dicen o hacen cosas que no se ajustan a la realidad.
    - ♦ **Deep voices o voice hacking:** en este caso, son manipulaciones de audio donde la voz de una persona es clonada y utilizada para generar discursos o declaraciones falsas. Esto puede ser especialmente peligroso cuando se utiliza para falsificar declaraciones de políticos, artistas, periodistas o cualquier otra persona con reconocimiento y repercusión pública.
- ♦ **Evasión de censura:** a pesar de que muchos sistemas de IA están programados para no dar respuestas sobre temas ilegales o controvertidos, algunos usuarios buscan saltarse estas restricciones compartiendo métodos para liberar la versión de estos y usarlo sin limitaciones éticas.
- ♦ **Creación de perfiles falsos:** la IA puede crear perfiles de usuario falsos en distintas plataformas (foros, redes sociales, aplicaciones de mensajería instantánea, etc.) que se utilizan para difundir mensajes maliciosos o que intentan recopilar datos personales o bancarios a través de interacciones con otros usuarios. Algunos ejemplos:
  - ♦ **Estafas de citas en línea:** los estafadores utilizan chatbots para crear perfiles falsos en aplicaciones de citas y engañar a los usuarios para que proporcionen dinero o información personal.
  - ♦ **Manipulación de opiniones y reseñas:** los chatbots pueden publicar reseñas falsas o manipuladas en sitios web y redes sociales, influyendo en la opinión que pueden tener los usuarios de un producto o servicio.
  - ♦ **Fraude de soporte técnico:** los ciberdelincuentes crean chatbots que se hacen pasar por agentes de soporte técnico reales e intentan engañar a los usuarios para que proporcionen acceso remoto a sus dispositivos o información personal.

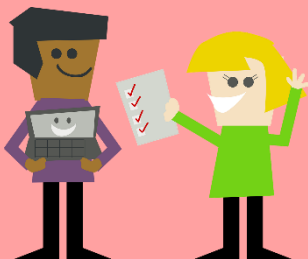
### Pistas para identificar contenido falso generado por IA

1. **Verifica la fuente:** asegúrate de que el contenido proviene de una fuente confiable o con buena reputación. Desconfía de las noticias de sitios web o perfiles desconocidos para ti. Consulta su reputación y comprueba si otros medios o usuarios confiables se hacen eco de la misma información.
2. **Analiza la calidad del contenido:** presta atención a ciertos detalles para desenmascararlos en función del tipo de contenido:
  1. **Texto:**
    1. **Coherencia y gramática:** verifica si el texto tiene errores gramaticales o incoherencias que no son comunes en artículos escritos por humanos.
  2. **Vídeo:**
    1. **Parpadeos y movimientos faciales:** los *deepfakes* a menudo presentan un número anormal de parpadeos o movimientos faciales poco naturales.
    2. **Incongruencias entre el rostro y el cuerpo:** observa si hay desajustes entre la expresión facial y los movimientos corporales.
    3. **Calidad del sonido:** el sonido puede no concordar con la imagen, mostrando desfases o variaciones en el tono que no corresponden con la escena.
  3. **Audio:**
    1. **Tono y ritmo:** analiza si el tono de voz y el ritmo del habla son consistentes. Las clonaciones de voz pueden presentar variaciones inusuales.
    2. **Ruido de fondo:** la falta de ruido de fondo o la presencia de sonidos extraños puede indicar manipulación.
    3. **Contexto del discurso:** verifica si el contenido del discurso es consistente con lo que la persona normalmente diría o en el contexto en el que suele hablar.
  4. **Imagen:**
    1. **Detalles finos:** pueden tener fallos en ciertos detalles, como manos con dedos desproporcionados o fondos que no se alinean correctamente.
    2. **Iluminación y sombras:** revisa si la iluminación y las sombras son coherentes en toda la imagen.

## EL POST-IT

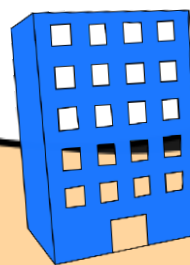
### Uso de las aplicaciones y sistemas

[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.



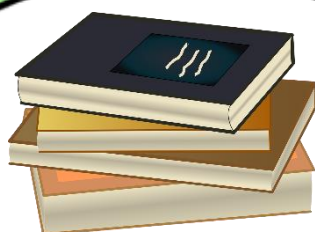
Se utilizarán exclusivamente las aplicaciones y sistemas que les haya habilitado la Administración de la Junta, para el desempeño de sus funciones.

Las aplicaciones y sistemas podrán pertenecer a otras Administraciones Públicas u otras entidades.



Se deberán cerrar las sesiones al finalizar el uso de la aplicación. Se recomienda utilizar las funcionalidades dispuestas para ello en la misma («desconexión», «cerrar sesión», «salir» o similar) y no simplemente cerrando la ventana de trabajo.

Se atenderá a las guías, instrucciones y manuales establecidos para el uso de las aplicaciones y sistemas.



Se seguirán los protocolos y mecanismos establecidos para gestionar incidencias y solicitudes de permisos.



## LA PELÍCULA



### DÉJAME ENTRAR

¡¡NO!!

No compartas nunca, ni dejes entrar a nadie con tu contraseña en tu ordenador y en ninguna aplicación en la que estés dado de alta, sobre todo en las redes sociales.

Refuerza las medidas de seguridad y asegúrate de tener claves robustas para todos tus accesos.



**Revisa**



**Cambia**



**Comprueba**



**Actúa**

### 01. Revisa

Revisa tu puesto de trabajo de forma habitual y asegúrate de que todo está correctamente.

### 02. Cambia

Cambia la contraseña. Es importante que cambies la contraseña con cierta frecuencia, y elige cada vez una totalmente distinta para que sólo la conozcas tú.

### 03. Comprueba

Comprueba que la información ubicada en el equipo informático que te ha sido asignado no ha sido modificada, eliminada o movida. Que las aplicaciones se encuentran en correcto funcionamiento, y que no han aparecido aplicaciones nuevas que hayan sido instaladas sin tu conocimiento, a menos que sean provistas por la Consejería.

### 04. Actúa

Ante cualquier duda sobre una posible modificación de todo lo expuesto anteriormente, notifícalo al CAU de tu Consejería.

## CONTRAPORTADA

### ¿Te han pedido alguna votación por WhatsApp? ¡Mucho ojo!

“Mi hija está participando en una competición del cole. ¿Puedes votarla?”. Detrás de lo que parece un inofensivo mensaje, puede esconderse un intento de smishing. El engaño está en que los ciberdelincuentes crean sitios web falsos, y piden que para votar te verifiques por WhatsApp. [Aquí tienes más info.](#)



### El Ministerio de Sanidad no está solicitando la renovación de tu tarjeta sanitaria

Se ha identificado una campaña fraudulenta de correos electrónicos y mensajes de texto que comunica a las víctimas la sustitución obligatoria de la Tarjeta Sanitaria Individual (TSI), con motivo de la implantación de un nuevo sistema de verificación. Para más información, pulsa [aquí](#).



### Campaña de phishing haciéndose pasar por Endesa

INCIBE ha comunicado la detección de una nueva campaña de phishing que intenta suplantar a la compañía energética Endesa. A través de un correo electrónico con una supuesta factura adjunta, los ciberdelincuentes buscan que la descargues para instalar software malicioso en tu equipo. [¡Infórmate bien aquí!](#)



### Magis TV, el 'Netflix pirata', podría espiar tus dispositivos y abrir la puerta al robo de datos

Magis TV, ahora conocida como Flujo TV, es uno de los servicios de IPTV pirata más conocidos y usados en el mundo. Sin embargo, tiene un gran lado oscuro que deberías conocer. [Más info.](#)



¿Has observado un comportamiento digital sospechoso? ¿Estás recibiendo intentos de phishing?  
¿Has sufrido un incidente de seguridad? ¡Notifícalo de inmediato por correo o teléfono!

[incidentes.soc@juntadeandalucia.es](mailto:incidentes.soc@juntadeandalucia.es) / 955 060 974 (Corporativo 360974)