

TITULARES

Cómo proteger la red WiFi de tu casa y navegar con tranquilidad

Vivimos rodeados de tecnología, en cualquier casa tenemos: móviles, ordenadores, televisores, altavoces inteligentes, cámaras de seguridad, consolas... Todos estos dispositivos tienen algo en común: dependen de tu red WiFi.

[Pág. 2](#)**¿Estás preparado para un posible desastre? Cómo las copias de seguridad en la nube pueden salvar tus datos**

En la actualidad disponemos de varios servicios de almacenamiento en la nube, en los que podemos hacer copias de seguridad con la ventaja de tener acceso a esos datos cuando y donde queramos, desde cualquier dispositivo, con el único requisito de disponer de conexión a Internet.

[Pág. 3](#)**AlertCops, la app de la Policía y la Guardia Civil**

Se trata de un servicio gratuito que nos permite mandar avisos, incluso geolocalizados, con fotografías o audios, a los agentes de la Policía Nacional y Guardia Civil.

[Pág. 4](#)

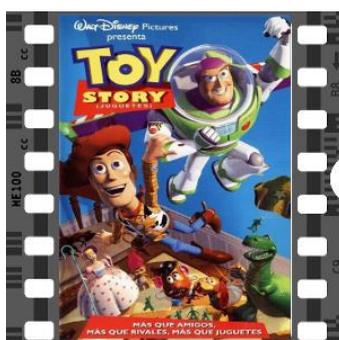
Como cada año, el 17 de mayo se celebró el **#DíaDeInternet**. El tema elegido para la edición de 2025 fue **"Por una nueva generación de Internet comprometida con las personas"**, con el objetivo de transformar Internet en un espacio más seguro, accesible, sostenible y respetuoso con los derechos.

Desde [incibe](#) se organizó un [taller](#) con el objetivo de aprender a tomar decisiones inteligentes frente al ciberacoso, los contenidos perjudiciales o los retos virales, a través de diversos casos que les hacen decidir y aprender las consecuencias asociadas.

EI POST-IT



LA PELÍCULA



CONTRAPORTADA

Cada día, hay 2,3 millones de ciberataques nuevos 

Ataque al becario: así es el nuevo timo que engaña a estudiantes recién contratados 

Datos que nunca deberíamos compartir con una IA 

El nuevo DNI digital: lo que puedes hacer con él y lo que no 

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

TITULARES

Cómo proteger la red WiFi de tu casa y navegar con tranquilidad

Cuando hablamos de seguridad digital solemos pensar en antivirus, contraseñas o fraudes por correo electrónico. Pero la red WiFi de casa es un elemento crítico que muchas veces pasamos por alto. ¿Por qué? Porque todos tus dispositivos se conectan a través de ella.

Si alguien consigue acceder a tu red, puede interceptar comunicaciones, acceder a tus archivos o incluso controlar dispositivos inteligentes. En algunos casos, sin que te des cuenta.

La red de casa es como la puerta de entrada al mundo digital de tu familia. Y como cualquier puerta, merece cerradura y vigilancia.

Hay medidas sencillas pero muy eficaces que puedes aplicar tú mismo

- Cambia la contraseña del router y el nombre de la red.
- Asegúrate de usar cifrado WPA2 o WPA3.
- Actualiza el firmware del router.
- Revisa qué dispositivos están conectados.
- Crea una red WiFi para invitados.
- Refuerza la seguridad de tus dispositivos cuando navegues por Internet.



Cómo proteger tu red WiFi (Vídeo)

Vídeo con consejos sobre cómo proteger tu red WiFi para garantizar la privacidad, la confidencialidad y seguridad de tus datos. Además, informa sobre los riesgos y consecuencias de no llevar a cabo dichas medidas.

¿Estás preparado para un posible desastre? Cómo las copias de seguridad en la nube pueden salvar tus datos

Ventajas

DE USAR LA NUBE

- 1 Es un **método de almacenamiento de información** en línea que te facilita acceder a tus archivos desde cualquier lugar y dispositivo con conexión a internet.
- 2 Te permite realizar **copias de seguridad** de la información de manera automática, sin tenerte que preocupar de hacerlo manualmente.
- 3 Almacena la información en sus **servidores** de manera cifrada, para que esté **más segura** y solo tú puedas saber que contienen los archivos.
- 4 Es **escalable** y puede crecer junto a tus necesidades de almacenamiento.
- 5 Evita tener que disponer de dispositivos de almacenamiento externos como **discos duros** o **USB**.
- 6 Facilita las **tareas de mantenimiento**, preocupándote solo de actualizar la aplicación a través de la que accedes a tu información.

Y si no haces copias en la nube

¿Qué puede pasar?

- 404 Pérdida de datos**
 Si el dispositivo que contiene se **estropea** o da algún fallo.
- Seguridad Física**
 Los datos pueden ser robados si el dispositivo con las copias **cae en malas manos**.
- Costes adicionales**
 El **almacenamiento y mantenimiento** de los datos en distintos soportes pueden resultar más elevados.
- Dificultad de acceso**
 Si no estás **físicamente** presente en la ubicación donde se guardan los datos, no podrías consultarlos.

Qué comprobaciones

de un servicio realizar antes de usarlo

- Seguridad y privacidad**
 Asegúrate de que el proveedor de servicios en la nube tenga **medidas sólidas de seguridad**, como cifrado de datos o autenticación de dos factores, para salvaguardar tus datos personales.
- Almacenamiento y capacidad**
 Comprueba que ofrezca **suficiente almacenamiento y capacidad** para tus necesidades actuales y futuras.
- Precios**
 Compara los **planes de precios** ofrecidos por diferentes proveedores. Ten en cuenta los costes mensuales o anuales, así como cualquier otro importe adicional que pueda aplicarse.
- Experiencia del usuario y facilidad de uso**
 Asegúrate que puedas utilizar el servicio de **manera sencilla y eficiente**. Considera la interfaz de usuario, la facilidad de configuración, la capacidad de compartir y gestionar archivos.
- Soporte técnico y servicio al cliente**
 Revisa si el proveedor ofrece un **buen servicio de atención al cliente**, incluyendo opciones de contacto y tiempos de respuesta en caso de que encuentres problemas o te surjan dudas.
- Políticas de privacidad**
 Dedica el tiempo que sea necesario para entender **cómo la empresa trata los datos de los usuarios**. Por ejemplo, si los almacena cifrados, si los comparte con terceros, etc.
- Reputación y comentarios**
Investiga a la empresa y **busca comentarios** de otros usuarios para conocer sus experiencias y opiniones sobre la misma.

Cómo acceder a las principales plataformas

Sigue los siguientes pasos para localizar el servicio

1



Google Drive

Accede a través de este enlace:
<https://www.google.com/drive>



Dropbox

Accede a través de este enlace:
<https://www.dropbox.com>



OneDrive

Accede a través de este enlace:
<https://www.onedrive.live.com>



iCloud

Accede a través de este enlace:
<https://www.icloud.com>

AlertCops, la app de la Policía y la Guardia Civil



¿QUÉ ES ALERTCOPS?
Una aplicación móvil gratuita que actúa como canal bidireccional entre el ciudadano y los cuerpos policiales

¿EN QUÉ CONSISTE?
Permite enviar desde tu smartphone una alerta de delito o situación de riesgo de la que estás siendo víctima o testigo, para ser atendido de manera rápida y eficiente

PASOS A SEGUIR TRAS LA DESCARGA DE ALERTCOPS

- 1** Regístrate como nuevo usuario facilitando tus datos y activando el GPS
- 2** Recibirás un SMS con un código de validación
- 3** Selecciona en el menú de iconos la alerta que quieres enviar
- 4** Responde a las preguntas que realiza el sistema mediante iconos antes de enviar la alerta. ¿Dónde ha sucedido? ¿A quién le ha sucedido?
- 5** Los cuerpos policiales pueden comunicarse contigo por Chat para obtener más información

MÁS INFORMACIÓN


¿Qué funciones tiene AlertCops?

Chat: Si eres víctima o testigo de un delito, contacta a través del chat, envía fotos y vídeos y obtendrás una respuesta inmediata.

Avisos localizados: Según la zona en la que nos encontremos, podremos recibir avisos de seguridad ciudadana para estar prevenido y colaborar con las fuerzas y cuerpos de seguridad del estado.

Guardián: Siempre que queramos podremos nombrar a contactos como «guardianes» y podremos compartir nuestra posición con ellos y/o en caso de ser necesario, con los servicios de rescate.

Botón SOS: Nos permite enviar un aviso inmediato a tus guardianes con nuestra ubicación y un audio de 10 segundos. Además, en caso de formar parte de un colectivo vulnerable, este botón avisa instantáneamente a las fuerzas policiales más cercanas para una atención urgente.

¿Dónde descargar la aplicación?

La aplicación se encuentra disponible de forma gratuita tanto en la [Google Play Store de Android](#), como en la [App Store de Apple](#).

Descárgate AlertCops, para tu seguridad



EL POST-IT

Conductas no permitidas

[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.



[EL redactor de un periódico, crea una "granja de enlaces" a la empresa de apuestas de su mujer.](#)

¿Y si instalo un programa malicioso?



[Consecuencias](#)



No está permitida la instalación, visualización, acceso o remisión de cualquier fichero o mensaje con contenidos de carácter racista, xenófobo, pornográfico, sexista, de apología del terrorismo, que atenten contra los derechos humanos o las libertades, o que actúen en perjuicio de los derechos a la intimidad, al honor, a la propia imagen o contra la dignidad de las personas.

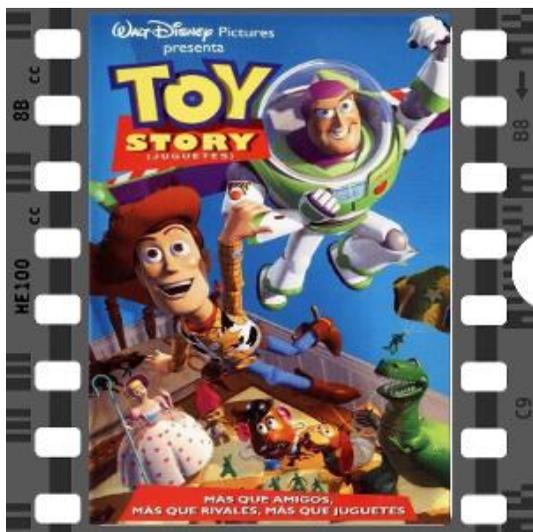
[Vigilante de seguridad, despedido por ver una famosa serie durante el trabajo.](#)



[Conoce los riesgos de grabar imágenes en tu entorno laboral sin autorización.](#)



LA PELÍCULA



TOY STORY

Existen juguetes infantiles con comunicaciones a Internet que pueden enviar vídeos, fotos, geolocalización y otra información sensible, sobre nuestros hijos, a desconocidos.

Debemos tener especial precaución con los juguetes que interactúan con otras personas a través de Internet.



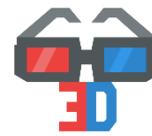
Cámaras



Voz



Menores



Desconocidos

01. Cámaras

Deshabilita las cámaras, así como las configuraciones de transmisión de contenido multimedia y geolocalización.

02. Voz

No permitas que reconozcan tu voz, evita tener siempre activado los micrófonos y comprueba donde se almacenan esas grabaciones.

03. Menores

Si es un menor, acompáñalo en el juego, así podrás supervisar las interacciones.

04. Desconocidos

Al navegar o comunicarte a través de Internet, evita la comunicación con desconocidos.

CONTRAPORTADA

Cada día, hay 2,3 millones de ciberataques nuevos

Veinte años atrás, los expertos en ciberseguridad centraban sus esfuerzos en ordenadores y poco más. Hoy el campo a vigilar se ha extendido exponencialmente y es casi imposible encontrar un dispositivo que no esté conectado a la red y que no sea vulnerable. Para más información, pulsa [aquí](#).



Ataque al becario: así es el nuevo timo que engaña a estudiantes recién contratados

Se trata de una variante del conocido fraude del CEO. Los ciberdelincuentes aprovechan ahora la inexperiencia de los jóvenes profesionales para realizar fraudes personalizados utilizando datos de redes sociales. Para más información, pulsa [aquí](#).



Datos que nunca deberíamos compartir con una IA

Debido a la multitud de funciones que posee y lo accesible que es para cualquier usuario, es muy numerosa la cantidad de información comprometida que esta tecnología capta alrededor del mundo. Para más información, pulsa [aquí](#).



El nuevo DNI digital: lo que puedes hacer con él y lo que no

El nuevo documento no sustituirá al físico, pero sí permitirá que los ciudadanos puedan identificarse a través de una aplicación móvil que actuará como su réplica virtual. Para más información, pulsa [aquí](#).

