

TITULARES

Geolocalización y privacidad en dispositivos móviles

Se trata de una función esencial en nuestros teléfonos móviles. Se utiliza para encontrar direcciones, localizar tiendas, conocer las condiciones climáticas en tiempo real, y mucho más. Sin embargo, la recopilación de estos datos también puede ser una amenaza para la privacidad del usuario. [Pág. 2](#)

Terminología de navegadores web

Los 10 términos relacionados con navegadores web que debes conocer. La próxima vez que estés navegando y te aparezca una notificación relacionada con ellos, ya sabrás que hacer. [Pág. 3](#)

Técnicas de ingeniería social: ¿Cómo consiguen engañarnos?

La ingeniería social es una técnica que se basa en la manipulación de las personas para conseguir que realicen alguna acción sin ser conscientes de que están siendo engañados. [Pág. 4](#)

Borra tu huella digital paso a paso

¿Eres consciente de que la imagen que proyectas en Internet está basada en gran medida en la información que publicas tú mismo? [Ver más.](#)



DE INTERÉS

Puesto de trabajo despejado

Utiliza los medios dispuestos por tu Consejería para custodiar los documentos en papel (armarios, cajones, estanterías, salas de archivo, etc.), especialmente cuando la información sea considerada confidencial o contenga datos personales.

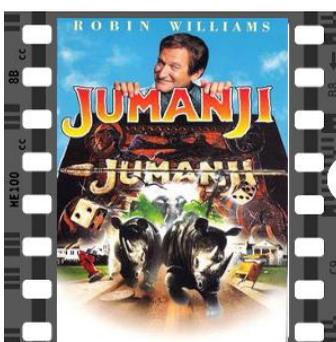


Y recuerda, no dejes post-it o similares pegados en la pantalla o por la mesa, sobre todo si contienen información delicada, como usuarios y contraseñas.

EI POST-IT



LA PELÍCULA



CONTRAPORTADA

Así es cómo conseguí darme cuenta de que había descargado sin querer un virus en mi ordenador.

Antivirus gratuitos en 2024: ¿Son realmente vitales o son innecesarios cuando te compras un PC?

Si tienes alguna de estas aplicaciones en tu móvil, mejor desinstalar: ponen en peligro tu seguridad y tienen virus.

"La regla de los cinco minutos", el sencillo hábito que recomiendan los expertos para evitar que hackeen tu móvil.

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

TITULARES

Geolocalización y privacidad en dispositivos móviles

La geolocalización es la capacidad de determinar la ubicación física de un dispositivo utilizando señales de GPS, Wi-Fi o torres de telefonía entre otros. Esta información se utiliza para proporcionar servicios basados en la ubicación como mapas, clima, redes sociales y publicidad dirigida. Además, la geolocalización también se utiliza en aplicaciones de seguridad y para la gestión de desplazamiento, así como para la localización de vehículos y paquetes.



¿Cómo afecta la geolocalización a la privacidad del usuario y sus dispositivos?

Los datos de geolocalización pueden utilizarse para crear perfiles detallados de los usuarios, incluyendo sus patrones de movimiento y comportamiento.

La recopilación de datos de geolocalización puede exponer la ubicación de un usuario a otras personas, incluyendo a posibles delincuentes.

La recopilación de datos de geolocalización puede afectar el rendimiento y la duración de la batería de los dispositivos móviles.

Los datos de geolocalización también pueden ser utilizados en combinación con otras informaciones para llevar a cabo actividades fraudulentas o de robo de identidad. Los delincuentes pueden utilizar los datos de geolocalización para rastrear patrones de comportamiento y ubicaciones frecuentes, lo que podría ayudarles a crear perfiles detallados y facilitar el acceso a información sensible a través de técnicas de ingeniería social.

En la actualidad, muchos dispositivos de nuestro día a día tienen la capacidad de compartir nuestra ubicación en tiempo real. Algunos de los dispositivos más comunes que comparten nuestra localización incluyen:

- Teléfonos móviles.
- Ordenadores portátiles y de escritorio.
- Smartwatches y wearables.
- Dispositivos de navegación para vehículos.
- Cámaras de seguridad.

¿Cómo se limitan los datos de geolocalización en diferentes dispositivos?

Las personas usuarias pueden limitar la recopilación de datos de geolocalización en diferentes dispositivos mediante diferentes métodos. En los dispositivos móviles, por ejemplo, los usuarios pueden desactivar la opción de compartir la ubicación en las configuraciones del dispositivo.

Deshabilitar la ubicación en un dispositivo móvil



Desactivar permisos de ubicación para una aplicación



Deshabilitar la ubicación exacta en un dispositivo móvil



Esta comunicación está destinada a los profesionales públicos de la Administración

incidentes.soc@juntadeandalucia.es

Terminología de navegadores web

HTTPS
Protocolo de seguridad que aplica medidas de cifrado para la transmisión segura de información entre tu dispositivo y el servidor de un servicio.

Notificaciones
Un sitio web, una aplicación o una extensión pueden enviarte avisos, mensajes o noticias a través de notificaciones.

Notificación: ¿Desea recibir notificaciones de este sitio? Saber más...
Permitir notificaciones No permitir

Toolbar
Barra de herramientas que aparece en la parte superior de tu navegador. Generalmente sirve para acceder de manera rápida a la configuración, favoritos, seguridad y privacidad.

Algunos virus pueden realizar modificaciones en la configuración de la toolbar creando un mal funcionamiento o redireccionando a sitios desconocidos y peligrosos.

Motor de búsqueda
Es un software cuya función es buscar contenidos a través de Internet.

Revisa bien los resultados de las búsquedas para no acabar accediendo a algún sitio web malicioso que aloje fraudes, malware o contenga informaciones falsas.

HTML
Es el principal lenguaje utilizado para crear y dar formato a las páginas web.

Un usuario malintencionado podría insertar fragmentos de código malicioso en una web para, por ejemplo, descargar malware en el dispositivo del usuario.

Historial navegación
Histórico de todas las páginas web que has visitado, así como de toda tu actividad online.

Si no quieres que esta información esté al alcance de terceros y pueda verse comprometida tu privacidad, bórralo periódicamente.

Cookie
Información que se intercambia entre tu navegador y una página web para identificarte y ofrecerte una experiencia de navegación personalizada.

Para que un sitio web no conozca tus hábitos de navegación, no las aceptes, especialmente si se trata de una página que no informa sobre el tratamiento que hará de tus datos.

Utilizamos cookies propias y de terceros para mejorar la experiencia del usuario a través de su navegación. Si continúas navegando, aceptas su uso. **Aceptar**

Pop ups
Son ventanas emergentes que aparecen de forma repentina durante la navegación y que generalmente muestran publicidad.

Pueden estar vinculados a webs fraudulentas o contener información falsa.

Addons
Son extensiones, complementos y plugins que añaden funcionalidades extra al navegador.

Existen versiones maliciosas que buscan controlar tu equipo o robar tu información.

Caché
Almacena la información de las webs que visitas para reducir el tiempo de carga.

Puede llegar a ocupar demasiado espacio en tu equipo, por lo que se recomienda borrarlo eventualmente.

DESCUENTO 50% COMPRAR

220 Mb/s

Ahora ya conoces un poco mejor los términos y elementos que rodean a los navegadores web

La próxima vez que estés navegando y te aparezca alguna notificación relacionada con ellos, sabrás qué hacer con ellas.

EL POST-IT

Almacenamiento y formato de la información

[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.

[La AEPD prohíbe en una reciente resolución que la policía fotografíe DNIs con móviles personales y sean subidos a la nube.](#)



[Un funcionario pierde un USB con información de 500.000 ciudadanos tras salir de fiesta.](#)



[Roban todo el material informático de las oficinas de Empleo de Pinos Puente \(Granada\)](#)



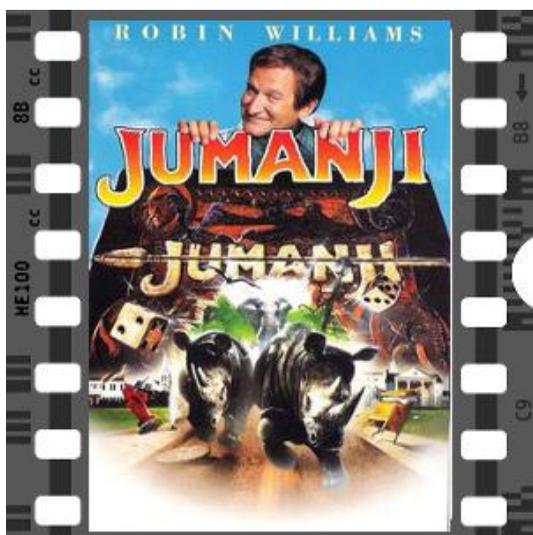
[Acceso y reutilización de la información pública.](#)



[Accesibilidad de los contenidos a publicar en los sitios web de la Junta de Andalucía.](#)



LA PELÍCULA



JUMANJI

Los correos no solicitados con archivos adjuntos pueden conllevar un gran riesgo, si se ejecutan podríamos ser víctimas de algún tipo de software malicioso.

Ejecutar archivos adjuntos de correos no solicitados puede ser tan peligroso como iniciar una partida en el encantado juego de... "Jumanji".

Te verás atrapado en un sinfín de aventuras no deseadas hasta terminar la partida.



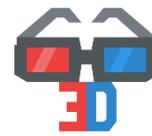
Analiza



Desconfía



Elude



Evita

01. Analiza

Utiliza un antivirus actualizado y analiza el adjunto antes de abrirlo.

02. Desconfía

Desconfía del adjunto aunque aparente ser inofensivo. También los amigos pueden enviarnos malware si han sido infectados.

03. Elude

No descargues ni abras nunca los archivos adjuntos que llegan en correos no solicitados de desconocidos.

04. Evita

Algunos correos no contienen el adjunto, sino un enlace que nos lleva a su descarga. No accedas nunca en estos enlaces.

CONTRAPORTADA

Así es cómo conseguí darme cuenta de que había descargado sin querer un virus en mi ordenador

Hay varios métodos para darte cuenta de si has descargado un virus sin querer, pero actuar de inmediato te ayudará a proteger tu dispositivo y tu información personal. Para más información, pulsa [aquí](#).



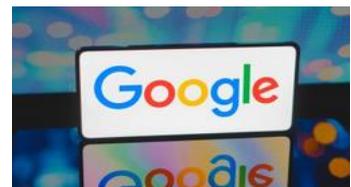
Antivirus gratuitos en 2024: ¿Son realmente vitales o son innecesarios cuando te compras un PC?

A medida que los ciberataques se vuelven más complicados de detectar y resolver, la necesidad o no de un antivirus no para de ser una gran duda. Para más información, pulsa [aquí](#).



Si tienes alguna de estas aplicaciones en tu móvil, mejor desinstalar: controlan tus movimientos, ponen en peligro tu seguridad y tienen virus

Google ha tomado medidas tras descubrir que más de 30 extensiones de su navegador Chrome estaban comprometidas. Para más información, pulsa [aquí](#).



"La regla de los cinco minutos", el sencillo hábito que recomiendan los expertos para evitar que hackeen tu móvil

Reiniciar el móvil todos los días durante unos pocos minutos puede ayudar a la seguridad de tu móvil, incluso la agencia de seguridad de EE.UU. lo recomienda. Para más información, pulsa [aquí](#).

