



# WhatsApp

## Guía de la campaña de concienciación



**Unión Europea**

Fondo Europeo de Desarrollo Regional  
*Una manera de hacer Europa*

## Sobre CSIRT-CV

**CSIRT-CV** es el Centro de Seguridad TIC de la Comunitat Valenciana. Nace en junio del año 2007, como una apuesta de la **Generalitat Valenciana** por la seguridad en la red. Fue una iniciativa pionera al ser el primer centro de estas características que se creó en España para un ámbito autonómico.

Está formado por un equipo multidisciplinar de personal técnico especializado en los distintos ámbitos de la seguridad y dedicado a desarrollar medidas preventivas y reactivas para mitigar los incidentes de seguridad en sistemas de información dentro del ámbito de la Comunidad Valenciana, que abarca tanto la Administración Pública, como PYMES y ciudadanos.

CSIRT-CV ha certificado su Sistema de Gestión de Seguridad de la Información con AENOR según la norma UNE-ISO/IEC 27001:2014 cuyo alcance son los sistemas de información que dan soporte a los servicios prestados a la Generalitat Valenciana, otras Administraciones Públicas, Ciudadanos y Pymes de la Comunidad Valenciana, para la prevención, detección y respuesta ante incidentes de seguridad en las TIC's.



## Datos de contacto

CSIRT-CV Centro de Seguridad TIC de la Comunitat Valenciana

<http://www.csirtcv.gva.es/>

<https://www.facebook.com/csirtcv>

<https://twitter.com/csirtcv>

## Licencia de uso

Este documento es de dominio público bajo licencia Creative Commons Reconocimiento – NoComercial – CompartirIgual (by-nc-sa): No se permite un uso comercial de la obra original ni de las posibles obras derivadas, la distribución de las cuales se debe hacer con una licencia igual a la que regula la obra original.



# Índice de contenido

1.	Acerca de WhatsApp .....	4
2.	Campaña en el Facebook de CSIRT-CV .....	5
3.	Consejos de seguridad .....	6
4.	Curiosidades .....	16
5.	Novedades .....	19
5.1.	Llamadas WhatsApp .....	19
5.2.	Doble check azul.....	20
5.3.	WhatsApp Web .....	22
5.4.	Listas de difusión .....	23
5.5.	Bloqueo de usuarios .....	25
6.	Conclusiones.....	27

## 1. Acerca de WhatsApp

[WhatsApp](#) es una aplicación de mensajería multiplataforma que permite enviar y recibir mensajes mediante Internet sustituyendo a los servicios tradicionales de mensajes cortos o sistemas de mensajería multimedia. Desde mediados de 2015 se incluye una nueva funcionalidad: Llamada WhatsApp.

La aplicación apareció en el mercado en el año 2009 y el hecho de ser una de las aplicaciones más descargadas en 16 países hace que esté en el punto de mira de ciberatacantes, que persiguen obtener todo tipo de información de los usuarios.

Esta aplicación para móviles no es una red social del estilo de Twitter o Facebook, ya que sus funcionalidades se limitan a conversar con otros usuarios o grupos, y enviarse entre ellos un número ilimitado de imágenes, vídeos y mensajes de audio.

La aplicación está disponible para los sistemas operativos Windows Phone, iOS, BlackBerry OS, Android, y algunos de los dispositivos que utilizan Symbian de Nokia.

No existen versiones para Windows, Mac o Linux pero sí emuladores de Android que permiten el uso de WhatsApp en Windows, Mac o navegadores web. Aunque últimamente están apareciendo versiones como WhatsApp Web para PC, actualmente no existe forma oficial de instalar o descargar WhatsApp para PC como sustituto permanente a la aplicación móvil.

Más información de WhatsApp Web en el apartado de "[Novedades](#)".

## 2. Campaña en el Facebook de CSIRT-CV

WhatsApp es la utilidad preferida entre la mayoría de usuarios principalmente por su facilidad de uso y su sistema multiplataforma.

No obstante hay cuestiones mejorables en cuanto a seguridad, además de existir pequeños trucos que permiten un funcionamiento más eficaz. Desde CSIRT-CV se realizó una **campaña de concienciación**, en 2013, a través de nuestras redes sociales con el nombre *“WhatsApp... todo lo que realmente hay que saber”*.

Si se desea acceder a la campaña puede hacerlo a través de nuestra [cuenta de Facebook](#) y echar un vistazo a cada uno de los consejos y/o curiosidades, así como a las opiniones del resto de usuarios, participando en ellas. También encontrará el resumen que hemos realizado acerca de la misma en [nuestro portal](#).

La campaña estuvo formada por 12 consejos de seguridad/funcionalidad y 8 curiosidades de la aplicación. Un total de 20 recomendaciones a tener en cuenta para un mejor uso de esta aclamada herramienta.

Más información en [CSIRT-CV](#).

### 3. Consejos de seguridad

Vamos a ver con algo más de detalle cada uno de los consejos que formaron esta campaña de concienciación.

El primer consejo de esta campaña se publicó el 27 de febrero de 2013 y nos contaba como obtener información de los datos enviados por WhatsApp:

#### Consejo 1

Una opción poco conocida de esta aplicación es el control de todos los datos que se envían, como la cantidad de mensajes y estadísticas de uso.

Para conocer esta información ingresar en Menú > Ajustes > Cuenta > Uso de red.

Los datos que podremos ver son:

- El total de mensajes enviados y recibidos.
- Los bytes multimedia enviados y recibidos.
- Los bytes de mensajes enviados y recibidos.
- Llamadas WhatsApp salientes y entrantes.
- Los bytes de llamadas enviadas y recibidas.
- El total de bytes enviados y recibidos.

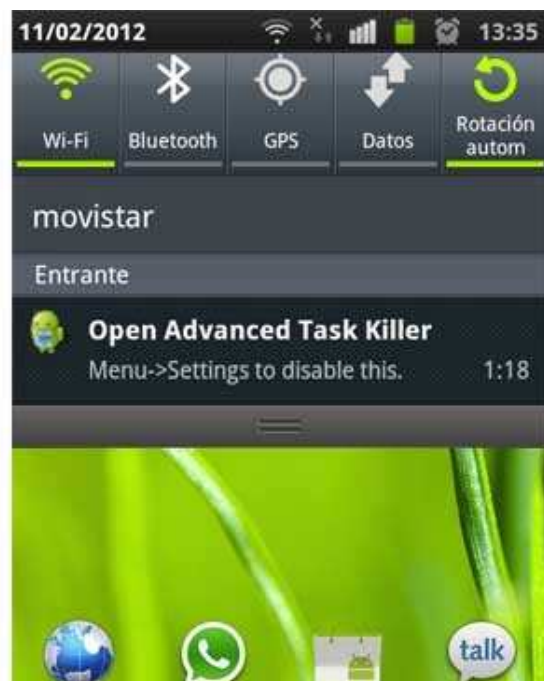
El segundo consejo describe el tipo de conexión que puede utilizar WhatsApp y ciertas precauciones a tener en cuenta:

## Consejo 2

WhatsApp es un sistema de mensajería instantáneo y gratuito gestionado a través de Internet. La conexión que utiliza puede consistir en una tarifa de datos contratada con una compañía (tarifas planas normalmente) o una conexión inalámbrica Wi-Fi. En cualquiera de los dos casos, los mensajes no aportan un gasto adicional.

Sin embargo, hay que conocer la cobertura que ofrece la compañía en las tarifas de datos, sobre todo si se va a viajar al extranjero, puesto que quizá los mensajes se cobren como datos descargados fuera de la factura.

La solución más sencilla es desactivar los paquetes de datos o la conexión por 3G del terminal, pudiendo utilizar la red Wi-Fi sin miedo a costes extras.



La novedad se presenta con las llamadas WhatsApp. Accede a este [apartado](#) para ampliar la información sobre posibles costes asociados.

Vamos a por el tercer consejo de la campaña: se publicó el 1 de marzo de 2013 y trata sobre los términos de privacidad de la aplicación:

### **Consejo 3**

Para utilizar esta aplicación es necesario registrar el número de teléfono. De esta forma, los mensajes llegarán al usuario correcto.

El servicio que ofrece se parece a los antiguos mensajes SMS y su manejo es sencillo incluso para los usuarios menos habituados a las nuevas tecnologías.

Existe una página web oficial donde se especifican, en inglés, todos los términos de privacidad de WhatsApp. En ella se explica que la aplicación registra una gran cantidad de datos de usuarios, aunque afirma que ninguno será vendido jamás.

Además, este consejo nos lleva a los [términos de privacidad](#) de WhatsApp.



El consejo no 4, o lo que es lo mismo, ¿qué debemos hacer si cambiamos de número de teléfono?

#### Consejo 4

¿Qué hacer si cambiamos de número de teléfono?

WhatsApp aconseja realizar estos 2 sencillos pasos:

1. Actualizar el estado de la cuenta con el nuevo número de teléfono.
2. Desinstalar la aplicación y reinstalarla después registrando el nuevo número.

El servidor deberá reconocer el cambio de números del usuario y mantener los datos.



Como curiosidad cabe mencionar que este consejo fue el más visitado de la campaña.

El consejo 5, o el caso del doble check, fue un consejo con una divertida situación que muchos habremos vivido. Venía acompañado de un vídeo:

### Consejo 5

Doble check: opción de WhatsApp con cierto nivel de polémica. Nos referimos a los 2 check que aparecen al enviar un mensaje (doble confirmación). Es un error bastante común pensar que esos 2 iconos confirman la lectura del mensaje enviado.

Cuando enviamos un mensaje y aparece el primer check, indica que el mensaje ha llegado al servidor. El segundo, confirma LA LLEGADA del mensaje desde el servidor al dispositivo del destinatario.

Por tanto, NO IMPLICA que la otra persona haya abierto y leído ese mensaje.

El siguiente [vídeo](#) muestra, en modo irónico, las situaciones y quebraderos de cabeza que puede generar este concepto :)

Un año después de nuestra campaña apareció una nueva variante: doble check azul. Más información en el [apartado de "Novedades"](#) de esta guía.

Llegamos a la mitad de las recomendaciones con...

### Consejo 6

¿Qué significan "últ. vez" y "en línea" exactamente?

"En línea" significa que la persona tiene WhatsApp abierto y está conectado. Para el iPhone, hay que tener en cuenta que alguien puede permanecer "en línea" hasta 5 minutos después de que haya cerrado la aplicación, o después de 5 minutos de inactividad en el iPhone.

"últ. vez..." se refiere a la última vez que alguien se conectó a WhatsApp. Lo que no quiere decir que aunque se hubiera conectado a WhatsApp leyera todos los mensajes que tuviera pendientes.

El consejo número 7 estaba dedicado a la seguridad de nuestros contenidos.  
No os lo perdáis:

### **Consejo 7**

Hoy vamos a explicar que hacer si perdemos o nos roban el móvil y, no se encuentra protegido.

En tal caso, cualquiera que tenga acceso al mismo se puede hacer pasar por nosotros en "conversaciones" con otros usuarios de WhatsApp.

Esto se denomina suplantación de identidad en caso de producirse de forma esporádica. Si la apropiación es continua, pasa a ser un robo de identidad.

En caso de robo, hay que denunciarlo a la policía y avisar a la operadora para que invaliden la tarjeta SIM (realmente se invalida el número de teléfono). Nos enviarán otra tarjeta con el mismo número y con ésta nos registraremos en WhatsApp de nuevo.

Como el número de teléfono es el mismo que teníamos, WhatsApp anula el registro anterior (el del móvil robado) y activa el nuevo.

De esta forma, volvemos a tener nuestra identidad de WhatsApp.

A pesar de todo, el ladrón habrá tenido acceso a nuestras conversaciones anteriores por lo que recomendamos no compartir información sensible en WhatsApp y no guardar el histórico de las conversaciones.

Por último, mencionar que incluso existen técnicas para recuperar mensajes borrados.

Tenéis más información al respecto en esta [página](#).

Consejo 8, o los problemas de conectarse a una red wifi pública:

### Consejo 8

Recomendamos no conectarse a una red Wi-Fi pública si se va a hablar por WhatsApp puesto que, algunas aplicaciones permiten transferir datos de una red inalámbrica hacia el smartphone donde está instalada.

Es decir, si estás usando la misma red Wi-Fi que quien tiene instalada esta aplicación, esta persona podría ver todas las conversaciones enviadas y recibidas, así como fotografías y/o vídeos.

Por ello repetimos la importancia que tiene no compartir información confidencial en WhatsApp.

Más información del nivel de seguridad de WhatsApp mediante el consejo 9:

### Consejo 9

Es muy fácil suplantar la identidad en WhatsApp; solo basta seguir unos sencillos pasos para que cualquiera se registre con un número de teléfono ficticio o el número de un amigo, familiar, ...

Por eso, como bien estamos repitiendo, no se aconseja enviar contenido que pueda dañar la reputación tanto personal como profesional.

Tampoco es aconsejable enviar datos bancarios o contraseñas. Ya conocéis la polémica ocasionada sobre si el sistema cifraba o no el contenido.

A pesar de todo, su nivel de seguridad sigue siendo bajo y con ciertos programas aún podrían obtenerse datos. Además los mensajes no se borran, ya que puedes eliminarlos del registro pero quedan guardados en una base de datos y nunca desaparecen.

Este consejo nos ofrece este [enlace](#) para más información.

Siguiendo con el tema de la seguridad en WhatsApp, vamos a comentar con más detalle la falta de ésta a la hora de darse de alta y comprobar que el usuario final es quien dice ser.

El proceso para darse de alta consiste en introducir un número de teléfono al que llegará un SMS con un código que debe ser introducido para demostrar la autenticación del usuario. Pero la realidad es que este PIN podría ser interceptado.

Lo que sucede realmente es que el código de activación se crea directamente en el entorno de la aplicación, antes de ser enviado a los servidores que mandan el SMS final. Así que, solo faltaría interceptar la petición HTTP(S) y averiguar el código de activación (de tres dígitos, por cierto) asociado al parámetro auth. Y el SMS de activación nunca llegaría al teléfono móvil; el atacante podría enviar a la aplicación una supuesta respuesta del servidor para fingir que el SMS se envió con éxito.

Ahora el intruso podría usar ese código en otro dispositivo móvil e interceptar una segunda petición que es la que secuestraría cualquier número de teléfono para ser asociado a su "Unique Device Identifier".

A partir de ese momento, se utilizará el número de teléfono y el UDID como usuario y contraseña, respectivamente.

Por tanto, cualquiera podría hacerse con la cuenta de otro usuario y, leer y mandar mensajes. Los mensajes de la propia aplicación también llegarían al intruso.

La víctima no se dará cuenta de todo esto hasta que intente conectarse a la aplicación; una vez que el mal ya está realizado.

Una sugerencia acerca del uso de este programa con el GPS del teléfono móvil es lo que describe el consejo número 10:

### Consejo 10

Si no quieres que sepan dónde estás y qué estás haciendo... no permitas que WhatsApp utilice el GPS del teléfono puesto que, el sistema guarda la localización desde la que se está enviando un mensaje y tu ubicación quedaría descubierta.

De esta forma, un intruso podría utilizar esta información confidencial para fines ilegales.

Aunque todo esto también puede tener su parte positiva, como bien narran las noticias siguientes:

[Noticia 1](#)

[Noticia 2](#)

Tenemos más información en este otro [enlace](#).

En el consejo 11 también hablamos de la adicción que puede crear el mal uso de esta aplicación:

### Consejo 11

El uso indebido de esta aplicación, WhatsApp, podría ser peligroso ya que crea adicción en algunas personas y deja rastros difíciles de controlar y borrar.

La aplicación móvil podría provocar conflictos (amorosos, entre amigos,...) si los usuarios lo utilizasen de forma irracional y como una herramienta de control. Entre el 5% y el 9% realiza un uso inadecuado de esta herramienta.

Os mostramos más información en este [enlace](#).

Y para finalizar la parte de los consejos, os dejamos un enlace sobre un exploit de esta aplicación:

### **Consejo 12**

Os dejamos un interesante vídeo acerca de esta aplicación...

[Vídeo](#)

## 4. Curiosidades

El 15 de marzo de 2013 se publicó la primera curiosidad acerca de WhatsApp en nuestra campaña de concienciación.

El objetivo de estas curiosidades era dar a conocer de una manera simple y atractiva para los usuarios, la cronología con los hitos más importantes de esta aplicación.

A continuación mostramos un resumen de esta sección de la campaña:

### Curiosidad 1

En mayo de 2011... se informó de un agujero de seguridad en WhatsApp que dejó las cuentas de los usuarios expuestas a robo. Según algunas fuentes, se cree que esta modificación fue realizada, y más tarde reparada, gracias a Liroy van Hoewijk, directivo de CoreISP.net que ayudó a WhatsApp a reproducirla en Android y Symbian.

### Curiosidad 2

Desde mayo de de 2011... se está informando de que las comunicaciones mediante WhatsApp no están cifradas y los datos se reciben en texto plano, lo que significa que los mensajes pueden leerse fácilmente si se dispone de los paquetes enviados.

En mayo de 2012 los investigadores de seguridad dijeron que las nuevas actualizaciones de WhatsApp ya no enviaban los mensajes en texto plano.



### Curiosidad 3

Septiembre de 2011: aparece una nueva versión de la aplicación WhatsApp Messenger para iPhones.

En esta nueva versión, los desarrolladores resuelven algunos agujeros críticos de seguridad que permitían enviar mensajes falsos y que, los mensajes enviados desde cualquier usuario de WhatsApp se pudieran leer.

La siguiente curiosidad fue una de las que más visitas obtuvieron:

### Curiosidad 4

El 6 de enero de 2012 un hacker desconocido publicó un sitio de internet (WhatsAppStatus.net) que permitía cambiar el estatus de cualquier usuario de WhatsApp del que se supiera el número de teléfono.

Solamente había que reiniciar la aplicación para que funcionase. Según el hacker este era sólo uno de los asuntos preocupantes de la seguridad en WhatsApp.

Tres días después, WhatsApp informó de que había implementado una solución definitiva: bloquear la dirección IP del sitio. Esto provocó que una herramienta para Windows que, facilitaba la misma funcionalidad, se pusiese a disposición para su descarga.

Este problema parece no estar solucionado por ahora. La primera notificación del problema fue recibida por WhatsApp en septiembre de 2011.

### Curiosidad 5

La aplicación se retiró del iOS App Store el 13 de enero de 2012, sin razón aparente, y se volvió a incluir 4 días después.

### Curiosidad 6

Usando WhatsAPI, el blog alemán "*The H*" demostró cómo tomar cualquier cuenta de WhatsApp.

WhatsApp Inc. respondió con una amenaza legal a los desarrolladores de WhatsAPI, forzándolos a dar de baja el código fuente (14 de septiembre de 2012)

### Curiosidad 7

Y nos acercamos al año 2013... El 20 de diciembre de 2012 WhatsApp anuncia que la descarga de su aplicación podrá realizarse de manera gratuita para el sistema operativo iOS de Apple, modificando así su política de pago estándar de \$0.99 por el servicio para este sistema operativo.

Otra de las curiosidades más leídas fue la número 8:

### Curiosidad 8

28 de enero de 2013: Denuncian a WhatsApp por violar leyes de privacidad internacionales puesto que, obliga a los usuarios a proporcionar acceso a toda su libreta de direcciones (incluyendo tanto a los usuarios como a los no usuarios de la aplicación)

Con motivo de la actualización de esta guía en 2015, podríamos añadir las siguientes curiosidades:

- El 19 de febrero de 2014, Facebook anuncia la compra de WhatsApp.
- El 22 de febrero de 2014 la aplicación sufre unos fallos de servicio a nivel mundial. Fallos que se repetirían el 2 de abril y 25 de mayo del mismo año.
- Finales de 2014: WhatsApp añade el doble check azul.
- En 2015 se habilitan las llamadas de voz en la aplicación.

## 5. Novedades

### 5.1. Llamadas WhatsApp

Desde 2015 existe esta nueva función en WhatsApp. Permite realizar llamadas gratuitas a tus contactos de la aplicación, incluso si están en otro país. Está disponible para los usuarios de WhatsApp con Android, iPhone, Windows Phone y BlackBerry 10 que tengan la función activada. No permite hacer llamadas a números de servicios de emergencia.

Funciona con la conexión a internet de tu teléfono en vez de, con el plan de llamadas de tu operador de telefonía móvil. Por lo tanto, podrías recibir cargos por el uso de datos móviles, según la tarifa contratada. Hay que tener en cuenta que, a diferencia de las llamadas tradicionales, tanto el emisor como el receptor gastarán tarifa de datos, incluso con las llamadas perdidas. Se recomienda utilizar este servicio con una conexión Wi-Fi segura.

La tecnología utilizada se llama [VoIP](#) (Voz sobre IP), que convierte la voz en datos digitales para poder transmitirlos. Al ser un servicio dependiente de Internet, la calidad varía en función de la red. Cuidado porque no todas las tarifas incluyen llamadas IP.

Se recomienda no hacer caso de las aplicaciones fraudulentas que indican que hay que ejecutar un archivo, o instalar otra aplicación, para realizar llamadas por WhatsApp.

En Google Play se encontró una aplicación llamada "**Activar Llamadas WhatsApp**" y que realmente es una aplicación fraudulenta. Con la novedad del servicio, se pretende engañar a los usuarios para que se suscriban a servicios SMS Premium. Supuestamente, no se solicita ningún permiso al instalar pero si se pincha en el botón "Activar Llamadas", se redirecciona a un formulario que solicita nuestro número de teléfono. Si se continua con el proceso, nos habremos suscrito al servicio de tarificación especial, cuyo coste podría ascender a 40 euros mensuales. Estas famosas llamadas saldrían entonces un poco caras.



## 5.2. Doble check azul

Esta funcionalidad fue incorporada en WhatsApp en 2014. Ha sido la más polémica dado que permite conocer cuando un usuario ha leído los mensajes recibidos.

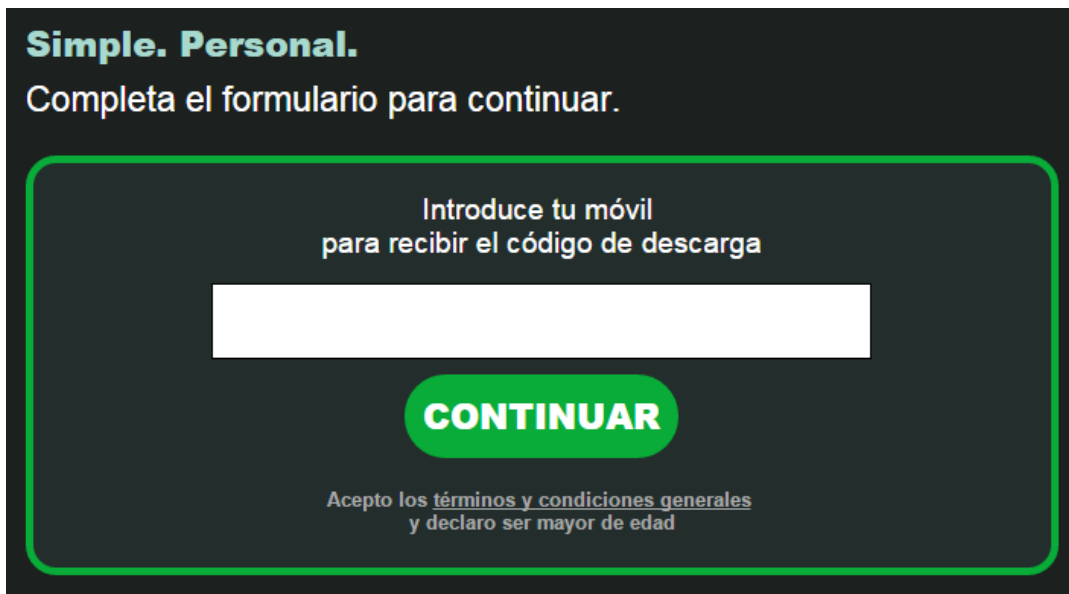
Inicialmente, el primer check indicaba el envío del mensaje y el segundo su recepción, que no su lectura. Ahora, cuando el doble check se vuelve azul, indica que el destinatario ha visto el mensaje.

Este nuevo sistema vulnera nuestra privacidad. Algo similar ocurrió al mostrar la hora de última conexión.

Actualmente, ambas opciones pueden desactivarse si contamos con una versión actualizada de la aplicación. Basta con acceder a los ajustes de WhatsApp y luego a Cuenta/Privacidad. Podrás desactivar las "Confirmaciones de lectura" y configurar el campo de "Hora de últ. vez" (debemos tener en cuenta que esta acción hará que tampoco nosotros sepamos si han leído nuestros mensajes, excepto en los chats de grupo, y la hora de última vez de los demás)

Al igual que en el caso anterior, con las llamadas de WhatsApp, cuando ésta funcionalidad surgió aparecieron bulos para engañar a los usuarios y conseguir que se suscribieran a servicios SMS Premium, con la esperanza de desactivar la opción del check azul.

Supuestamente, solo era necesario acceder a un enlace donde se solicitaba el número de móvil:



**Simple. Personal.**  
Completa el formulario para continuar.

Introduce tu móvil  
para recibir el código de descarga

**CONTINUAR**

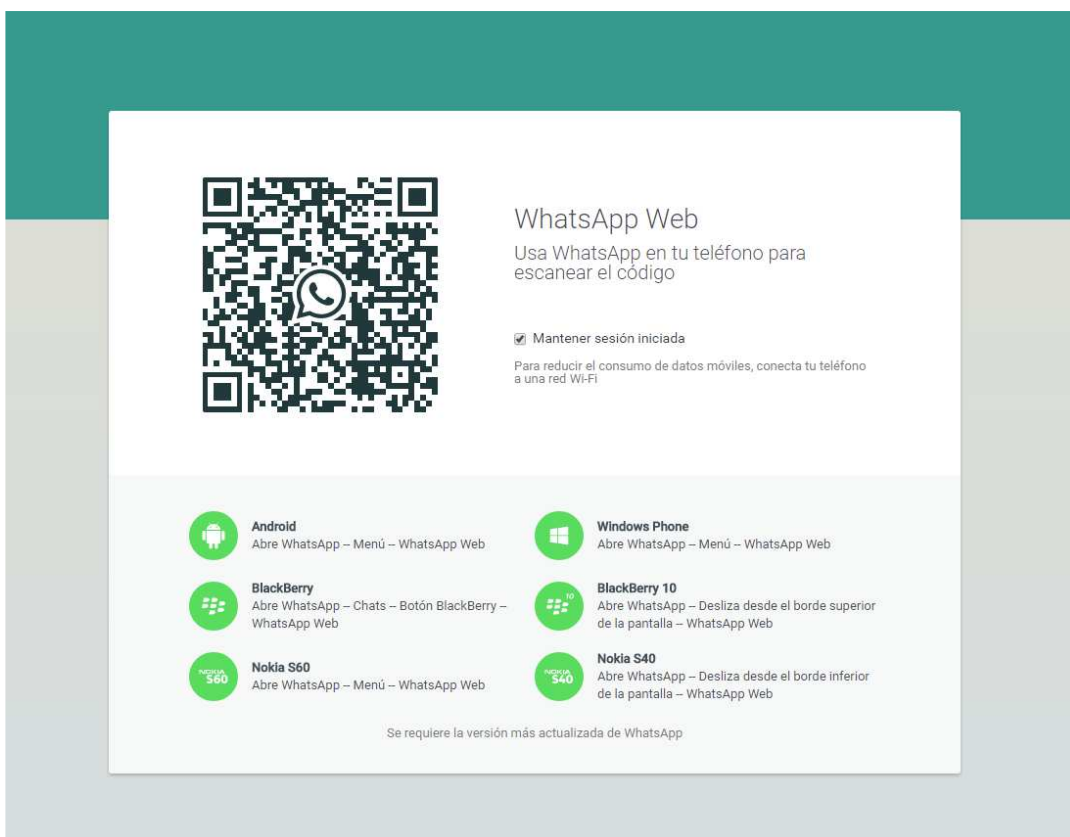
[Acepto los términos y condiciones generales](#)  
y declaro ser mayor de edad

Como siempre, se recomienda sospechar de aquellos servicios que nos soliciten el número de teléfono, ya que pueden estar asociados a servicios de pago. También debe contrastarse la información con la página oficial.

### 5.3. WhatsApp Web

Existe una nueva forma de utilizar esta mensajería instantánea; ahora también desde el ordenador.

Simplemente hay que acceder a la [página principal](#) desde un navegador del PC (Firefox, Chrome u Opera) y cuando aparezca la siguiente imagen, abre WhatsApp en tu móvil y accede al menú, a la opción "WhatsApp Web":



Escanea el código QR y la aplicación se abrirá en el ordenador, lista para usar, gratis. Esta opción no está actualmente disponible para usuarios de iPhone (julio 2015).

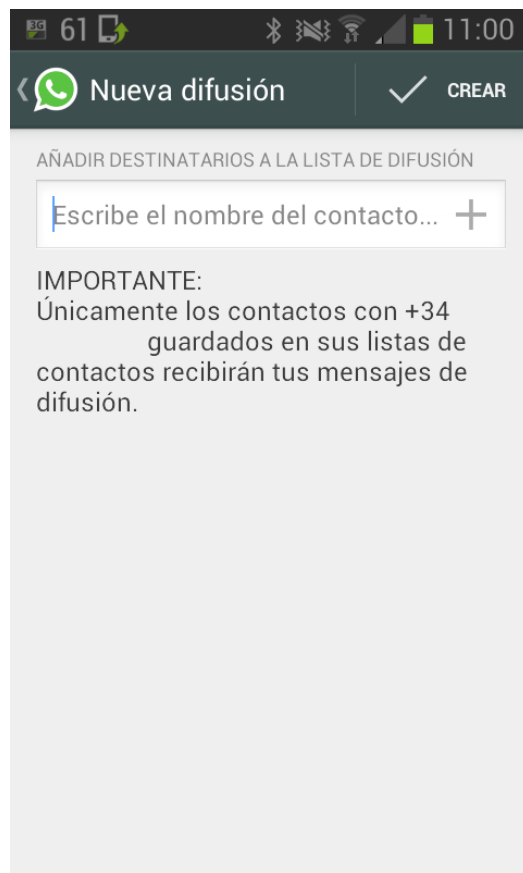
Realmente se trata de una extensión de WhatsApp; como una segunda pantalla. Verás lo mismo que en tu smartphone pero en mayor tamaño. Por tanto, es necesario que el móvil y su conexión a Internet permanezcan activos.

## **5.4. Listas de difusión**

Realmente es como enviar un mensaje a un grupo pero los destinatarios lo reciben de forma individual. El emisor si tiene forma de diferenciar que mensajes ha enviado como lista de difusión pero, los destinatarios pensarán que el mensaje recibido es personal, único y privado.

Las listas admiten más destinatarios que los grupos. Por otra parte, es más fácil saber si tu mensaje ha sido leído puesto que, en los grupos es más probable que algún contenido pase desapercibido y no se llegue a leer debido a la gran cantidad de envíos que pueden llegar a realizarse.

Para crear una lista de difusión pincha en Menú > Nueva difusión. Añade los contactos deseados escribiendo el nombre o seleccionándolos mediante el símbolo "+". Cuando crees la lista observarás que aparece un amplificador como imagen. Puedes cambiar el nombre de lista, añadir y borrar participantes.



Al emisor le aparecerá el símbolo del amplificador, al lado del doble check azul, para que sepa que el mensaje lo envió mediante una lista de difusión. Al receptor le aparecerá como un mensaje normal.

Cuando un participante responda, la respuesta no llegará al resto; solamente al emisor y como mensaje normal. Ésta es una de las principales diferencias entre grupo y lista de difusión. Si lo que se pretende es que haya comunicación entre todos los participantes, entonces se deberá crear un grupo y no una lista.

Una cosa a tener en cuenta es que los destinatarios de la lista de difusión deben tenerte como contacto registrado, sino no recibirán los mensajes de la lista.



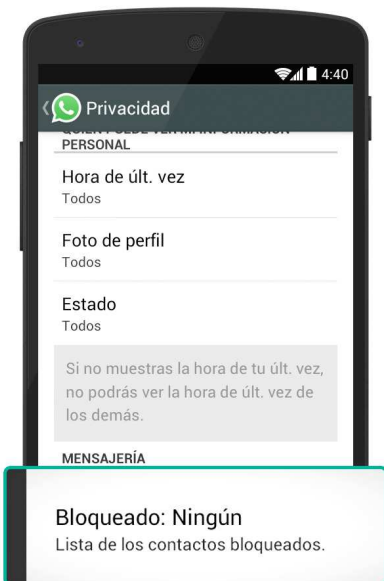
## 5.5. Bloqueo de usuarios

Si unimos las dos nuevas funcionalidades de los puntos [5.3](#) y [5.4](#) obtenemos que la aplicación puede utilizarse más fácilmente con WhatsApp Web y que, se puede enviar información a un gran número de contactos a la vez. ¿Estaremos ante una nueva variante de SPAM?

WhatsApp ofrece la posibilidad de bloquear contactos. Para ello solamente hay que acceder a la conversación privada del contacto a bloquear y, pinchar en Menú > Más > Bloquear.

Para consultar que contactos tienes bloqueados dirígete a la pestaña de Chats y luego pincha en Menú > Ajustes > Cuenta > Privacidad > Bloqueado.

Otra forma de bloquear a un contacto es pulsando en el icono que encontraremos en esa misma pantalla, en la esquina superior derecha (*"Agregar contactos bloqueados"*).



De esta forma, dejarás de recibir llamadas y mensajes del contacto bloqueado. Éste tampoco podrá ver si estas en línea ni la última vez que te conectaste. Tampoco verá los cambios que realices de tu estado y foto de perfil. Obviamente, tampoco tú podrás mandarle mensajes.

El usuario bloqueado podría enterarse de su estado por alguna de estas razones:

- No podrá llamarte por WhatsApp.
- Los mensajes que te envíe se marcarán con un solo tick (palomita) puesto que nunca te llegarán.
- No verá las actualizaciones de tu perfil.
- Tampoco verá la hora de tu última conexión. Aunque esto también podría ocurrir si esta opción la hemos configurado así. Más información en el [punto 5.2](#) de esta guía.

Para desbloquear debes mantener presionado el nombre del contacto en la pantalla de "Contactos bloqueados" y luego, selecciona "Desbloquear". Si desbloqueas a un contacto, no recibirás los mensajes que te haya enviado durante el bloqueo.

También puedes bloquear y denunciar como spam si recibes mensajes de un desconocido.

## 6. Conclusiones

La campaña “WhatsApp... todo lo que realmente hay que saber” finalizó el 28 de marzo de 2013, un mes después de su comienzo.

Sigue estando disponible en nuestras redes sociales para que continuéis visitándola y aprendiendo más cosas acerca de sus consejos.

Además del contenido que forma esta campaña, disponéis de otras noticias acerca de esta aplicación en nuestras redes sociales, a través del contenido que diariamente vamos actualizando.

Por otra parte, existe un [resumen](#) de esta campaña y de cada una de las anteriores que hemos realizado en nuestro portal de [CSIRT-CV](#).

Este documento ha sido una breve guía de utilización segura de WhatsApp y un repaso a nuestra campaña. Desde CSIRT-CV se recomienda utilizar esta aplicación evitando intercambiar datos e información que podrían dañar nuestra reputación.

Como acostumbra a ser frecuente con todos los servicios de Internet, cualquier medida de seguridad o curso de formación no sirve de nada si el usuario no actúa con sentido común.

Antes de utilizar un servicio es recomendable familiarizarse con él y aplicar las normas básicas de seguridad comunes a cualquier aplicación online. Estas recomendaciones deben siempre aplicarse de forma proporcional a lo privado y confidencial que sean los datos que se están exponiendo, por lo que os hemos propuesto medidas desde lo más genéricas y simples, hasta las más estrictas.

*Nota: guía actualizada con las nuevas funcionalidades de WhatsApp, en Julio de 2015.*