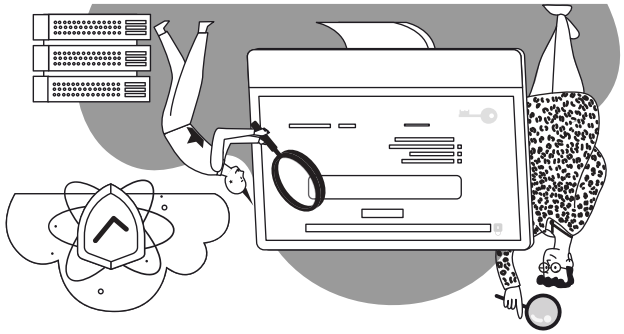


DESMINTIENDO ALGUNOS MITOS DE LA VIGILANCIA EN LAS COMUNICACIONES

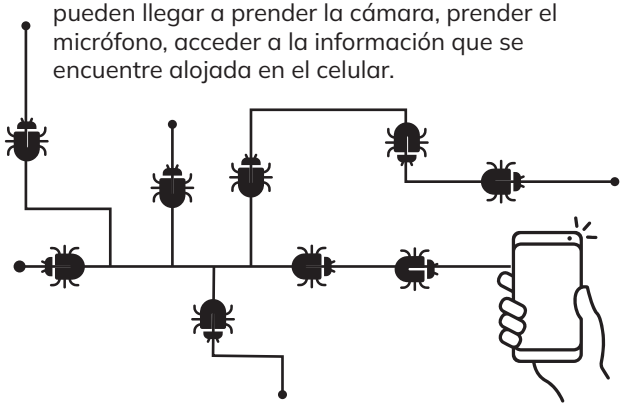
La vigilancia de las comunicaciones a periodistas, líderes y lideresas, así como a personajes públicos por parte de privados y estados es una realidad mundial y Colombia no es la excepción.

Estas prácticas han puesto en riesgo la vida de las personas y han dado pie a un sinnúmero de mitos y de eventos de desinformación. Aquí te compartimos información de valor para desmentirlos.

8 Mito 8: Los virus son solo para computadores

¡Falso! Esto ya ha cambiado mucho.

Anteriormente los virus o Malware (software malicioso) estaban pensados para los computadores, pero en la medida que la tecnología avanza y el uso de celulares aumenta, se han creado virus para los teléfonos, los cuales pueden llegar a prender la cámara, prender el micrófono, acceder a la información que se encuentre alojada en el celular.



1 Mito 1: ¡Mi teléfono está chuzado, escucho ruidos extraños en las llamadas!

¡Falso! Esto se debe (normalmente) a un problema con la infraestructura del país.

¿Has escuchado sonidos extraños mientras hablas por teléfono? Como si hubiera una tercera persona en la llamada, incluso escuchas respiros, ecos o retorno (¿escuchas tu propia voz?). Te has preguntado, ¿será que mi comunicación está siendo interrumpida o cruzada?

- Aunque sabemos que suena difícil de creer, la razón por la que normalmente escuchas estos ruidos extraños en las llamadas es porque la infraestructura de la red telefónica en Colombia no es la mejor, especialmente en zonas rurales.
- Esto ocasiona algunos problemas como que las llamadas se crucen o escuchemos ruidos o ecos.

ÑAPA: Te compartimoscuatro consejos para que gestiones tu seguridad digital.

- Revisa y ajusta los permisos de las aplicaciones en tu teléfono para limitar el acceso no autorizado.
- Ten cautela al hacer clic en enlaces o descarga de archivos, especialmente de correos electrónicos o mensajes de texto que parezcan sospechosos.
- Descarga aplicaciones siempre desde los sitios oficiales en la Play Store para Android y en Iphone AppS.
- Siempre que puedas, actualiza el sistema operativo del teléfono, esto lo hace más seguro.

Fundación Karisma <K+LAB>

<K+LAB>
Fundación Karisma

Encuentra toda la información aquí:
bit.ly/karisma-mitos-comunicaciones

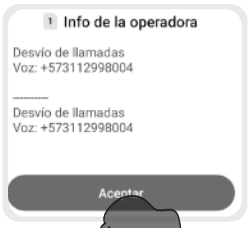
www.karisma.org.co

Karismacol @Karisma Karismacol fundacionKarismaa

2 Mito 2: Si marco *#62# ó *#21# y aparece un número desconocido es porque el teléfono está chuzado

¡Falso! **Hagamos el intento. Lo que te sale es el número predeterminado para el desvío de llamadas.**

Cuando marcamos a alguna de estas opciones (luego de una espera de unos cuantos segundos), el teléfono nos dirige a un número predeterminado que el prestador de telefonía nos da para el desvío de llamadas.

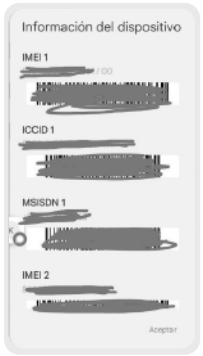


- El desvío de llamadas es un servicio que permite redirigir las llamadas a otra línea y que usamos cuando esta se va a correo, por ejemplo.
- ¿Por qué no aparece el mismo número para todas las personas? Porque cada empresa tiene varios números de desvío.

3 Mito 3: Si marco *#06# y me sale un número que tiene 2 ó 3 ceros al final el teléfono está intervenido

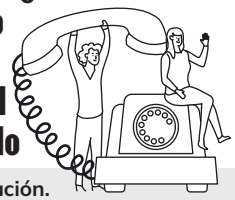
¡Falso! **Esto no es verdad, lo que te sale es el IMEI.**

El mito con este código es que si termina en dos ceros el celular está intervenido y están escuchando tus llamadas, si termina en tres ceros pueden escuchar tus llamadas y tienen acceso a la galería del celular.



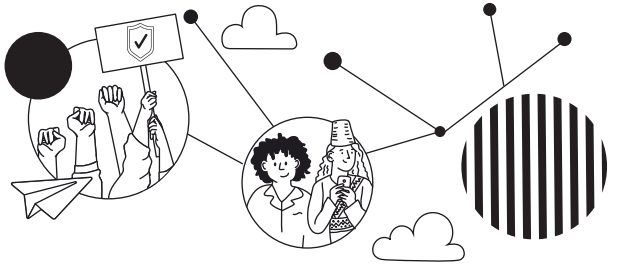
- Cuando marcamos al ***#06#** nuestros celulares nos muestran el IMEI; un código de 15 a 18 dígitos que identifica al celular de forma única.
- El IMEI no te dirá si tu celular está intervenido, cuando aparecen estos ceros lo que nos indica es la versión o nivel de actualización del sistema interno del celular.

4 Mito 4: Si marco*#16 seguido del número de teléfono y luego me aparece "marcación errada", el celular está intervenido



¡Falso! **Esto solo es una marcación.**

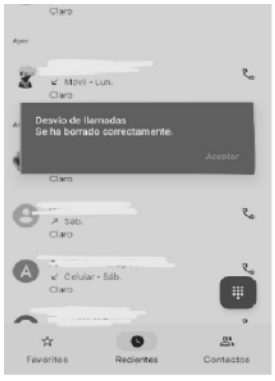
Básicamente, esto ocurre porque ***#16** seguido de un número de teléfono es una marcación inválida o inexistente. Este mito es absurdo, el teléfono dice que la marcación es errada, porque lo es.**¯_(ツ)_/¯.**



5 Mito 5: Si marco ##002# puedo quitar la "chuzada" de un celular

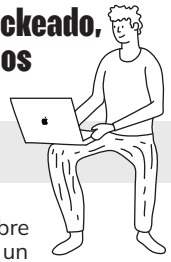
¡Falso! **Lo que puede pasar es que te quedes sin escuchar los mensajes de voz.**

Cuando marcamos a este número nos remite al borrado de desvío de llamadas, tal cual como se ve en la siguiente imagen:



- Normalmente, los celulares tienen un desvío de llamadas, que es a donde se van y se guardan los mensajes de voz que nos envían cuando no podemos contestar.
- Si borramos los números predeterminados que nos asignan los prestadores de telefonía móvil, en el futuro no se almacenarán los mensajes de voz.

6 Mito 6: Tengo el teléfono hackeado, alguien está respondiendo los mensajes por mí



¡Cuidado! **Aquí puede haber tanta realidad como ficción.**

Antes de sacar conclusiones apresuradas sobre porque un contacto de WhatsApp respondió un mensaje que no hemos visto, como si alguien o algo estuviera viendo los mensajes antes que nosotras. Piensa si recientemente has usado Whatsapp Web, porque puede ser que tengas una sesión iniciada en algún computador y eso pueda estar ocasionando esta confusión.

- Sin embargo, hay una amenaza real: la clonación de la SIM CARD o SIM Swapping, una técnica que consiste en "sacar una copia" de manera fraudulenta de una SIM CARD y cuando esto pasa, la SIM CARD original deja de funcionar y solo funciona "la copia". Con este fraude no solo se puede acceder a WhatsApp sino a muchas otras aplicaciones que usan mensajes de texto para autenticar a sus usuarios.
- En este caso es importante estar atentas y atentos a pérdidas intempestivas y prolongadas de señal y contactar a la empresa telefónica para comprobar cuál es el problema ya que si te clonan la SIM CARD pierdes la cobertura.

7 Mito 7: Si desactivo el GPS ya no me pueden rastrear

¡Falso! **Así no funcionan las cosas.**

Apagando el GPS solo establecemos límites dentro del teléfono (es decir si estamos en la ciudad de Bogotá el teléfono no podría saberlo y no podría decirnos en clima).Y empresas como Google también te pueden localizar a partir de los puntos WIFI cercanos.

- Sin embargo, las empresas de telefonía tienen acceso a la ubicación de nuestros celulares a través de datos que recolectan de sus antenas telefónicas.
- No todo son arcoíris y rosas, esto es un problema muy real y es inevitable a menos que el celular esté apagado o en modo avión.