

# Uso seguro de redes sociales e internet

Ing. Angie Aguilar Domínguez

*Coordinación de Seguridad de la Información*

*UNAM-CERT*



# Equipo CSI/UNAM-CERT

Ingeniería en  
computación



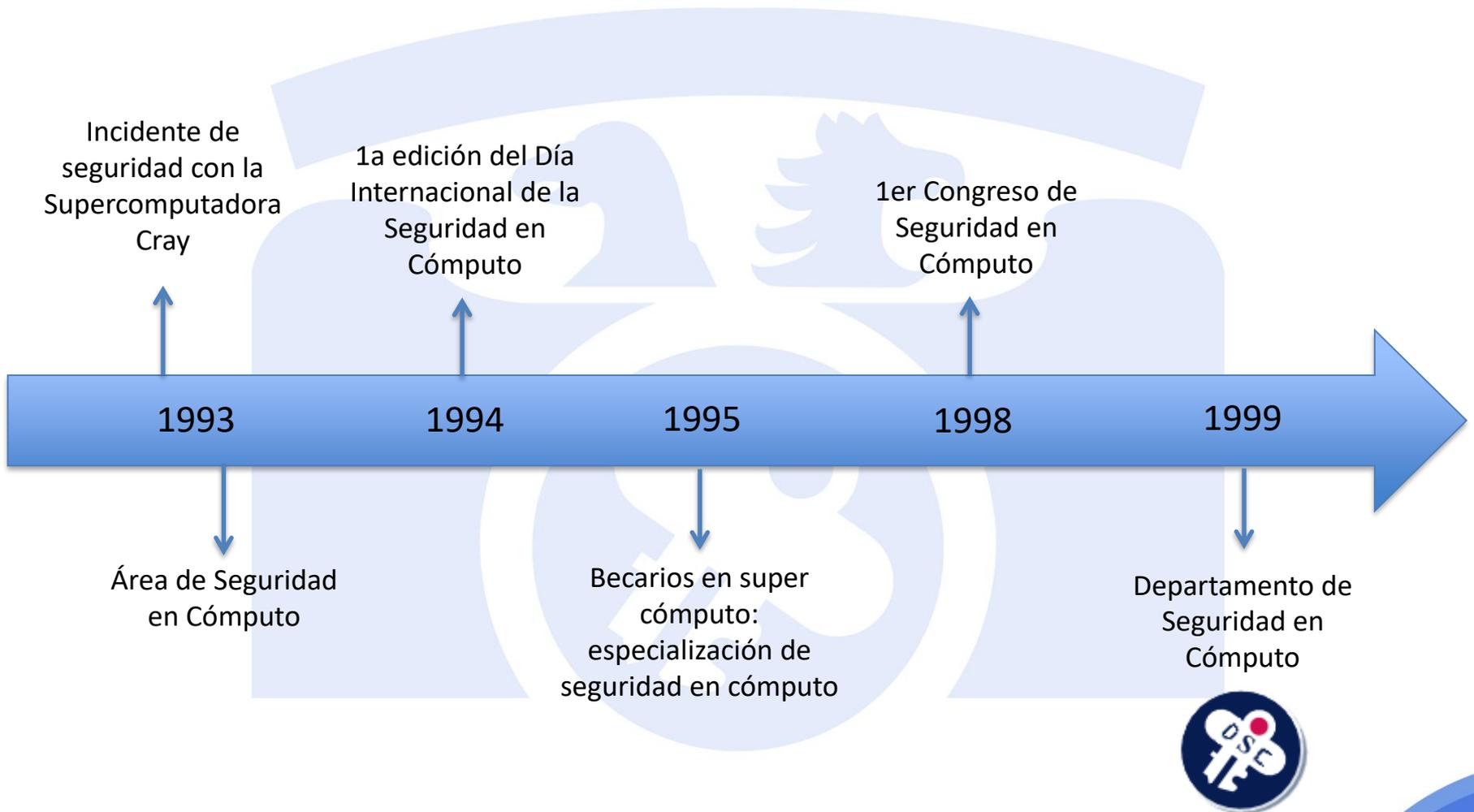
# Agenda

- UNAM-CERT
- Redes sociales
- Internet
- Dispositivos electrónicos

# Coordinación de Seguridad de la Información/UNAM-CERT

Contribuir al desarrollo de la UNAM, a través de la prestación de **servicios especializados**, la **formación** de capital humano y el fomento de la **cultura de seguridad de la información**.

# Historia



# Historia



Acreditación  
ante FIRST

2001

2005

2010

2014

2015

Obtención de la  
certificación ISO  
27001:2005

Transición al ISO  
27001:2013

Honeynet Project:  
UNAM Chapter



Coordinación de  
Seguridad de la  
Información

# Colaboración



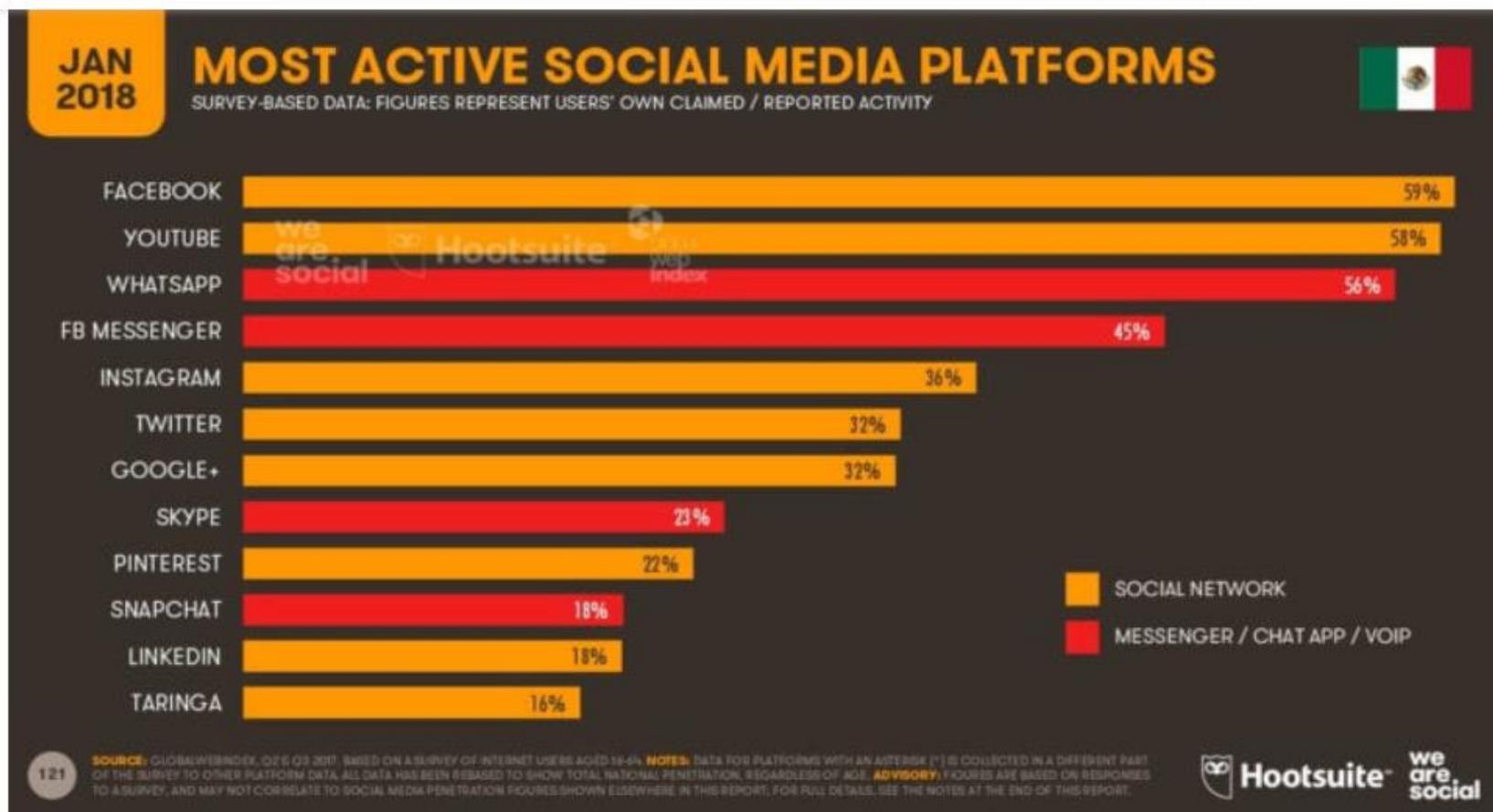
# Redes sociales

## México, cuarto lugar a nivel mundial en uso de redes sociales

*Alrededor de 63 de los 120 millones de habitantes están conectados a internet y tienen perfiles en alguna red social*

- Después de: Filipinas, Brasil y Argentina.
- Promedio: 8 horas de uso.
- ¿Cuánta información se proporciona?

# Las más usadas



# Amenazas en redes sociales

- Perfiles falsos que distribuyen malware

The image shows a screenshot of a Facebook web interface. On the left, the navigation menu includes 'Alfredo Perez', 'News Feed', 'Messenger', and 'EXPLORE'. The main content area shows a 'Recent (1) Message Requests' section with a message from 'Karlos Zantos (1)' from 'Alfredo Video' containing a suspicious URL. On the right, a chat window with 'Karlos Zantos' is open, showing three messages from 'Alfredo Video' with thumbs up and various URLs: <http://t.cn/XYZ3jab?Alfredo>, <http://tinyurl.com/asdcvgira>, and <http://tinyurl.com/vfrijshivdetgbn?Alfredo>. The browser address bar shows 'https://www.facebook.com'.

# Amenazas en redes sociales

- Robo de identidad



Facebook ✓  
@FacebookEspaña



Twitter ✓  
@Twitter



Instagram ✓



**UNAM** ✓  
@UNAM\_MX

La Universidad Nacional Autónoma de México tiene como propósito estar al servicio del país y la humanidad mediante educación, investigación y difusión cultural.

📍 Mexico

🌐 unam.mx

📅 Se unió en junio de 2009

Twitter a

Mensaje



# Amenazas en redes sociales

- Robo/filtración de datos
- Estafa



**iPhone Argentina**  
Te gusta esta página · 25 de junio ·

**100% FRAUDE**

Hola chicos, estamos muy felices por la buena aceptación que han tenido nuestros sorteos anteriores, por eso queremos celebrarlo con todos ustedes sorteando 100 nuevos IPHONE 6 PLUS SOLO para ARGENTINA!

El día 06 de Julio de 2015 a las 12:00 del mediodía sortearemos 30 negros, 30 Plateados y 40 Dorados. Los ganadores los llamaremos el mismo día del sorteo a su número de móvil, y les enviaremos el iPhone a la dirección que deseen.

¿Querés uno? Sólo tenes que seguir estos 5 sencillos pasos:

- 1) "COMPARTIR" esta publicación
- 2) Hacer clic en "ME GUSTA" en esta publicación
- 3) COMENTAR EL COLOR que te guste solo una vez: negro, plateado o dorado.

Ojo: esta parte es **MUY IMPORTANTE**, ya que solo los números registrados en nuestra web estarán participando, de esa forma llamaremos a los ganadores.

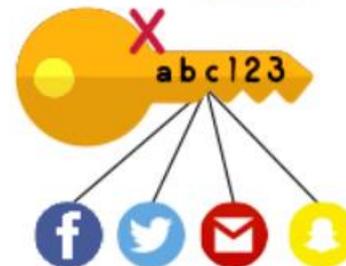
**4) ENVIAR** tu número de móvil aquí:  
<http://bit.ly/argentinacatocconline>

Escribe un comentario...

# Algunos consejos

## No recicles ni reúses tus contraseñas

No es recomendable **usar una misma contraseña** para todas tus cuentas y tampoco debes **reciclar** los elementos de una clave, como los números y las palabras, pues ambas prácticas **debilitan la seguridad** de tus credenciales de acceso.



[www.seguridad.unam.mx](http://www.seguridad.unam.mx)



ACONSEJA



# No compartas información indiscriminadamente

Tu información es valiosa, por ello te recomendamos distinguir en quién puedes confiar y en quién no. **Crea grupos en tus redes sociales para que controles quién puede ver tu información.**



[www.seguridad.unam.mx](http://www.seguridad.unam.mx)



ACONSEJA



# No creas todo lo que publican en las redes

Cuando lees noticias en redes sociales piensa dos veces antes de compartir la información. **Verifica que la nota sea real y que no sea parte de una campaña maliciosa.**



[www.seguridad.unam.mx](http://www.seguridad.unam.mx)



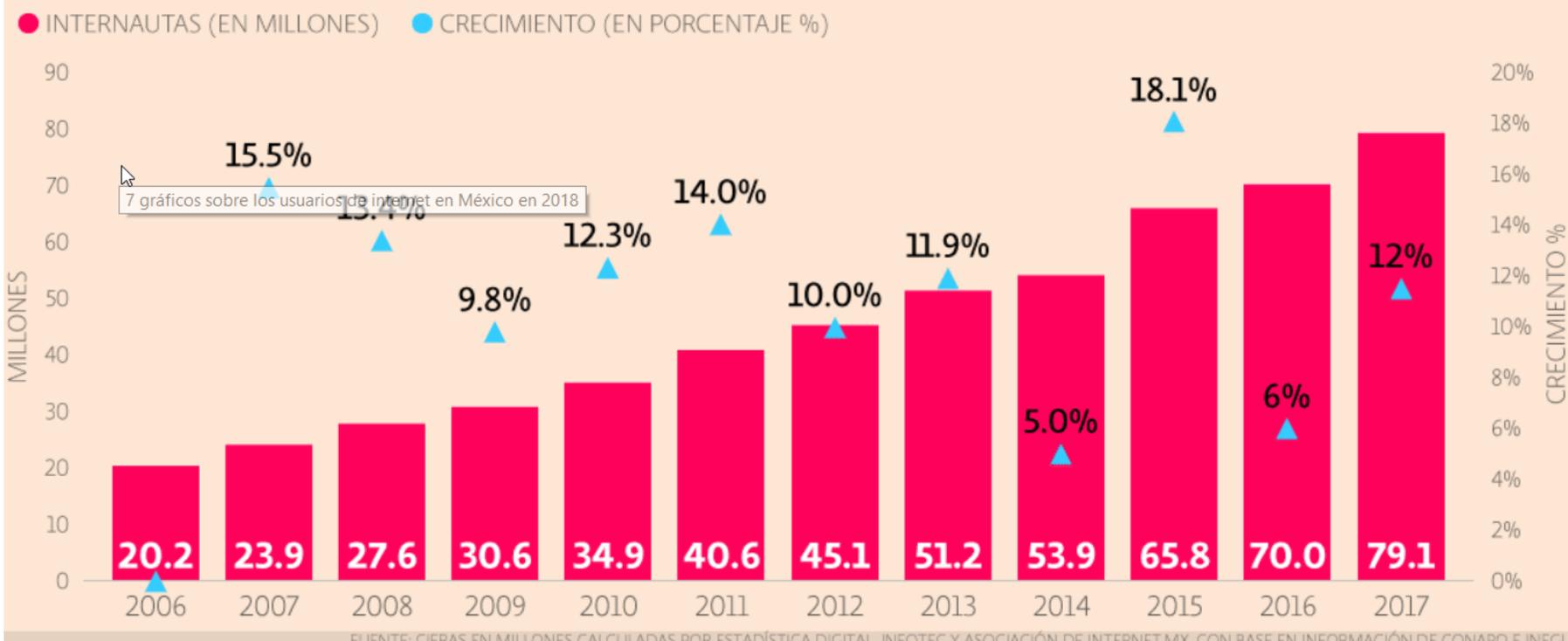
ACONSEJA



DGTIC

# Navegación por internet

## USUARIOS DE INTERNET EN MÉXICO | 2006 - 2017



# Navegación por internet

- Conexión desde:
  - Casa
  - Trabajo
  - Redes públicas
- Miles de sitios web con distintos tipos de contenido:
  - ¿Qué tan peligroso puede ser?
  - ¿Qué tanto se puede perder?
  - Un solo sitio visitado...

# Consejos



ACONSEJA



## Guarda copias de tus transacciones

Quando realices alguna operación monetaria, haz una copia o guarda la información. Te podría servir para una aclaración posterior.



Mayor Información <http://www.seguridad.unam.mx>

# Más recomendaciones

- Navega siempre sitios web verificados: evita aquellos que se vean sospechosos.
- Activa el bloqueo de ventanas emergentes del navegador.
- No sigas la publicidad engañosa que abunda en las páginas web.
- Emplea contraseñas difíciles de adivinar.

# ¿Cómo crear una contraseña?

## No compartas tus contraseñas con nadie

---

No puedes estar completamente seguro de la privacidad de tus cuentas si compartes tus contraseñas con alguien más, mucho menos si las anotas donde alguien podría verlas.

## No utilices datos personales

---

Los datos personales, como fecha de nacimiento o número telefónico, son fáciles de obtener. Si utilizas esta información estás aumentando la posibilidad de que alguien la adivine.

## Cambia tus contraseñas periódicamente

---

Para un atacante es más fácil encontrar una contraseña que siempre es igual a una que cambia con el tiempo. Recomendamos cambiarla cada seis meses.

## Una frase es mucho más segura

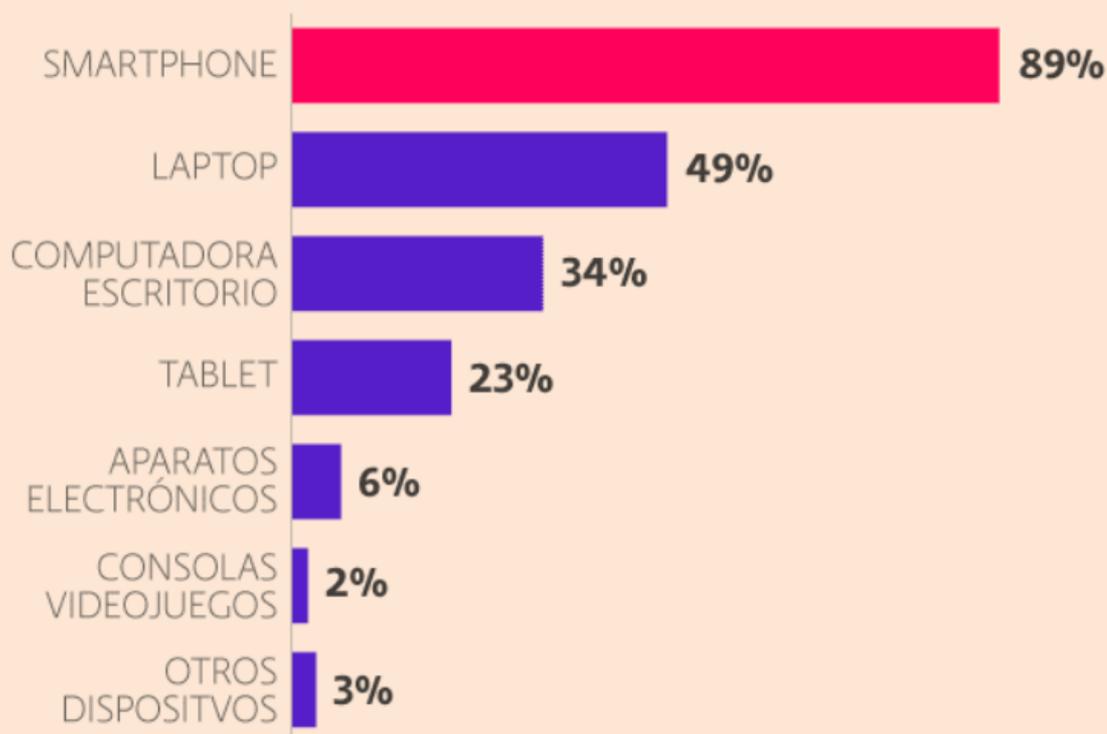
---

Pensar en una frase personal, que sea fácil de recordar pero difícil de adivinar, puede aumentar la seguridad de tus cuentas.

# Dispositivos de conexión

## 9 DE CADA 10 PREFIEREN TELÉFONOS MÓVILES PARA CONECTARSE

DISPOSITIVOS DE CONEXIÓN | CIFRAS EN PORCENTAJE



FUENTE: CIFRAS EN MILLONES CALCULADAS POR ESTADÍSTICA DIGITAL, INFOTEC Y ASOCIACIÓN DE INTERNET.MX, CON BASE EN INFORMACIÓN DE CONAPO E INEGI.

# Problemas con los dispositivos

- Apps maliciosas.
- Falta de actualizaciones.
- Falta de antivirus.
- Configuraciones por defecto.

# Algunos consejos

## Activa el bloqueo de tus dispositivos

**Bloquea tus dispositivos cuando no los uses, ya sea tu computadora o tu móvil.**

**Valora tu información para evitar que personas maliciosas hagan mal uso de ella.**



[www.seguridad.unam.mx](http://www.seguridad.unam.mx)



ACONSEJA



# Revisa los permisos que pide una app

Lee qué permisos otorgas a una aplicación antes de instalarla. Si los permisos no coinciden con su función, desconfía de ella y no la instales.



[www.seguridad.unam.mx](http://www.seguridad.unam.mx)



ACONSEJA



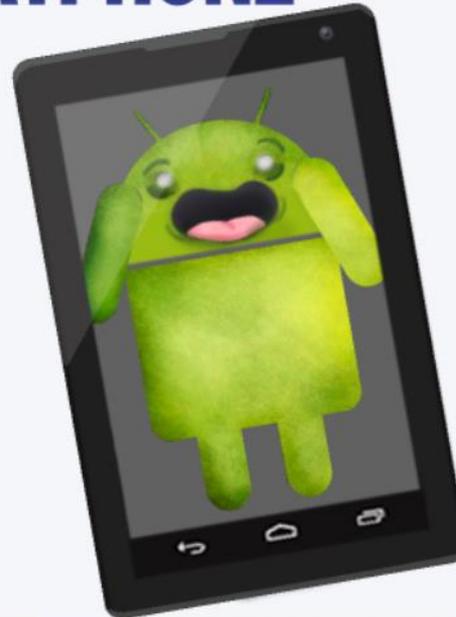
DGTIC

# CUIDADO CON LAS MODIFICACIONES A TU SMARTPHONE

23

**Modificar arbitrariamente el sistema operativo de tu dispositivo para personalizarlo puede representar un riesgo de seguridad**

*Miguel Ángel Mendoza*



<http://revista.seguridad.unam.mx>



ACONSEJA



# Consejos finales

- No confiar ciegamente en todo lo que hay en internet: redes sociales, sitios, etc.
- Mantener actualizados dispositivos y versiones de aplicaciones.
- Evitar software y descargas ilegales.
- Mantenerse informado sobre los problemas de seguridad existentes: permite tomar la delantera.
- Tener siempre presente: el mal no descansa.

# Difusión

- Sitio de UNAM-CERT:
  - [www.seguridad.unam.mx](http://www.seguridad.unam.mx)
  - [www.cert.org.mx](http://www.cert.org.mx)
- Revista .Seguridad Cultura de prevención para TI:
  - [revista.seguridad.unam.mx](http://revista.seguridad.unam.mx)
- Boletín Ouch! (colaboración con SANS Institute):
  - [www.seguridad.unam.mx/ouch](http://www.seguridad.unam.mx/ouch)

# Redes sociales

- Twitter:
  - @unamcert
- Facebook:
  - /unamcert
- YouTube:
  - /user/SeguridadTV

# GRACIAS POR SU ATENCIÓN

Ing. Angie Aguilar Domínguez

angie.aguilar@cert.unam.mx

