

Consejos para protegerse del mal(ware)

Angie Aguilar Domínguez

Coordinación de Seguridad de la Información



Equipo CSI/UNAM-CERT

Ingeniera en
computación



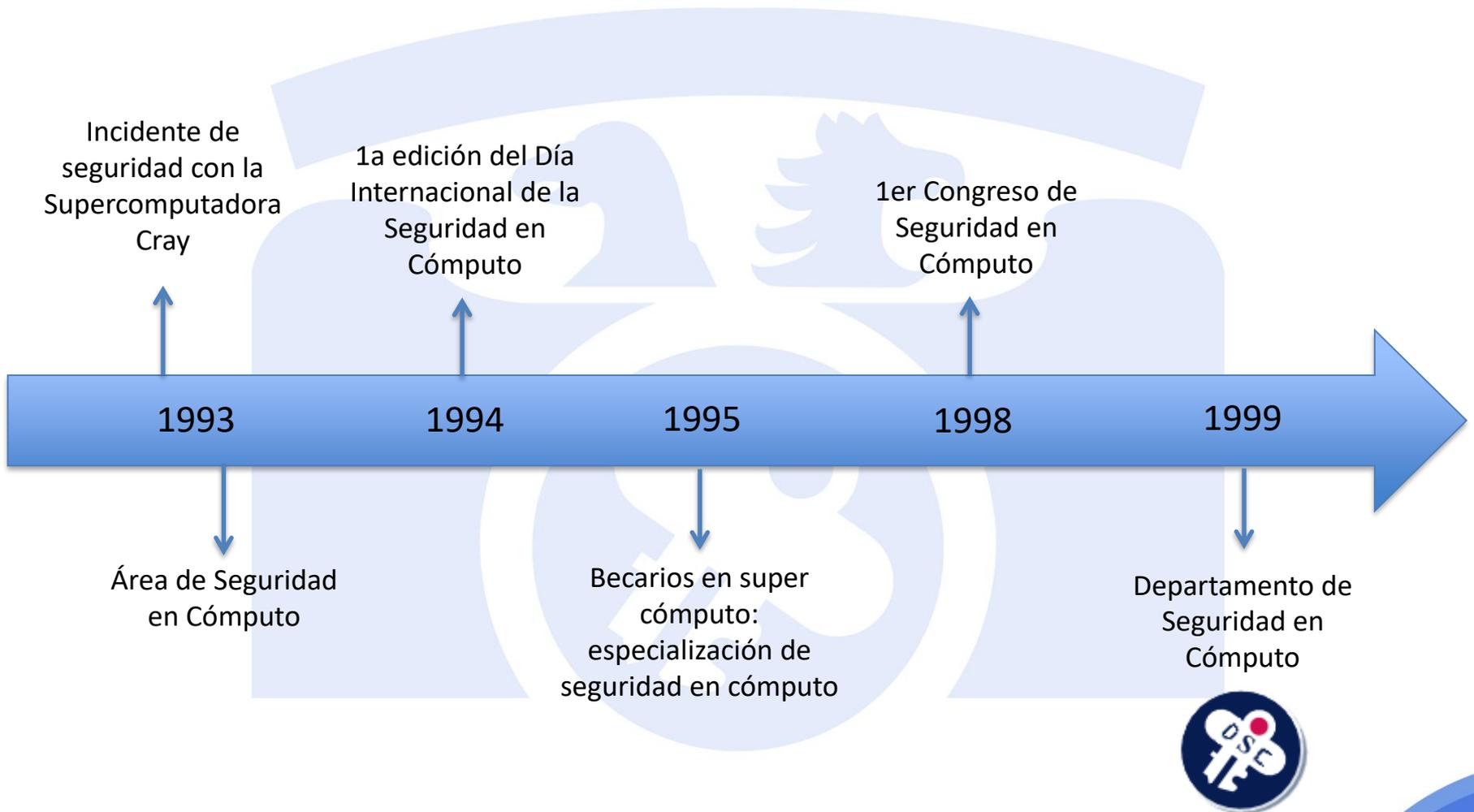
Agenda

- UNAM-CERT
- ¿Qué es el malware?
- Consejos para el equipo de cómputo
- Consejos para dispositivos electrónicos
- Consejos para Internet

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



Malware

- malicious + software = malware
- Software, programa, código malicioso
- Comúnmente conocido como virus.

Malware

- Gusanos
- Keyloggers
- Rootkits
- Caballos de Troya
- Aplicaciones de espionaje
- Bots y botnets
- SPAM
- Ransomware



Malware

It must be Tiffany. Spam x



Tiffany&Co Outlets <rjpgjh1600@szjh.vip>
para yo ▾

lun., 22 oct. 11:49



¿Por qué está en la carpeta Spam este mensaje? Es similar a mensajes que se identificaron como spam en el pasado.

Informar que no es spam



Mrs. Rona FAirHead <static@kingnet.net.tw>
para Recipients ▾

vie., 26 oct. 11:03 (Hace 11 días.)



Este mensaje parece peligroso

Se usaron mensajes similares para robar información personal a los usuarios. Evita hacer clic en vínculos, descargar archivos adjuntos o responder con datos confidenciales.

Parece seguro



Malware



LOS CELOS
Son para débiles.
No hay como aprender
a confiar, respetar e
instalar un keylogger



SMB (MS17-010)



```
0100101011 101001001010
10010010100 010101001
000010101010 1010110111
01010101010 01001001101
01101101001 01101110101
010010011110 010100100
101010010100 1010101010
```

Se descubre una vulnerabilidad crítica en el servicio SMB (usado para compartir archivos en red).

Los ciberdelincuentes crearon una mezcla de ransomware y gusano que explota la vulnerabilidad.

La vulnerabilidad puede ser explotada por la herramienta #EternalBlue. En marzo de 2017 fue parchada por Microsoft.



El ransomware cifra la información del usuario y exige un rescate para descifrarla.

Ransomware

```
0101000101001010
0111010101110101
0101010100010101
1010100101000101
1011101110101100
```



Gusano

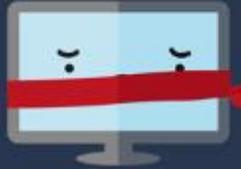


El gusano se propaga por la red.

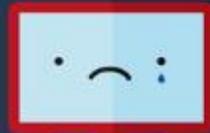


WANNACRY

12/05/17



El #ransomworm se dispersó rápidamente en cientos de miles de equipos en más de 150 países.



Exige como rescate el equivalente a \$300 USD en Bitcoins (moneda virtual).

3.0



```
0010101110101011
1010 0101000101001010
1011 0111010101110101
0011 0101010101010101
0111 1010100101000101
1011101110101100
```

2.0

Se liberaron diferentes versiones de WannaCry, algunas sin un interruptor de emergencia y no se sabe si habrá otras variantes.



¿Qué hago?

Prevención



Actualiza el sistema operativo



Respalda tu información



Usa un antivirus

Reacción



Desconecta el equipo de la red



No pagues rescate



Formatea el equipo



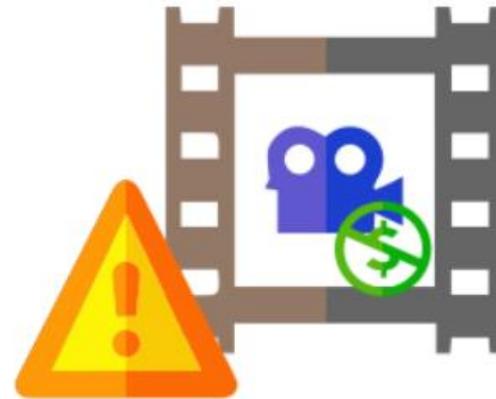
Vacuna
#nomorecry



Consejos para el equipo

Evita los sitios de películas, series y software gratis

Ver películas y series sin licencia de distribución en Internet puede infringir los derechos de autor y convertirse en una amenaza para la seguridad de tu sistema y tu información.



www.seguridad.unam.mx



ACONSEJA



Consejos para el equipo

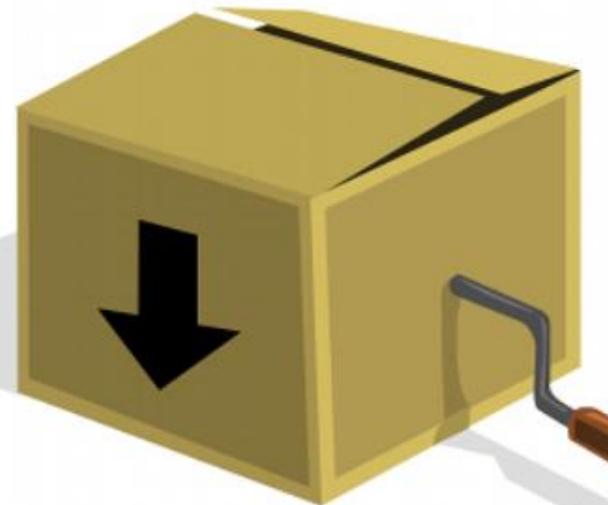


ACONSEJA



Descarga programas de páginas seguras

Si la página o el archivo que descargas te genera dudas, evita descargarlo, hay otras opciones a las que puedes acudir.



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

¿Y los dispositivos?

- Apps maliciosas
- Conexiones a redes inalámbricas abiertas
- Ausencia de software de seguridad
- Falta de actualizaciones
- Falta de respaldos
- Robo del dispositivo

Consejos para dispositivos

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



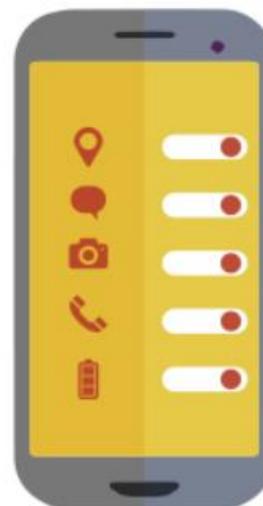
ACONSEJA



Consejos para dispositivos

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



ACONSEJA



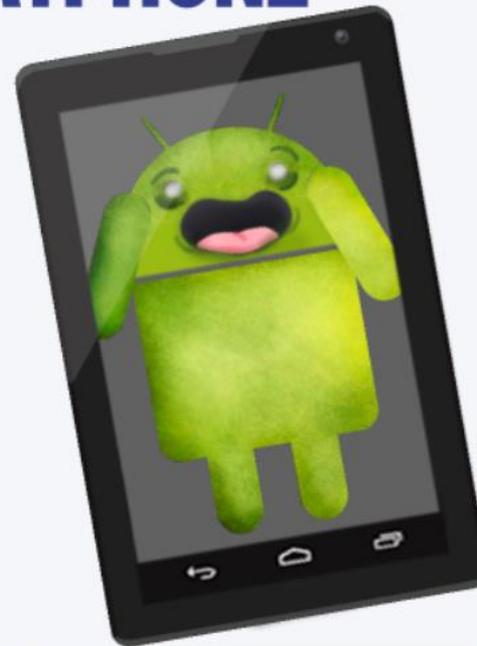
Consejos para dispositivos

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>

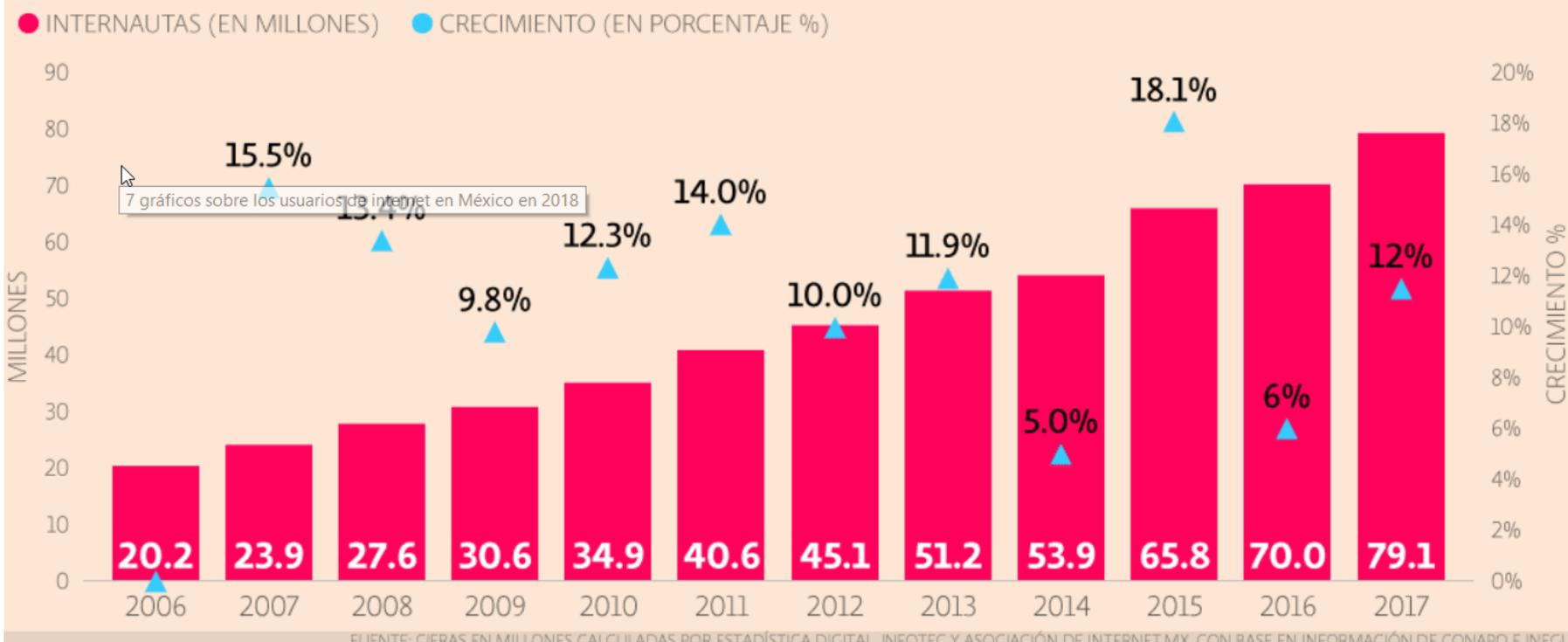


ACONSEJA



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 para internet



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>

Consejos para internet

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



ACONSEJA



Consejos para internet



Aconseja



¿Qué dice Internet de ti?

Ten cuidado con la información que compartes y con quién la compartes. Siempre revisa qué se dice de ti en redes sociales y en la Web.

Más consejos

- 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.

Difusión

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

