Consejos para protegerse del mal(ware)

Angie Aguilar Domínguez

Coordinación de Seguridad de la Información

UNAM CERT

DGTIC

DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Equipo
CSI/UNAM-CERT

Ingeniera en computación

DGTIC

Agenda

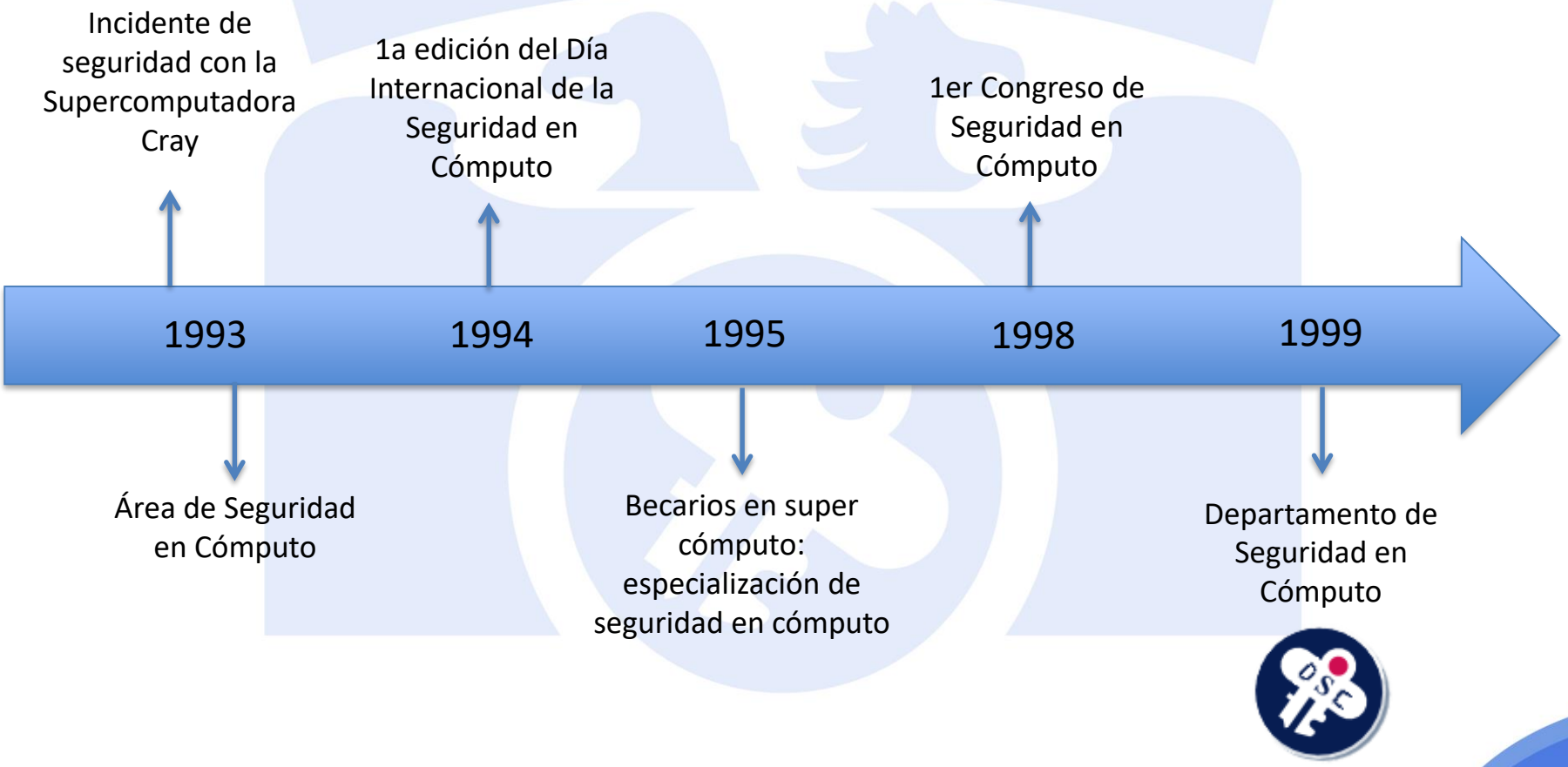
- UNAM-CERT
- ¿Qué es el malware?
- Consejos para el equipo de cómputo
- Consejos para dispositivos electrónicos
- Consejos para Internet

DGTIC

Coordinación de Seguridad de la Información/UNAM-CERT

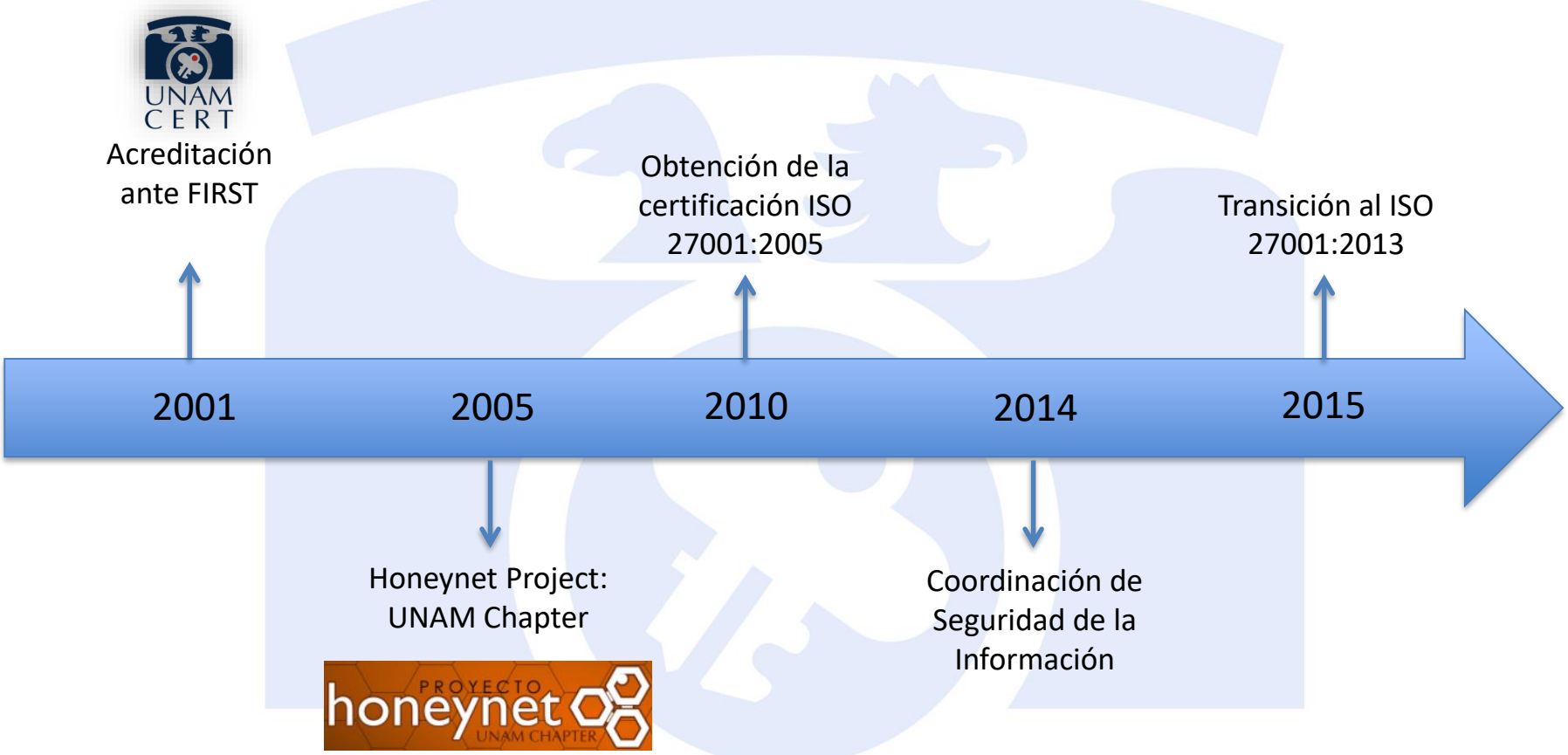
Contribuir al desarrollo de la UNAM, a través de la prestación de servicios especializados, la formación de capital humano y el fomento de la cultura de seguridad de la información.

Historia



DGTIC

Historia



DGTIC

Colaboración

DGTIC

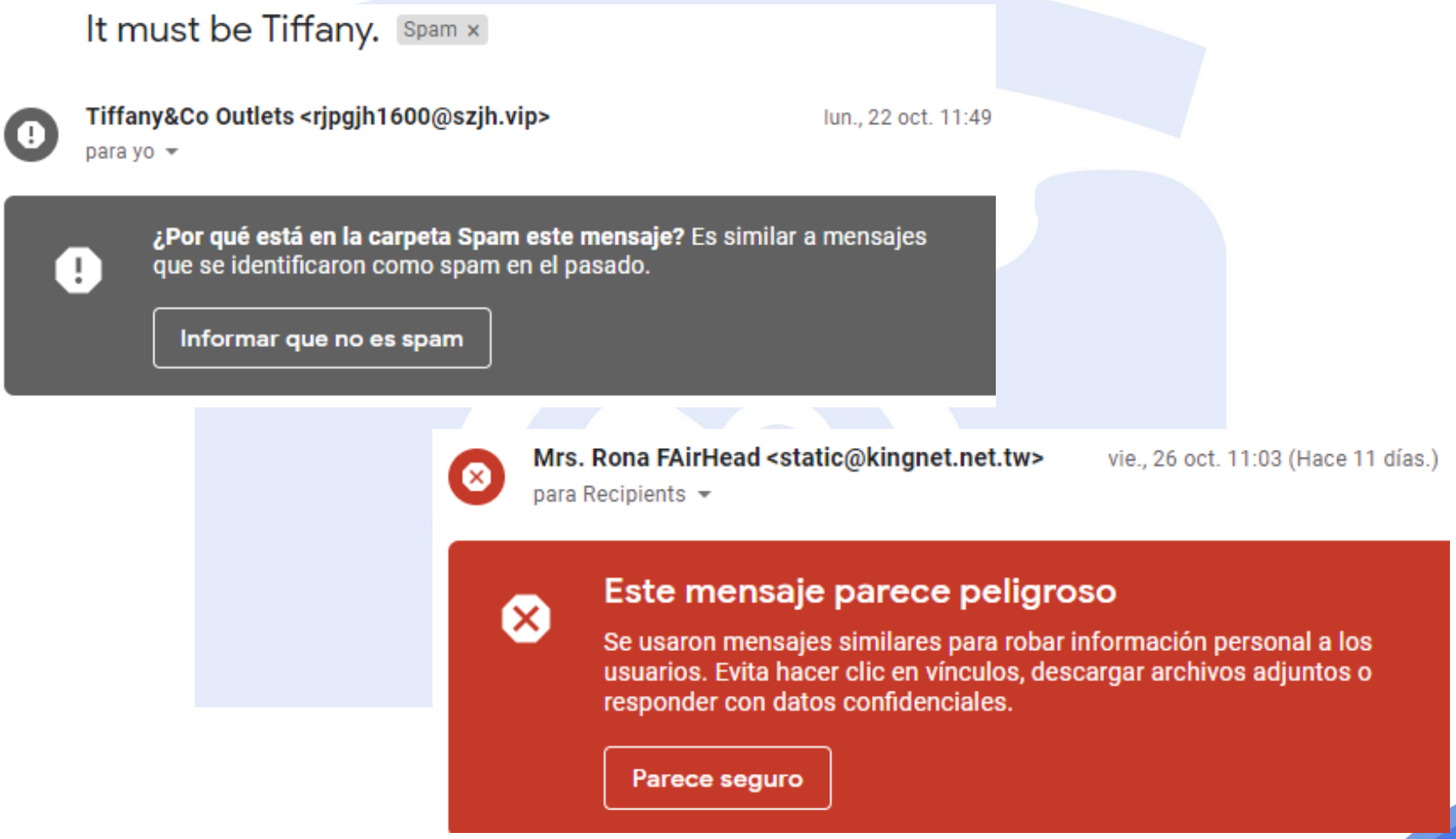
Malware

- 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

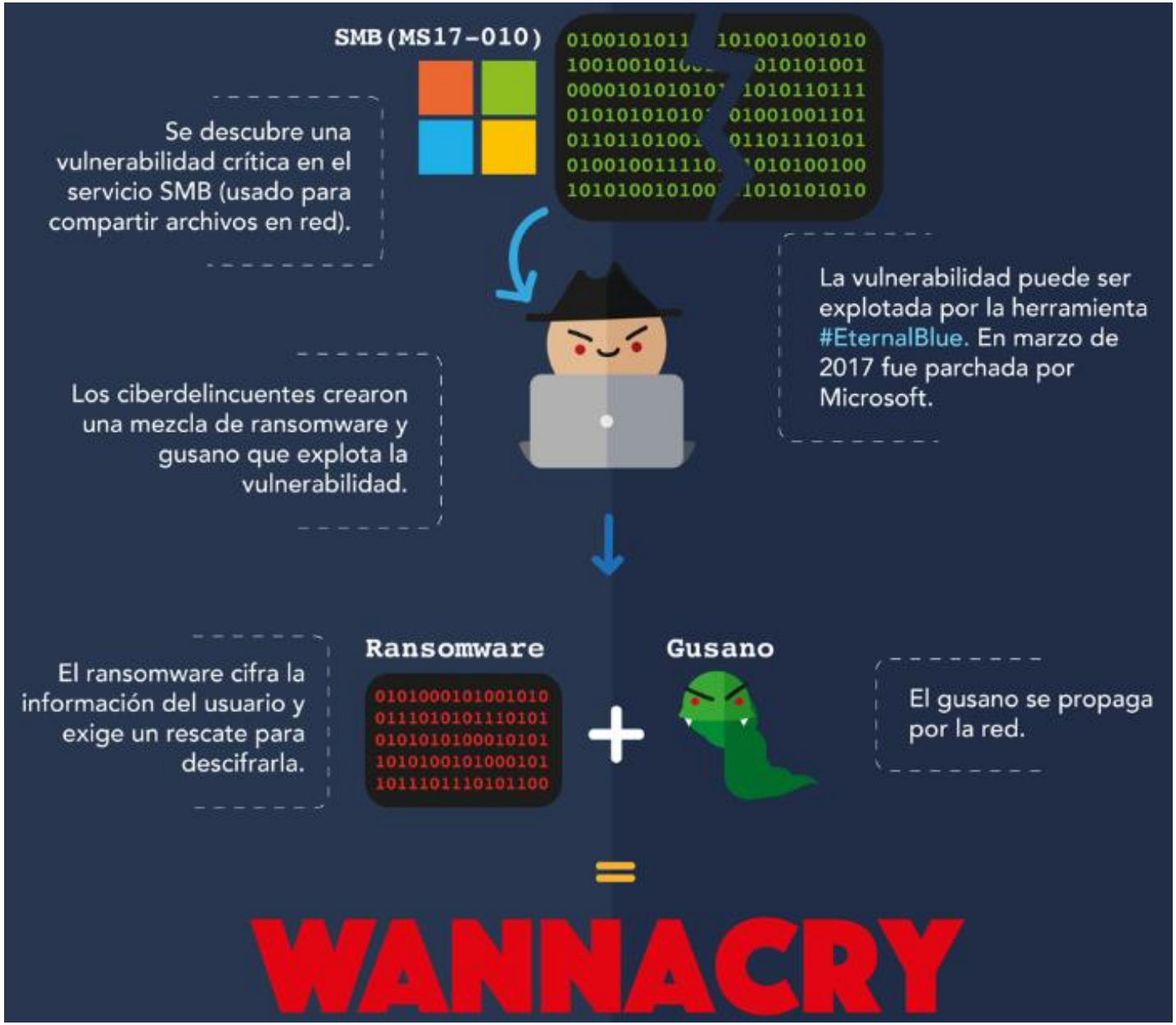


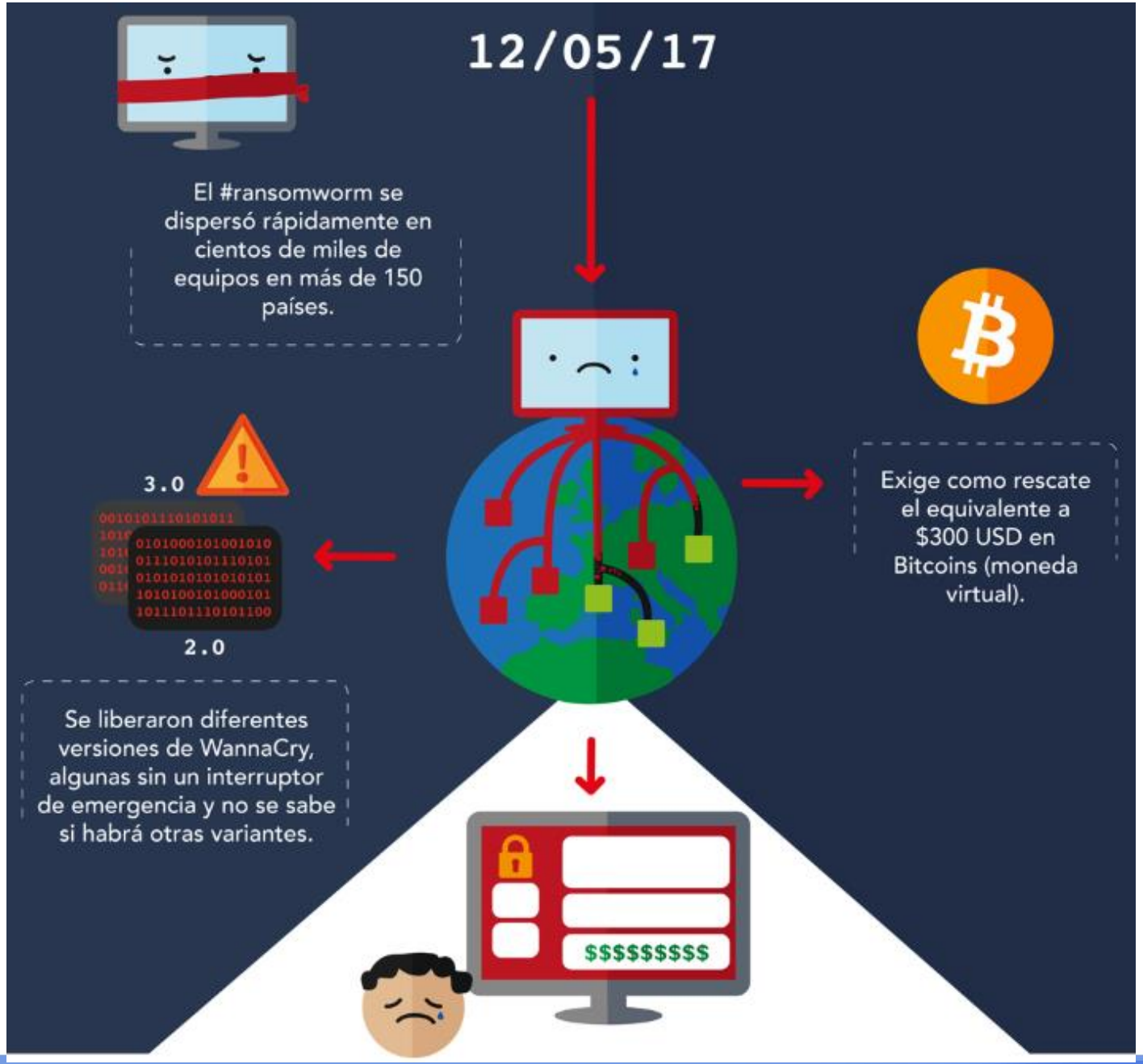
DGTIC

Malware


BOT


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


SMB (MS17-010)
Se descubre una vulnerabilidad crítica en el servicio SMB (usado para compartir archivos en red).
La vulnerabilidad puede ser explotada por la herramienta #EternalBlue. En marzo de 2017 fue parchada por Microsoft.
Los ciberdelincuentes crearon una mezcla de ransomware y gusano que explota la vulnerabilidad.
El ransomware cifra la información del usuario y exige un rescate para descifrarla.
Ransomware
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
2.0
Se liberaron diferentes versiones de WannaCry, algunas sin un interruptor de emergencia y no se sabe si habrá otras variantes.
$$$$$$$$

DGTIC

¿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

DGTIC

unamcert

UNAM CERT

DGTIC

Consejos para el equipo

DGTIC

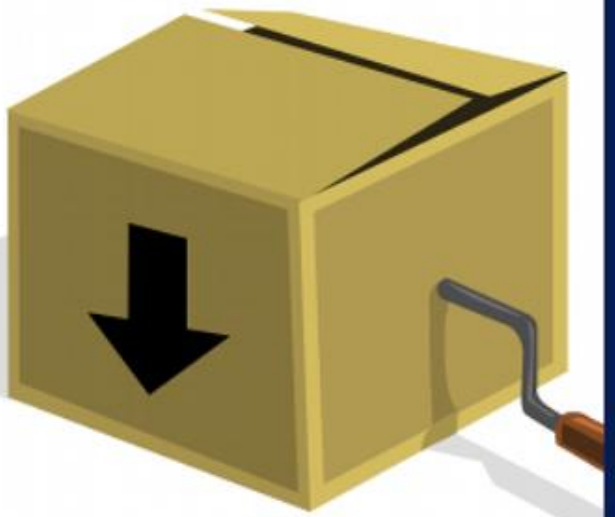
Consejos para el equipo

UNAM CERT

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

DGTIC

¿Y los dispositivos?

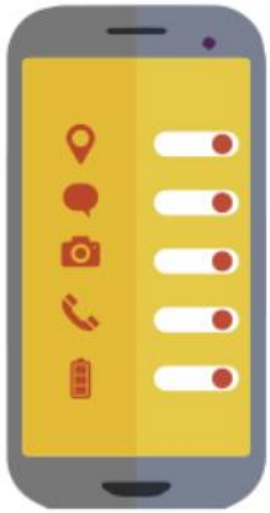
- Apps maliciosas
- Conexiones a redes inalámbricas abiertas
- Ausencia de software de seguridad
- Falta de actualizaciones
- Falta de respaldos
- Robo del dispositivo

Consejos para dispositivos

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 UNAM CERT ACONSEJA

DGTIC

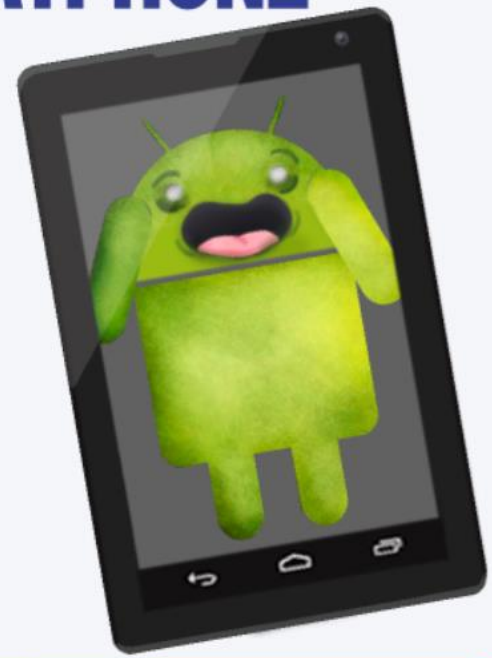
Consejos para dispositivos

CUIDADO CON LAS MODIFICA-CIONES A TU SMARTPHONE

23

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

Miguel Ángel Mendoza



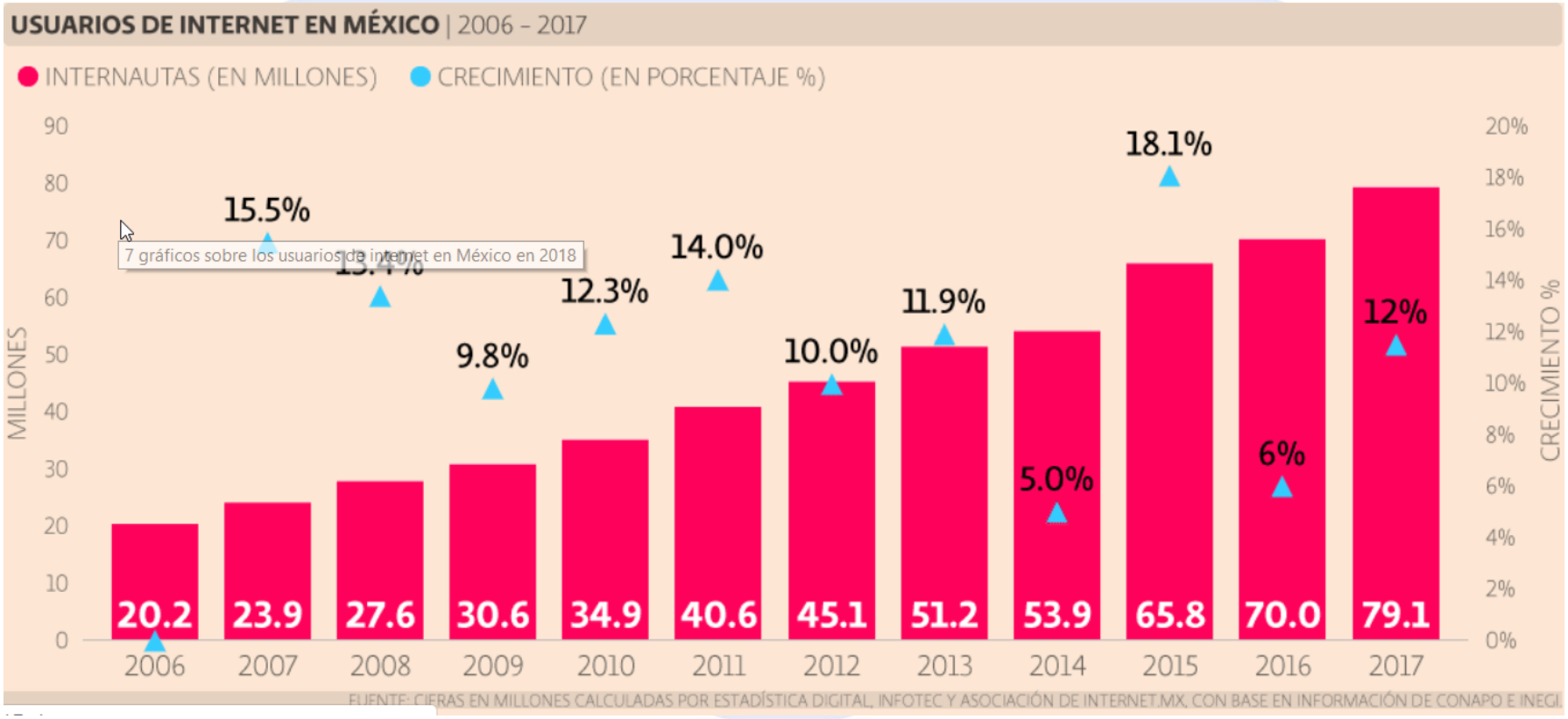
http://revista.seguridad.unam.mx

UNAM CERT

ACONSEJA

DGTIC

Navegación por internet



DGTIC

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…

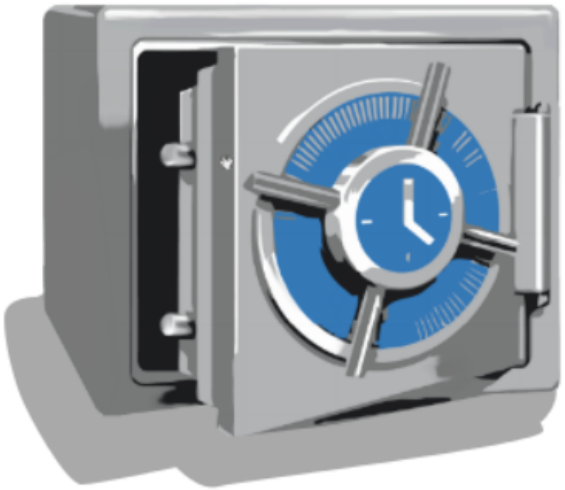
Consejos para internet

UNAM CERT

ACONSEJA

Guarda copias de tus transacciones

Cuando 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

DGTIC

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 UNAM CERT ACONSEJA

DGTIC

Consejos para internet

DGTIC

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

DGTIC

GRACIAS POR SU ATENCIÓN

Ing. Angie Aguilar Domínguez

angie.aguilar@cert.unam.mx

UNAM CERT

DGTIC

DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN