

Seguridad en cómputo

Ing. Angie Aguilar Domínguez

Coordinación de Seguridad de la Información

UNAM-CERT



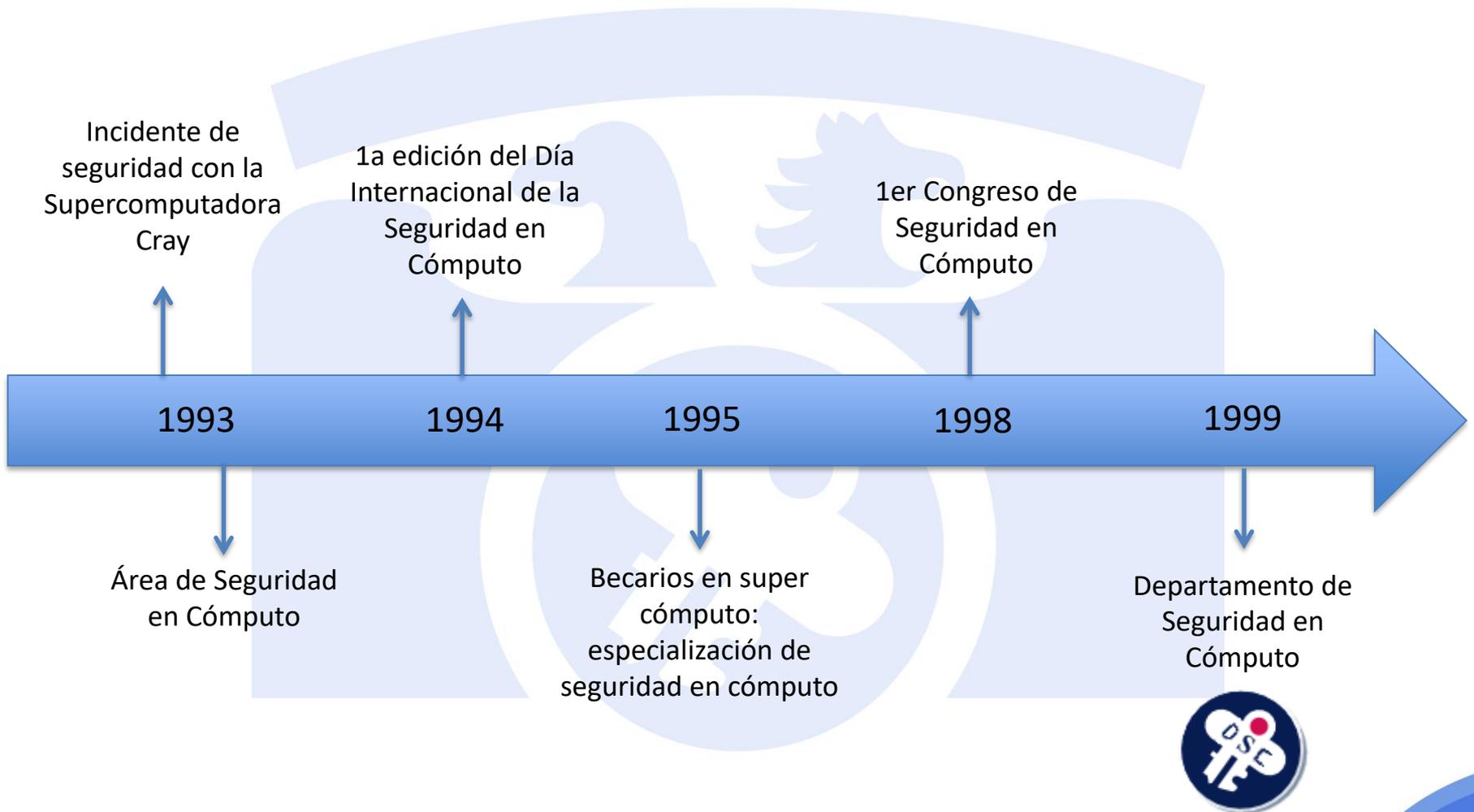
Agenda

- UNAM-CERT y su historia
- Principales problemas actuales
- Consejos de seguridad

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



Servicios

- Implementación de SGSI de acuerdo con el estándar ISO/IEC 27001
- Auditoría informática
- Análisis forense
- Análisis de vulnerabilidades y pruebas de penetración
- Análisis de tráfico de red
- Análisis de riesgos
- Respuesta a incidentes de seguridad de la información
- Revisión de configuraciones
- Creación de políticas de seguridad de la información
- Revisiones de seguridad para aplicativos web

Pasa todos los días...

Facebook Says Breach Affected About 50 Million Accounts

Uber deberá pagar una multa de 148 millones de dólares por filtración de datos

Una nueva extorsión circula vía correo electrónico

Claves débiles en el 50% de los empleados públicos estadounidenses

Y vuelve a pasar...

¡Cuidado! Circula nuevo fraude con mensaje falso de “Bancomer”

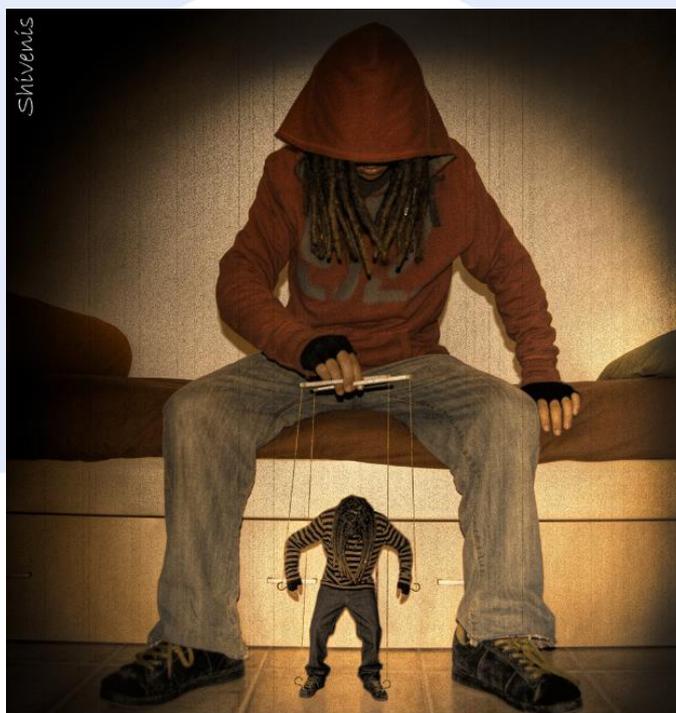
El cibercrimen impactó a 33 millones de mexicanos en 2017

Una campaña de phishing suplanta a Openbank

Una vulnerabilidad pone en peligro a los usuarios de Adobe Reader y Acrobat

Ingeniería Social

Métodos que emplean los atacantes para engañar a las víctimas y que realicen determinadas acciones.



Consejo práctico

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



Más recomendaciones

- Implementar políticas de seguridad en la organización que minimicen las acciones de riesgo.
- Contar con controles de seguridad física para reducir el peligro de ingreso de personal no autorizado.
- Llevar a cabo programas de concientización sobre la seguridad de la información.

Phishing

Técnica utilizada con el propósito de robar información bancaria, nombres de usuarios y contraseñas.

The collage consists of four overlapping screenshots:

- Top Left:** A fake email from Apple with the subject "Dear Client" and a Spotify Premium promotion. It includes the Profeco logo and a link to a fake support page.
- Top Center:** A fake Banorte bank page with the header "BANORTE EL BANCO FUERTE DE MEXICO" and a "Info e-mail e Info Celular" section featuring a cartoon robot.
- Top Right:** A screenshot of a text message from a number starting with +14076550286, claiming to be from Apple support and providing a link to a fake support page.
- Bottom Center:** A screenshot of an Apple login screen titled "Iniciar sesión en iCloud" with fields for "ID de Apple" and "Contraseña".

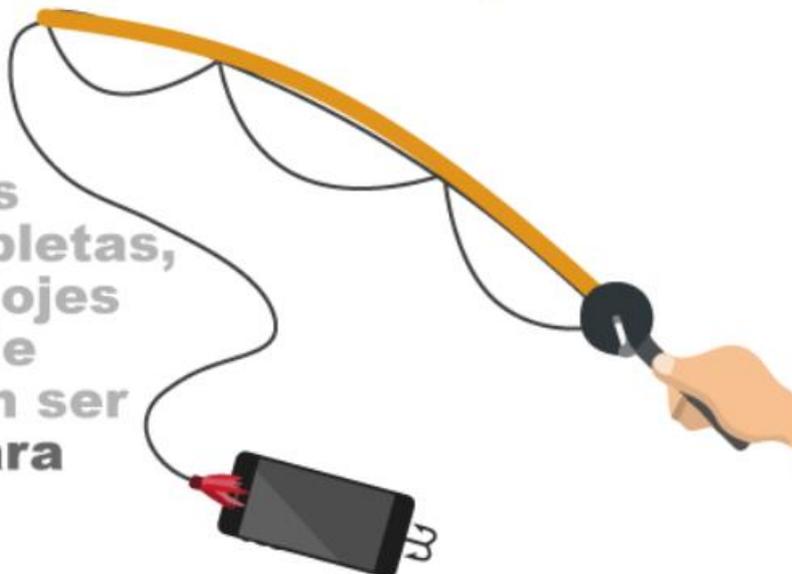
Phishing



Consejo práctico

No compartas tus datos en internet a cambio de regalos

Dispositivos móviles, computadoras portátiles, tabletas, cámaras y relojes inteligentes de regalo pueden ser un anzuelo para robar datos.



www.seguridad.unam.mx



ACONSEJA



DGTIC

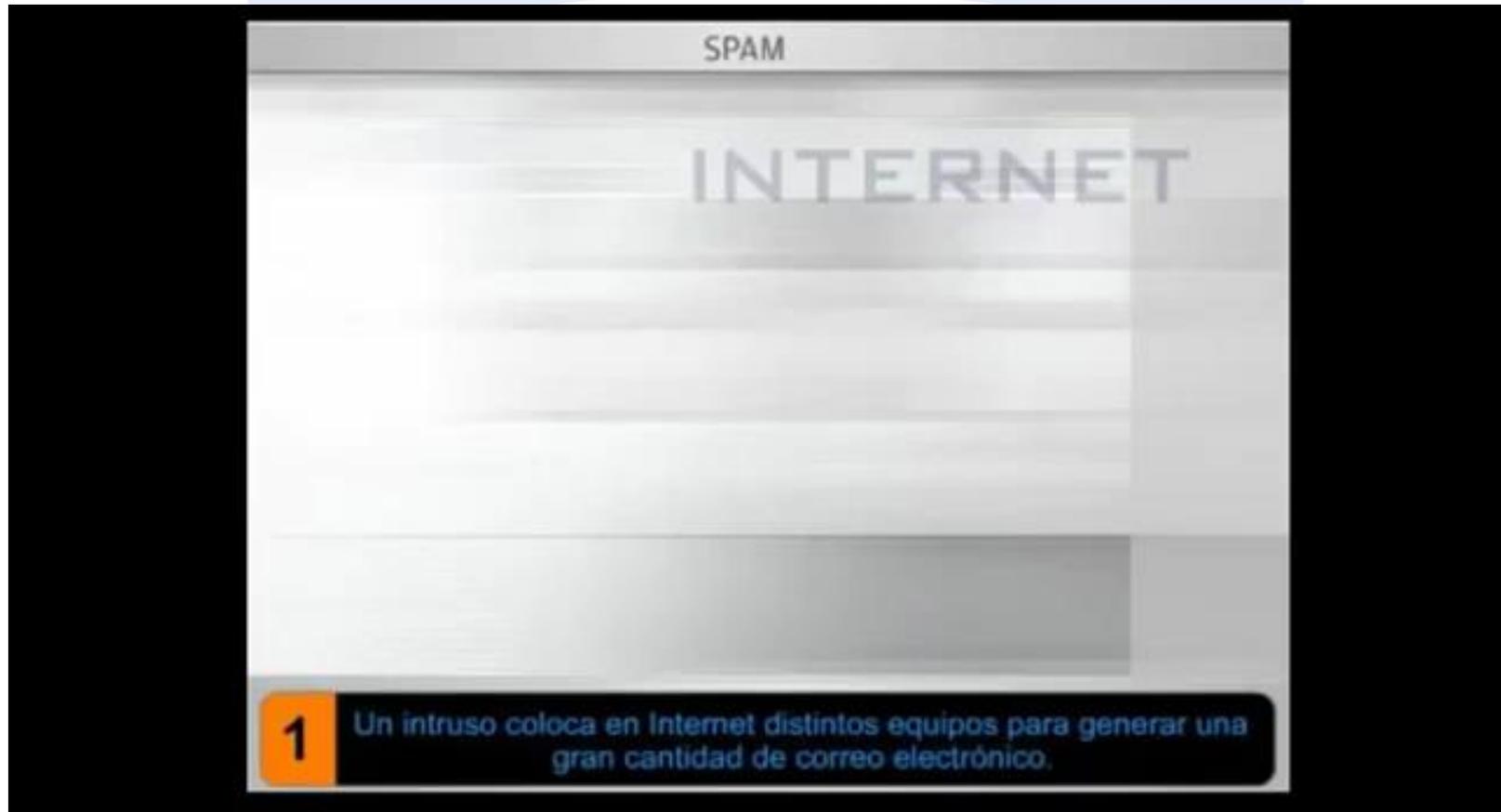
Más recomendaciones

- Sospechar de: problemas técnicos, promociones, premios o actualización de datos.
- Nunca proporcionar: nombre de usuario, contraseñas, número de tarjeta de crédito vía telefónica o por correo.
- Verificar el nombre, apellido del remitente: el phishing frecuentemente carece de estos elementos.
- No llenar información personal en formularios de correos.

Más recomendaciones

- No seguir enlaces incluidos en correos de dudosa precedencia: mejor visitar directamente la páginas web.
- Antes de proporcionarle cualquier dato, verificar que se visita un sitio web seguro.
- Mantener al navegador web actualizado.

Spam



1

Un intruso coloca en Internet distintos equipos para generar una gran cantidad de correo electrónico.

Consejo práctico



ACONSEJA



Reporta spam o abusos

Cada mensaje malicioso o spam en las redes sociales es parte de un ataque mayor, puedes detenerlos o evitar que se extiendan cuando reportas a tiempo.



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

Más recomendaciones

- No enviar cadenas: generalmente son algún tipo de engaño.
- Muchos destinatarios: Con Copia Oculta (CCC), evita ver y obtener direcciones de correo.
- No publicar el correo electrónico en sitios web, foros y conversaciones: facilita su obtención a quienes envían spam.
- No responder mensajes de remitentes desconocidos: confirma la dirección de correo, desencadenando más spam.
- Contar con varias cuentas de correo: laboral, personal y contacto público (distribución masiva).

Ransomware

Programa que impide acceder a los archivos o a los equipos hasta que se paga un rescate.

Your personal files are encrypted by CTB-Locker.

Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press 'View' to view the list of files that have been encrypted.

Press 'Next' for the next page.

WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.

View **95:40:08** Next >>

Malware UNAM-CERT

Consejo práctico

Evita que el ransomware te afecte

Tener respaldos te asegura que jamás tendrás que pagar un rescate si tu información es secuestrada por un ransomware.



www.seguridad.unam.mx



ACONSEJA



DGTIC

Más recomendaciones

- Realizar copias de seguridad (y probarlas).
- No seguir ningún enlace proporcionado vía correo electrónico que sea sospechoso.
- No pagar el rescate: no hay garantía de que el atacante descifre la información después de pagar.

DoS

Ataque que intenta sobrecargar o bloquear un servicio para que los usuarios legítimos no puedan usarlo. Variante: cuando el ataque se realiza de forma distribuida: DDoS.



Recomendaciones

- Identificar las direcciones IP causantes de ataque y bloquearlas.
- Usar otros servidores como balanceadores de carga distribuyendo así el trabajo del servidor crítico.
- Colocar una versión ligera del sitio atacado: ayuda a reducir el tiempo de respuesta y minimizar la carga de procesamiento del servidor.

Recomendaciones generales

- Validar que el dominio del sitio a visitar sea el deseado.
- Usar un correo electrónico alternativo para registro en sitios poco confiables.
- Mantener actualizados dispositivos y software que se emplean.

Recomendaciones generales

- No confiar en todo lo que dice internet.
- Configurar la privacidad en redes sociales, no responder ni compartir encuestas del tipo: 10 preguntas para encontrar al amor de tu vida.
- Evitar las descargas ilegales de cualquier tipo.

Reporta

- Correos de contacto para reportar:
- phishing@cert.unam.mx
- incidentes@cert.unam.mx

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

