Seguridad en cómputo

Ing. Angie Aguilar Domínguez

Coordinación de Seguridad de la Información

UNAM-CERT

UNAM CERT

DGTIC

DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Agenda

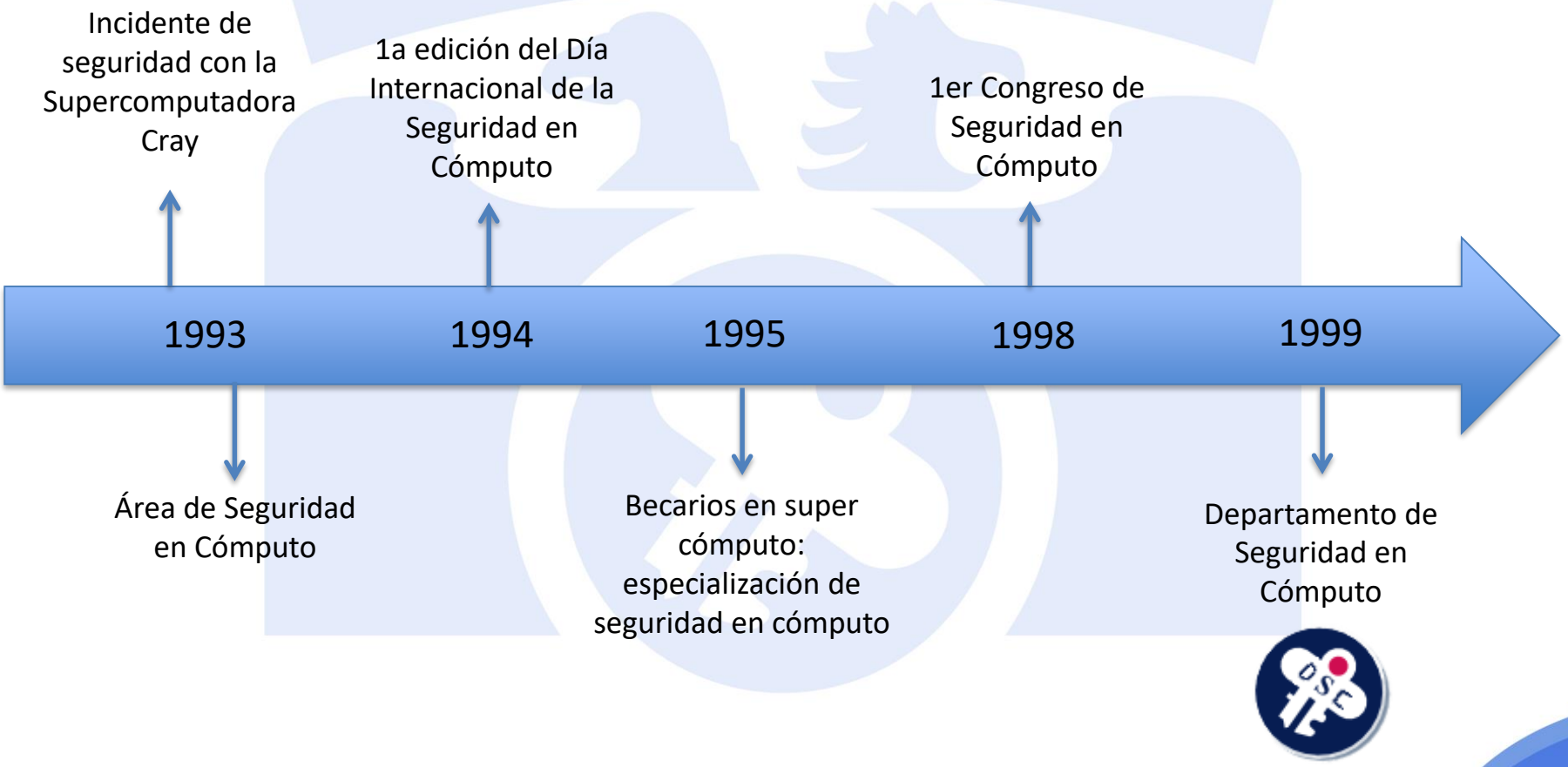
- UNAM-CERT y su historia
- Principales problemas actuales
- Consejos de seguridad

DGTIC

Coordinación de Seguridad de la Información/UNAM-CERT

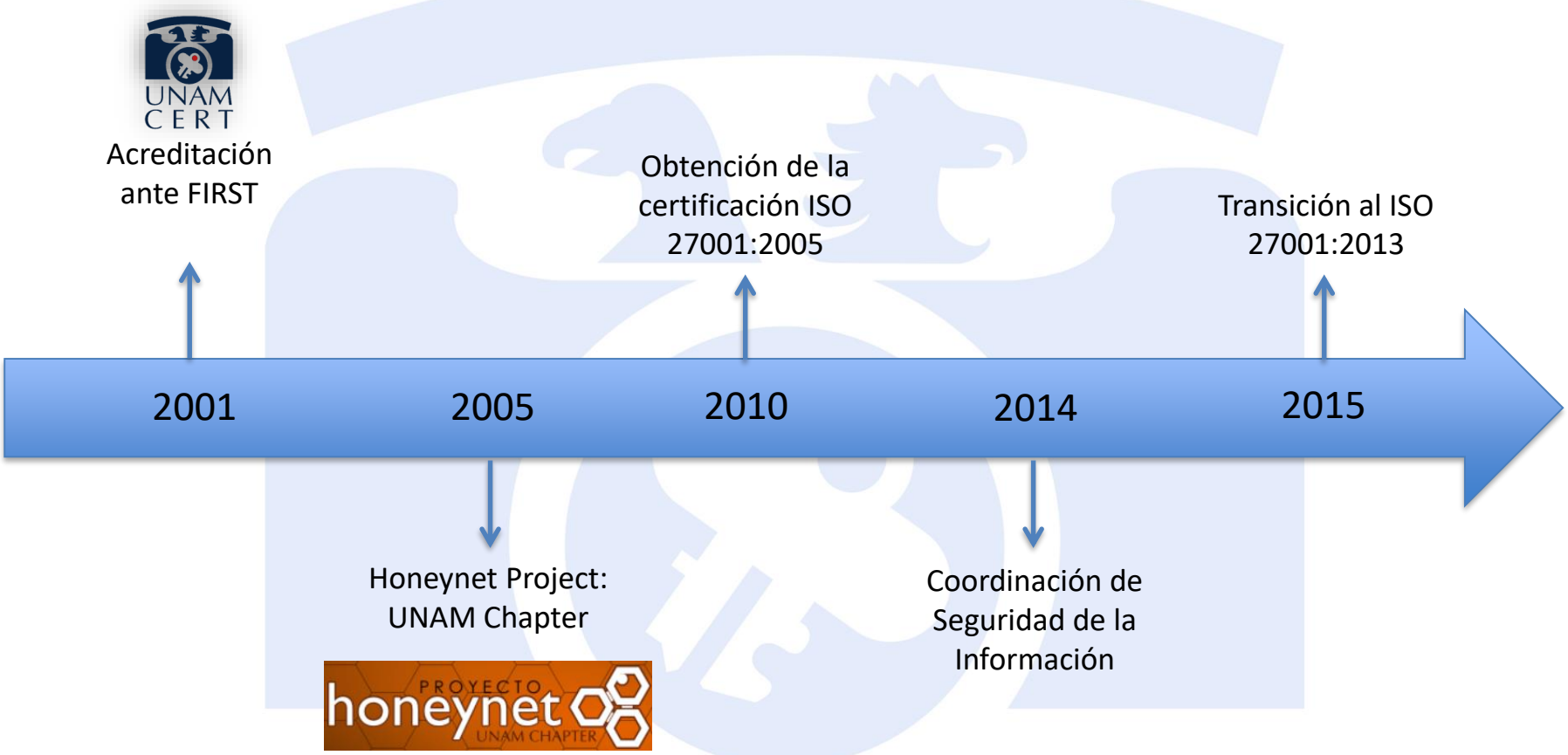
Contribuir al desarrollo de la UNAM, a través de la prestación de servicios especializados, la formación de capital humano y el fomento de la cultura de seguridad de la información.

Historia



DGTIC

Historia



DGTIC

Colaboración

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…

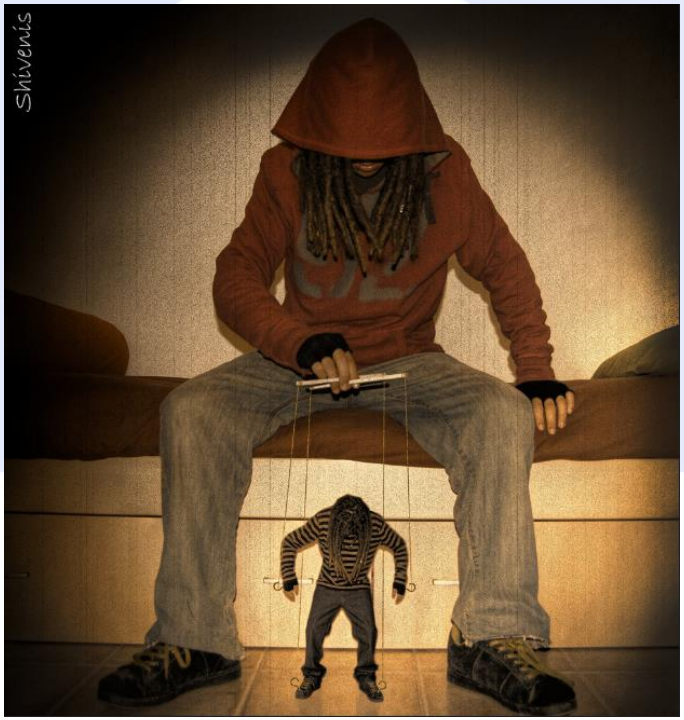
¡Cuidado! Circula nuevo fraude con mensaje falso de "Bancomer"

El cibercrimen impactó a 33 millones de mexicanos en 2017

DGTIC

Ingeniería Social

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



Consejo práctico

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.

DGTIC

Phishing

DGTIC

Consejo práctico

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

Correos electrónicos no deseados que llegan de forma masiva no solicitada.

Correo SPAM: Tú nueva contraseña de FaceBook !!!

Al comienzo de la semana, recibimos la notificación de un correo spam que se está propagando de una forma alarmante y aún el día de hoy, capturamos varios de estos correos, los cuales contienen un archivo adjunto, llamado **New_Password_IN75652.zip.**

```
----- Mensaje reenviado de sign@facebook.com -----
   Fecha: Mon, 11 Apr 2011 09:45:53 -0400
      De: Service of Facebook <sign@facebook.com>
Responder-A: Service of Facebook <sign@facebook.com>
 Asunto: ***SPAM*** Facebook Support. Personal data has been changed! ID66106
    Para: [redacted]

 Dear user of FaceBook.

   Your password is not safe!
   To secure your account the password has been changed automatically.

   Attached document contains a new password to your account and detailed
   information about new security measures.

   Thank you for attention,
   Your Facebook
```

Spam


SPAM
INTERNET
1
Un intruso coloca en Internet distintos equipos para generar una gran cantidad de correo electrónico.

Consejo práctico

DGTIC

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.

DGTIC

Consejo práctico

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 alterno 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

DGTIC

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