Seguretat Informatica (SI)

Tema 1. Introducción

Davide Careglio

Fuentes: Jordi Nin, "Introduction", Computer Security, 2014
A. Rodriguez, "Introduction", Computer Security, 2018

Temario

- Tema 1. Introducción
- Tema 2. Criptografía
- Tema 3. Infraestructura PKI

- Tema 4. Seguridad en la red
- Tema 5. Seguridad en las aplicaciones

- Tema 6. Seguridad en los sistemas operativos
- Tema 7. Análisis forense

Temario

- Tema 1. Introducción
- Tema 2. Criptografía
- Tema 3. Infraestructura PKI

- Tema 4. Seguridad en la red
- Tema 5. Seguridad en las aplicaciones

- Tema 6. Seguridad en los sistemas operativos
- Tema 7. Análisis forense

Tema 1. Introducción

- Índice
  - La ciberseguridad
  - Objetivos
  - Amenazas
  - Organización
  - Personas
  - Tecnología de la información

Tema 1. La Ciberseguridad

- Recomendación ITU–T X.1205
  - La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno.
  - Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno.
  - La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno.

Tema 1. Introducción

- ¿Por qué necesitamos ciberseguridad?

  https://www.youtube.com/watch?v=nBjg2TN6D2g
  (minuto 4:38)

Tema 1. Objetivos

- ¿Que se quiere proteger?

Tema 1. Objetivos

- ¿Que se quiere proteger?
- Los datos
  - **Confidencialidad**: solo pueden acceder a los datos los que tienen los privilegios necesarios
  - **Integridad**: hay que asegurar que solo los que tienen estos privilegios puedan alterar, eliminar o añadir datos
  - **Disponibilidad**: los datos deben ser accesibles y disponibles a los usuarios

Tema 1. Objetivos

- ¿Que se quiere proteger?
- Los datos
  - **Confidencialidad**: solo pueden acceder a los datos los que tienen los privilegios necesarios
  - **Integridad**: hay que asegurar que solo los que tienen estos privilegios puedan alterar, eliminar o añadir datos
  - **Disponibilidad**: los datos deben ser accesibles y disponibles a los usuarios
- Los recursos
  - **Daños** o **desconfiguración** de los recursos corporativos
  - **Autentificación**: solo los autorizados pueden acceder a los recursos (y datos)
- La reputación

Tema 1. Ejemplo

- España asume la Presidencia de la Unión Europea el 4/1/2010
- La presidencia tenía previsto invertir 11,9M€ en la seguridad de su web
- Pero

Tema 1. Ejemplo

- España asume la Presidencia de la Unión Europea el 4/1/2010
- La presidencia tenía previsto invertir 11,9M€ en la seguridad de su web
- Pero

Tema 1. Ejemplo

- En este caso, la web no fue realmente hackeada
- Se aprovechó de un fallo de seguridad (muchas veces mal considerado de bajo riesgo), para que el cliente viera algo diferente de los esperado
- Fallo de seguridad conocido como Cross-Site Scripting (XSS)
- En este caso especifico, un enlace hacia la web de la Presidencia tenía incluido directamente unos parámetros de búsqueda que daba como resultado esta imagen de Mr. Bean
  - http://www.eu2010.es/en/resultadoBusqueda.html?query=%3Cscript%3Edocument.write%28%27%3Cimg%20src%3D%22http%3A%2F%2Fblog.tmcnet.com%2Fblog%2Ftom-keating%2Fimages%2Fmr-bean.jpg%22%20%2F%3E%27%29%3C%2Fscript%3E&index=buscadorGeneral_en
- Los responsable de la web de la Presidencia deberían haber bloqueado estos tipos de conexiones

Tema 1. Ejemplo

- Si la intención no era robar/modificar datos
- O denegar el servicio
- ¿Que es lo que se buscaba entonces con este ataque?

EL MUNDO | Unión Europea
Eurocámara
Líder mundial en español | Lunes 04/01/2010. Actualizado 19:55h.

Portada España Mundo Europa Opinión Deportes Economía Cultura Ciencia Salud Tecnología Comuni

Edición ESPAÑA | Madrid Barcelona Baleares C. Valenciana Castilla y León País Vasco Andalucía

Enviar a un amigo
Valorar
Imprimir
En tu móvil
Rectificar
Pásalo

Fallo de seguridad

Mr. Bean 'se cuela' en la web oficial de la presidencia

Mr Bean saluda a los internautas en la web de la presidencia española de la UE

BBC | BBC Account | Menú

NEWS | MUNDO

Noticias | América Latina | ¿Hablas español? | Internacional | Economía | Tecnología | Cien

ABC ESPAÑA

España ▾ Internacional Economía ▾ Sociedad Madrid ▾ Familia ▾

ABC ESPAÑA Casa Real Aragón Canarias Castilla y León Cataluña

POLÍTICA OPINIÓN MEMORIA PÚBLICA MUJER

Mr. Bean se 'cue presidencia e

Unos hackers se saltan los sistemas de seguridad, bloque

OS SOCIEDAD ESPAÑA MUNDO

'Mr Bean', pres presidencia

Reuters

AGENCIAS

Mr Bean, el conocido personaje de humor interpretac

Cuatro/CNN+ • 04/01/2010 - 19:05 h.

El Gobierno español ha abierto una **investigación interna** después de que un

El nuevo presidente europeo es... Mr. Bean

Redacción
BBC Mundo

5 enero 2010 | Compartir

La Unión Europea (UE) estrenó con el año nuevo la sede de la presidencia de turno de la organización. Como viene siendo habitual, en el sitio web del país anfitrión apareció el mensaje del mandatario que recibirá a sus homólogos en las grandes reuniones. En esta ocasión, ese "líder" fue Mr. Bean, el popular personaje de humor.

En España muchos bromean con el supuesto parecido entre Zapatero y Mr. Bean.

Una foto del torpe Mr. Bean, encarnado por el actor británico

El Gobierno español ha abierto una investigación interna después de que un 'hacker' consiguiera colgar en el sitio web de la presidencia una foto del popular personaje

Mr. Bean 'hackea' la web de la presidencia española de la UE

Tema 1. Ejemplo

- Si la intención no era robar/modificar datos
- O denegar el servicio
- ¿Que es lo que se buscaba entonces con este ataque?

- La reputación
  - De la Presidencia
  - Y en segunda medida, de la empresa encargada de crear y gestionar la web (Telefónica)

Tema 1. Ejemplo

- Si la intención no era robar/modificar datos
- O denegar el servicio
- ¿Que es lo que se buscaba entonces con este ataque?

- La reputación
  - De la Presidencia
  - Y en segunda medida, de la empresa encargada de crear y gestionar la web (Telefónica)

- Y de paso también la disponibilidad
  - La web estuvo no disponible durante varias horas seguidas hasta las 13.00 del mismo día

Tema 1. Ejemplo

- Las nuevas tecnologías muchas veces se comercializan sin pensar en los riesgos

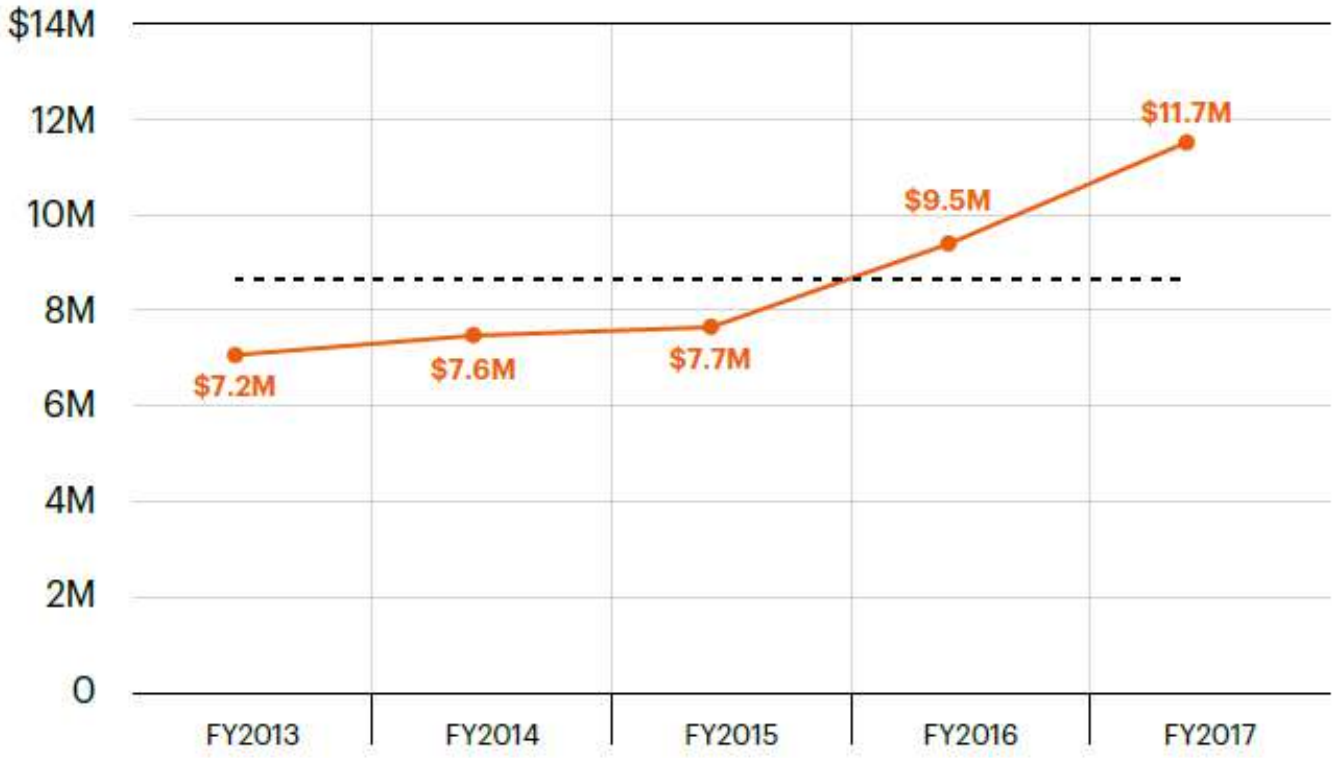
Tema 1. Ejemplo

- Las nuevas tecnologías muchas veces se comercializan sin pensar en los riesgos

Tema 1. Ejemplo

Tema 1. Costes de la ciberseguridad

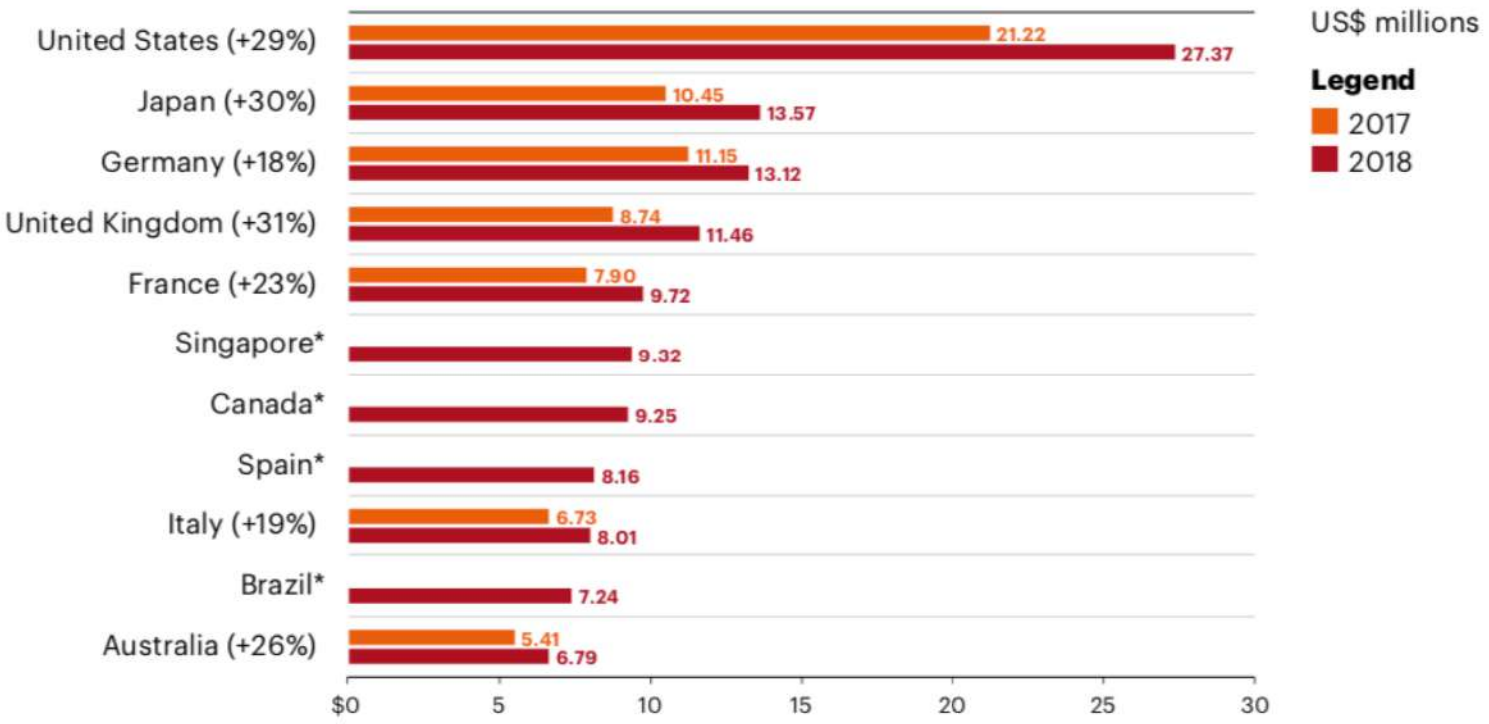
- Gasto medio de cada empresa
  - Estudio hecho sobre 355 empresas



Fuentes: 2017 Cost of cybercrime study, Ponemon Institute LLC, 2017
9th Annual cost of cybercrime study, Accenture, 2019

Tema 1. Costes de la ciberseguridad

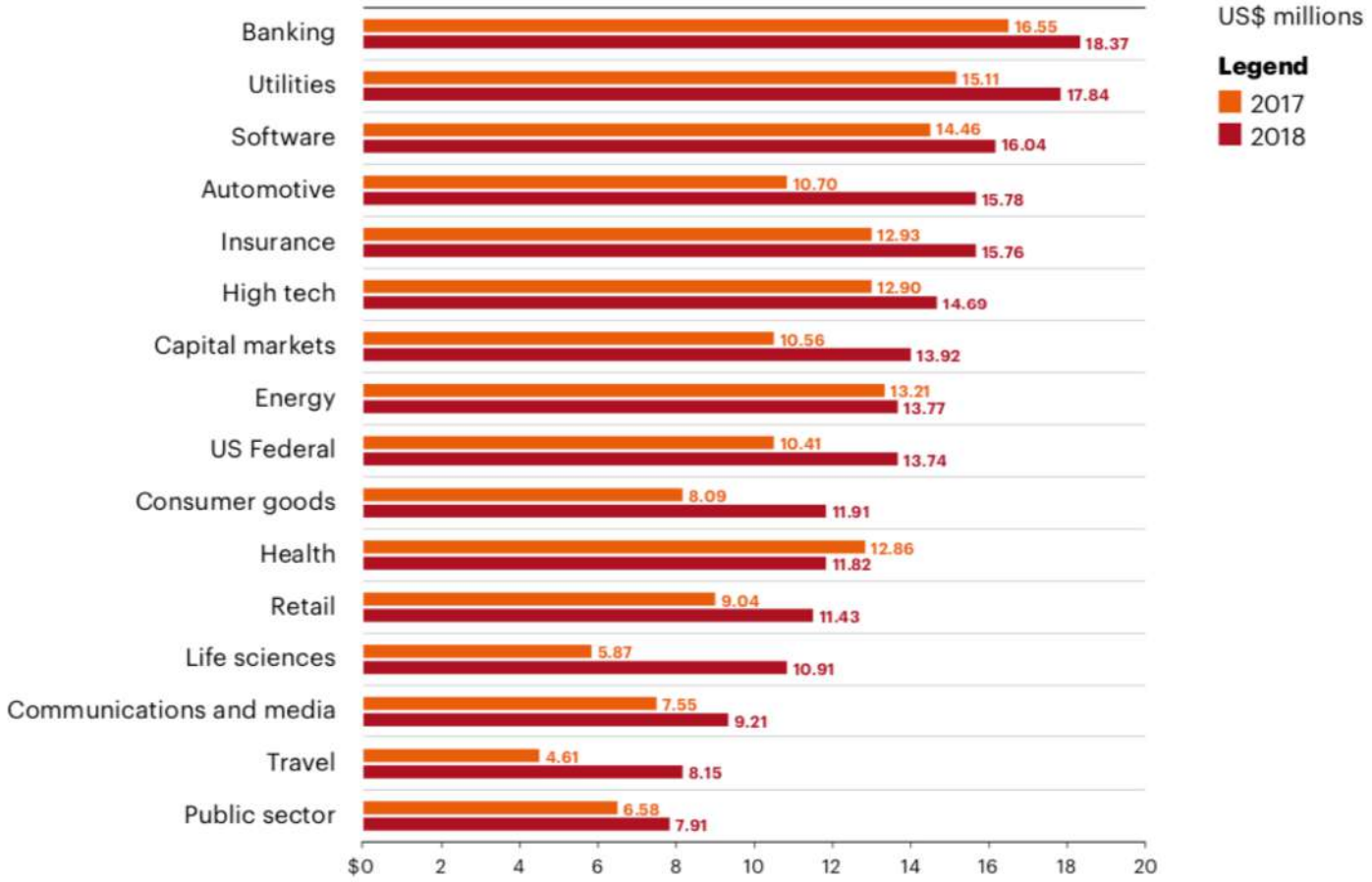
- Gasto medio según el país



Fuente: 9th Annual cost of cybercrime study, Accenture, 2019

Tema 1. Costes de la ciberseguridad

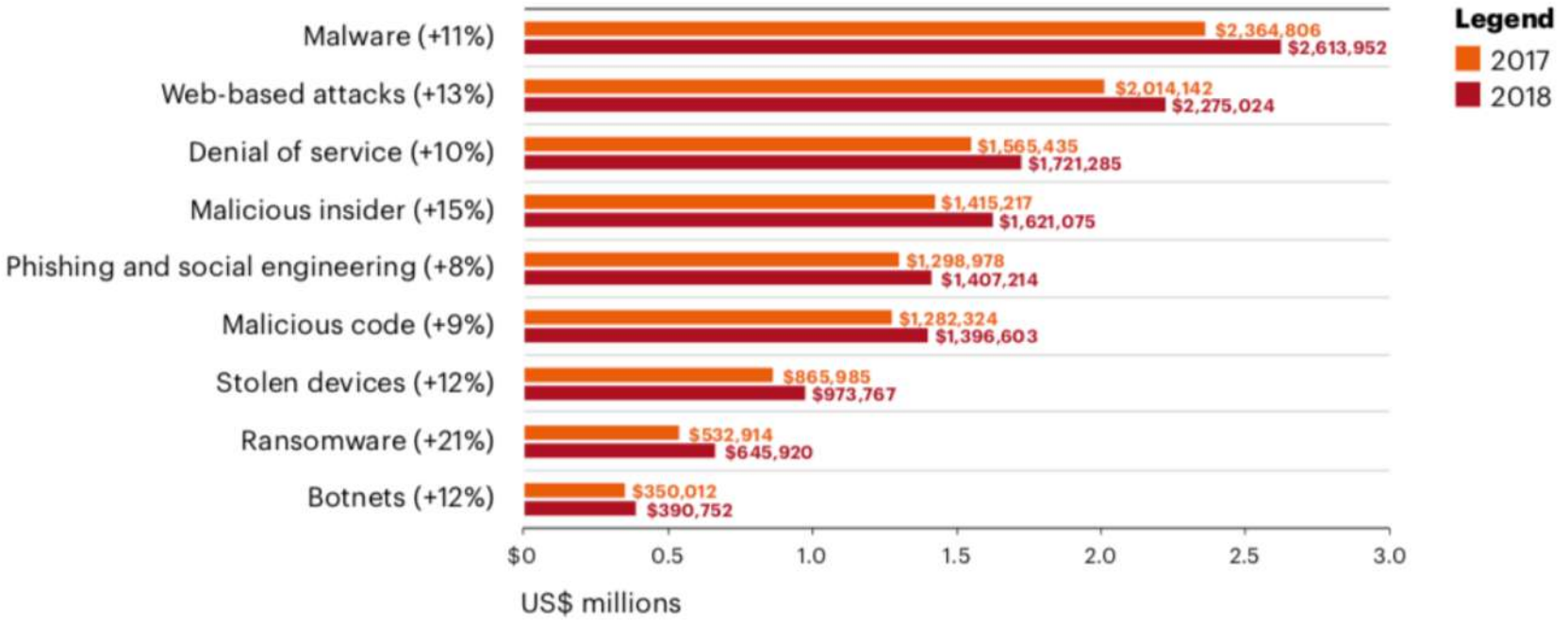
- Gasto medio según el sector



Fuente: 9th Annual cost of cybercrime study, Accenture, 2019

Tema 1. Costes de la ciberseguridad

- Tipos de ataque



Fuente: 9th Annual cost of cybercrime study, Accenture, 2019

Tema 1. Amenazas

- ¿Por qué?

Tema 1. Amenazas

- ¿Por qué?

- Antes: "bad boys"
  - Demostrar que eran los mejores
  - Ideología

Tema 1. Amenazas

- ¿Por qué?

- Antes: "bad boys"
  - Demostrar que eran los mejores
  - Ideología

- Ahora: crimen organizado
  - Dinero

Tema 1. Amenazas: ¿qué buscan?

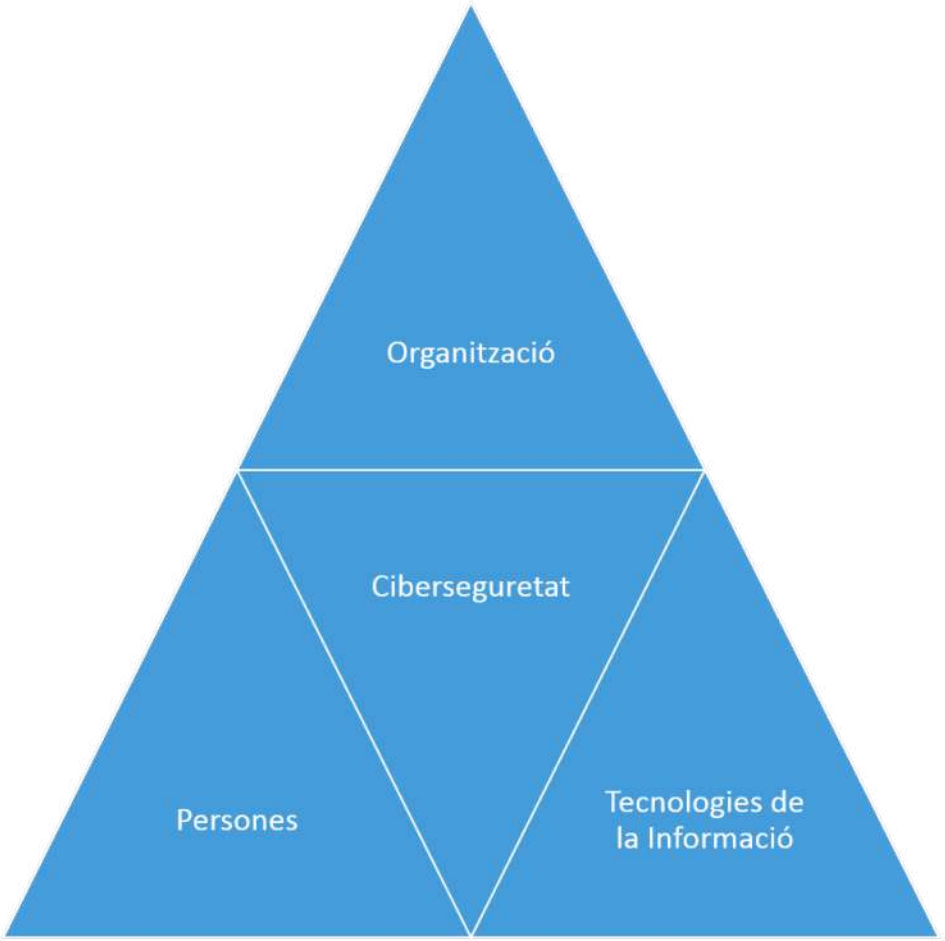
- Nombres de usuario y contraseña (acceso):
  - Banca (robo o transferencia de dinero)
  - iCloud, Google Drive, Dropbox (acceso a datos confidenciales)
  - Amazon (obtener bienes en nuestro nombre)
  - UPS, DHL (enviar bienes robados en nuestro nombre)
  - etc. . .
- Recolección de direcciones de correo electrónico (venta)
  - Nombres, correos, números de teléfono
  - Correos personales o del trabajo
- Bienes virtuales (venta)
  - Personajes de juegos on-line
  - Licencias de software
- Botnet (realizar acciones maliciosas)
  - Envío de spam
  - DDoS

Tema 1. Amenazas: ¿qué buscan?

- Suplantación de identidad (fraude o venta)
  - Cuentas de Facebook, Twitter, Linkedin, etc.
  - Cuentas de correo
  - Cuentas de Skype u otros servicios de mensajería instantánea
- Servidores (realizar acciones ilícitas)
  - Alojar webs de phishing o de distribución de herramientas de ataques
  - Distribución de pornografía o material protegido por derechos de autor
- Finanzas (Información, venta)
  - Información sobre tarjetas de crédito
- Extorsión o chantaje
  - Realizar fotografías con la webcam y pedir dinero (bitcoins)
  - Cifrar los datos del disco y pedir dinero para recuperarlo
- Y mucho mas…

Tema 1. La Ciberseguridad

- Elemento central en las organizaciones



Tema 1. Organizaciones y normativas

- Existen normativas
  - General Data Protection Regulation (EU) 2016/679 (GDPR)
  - Esquema Nacional de Seguridad (ENS) BOE-A-2010-1330
- Definen conceptos útiles para gestionar la ciberseguridad
  - Chief Information Security Officer (CISO)
  - Data Protection Officer (DPO)
  - Política de seguridad
  - Remedios, responsabilidad y sanciones
  - Derechos y obligaciones
  - …

Tema 1. Organizaciones: políticas de seguridad

- Aprobada y promovida por la dirección
  - Colaboración activa de TI en su definición (CISO)
- Debe incluir (cuanto más, mejor):
  - Un inventario de activos a proteger (físicos o lógicos)
  - Una valoración del riesgo, por ejemplo

$$Riesgo = Probabilidad \times Impacto$$

  - En función del "que nos podamos permitir" definir:
    - Protocolos de prevención
    - Protocolos de actuación
    - Protocolos de recuperación

Tema 1. Personas

- ¿?

Tema 1. Personas

- Ejemplo
  - Descifrar Enigma
  - 158,962,555,217,826,360,000 diferentes maneras de configurar Enigma
  - Unbreakable en los 40

Tema 1. Personas

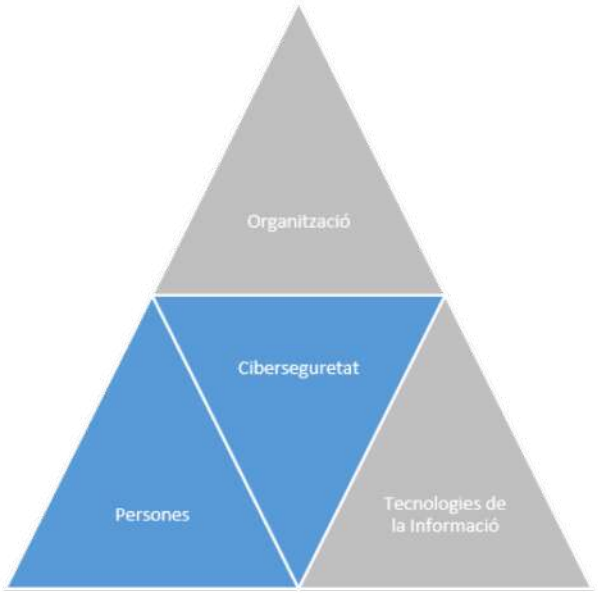
- Ejemplo
  - Descifrar Enigma
  - 158,962,555,217,826,360,000 diferentes maneras de configurar Enigma
  - Unbreakable en los 40

  - Pero …

Tema 1. Personas

Tema 1. Personas

- A menudo el eslabón más débil
  - Ataques dirigidos
- Hay que fortalecer este “eslabón"
  - Concienciación
  - Formación
  - Política de seguridad
    - Contraseñas
    - Permisos
    - …



Tema 1. Tecnología de la información

- El entorno de trabajo debe proporcionar unas condiciones adaguadas de seguridad
  - Estas condiciones deben estar definidas en la política de seguridad
    - Con la asignación de recursos correspondientes
- Es responsabilidad del departamento de TI velar por mantener la seguridad en los sistemas de información
- A menudo la seguridad va en contra de la usabilidad

Temario

- ~~Tema 1. Introducción~~
- Tema 2. Criptografía
- Tema 3. Infraestructura PKI

- Tema 4. Seguridad en la red
- Tema 5. Seguridad en las aplicaciones

- Tema 6. Seguridad en los sistemas operativos
- Tema 7. Análisis forense

Seguretat Informatica (SI)

Tema 1. Introducción

Davide Careglio

Fuentes: Jordi Nin, "Introduction", Computer Security, 2014
A. Rodriguez, "Introduction", Computer Security, 2018