

# Seguretat Informatica (SI)

Tema 1. Introducción

Davide Careglio

# 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 multimedia, 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

Bienvenido  
Benvingut  
Welcome  
Ong elom

Presidencia Española *eu* trio.es

A A A Contact

HOME THE SPANISH PRESIDENCY AGENDA DOCUMENTS & NEWS THE EUROPEAN UNION SPAIN IN FOCUS PRESS

You are here : Home

Resultados de búsqueda

!! No se han encontrado Resultados !!

Error

org.openoms.search.CntsSearchException: Búsqueda de "query:"

Agenda

JANUARY, 2010

Sun	Mon	Tue	Wed	Thu	Fri	Sat
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

See the calendar for:

European Council

cultura

# 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 lo esperado
- ▶ Fallo de seguridad conocido como Cross-Site Scripting (XSS)
- ▶ En este caso específico, 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](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 responsables 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?

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**

**ABC** ESPAÑA

España ▾ Internacional Economía ▾ Sociedad Madrid ▾ Familia ▾

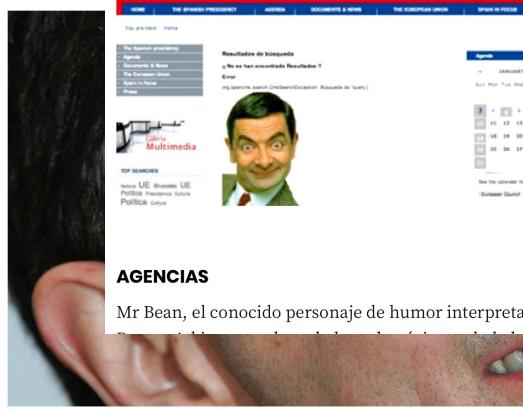
ABC ESPAÑA Casa Real Aragón Canarias Castilla y León Cataluña

POLÍTICA OPINIÓN MEMORIA PÚBLICA MUJER CL

Mr. Bean

OS SOCIEDAD ESPAÑA MUNDO ▾

**'Mr Bean', pres  
presidencia**



Cuatro/CNN+ • 04/01/2010 - 19:05 h.

14

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

**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

**El nuevo presidente europeo es... Mr. Bean**

Redacción  
BBC Mundo

5 enero 2010

f m t e 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.**

Una foto del torpe Mr. Bean, encarnado por el actor británico Rowan Atkinson, quinto en sucesión.

El Gobierno español ha abierto una investigación interna después de que un 'hacker' consiguiera



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

I - FÓRMULA 1 Y 0  
onfiran el  
curso de McLaren

REGISTR

icia



Mr. Bean 'haccea' 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

Hackers have taken control of a baby monitor to support YouTuber PewDiePie

The super-hacker who hacked the Chromebook of a US senator has been identified

Even though he's been arrested, the hacker behind the massive Equifax breach is still at large

## NEWS

### IoT botnet crushes 100,000 devices

Researchers have discovered a botnet that can conduct DDoS attacks against 50,000 HTTP servers



Sections

The Washington Post  
Democracy Dies in Darkness

Get 1 year for \$40



'I'm in your baby's room': A hacker took over a baby monitor and broadcast threats, parents say



A hacker manipulated a Nest camera that Ellen and Nathan Rigney use to monitor their 4-month-old son on Dec. 17 in Houston. (KPRC-TV)



By Catalin Cimpanu for Zero Day | September 9, 2019 -- 08:27 GMT (09:27 BST) | Topic: Security

50%

▶

A few hours ago, Toyota Australia has released an official statement stating that the digital assets of the car making company were targeted by a cyber attack recently. However, the world renowned car making company disclosed that none of its employee data or customer information was compromised in the incident.



en los

millions of

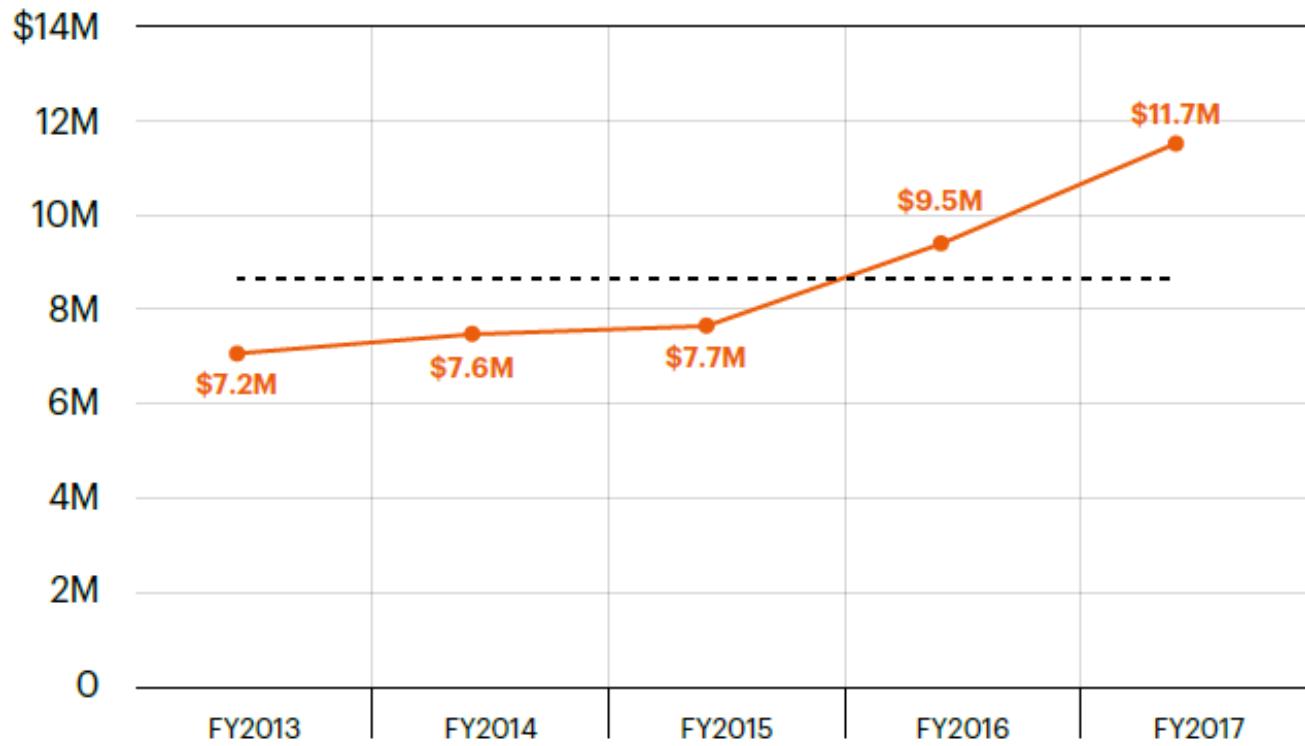
Google Chromecast devices have exposed various sensitive



## power grid swallows

# Tema 1. Costes de la ciberseguridad

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



**\$11.7m**  
Average cost of cybercrime  
in 2017

↓

**\$13.0m**  
Average cost of cybercrime  
in 2018

**+12%**  
Increase in the last year

**=72%**  
Increase in the last 5 years

Fuentes: 2017 Cost of cybercrime study, Ponemon Institute LLC, 2017,

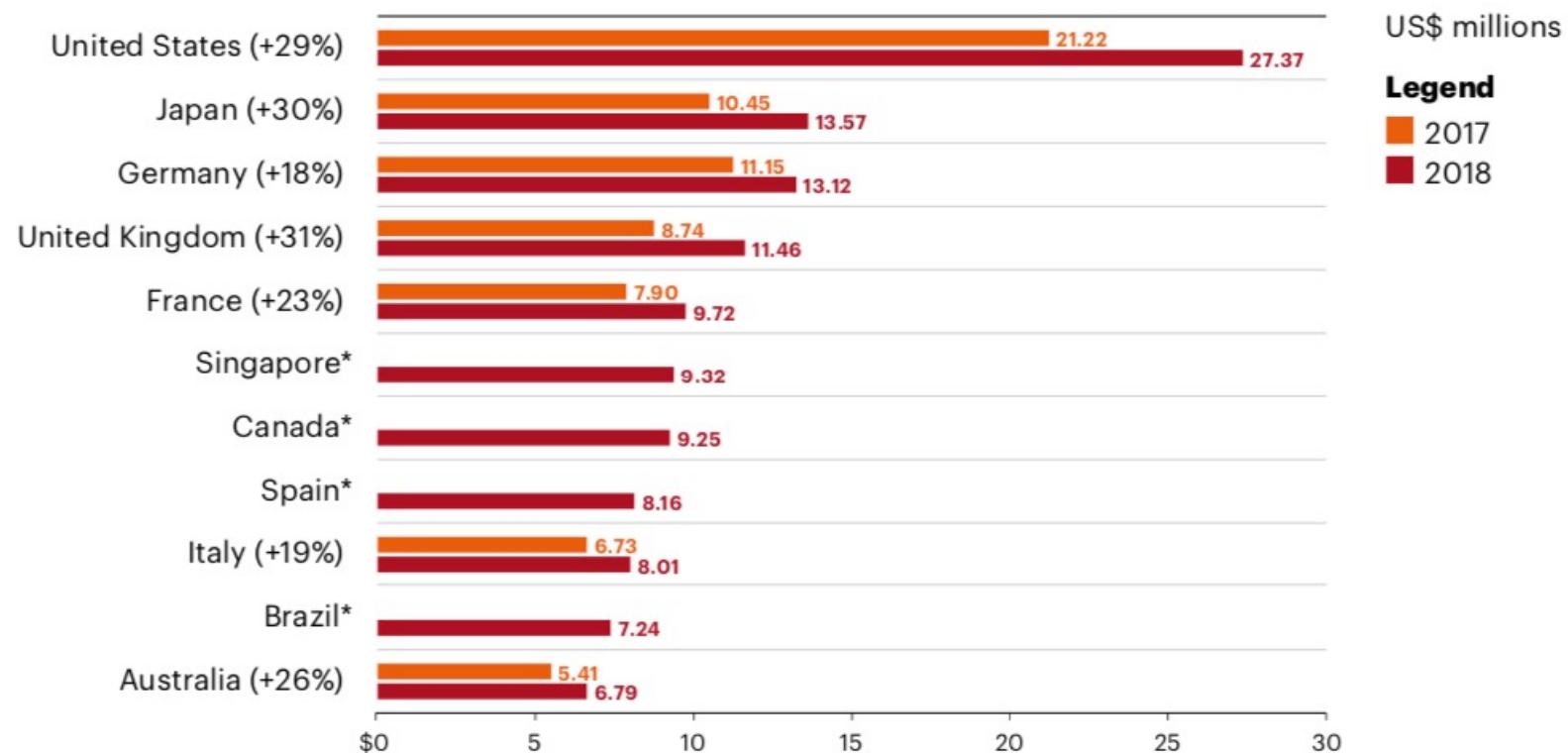
[https://www.accenture.com/\\_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf#zoom=50](https://www.accenture.com/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf#zoom=50)

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

[https://www.accenture.com/\\_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50](https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50)

# Tema 1. Costes de la ciberseguridad

## ► Gasto medio según el país

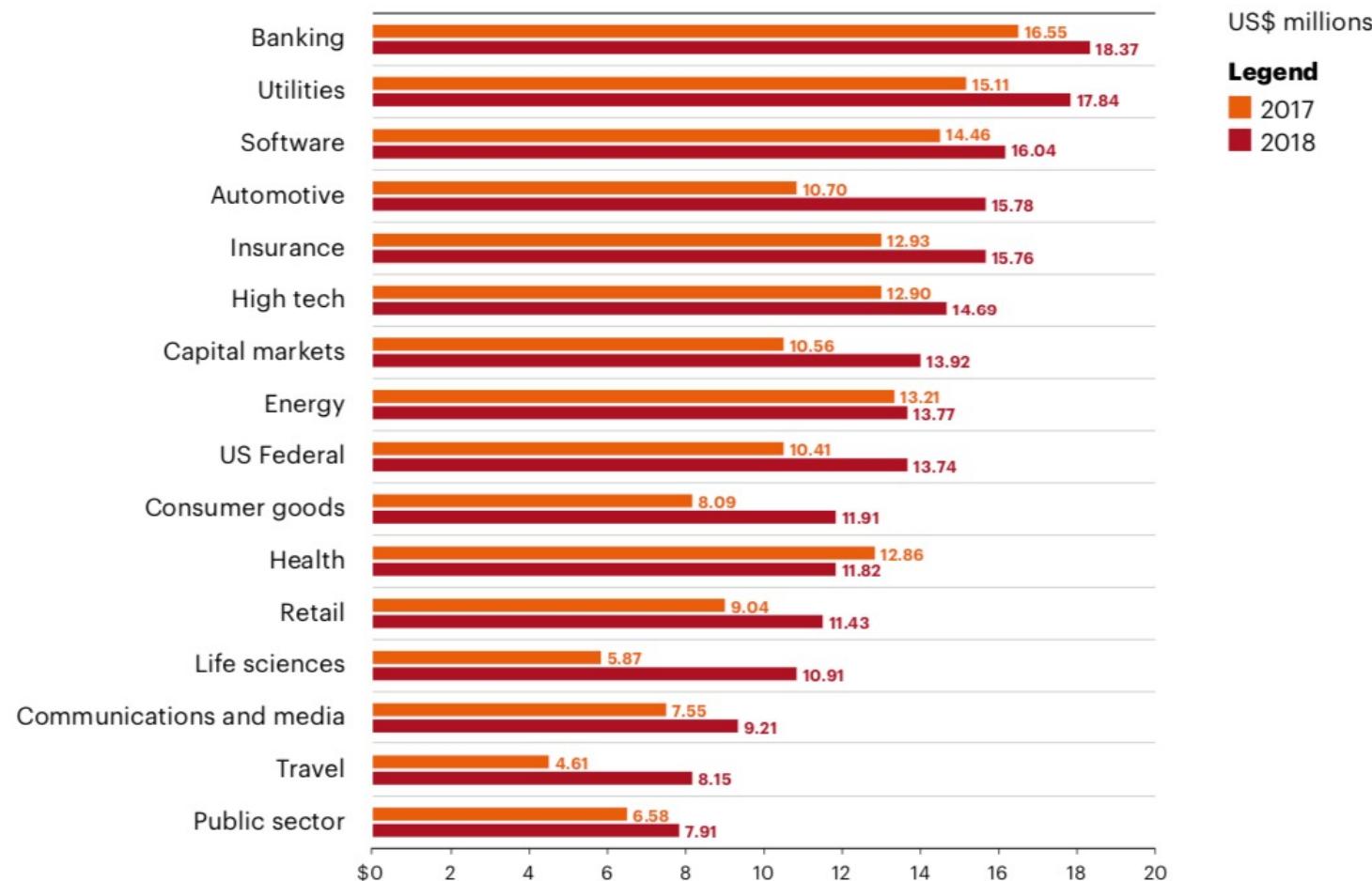


Fuentes: 9th Annual cost of cybercrime study, Accenture, 2019,

[https://www.accenture.com/\\_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50](https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50)

# Tema 1. Costes de la ciberseguridad

## ▶ Gasto medio según el sector

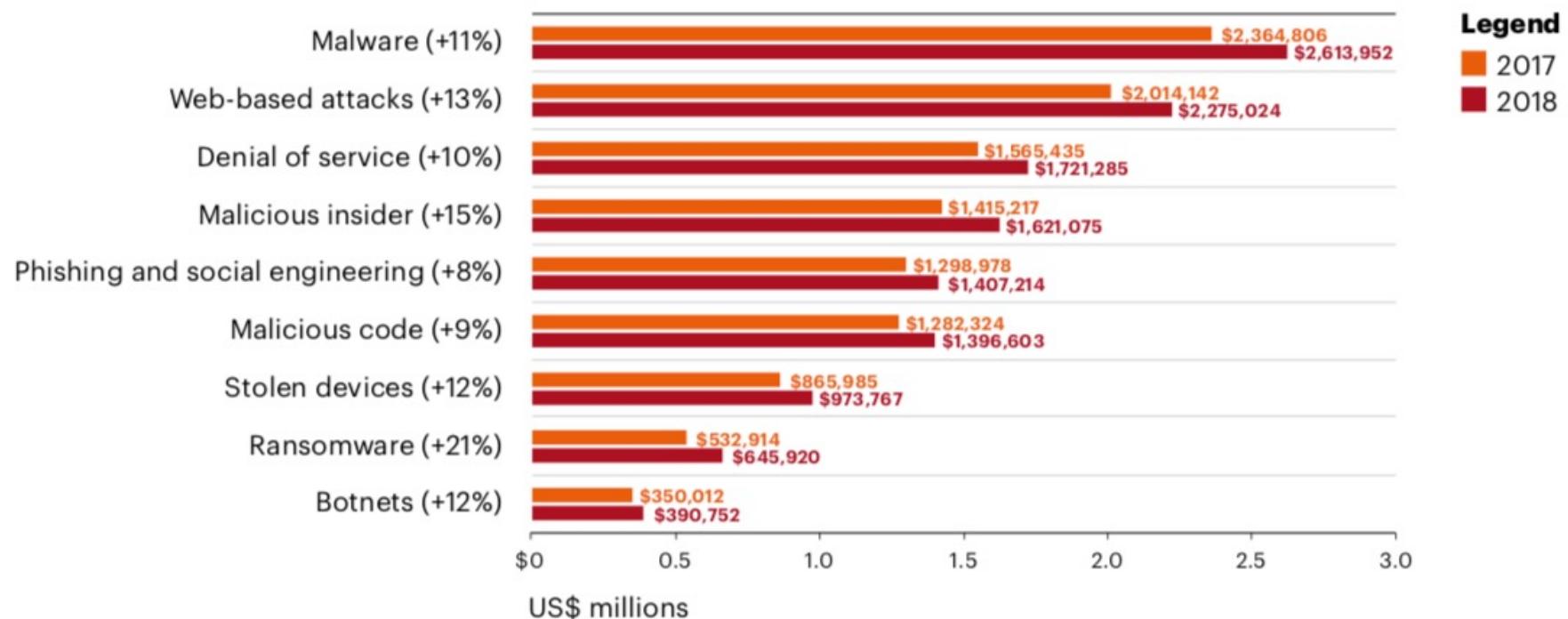


Fuentes: 9th Annual cost of cybercrime study, Accenture, 2019,

[https://www.accenture.com/\\_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50](https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50)

# Tema 1. Costes de la ciberseguridad

## ▶ Tipos de ataque



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

[https://www.accenture.com/\\_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50](https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50)

# 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?

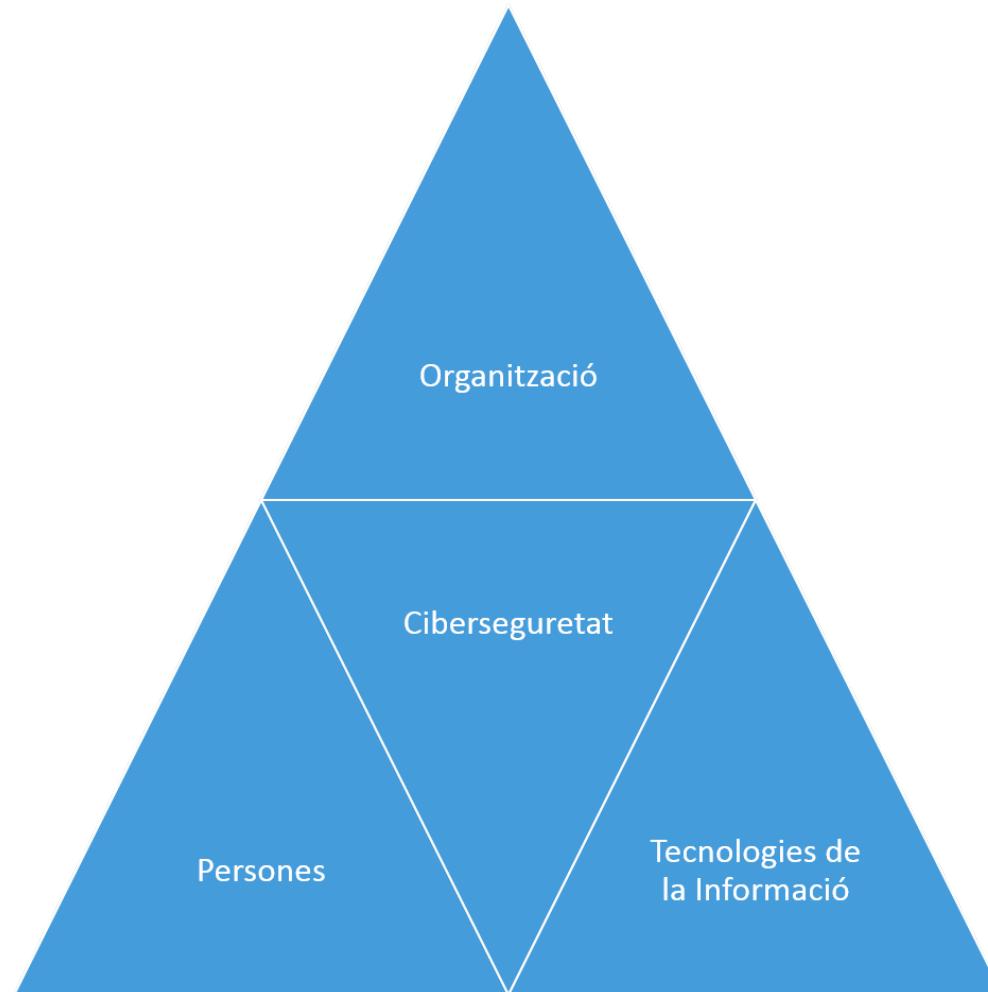
---

- ▶ **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

---

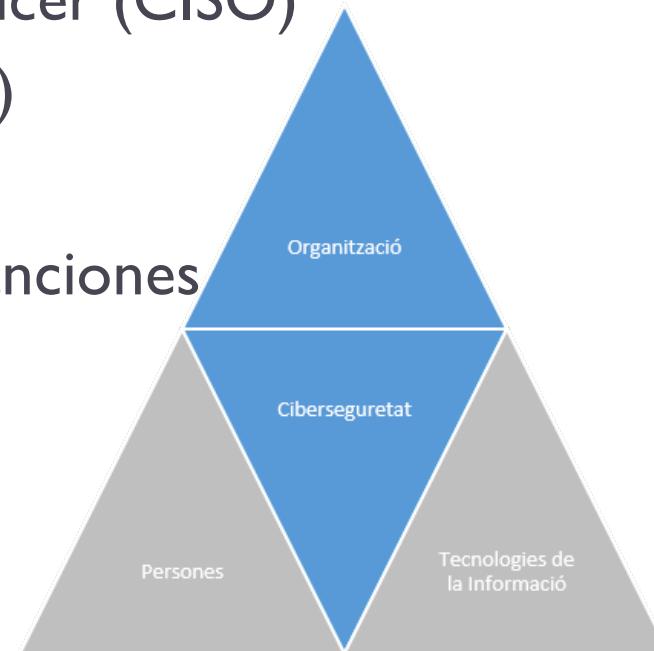
- ▶ Elemento central en las organizaciones



# 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 y normativas

## 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

$$\text{Riesgo} = \text{Probabilidad} \times \text{Impacto}$$

- ▶ En función del “que nos podamos permitir” definir:
  - ▶ Protocolos de prevención
  - ▶ Protocolos de actuación
  - ▶ Protocolos de recuperación

# Tema 1. Organizaciones y normativas

---

- ▶ ¿Es realmente importante tener algo tan organizado?

# Tema 1. Organizaciones y normativas

---

- ▶ ¿Es realmente importante tener algo tan organizado?

## 2020 United States federal government data breach

In 2020, a major cyberattack suspected to have been committed by a group backed by the Russian government penetrated thousands of organizations globally including U.S. Treasury Department and the National Telecommunications and Information Administration (NTIA), part of the U.S. Department of Commerce, NATO, the U.K. government, the European Parliament, Microsoft, SolarWinds, VMware, AstraZeneca, and others leading to a series of data breaches.

The global data breach occurred over the course of at least **8 or 9 months** during 2020.

# Tema 1. Organizaciones y normativas

---

- ▶ ¿Es realmente importante tener algo tan organizado?

## 2020 United States federal government data breach

In 2020, a major cyberattack suspected to have been committed by a group backed by the Russian government penetrated thousands of organizations globally including U.S. Treasury Department and the National Telecommunications and Information Administration (NTIA), part of the U.S. Department of Commerce, NATO, the U.K. government, the European Parliament, Microsoft, SolarWinds, VMware, AstraZeneca, and others leading to a series of data breaches.

The global data breach occurred over the course of at least **8 or 9 months** during 2020.

¿Nadie realmente se ha dado cuenta durante 8/9 meses?

Numerous federal cybersecurity **recommendations** made by the Government Accountability Office and others **had not been implemented**.

# Tema 1. Organizaciones y normativas

---

- ▶ ¿Es realmente importante tener algo tan organizado?

## 2020 United States federal government data breach

In 2020, a major cyberattack suspected to have been committed by a group backed by the Russian government penetrated thousands of organizations globally including U.S. Treasury Department and the National Telecommunications and Information Administration (NTIA), part of the U.S. Department of Commerce, NATO, the U.K. government, the European Parliament, Microsoft, SolarWinds, VMware, AstraZeneca, and others leading to a series of data breaches.

The global data breach occurred over the course of at least **8 or 9 months** during 2020.

¿Nadie realmente se ha dado cuenta durante 8/9 meses?

Numerous federal cybersecurity **recommendations** made by the Government Accountability Office and others **had not been implemented**.

¿Por qué?

**White House lacked a cybersecurity coordinator**, Trump having eliminated the post itself in 2018

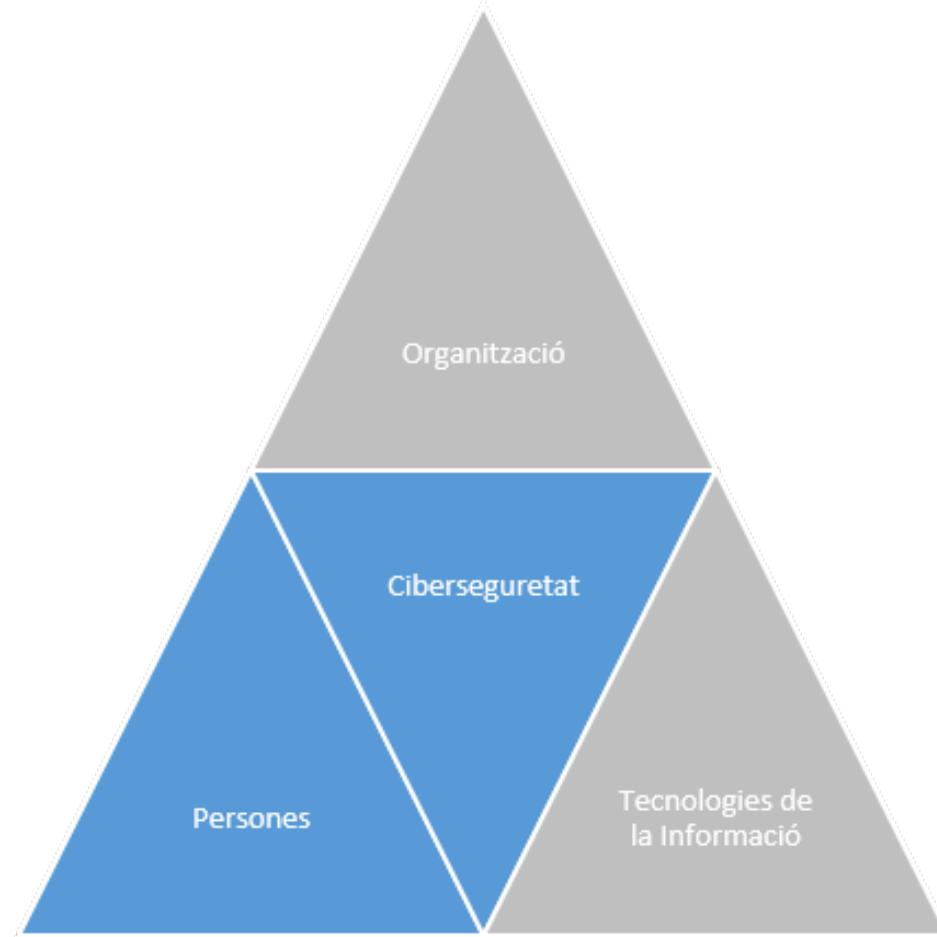
The U.S. also lacked a **Senate-confirmed Director of the Cybersecurity** and CISA, the nation's top cybersecurity official, responsible for coordinating incident response.

The **Department of Homeland Security** (DHS), which manages CISA, **lacked** a Senate-confirmed **Secretary**, **Deputy Secretary**, **General Counsel**, **Undersecretary** for Intelligence and Analysis, and **Undersecretary for Management**; and Trump had recently forced out the Deputy Director of CISA.

# 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



Fuente: The Imitation Game, 2014

# Tema 1. Personas

---

- ▶ Otro ejemplo
  - ▶ SolarWinds
    - ▶ Desarrolla software para empresas para ayudar a administrar sus redes, sistemas e infraestructura IT
    - ▶ Tenía alrededor de 300.000 clientes en diciembre de 2020, incluidas casi todas las empresas Fortune 500 y numerosas agencias federales
    - ▶ El producto Orion, utilizado por unos 33.000 clientes del sector público y privado, fue el foco del hackeo masivo del 2020, presuntamente perpetrado por la inteligencia rusa
    - ▶ La compañía declaró que menos de 18,000 de sus 33,000 clientes de Orion se vieron afectados

# Tema 1. Personas

---

## ▶ SolarWinds

- ▶ Los piratas informáticos insertaron código malicioso en actualizaciones de software legítimas para el software Orion que permiten a un atacante acceder de forma remota al entorno de la víctima
- ▶ En noviembre de 2019, un investigador de seguridad había advertido a SolarWinds que su servidor FTP dedicado a las actualización **no era seguro**, advirtiendo que "cualquier pirata informático podría cargar archivos maliciosos" que luego se distribuirían a los clientes de SolarWinds
- ▶ ¿Por qué no era seguro?

# Tema 1. Personas

---

## ▶ SolarWinds

- ▶ Los piratas informáticos insertaron código malicioso en actualizaciones de software legítimas para el software Orion que permiten a un atacante acceder de forma remota al entorno de la víctima
- ▶ En noviembre de 2019, un investigador de seguridad había advertido a SolarWinds que su servidor FTP dedicado a las actualización **no era seguro**, advirtiendo que "cualquier pirata informático podría cargar archivos maliciosos" que luego se distribuirían a los clientes de SolarWinds
- ▶ ¿Por qué no era seguro?
- ▶ La contraseña del servidor era **solarwinds123**

# Tema 1. Personas

---

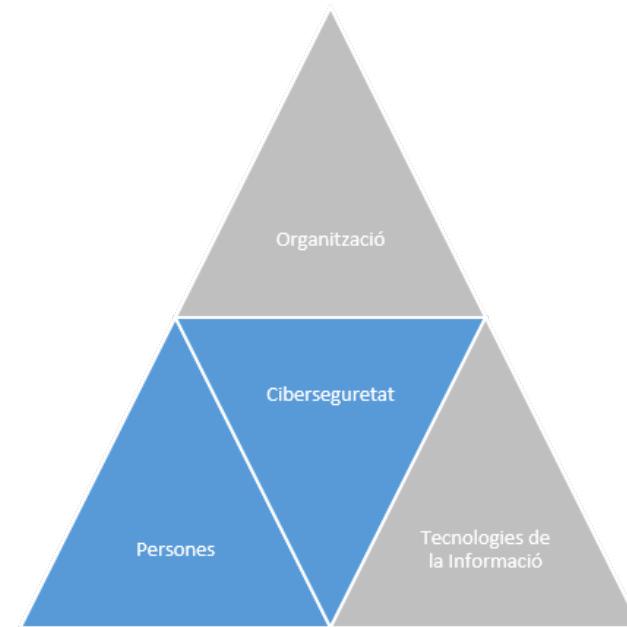
## ▶ SolarWinds

- ▶ Los piratas informáticos insertaron código malicioso en actualizaciones de software legítimas para el software Orion que permiten a un atacante acceder de forma remota al entorno de la víctima
- ▶ En noviembre de 2019, un investigador de seguridad había advertido a SolarWinds que su servidor FTP dedicado a las actualización **no era seguro**, advirtiendo que "cualquier pirata informático podría cargar archivos maliciosos" que luego se distribuirían a los clientes de SolarWinds
- ▶ ¿Por qué no era seguro?
- ▶ La contraseña del servidor era **solarwinds123**
- ▶ SolarWinds no tenía contratado un **chief information security officer**

# Tema 1. Personas

---

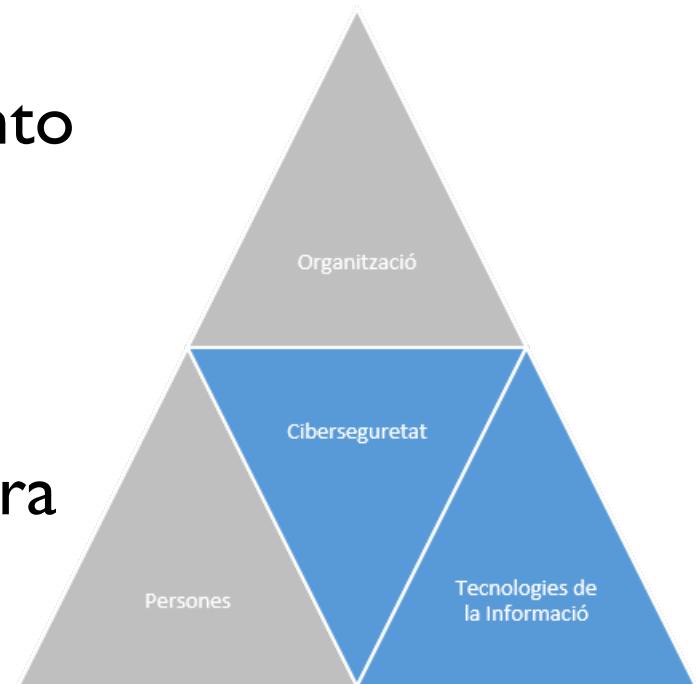
- ▶ A menudo el eslabón más débil
  - ▶ Ataques dirigidos
- ▶ Hay que fortalecer este “eslabón”
  - ▶ Concienciación
  - ▶ Formación
  - ▶ Política de seguridad
    - ▶ Contraseñas
    - ▶ Permisos
    - ▶ ...



# Tema 1. Tecnología de la información

---

- ▶ El entorno de trabajo debe proporcionar unas condiciones adagudas de seguridad
  - ▶ Estas condiciones deben estar definidas en la política de seguridad
    - ▶ Con la asignación de recursos correspondientes
- ▶ Es responsabilidad del departamento de IT debe 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