



# CRIPTOGRAFÍA PARA INGENIER@S

## Class4crypt

© Jorgeramió 2022

Aula virtual de  
criptografía  
aplicada

Diapositivas  
utilizadas en las  
clases grabadas  
de Class4crypt

Módulo 1 Ciberseguridad y criptografía

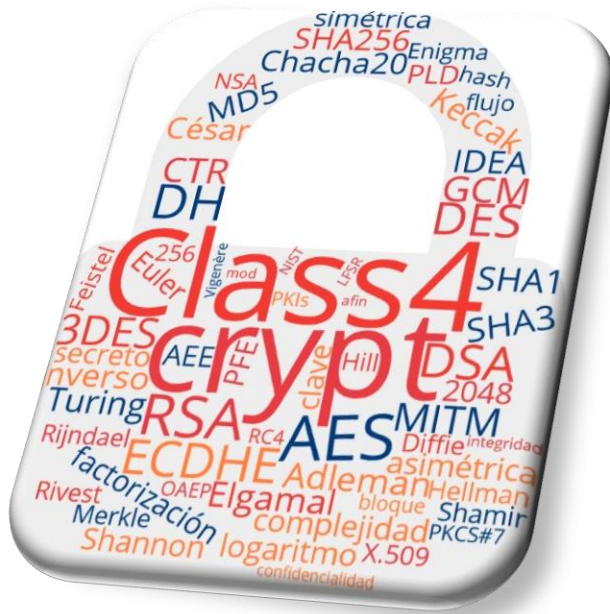
Dr. Jorge Ramió Aguirre © 2022



Attribution-NonCommercial-  
NoDerivatives 4.0 International  
(CC BY-NC-ND 4.0)

# Class4crypt

## Tu aula virtual de criptografía aplicada



<https://www.youtube.com/user/jorgeramio>

Dr. Jorge Ramío Aguirre

*El ingenio es intrínseco al ser humano,  
solo hay que darle una oportunidad  
para que se manifieste.*

<https://www.criptored.es/cvJorge/index.html>

- ➔ Módulo 1. Principios básicos de la seguridad
- Módulo 2. Matemáticas discretas en la criptografía
- Módulo 3. Complejidad algorítmica en la criptografía
- Módulo 4. Teoría de la información en la criptografía
- Módulo 5. Fundamentos de la criptografía
- Módulo 6. Algoritmos de criptografía clásica
- Módulo 7. Funciones hash
- Módulo 8. Criptografía simétrica en bloque
- Módulo 9. Criptografía simétrica en flujo
- Módulo 10. Criptografía asimétrica

# Class4crypt

## Módulo 1. Principios básicos de la seguridad

- 1.1. Ciberseguridad y criptografía
- 1.2. Percepción de la inseguridad según la década
- 1.3. Vulnerabilidades de la información y amenazas
- 1.4. Seguridad informática versus seguridad de la información
- 1.5. Tríada confidencialidad, integridad y disponibilidad

Lista de reproducción del módulo 1 en el canal Class4crypt

<https://www.youtube.com/playlist?list=PLq6etZPDh0kttEiJTA3ojMQc4hpG6OKyC>

# Class4crypt c4c1.1

## Módulo 1. Principios básicos de la seguridad

### Lección 1.1. Ciberseguridad y criptografía

1.1.1. Definiendo el concepto ciberespacio

1.1.2. El papel de la criptografía dentro de la seguridad informática

1.1.3. Enseñanza de la criptografía

1.1.4. Cómo estudiar criptografía

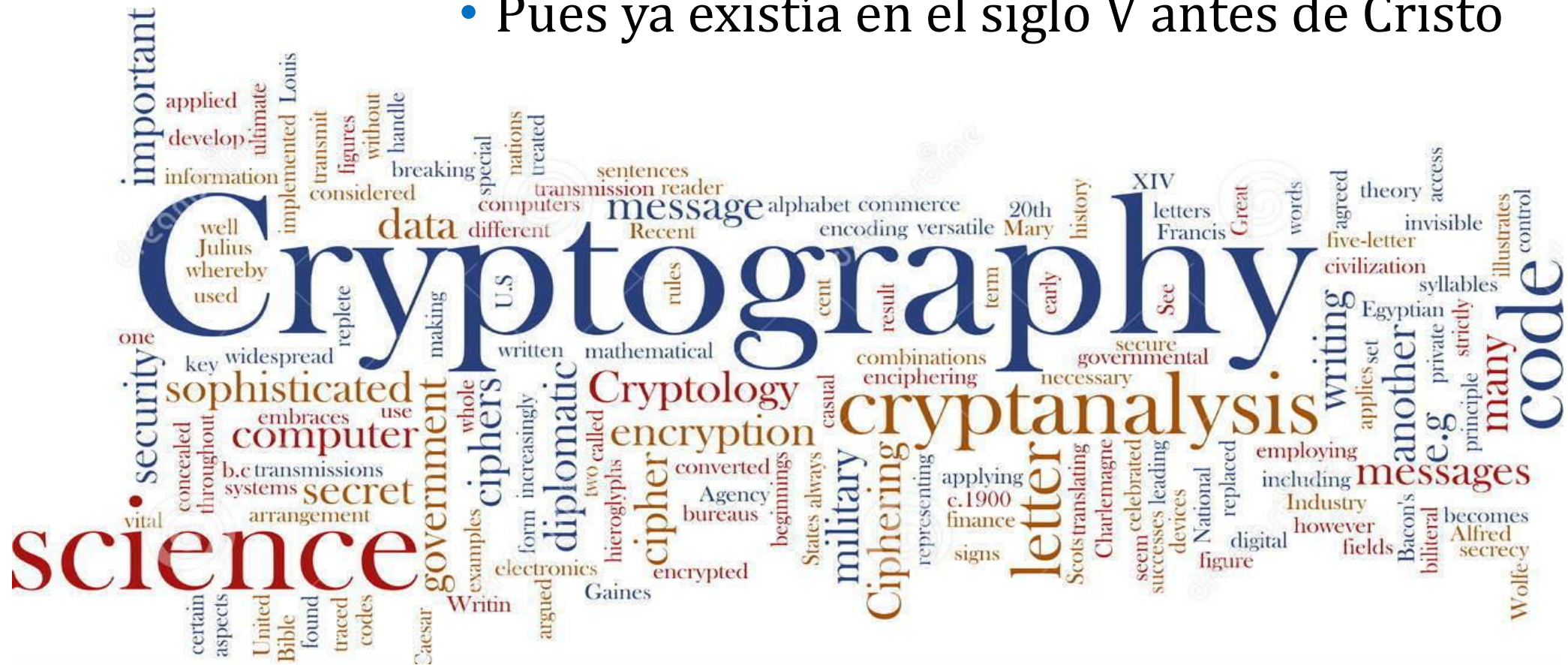
1.1.5. La criptografía que viene

Class4crypt c4c1.1 Ciberseguridad y criptografía  
<https://www.youtube.com/watch?v=bPl6Ra7sWpQ>



# En el principio... todo era criptografía

- Pues ya existía en el siglo V antes de Cristo



Pero hoy, todo es ciber o cyber





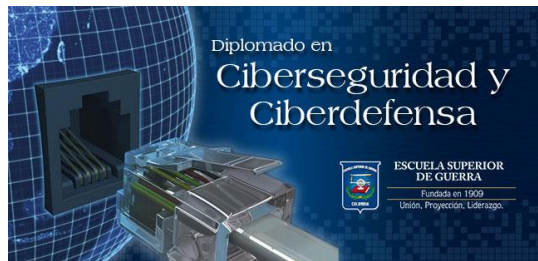
# Lo de ciber inunda incluso a la formación



Centro de Postgrado - Escuela de Ingeniería y Ciencias Basicas

**Máster Universitario en Ciberseguridad**

Campus Madrid - Puerta de Toledo



FORMACIÓN. LEÓN  
PREPARA EL MÁSTER  
EN CIBERSEGURIDAD

**MASTER EN CIBERSEGURIDAD**

# Pero, ¿de dónde viene el término ciber?

REAL ACADEMIA ESPAÑOLA

La institución Obras académicas Biblioteca y Archivo Consultas lingüísticas Boletines

Inicio » Recursos » Diccionarios » Diccionario de la lengua española

**Diccionario de la lengua española**

El *Diccionario de la lengua española (DRAE)* es la obra de referencia de la Academia. La última edición es la 23.<sup>a</sup>, publicada en octubre de 2014. Mientras se trabaja en la edición digital, que estará disponible próximamente, **esta versión electrónica permite acceder al contenido de la 22.<sup>a</sup> edición** y las enmiendas incorporadas hasta 2012.

ciber| 🔍

á é í ó ú ü ñ

*Ciber-loguensea*

Ayuda

**ciber-**

(De *cibernética*).

1. elem. compos. Significa 'cibernético'. *Ciberespacio, cibernauta*.

Real Academia Española © Todos los derechos reservados

Artículo enmendado

Busquemos entonces  
por cibernética



# Buscando el significado de cibernética


REAL ACADEMIA ESPAÑOLA

La institución Obras académicas Biblioteca y Archivo Consultas lingüísticas Boletines

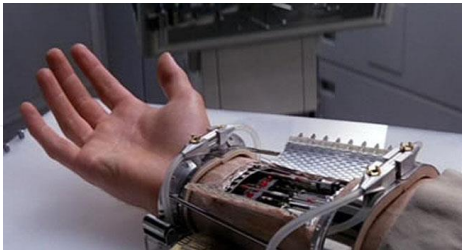
Inicio » Recursos » Diccionarios » Diccionario de la lengua española


**Diccionario de la lengua española**

El *Diccionario de la lengua española (DRAE)* es la obra de referencia de la Academia. La última edición es la 23.ª, publicada en octubre de 2014. Mientras se trabaja en la edición digital, que estará disponible próximamente, **esta versión electrónica permite acceder al contenido de la 22.ª edición** y las enmiendas incorporadas hasta 2012.

cibemética 

á é í ó ú ü ñ





**cibernetica.**

(Del fr. *cybernétique*, este del ingl. *cybernetics*, y este del gr. κυβερνητική, arte de gobernar una nave).

1. f. Estudio de las analogías entre los sistemas de control y comunicación de los seres vivos y los de las máquinas; y en particular, el de las aplicaciones de los mecanismos de regulación biológica a la tecnología.

Real Academia Española © Todos los derechos reservados

**cibernetico, ca.**

Artículo enmendado

1. adj. Perteneciente o relativo a la cibernética.

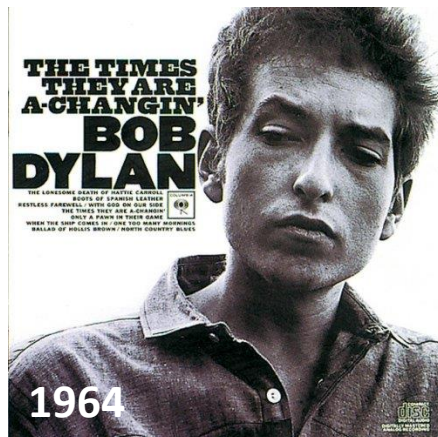
2. adj. Dicho de una persona: Que cultiva la cibernética. U. t. c. s.

Real Academia Española © Todos los derechos reservados

En realidad,  
hablamos  
de algo más  
parecido a  
esto...



# Es que... the times they are a changin'





# Y esto es lo que sucede cada segundo...



<https://www.secureworldexpo.com/industry-news/6-live-cyber-attack-maps>

<https://cybermap.kaspersky.com/>

# Pero, ¿qué es el ciberespacio?

## Glosario de términos CCN-CERT España

[https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias\\_Generales/401-glosario\\_abreviaturas/index.html](https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html)

- **Ciberespacio:** Dominio global y dinámico compuesto por infraestructuras de tecnología de la información incluyendo internet, redes de telecomunicaciones y sistemas de información.
- **Ciberseguridad:** Conjunto de actividades dirigidas a proteger el ciberespacio contra el uso indebido del mismo, defendiendo su infraestructura tecnológica, los servicios que prestan y la información que manejan. O bien, conjunto de actuaciones orientadas a asegurar, en la medida de lo posible, las redes y sistemas de que constituyen el ciberespacio:
  - Detectando y enfrentándose a intrusiones,
  - Detectando, reaccionando y recuperándose de incidentes, y
  - Preservando la confidencialidad, disponibilidad e integridad de la información.

Aquí entra en juego  
la criptografía





# Un desafío a afrontar conjuntamente



Mundo civil



Mundo militar

# La protección del ciberespacio



Tierra

**Un nuevo  
espacio, en  
donde**



Espacio

Mar



Aire



**Giberspacio**  
**El quinto elemento**

**la colaboración  
entre civiles y  
militares es vital  
y obligada**

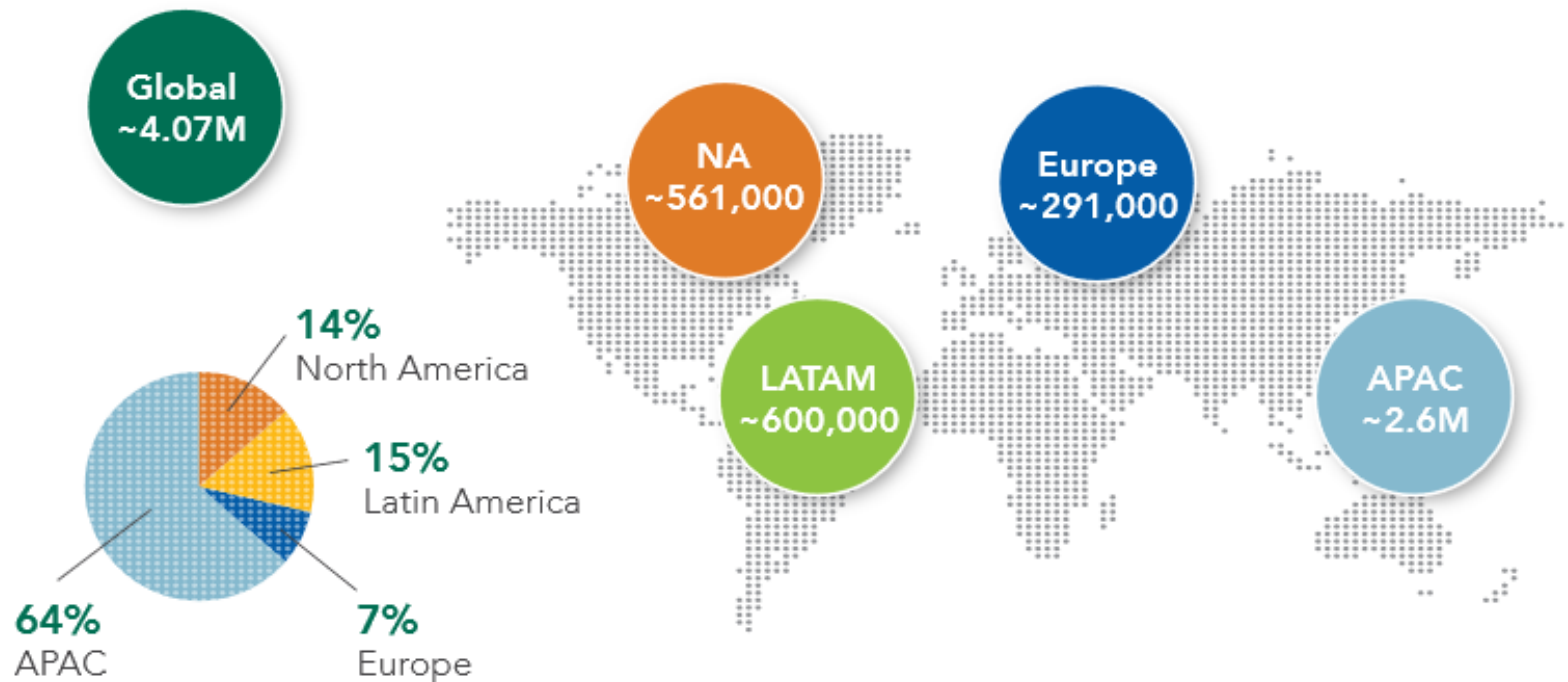




# Brecha laboral en ciberseguridad > 4M

## The Cybersecurity Workforce Gap by Region

- Profesionales hoy en ciberseguridad: 2,8 millones
- Mercado de trabajo en próximos años: 6,8 millones
- Brecha laboral en la década: 4 millones
- 150% incremento



- Strategies for Building and Growing Strong Cybersecurity Teams. (ISC)<sup>2</sup>, Cybersecurity Workforce Study, 2019

<https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=D087F6468B4991E0BEFFC017BC1ADF59CD5A2EF7>

# Papel de la criptografía y su enseñanza

- Como decíamos antes, permite la protección de la información
  - Para dotarle de confidencialidad
  - Para dotarle de integridad
- La criptografía ha pasado por diferentes estados
  - De ser el aspecto más importante (único) de la seguridad informática
  - A perder en parte su protagonismo, al surgir otras especialidades de la seguridad y por la demanda que hace el mercado de ellas
  - Para, hoy en día, volver a ser protagonista en diversos desarrollos, productos, protocolos, servicios
- Resumamos la historia de la enseñanza de la criptografía...



# Montaña rusa enseñanza criptografía 1



- **Años 1981/1990.** La criptografía lo era casi todo en la enseñanza de la seguridad
- **Años 1991/2010** (veinte años). En Seguridad Informática y en Seguridad de la Información (dos cosas distintas...) comienzan a aparecer nuevas líneas: seguridad en redes, firewalls, seguridad web, detectores de intrusos, seguridad en SSOO, SGSI, políticas de seguridad, planes contingencia, análisis y gestión del riesgo, BCP, DRP, normas internacionales, legislación en seguridad, programación segura, auditoría de máquina, técnicas forenses, ingeniería inversa, análisis de malware, seguridad en dispositivos y aplicaciones móviles, infraestructuras críticas, amenazas persistentes APT, ...
- La criptografía pierde ese gran protagonismo. Era lógico que sucediese y, además, necesario

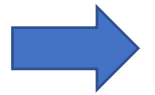
# Montaña rusa enseñanza criptografía 2



- **Años 2011/2020.** Ha nacido ya Bitcoin (2009) y comienzan a salir otros sistemas similares basados en algoritmos criptográficos y redes tipo blockchain. Se observan grandes avances en computación cuántica, que ponen en entredicho la seguridad actual de nuestros algoritmos para comunicaciones seguras, la seguridad de nuestros datos en la nube comienza a ser visto como grave un problema a solucionar, etc.
- Es decir, volvemos la mirada hacia la ciencia de la criptografía. Pero en cuanto a la enseñanza, lo haremos con una importante diferencia:
  - Lo que hasta hoy es una enseñanza universitaria básica, que requiere solo de unos conocimientos muy elementales de matemática discreta, (como en estas videoclases), se volverá bastante más compleja, en matemáticas e incluso en física, por la irrupción de la computación cuántica

# ¿Cómo estudiar la criptografía hoy?

- “I will give you an example of interesting kinds of things that might be taught. Yes, you have to teach cryptography because you need to know it, but a lot of times courses get too excited about the very theoretical kinds of things, and all of the maths and all of the proofs. And I don't think that's the really interesting part. I don't think the world needs more cryptographers, they need more people that understand how to use cryptography”.



Dra. Radia Perlman, conferencia inaugural “Adventures in Network Security”, congreso Día Internacional de la Seguridad de la Información DISI. Madrid, 1 de diciembre de 2008

<https://www.youtube.com/watch?v=zDyQ5TleDYg#t=7m5s>

# Radia Perlman y la criptografía





# ¿Qué nos traerá de nuevo la criptografía?

- Hoy no sólo es una herramienta que se usa en diversas aplicaciones de nuestra vida cotidiana (TLS, autenticación en sistemas, PKI, etc.)
- Comienza a haber un negocio alrededor de la “cripto”
- Todo hace presagiar que este negocio irá en aumento en 2021 - 2030
  - Redes blockchain
  - Criptomonedas
  - Cifrado homomórfico
  - Protocolos criptográficos
  - Criptografía ligera
  - Protección de datos en la nube
  - Criptografía con umbral
  - Criptografía postcuántica

# Conclusiones de la lección 1.1

- Ciberespacio: infraestructuras, Internet, redes y sistemas de información
- Ciberseguridad: protección del ciberespacio para defender esas infraestructuras tecnológicas, los servicios que prestan e información que almacenan o generan
- Papel criptografía: preservar la confidencialidad y la integridad de la información
- Necesidad de acciones conjuntas: civiles + militares
- Hoy nos preocupan las infraestructuras críticas: ataques dirigidos que pueden costar vidas humanas, manipulación de PLCs (Programmable Logic Controller), autómatas programables, seguridad industrial, guerra digital...
- Se acrecientan los puntos vulnerables y las amenazas por la Internet de las Cosas
- La criptografía tiene una segunda juventud desde 2010 (Bitcoin, etc.)

# Lectura recomendada

- Dos hitos aceleran la carrera por la computación cuántica, Raúl Limón, El País, octubre 2019
  - [https://elpais.com/tecnologia/2019/09/30/actualidad/1569859937\\_633976.html](https://elpais.com/tecnologia/2019/09/30/actualidad/1569859937_633976.html)
- Wikileaks: <https://es.wikipedia.org/wiki/WikiLeaks>
- PRISM: <https://es.wikipedia.org/wiki/PRISM>
- Stuxnet: <https://es.wikipedia.org/wiki/Stuxnet>
- Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país, Damien McGuinness, BBC, mayo 2017
  - <https://www.bbc.com/mundo/noticias-39800133>
- El gran reto de la computación segura en la nube: usando datos cifrados sin descifrarlos (I y II), Gonzalo Álvarez Marañón, junio 2019
  - <https://empresas.blogthinkbig.com/computacion-segura-en-la-nube-datos-cifrados-sin-descifrarlos-parte-1/>
  - <https://empresas.blogthinkbig.com/computacion-segura-en-la-nube-datos-cifrados-sin-descifrarlos-parte-2/>

# Class4crypt c4c1.2

## Módulo 1. Principios básicos de la seguridad

### Lección 1.2. Percepción de la inseguridad según la década

1.2.1. La inseguridad informática en la década de los años 70

1.2.2. La inseguridad informática en la década de los años 80

1.2.3. La inseguridad informática en la década de los años 90

1.2.4. La inseguridad informática en la década de los años 00

1.2.5. La inseguridad informática en la década de los años 10

Class4crypt c4c1.2 Percepción de la inseguridad según la década  
<https://www.youtube.com/watch?v=jZzA3rp7eEg>



# Lo que ha cambiado en los últimos 50 años

- Un breve repaso por los escenarios de la seguridad (inseguridad) en estos últimos 50 años
  - Década de 1971 a 1980
  - Década de 1981 a 1990
  - Década de 1991 a 2000
  - Década de 2001 a 2010
  - Década de 2011 a 2020
  - Década de 2021 a 2030... una incógnita

Es una manera de simplificar las cosas, pero como ejercicio es válido para observar cómo ha evolucionado este tema

# La seguridad en la década de los años 70

- Primeros computadores personales como el Apple II
- Desarrollo de los primeros algoritmos digitales de cifra para uso civil
- Primeros intentos de diseño de malware
- Papel de la criptografía: comienza a ser importante
- Amenaza principal: equipos personales simples o corporativos grandes
- Estado emocional y preocupación: incredulidad ante la novedad
- Criticidad: muy baja

# Una imagen vale más que mil palabras '70



# La seguridad en la década de los años 80

- Inicio efectivo de la era de los PCs con la aparición del IBM PC, ZX Spectrum, Commodore 64 y Apple Macintosh
- Seguridad asociada al equipo, normalmente el equipo del usuario final
- Aparecen programas malignos, virus que inciden en mi trabajo, el software o el hardware dejan de funcionar
- Papel de la criptografía: uso aún escaso
- Amenaza principal: mi equipo, es caro y casi único, pocos expertos me lo pueden reparar
- Estado emocional y preocupación: alarma en un entorno personal
- Criticidad: baja



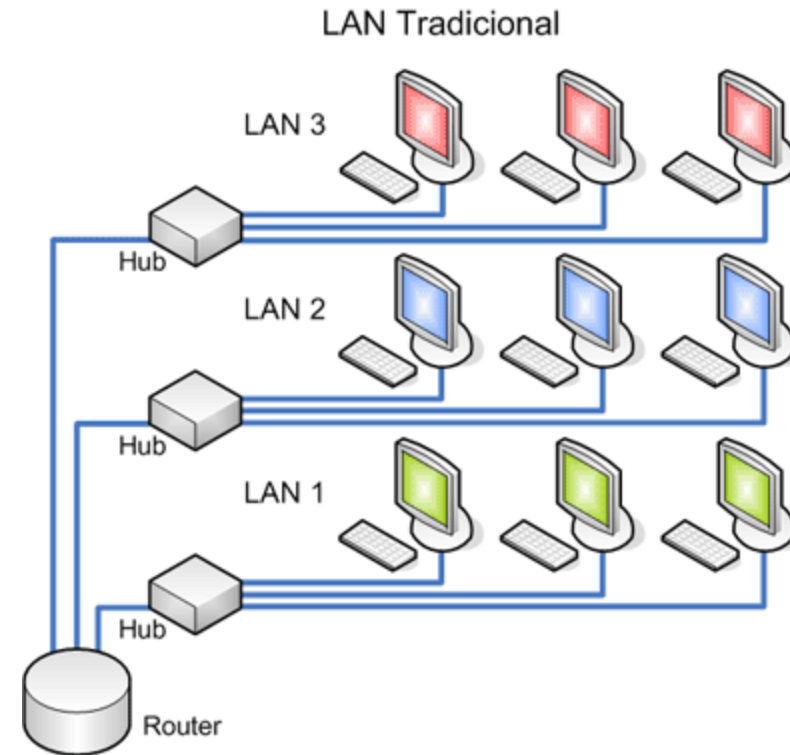
# Una imagen vale más que mil palabras '80



# La seguridad en la década de los años 90

- Seguridad asociada a redes locales que me entregan servicios y me facilitan el modo de trabajar
- Equipos servidores: filosofía cliente – servidor
- Aparecen los gusanos y otros programas malignos, inciden en la calidad de la producción, el software o el hardware dejan de funcionar, robo de datos, espionaje industrial
- Papel de la criptografía: aplicaciones de correo, conexiones seguras
- Amenaza principal: mi red local, no puedo seguir trabajando con el PC
- Estado emocional y preocupación: alarma corporativa, organización
- Criticidad: media/alta

# Una imagen vale más que mil palabras '90



# La seguridad en la década de los años 00

- Seguridad asociada a Internet que me entrega servicios y que me facilita trabajar. Los clientes también generan información, inicio del concepto nube. Comienza el intercambio de información en las redes sociales
- Malware generalizado, incide en la calidad de la producción, el software o el hardware dejan de funcionar, robo de datos, espionaje industrial, soborno, delito informático, exfiltración de información, ataques a aplicaciones móviles
- Internet facilita el envío de malware y las intrusiones a los sistemas
- Papel de la criptografía: importante, protección de datos, malware asociado
- Amenaza principal: Internet de todos, si se cae la red no puedo seguir trabajando con el PC de mi puesto de trabajo y muchos datos están ya en la nube
- Estado emocional y preocupación: alarma colectiva, afecta a miles de usuarios
- Criticidad: alta



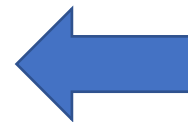
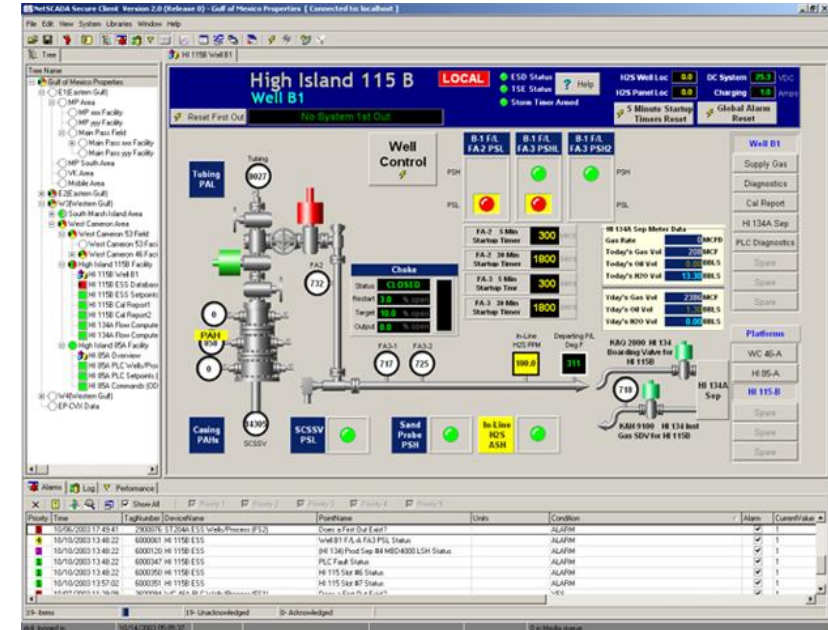
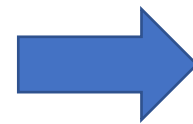
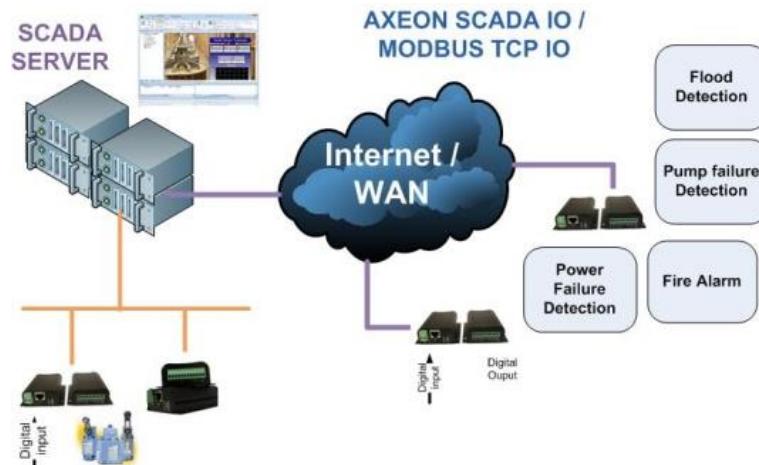
# Una imagen vale más que mil palabras '00



# La seguridad en la década de los años 10

- Aparece la seguridad asociada a la Internet de las Cosas que me entrega todo tipo de servicios y que me permite (ya no sólo facilita) trabajar y vivir cómodamente
- Equipos servidores, filosofía cliente - servidor difusa (disperso, nube)
- Entran en juego los sistemas de control industriales a través de IP y SCADA
- Ataques generalizados, aumento del ciberdelito, ciberejércitos, hostilidades entre países en el ciberespacio, ciberterrorismo, espionaje a gran escala
- Papel de la criptografía: muy importante, criptomonedas, malware esteganográfico
- Amenaza principal: las infraestructuras críticas de los países; si estas IC dejan de operar, pueden causar graves daños a la población, incluso costar vidas humanas
- Estado emocional y preocupación: alarma mundial, seguridad de un país
- Criticidad: muy alta

# Una imagen vale más que mil palabras '10



# Conclusiones de la lección 1.2

- De 1971 a 1980, la computación era algo incipiente, se crean los primeros programas malignos pero no es un tema que preocupe aún a la sociedad: riesgo muy bajo
- De 1981 a 1990, con los ordenadores personales PC, nos preocupan los virus informáticos, aunque sus efectos se circunscriben al entorno personal: riesgo bajo
- De 1991 a 2000, modelo cliente-servidor, se generalizan los gusanos en redes, comienza a usarse masivamente Internet: riesgo medio
- De 2001 a 2010, mundo interconectado, redes sociales, datos en la nube, robo de información, suplantación de identidad: riesgo alto
- De 2011 a 2020, ataques a infraestructuras críticas, amenazas persistentes, autómatas industriales, los ataques pueden costar vida humanas: riesgo muy alto
- La criptografía va adquiriendo cada vez un mayor protagonismo en la protección de la información, pero también en los ataques



# Lectura recomendada

- La historia de los virus informáticos, Javier Yanes, BBV Open Mind, noviembre 2017
  - <https://www.bbvaopenmind.com/tecnologia/mundo-digital/la-historia-de-los-virus-informaticos/>
- Una breve historia de los virus informáticos y lo que nos deparará el futuro, Kaspersky Labs
  - <https://latam.kaspersky.com/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds>
- Virus y gusanos: ¿Cuál es la diferencia?, Panda Security, mayo 2018
  - <https://www.pandasecurity.com/spain/mediacenter/malware/virus-gusanos-diferencia/>
- Trend Micro Security Predictions for 2020, Trend Micro Research, 2019
  - <https://documents.trendmicro.com/assets/rpt/rpt-the-new-norm-trend-micro-security-predictions-for-2020.pdf>

# Class4crypt c4c1.3

## Módulo 1. Principios básicos de la seguridad

### Lección 1.3. Vulnerabilidades de la información y amenazas

1.3.1. La información, el activo más importante a proteger

1.3.2. Vulnerabilidades de la información

1.3.3. Amenazas a la información

1.3.4. Clasificación de las amenazas a la información

1.3.5. Controles para la protección de la información

Class4crypt c4c1.3 Vulnerabilidades de la información y amenazas

<https://www.youtube.com/watch?v=zhLWbkyuuzQ>

# ¿Qué son los activos de una organización?

- Los activos de una organización son componentes o funcionalidades de un sistema de información, susceptibles de ser atacados deliberadamente o bien afectados accidentalmente, con consecuencias negativas para ella
- Un activo es cualquier bien que tiene un valor, tangible o intangible, para la empresa
- **Pregunta básica.** ¿Qué pasaría si nuestra empresa sufre un desastre por una pérdida grave de datos?
- Informes mundiales indican que en ese caso un 90% de las empresas quiebran en menos de 3 años




Tras un desastre con pérdida de datos



# Activos según la metodología Magerit 3.0

- Activos de un sistema de información

- La **información** que maneja 
- Los **servicios** que presta

- Otros activos relevantes

- **Datos** que materializan la información
- **Servicios** auxiliares que se necesitan para poder organizar el sistema
- Las aplicaciones informáticas (**software**) que permiten manejar los datos
- Los equipos informáticos (**hardware**) y que permiten hospedar datos, aplicaciones y servicios
- Los **soportes** de información que son dispositivos de almacenamiento de datos
- El **equipamiento** auxiliar que complementa el material informático
- Las **redes** de comunicaciones que permiten intercambiar datos
- Las **instalaciones** que acogen equipos informáticos y de comunicaciones
- Las **personas** que explotan u operan todos los elementos anteriormente citados

*Esta diapositiva es copia de la página 22 y 23 del documento "Magerit 3.0 Proyectos de análisis de riesgos", Miguel Ángel Amutio Gómez, Javier Candau y José Antonio Mañas, Ministerio de Hacienda y Administraciones Públicas, España, 2012.  
URL en la bibliografía recomendada*

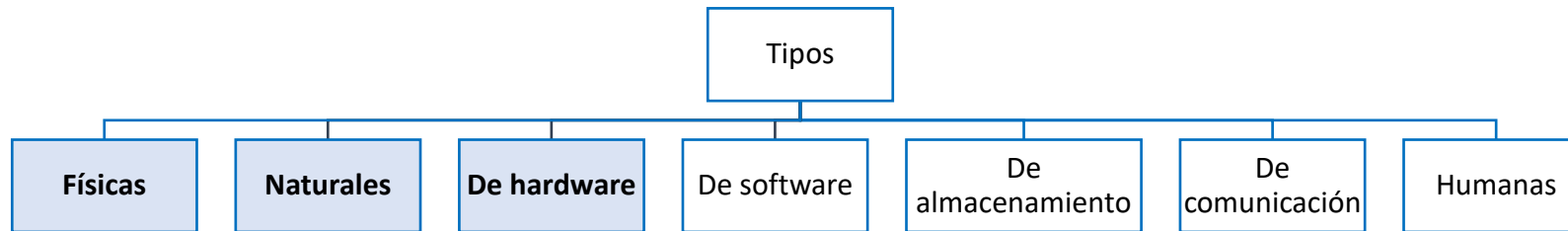
*¿Y la **imagen** de empresa?*



# Vulnerabilidades de la información

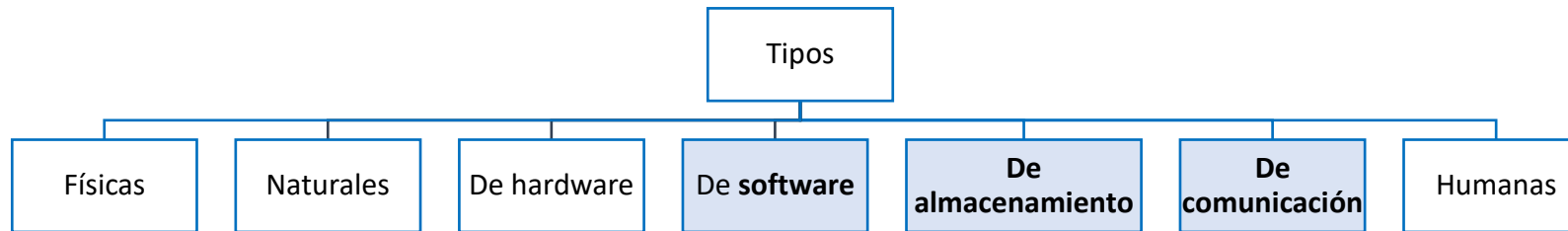
- ¿Qué son?
  - Debilidades de un activo o grupo de activos que pueden ser explotadas por una o más amenazas
  - Puntos débiles del sistema que pueden ser atacados o sufrir fallos
  - Pueden causar daños a los activos, con gran impacto económico, o bien perjudicar la continuidad del negocio
- ¿Qué hacer?
  - Identificarlas
  - Estudiar su importancia e incidencia en la organización
  - Definir medidas de seguridad, controles o salvaguardas
    - Ejemplo: aplicar herramientas criptográficas para proteger a la información

# Tipos de vulnerabilidades (1/3)



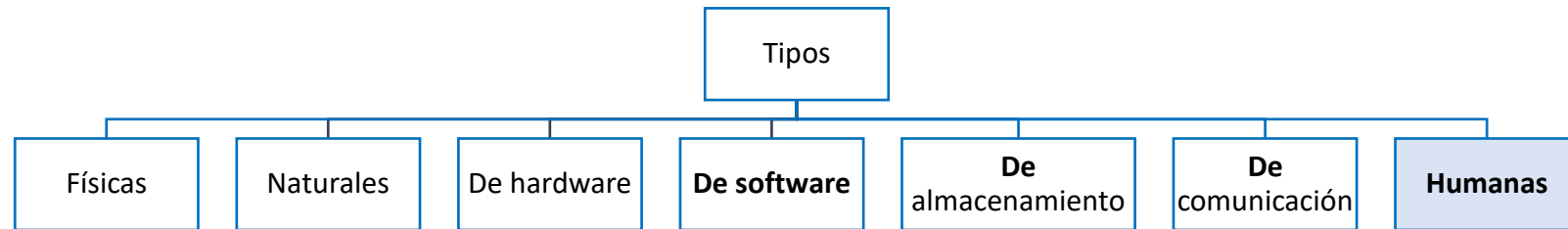
- **Físicas**
  - Instalaciones inadecuadas del espacio de trabajo, disposición desorganizada de cables de energía y de red, ausencia de identificación de personas y de locales, etc.
- **Naturales**
  - Locales próximos a ríos propensos a inundaciones, ambientes sin protección contra incendios, infraestructura incapaz de resistir a las manifestaciones de la naturaleza como terremotos, maremotos, huracanes, lluvias intensas, etc.
- **De hardware**
  - Conservación inadecuada de los equipos, la falta de una configuración de respaldos o equipos de contingencia, etc.

# Tipos de vulnerabilidades (2/3)



- De software
  - La configuración e instalación inadecuada, ausencia de actualización, etc.
- De almacenamiento
  - Plazo de validez y caducidad, defecto de fabricación, lugar de almacenamiento en locales insalubres o con alto nivel de humedad, magnetismo, moho, etc.
- De comunicación
  - La ausencia de sistemas de cifrado en las comunicaciones que pudieran permitir que personas ajenas a la organización obtengan información privilegiada
  - La mala elección de sistemas de comunicación para envío de mensajes de alta prioridad pudiera provocar que no alcanzaran el destino esperado o bien se interceptara el mensaje en su tránsito

# Tipos de vulnerabilidades (3/3)



- Humanas
  - Desconocimiento de las medidas de seguridad adecuadas para ser adoptadas por los miembros internos de la empresa
  - La falta de capacitación específica (diferenciada) para la ejecución de las actividades inherentes a las funciones de cada uno
  - La falta de conciencia de seguridad para las actividades de rutina, los errores, omisiones, insatisfacciones, etc.
  - Contraseñas débiles o compartidas
  - Falta de uso de criptografía en la comunicación y almacenamiento sensibles
  - Compartir identificadores como nombre de usuario, credenciales de acceso, etc.



# Ejemplo: vulnerabilidad de las contraseñas



No es inusual ver contraseñas de máquinas en un post it pegado al monitor y visible desde el exterior

Y desgraciadamente ésta sigue siendo la password más usada

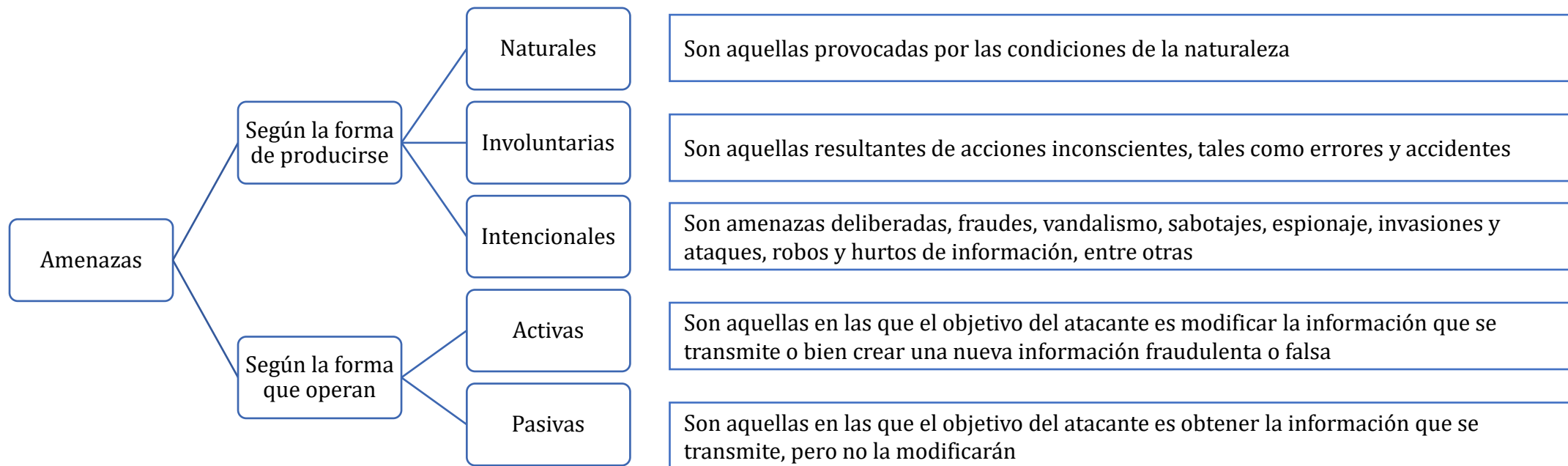


# Amenazas a la información

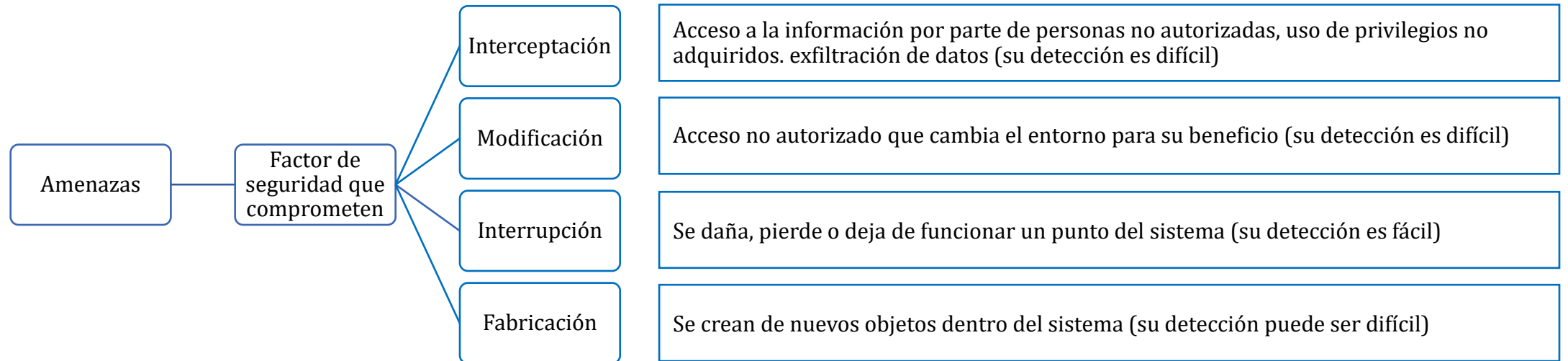


- ¿Qué son las amenazas?
  - Coloquialmente, son “cosas que ocurren”..., y nos interesa lo que pueda pasarle a nuestro activo más importante, la información
  - Son la posible causa de un **incidente de seguridad** no deseado, el cual puede ocasionar **daño** a la organización y cuyo **riesgo** de producirse puede ser significativo para la misma
    - **Incidente**: cualquier evento inesperado y no deseado que puede comprometer las operaciones de una empresa
    - **Daño**: el perjuicio que se produce cuando una amenaza ocurre
    - **Riesgo**: el producto entre la magnitud de un daño (d) y la probabilidad (p) de que éste tenga lugar (Riesgo  $R = p \times d$ ).
    - Análisis y Gestión de Riesgos: una rama muy importante de la Seguridad de la Información

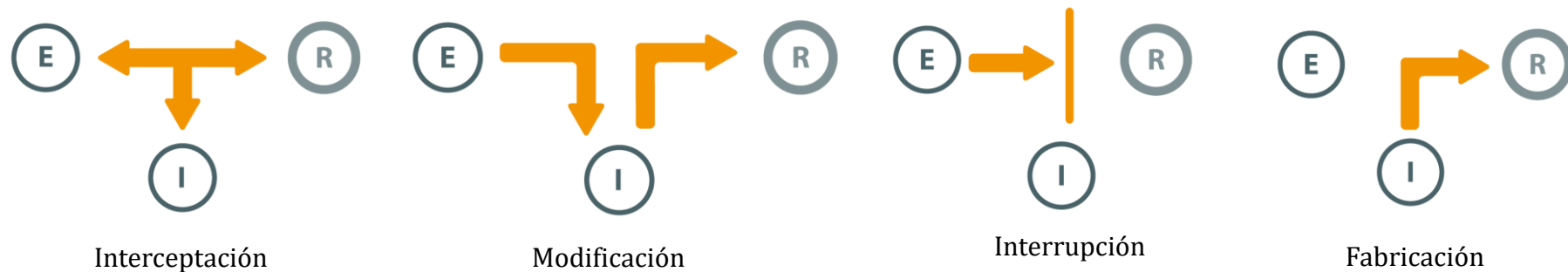
# Clasificación de las amenazas (1/2)



# Clasificación de las amenazas (2/2)



E: emisor, R: receptor, I: intruso





# El uso de controles o salvaguardas

- Aplicaremos controles o salvaguardas para proteger a la información
  - Los controles son aquellos procedimientos o mecanismos tecnológicos que nos van a permitir minimizar o eliminar el riesgo
- Hay amenazas que se resuelven simplemente organizándose adecuadamente
- Otras amenazas requieren el uso de elementos técnicos, programas o equipos
- Otras amenazas pueden surgir por medidas de seguridad física inadecuadas
- Otras amenazas pueden venir por una mala política de formación al personal
- En este curso de criptografía aplicada nos van a interesar los controles que adoptemos en este sentido para proteger a la información y dotarle de tres características básicas: la confidencialidad, la integridad y la disponibilidad

# Tipo de controles (1/3)

- De **Prevención**. Cuando reduce las oportunidades de que un incidente ocurra
  - Ejemplos: autorización previa de usuarios, planificación, metodología segura de desarrollo de software, el uso de **herramientas de criptografía**
- De **Disuasión**. Cuando tiene un efecto tal sobre los atacantes que estos no se atreven o se lo piensan dos veces antes de atacar
  - Ejemplos: guardias de seguridad, avisos sobre la persecución del delito o de la persecución del delincuente
- De **Eliminación**. Cuando impide que un incidente tenga lugar
  - Ejemplos: eliminación de cuentas estándar, de cuentas sin contraseña

# Tipo de controles (2/3)

- De **Minimización** del impacto. Cuando acota las consecuencias de un incidente
  - Ejemplos: desconexión de redes o equipos en caso de ataque, seguros de cobertura, cumplimiento de la legislación vigente
- De **Corrección**. Cuando habiéndose producido un daño, lo repara
  - Ejemplos: gestión adecuada de incidentes, líneas de comunicación alternativas, fuentes de alimentación redundantes
- De **Recuperación**. Cuando permite regresar al estado anterior al incidente
  - Ejemplos: copias de seguridad o backup, resiliencia de la organización

# Tipo de controles (3/3)

- De **Monitorización**. Cuando se está monitorizando lo que está ocurriendo o lo que ha ocurrido
  - Ejemplos: registros de actividad, registro de descargas del web
- De **Detección**. Cuando informa de que el ataque está ocurriendo
  - Ejemplos: antivirus, detectores de incendio, detectores de humedad
- De **Concienciación**. Son las actividades de formación en seguridad a todas las personas de la organización
  - Ejemplos: cursos de concienciación, cursos de formación
- De **Administración**. Afines con componentes de seguridad del sistema
  - Ejemplos: inventario de activos, análisis de riesgos, plan de continuidad

# Conclusiones de la Lección 1.3

- Una organización tiene diversos activos, tangibles e intangibles
- El activo más importante (aunque haya discrepancias) es la información
- La información tiene un conjunto de vulnerabilidades que, si se explotan, pueden convertirse en amenazas que producen daño a la organización
- Las vulnerabilidades pueden ser físicas, naturales, de hardware, de software, de almacenamiento, de comunicación y por el factor humano
- Los tipos amenazas se clasifican en naturales, involuntarias, intencionales, o bien en activas y pasivas
- Las amenazas a la información pueden ser por interceptación, modificación, interrupción y fabricación
- Existen una diversidad de controles para minimizar estos riesgos



# Lectura recomendada

- Encuesta Mundial sobre el Estado de la Seguridad de la Información 2018, Jesús Romero, 2019, PwC España
  - <https://www.pwc.es/es/digital/encuesta-mundial-ciberseguridad-2018.html>
- MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Miguel Ángel Amutio Gómez, Javier Candau y José Antonio Mañas, Ministerio de Hacienda y Administraciones Públicas, España, 2012
  - [https://administracionelectronica.gob.es/pae\\_Home/pae\\_Documentacion/pae\\_Metodologia/pae\\_Magerit.html#.X2eYmotS8uU](https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodologia/pae_Magerit.html#.X2eYmotS8uU)
- ¿Seguro que estás seguro?, Chema Alonso, UPM TASSI 2011 Conferencia 2, 2014, minuto 8:30
  - <https://www.youtube.com/watch?v=qbomp3LHaIk>
- Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian?, INCIBE, 2017
  - <https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian>

# Class4crypt c4c1.4

## Módulo 1. Principios básicos de la seguridad

### Lección 1.4. Seguridad informática versus seguridad de la información

- 1.4.1. Posible confusión entre los dos términos
- 1.4.2. Definición de seguridad informática
- 1.4.3. Entornos de la seguridad informática
- 1.4.4. Definición de seguridad de la información
- 1.4.5. Entornos de la seguridad de la información
- 1.4.6. Roles de responsables de seguridad en la empresa

Class4crypt c4c1.4 Seguridad informática versus seguridad de la información  
<https://www.youtube.com/watch?v=9hyIccyMrkg>

# Seguridad informática o de la información

- Décadas atrás, hasta comienzos década '90, seguridad informática y seguridad de la información podrían confundirse y entender que eran lo mismo, aunque se hablaba más de seguridad informática
- Pero hoy sabemos que son dos cosas distintas, con diferentes objetivos, aunque sean complementarias
- Veremos en esta clase que la seguridad informática está enfocada hacia el hardware, el software y los datos. En cambio, la seguridad de la información está enfocada hacia la gestión de la seguridad del activo más importante en una organización, la información

# ¿Seguridad informática según la RAE?

Si seguridad es la “*cualidad de seguro*” y seguro es “*libre y exento de todo peligro, daño o riesgo*”

Y sabemos que el propósito de los sistemas informáticos es generar, procesar, transmitir y almacenar información (incluso destruirla)

La seguridad informática estará relacionada con un sistema informático que es seguro porque maneja la información de una forma correcta, protegiéndola frente a las amenazas que entrañan un peligro o daño, y que significan un riesgo

# Definición seguridad informática

- La seguridad informática es un conjunto de acciones que tienen como objetivo la protección de sistemas informáticos, entendidos como la unión de datos (la información) y los componentes de hardware y software que darán soporte a dicha información
- Las personas que hacen uso de la misma serán un factor a tener en cuenta como posibles detonantes de amenazas
- Una cadena es tan fuerte como lo sea el eslabón más débil de ella (Thomas Reid, filósofo escocés del siglo XVIII)





# Entornos de seguridad informática

- Cuando hablamos de seguridad informática, estamos centrando nuestra atención en aquellos aspectos de la seguridad que inciden directamente en los medios informáticos en los que la información se genera, se gestiona, se transmite, se almacena o se destruye, desde el punto de vista tecnológico y telemático de la informática
- Ejemplos básicos de este entorno tecnológico de la seguridad
  - El uso de la criptografía para la protección y la seguridad de los datos
  - Las herramientas que permiten asegurar y fortificar las redes
  - Los métodos que añaden seguridad a las aplicaciones informáticas, programas y bases de datos

# Aspectos de la seguridad de información

- La seguridad de la información es un concepto más amplio, y que abarca no sólo la protección de los sistemas informáticos, sino que implica tomar medidas para proteger y salvaguardar la información, independientemente del soporte en el que se encuentre, y asegurar así la buena la gestión de la misma y la continuidad del negocio
- El objetivo común será asegurar la tríada CIA (CID en español)
  - La confidencialidad de la información (en inglés Confidentiality **C**)
  - La integridad de la información (en inglés Integrity **I**)
  - La disponibilidad de la información (en inglés Availability **A**)

# Definición de seguridad de la información

- La seguridad de la información es **un proceso** que engloba todas las actividades que de manera sistemática se llevan a cabo para adoptar medidas del tipo físicas, técnicas y organizativas, donde intervienen tecnología, procesos y personas, con la finalidad de:
  - Garantizar la confidencialidad, la integridad y la disponibilidad de la información
  - Proteger los activos de la organización
  - Mitigar vulnerabilidades y amenazas internas y/o externas



TECNOLOGÍA



PROCESOS

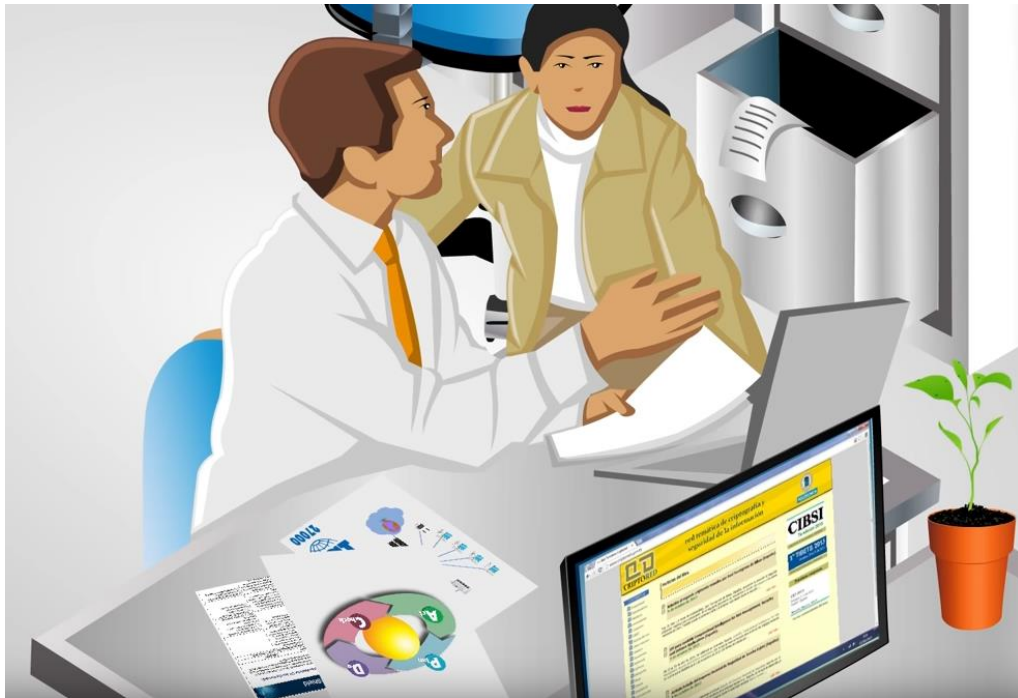


PERSONAS

# Entornos de seguridad de la información

- Cuando hablamos de seguridad de la información, especialmente se tienen en cuenta aspectos sistémicos de la gestión de dicha seguridad, como sería el caso de las políticas y planes contingencia y seguridad que toda empresa debe plantearse, la orientación de esta seguridad hacia la continuidad del negocio, así como su adecuación al entorno legal y a las normativas internacionales
- Ejemplos del entorno empresarial y estratégico de la seguridad
  - La gestión del riesgo y de la seguridad de la información
  - Las políticas de seguridad que permitan el buen gobierno
  - La adecuación de la seguridad a las normativas internacionales y a la legislación vigente

# Roles y objetivos complementarios



- No sería lo mismo un director o directora de seguridad informática que un director o directora de seguridad de la información
- El primero tiene un enfoque más tecnológico y el segundo tiene un enfoque más estratégico
- Se cubren con roles de CSO Chief Security Officer y de CISO Chief Information Security Officer



# Más información en píldoras Thoth



<https://www.youtube.com/watch?v=7MqTpfEreJ0>

# Conclusiones de la Lección 1.4

- No es lo mismo seguridad informática que seguridad de la información
- La seguridad informática está enfocada al hardware, el software y los datos
- Así, la seguridad informática es más tecnológica
- La seguridad de la información está centrada en el proceso de gestión que permite proteger a la información como un activo más de la organización
- Así, la seguridad de la información es más estratégica
- Ambas son complementarias y, dependiendo del tamaño de la empresa será el Chief Security Officer CSO o el Chief Information Security Officer CISO quien se haga carga de ella
- Cuando existen CSO y CISO, el CISO reporta al CSO y el CSO a la dirección

# Lectura recomendada

- ¿Seguridad Informática versus Seguridad de la Información?, Carlos Ormella, Criptored, 2009
  - [https://www.criptored.es/guiateoria/gt\\_m327d.htm](https://www.criptored.es/guiateoria/gt_m327d.htm)
- Seguridad Informática vs Seguridad de la Información, Jeimy Cano, 2012
  - <https://es.slideshare.net/aurixv/seguridad-informtica-vs-seguridad-de-la-informacin>
- Guion píldora formativa Thoth nº 1, ¿Seguridad informática o seguridad de la información?, Jorge Ramió, 2014
  - <https://www.criptored.es/thoth/material/texto/pildora001.pdf>
- CEO, CISO, CIO... ¿Roles en ciberseguridad?, INCIBE, 2016
  - <https://www.incibe.es/protege-tu-empresa/blog/ceo-ciso-cio-roles-ciberseguridad>

# Class4crypt c4c1.5

## Módulo 1. Principios básicos de la seguridad

### Lección 1.5. Tríada confidencialidad, integridad y disponibilidad

1.5.1. Confidencialidad de la información

1.5.2. Integridad de la información

1.5.3. Disponibilidad de la información

1.5.4. Objetivos de la CIA y estado seguro de la información

1.5.5. Servicios de seguridad: Autenticación, Control de acceso, No repudio y Trazabilidad

Class4crypt c4c1.5 Tríada confidencialidad, integridad y disponibilidad

<https://www.youtube.com/watch?v=nOrPm4ZPlVQ>

# ¿Por qué debemos usar la tríada CIA?



- Un objetivo en seguridad de la información es proteger a ésta frente a las amenazas que pueden explotar sus vulnerabilidades
- Las amenazas contra las vulnerabilidades de la información eran de tipo naturales, involuntarias, intencionales, activas y pasivas
- Y, en cada caso, la información podría verse afectada por amenazas de interceptación, modificación, interrupción y fabricación
  - Interceptación: relacionada con la Confidencialidad **C**
  - Modificación y Fabricación: relacionadas con la Integridad **I**
  - Interrupción: relacionada con la Disponibilidad **A**



# Confidencialidad de la información (ISO)

- Confidencialidad es la propiedad por la que la información no se pone a disposición o se revela a individuos, entidades o procesos que no sean los autorizados y tengan ese privilegio de conocer el secreto
- Tiene como propósito asegurar que sólo esas personas o procesos autorizados pueden acceder a dicha información confidencial
- En la práctica, la confidencialidad o secreto de la información se consigue aplicando técnicas de criptografía
  - Cifrando la información o conjunto de datos con un algoritmo de cifra simétrica, bien sea en bloque (AES) o en flujo (SALSA20)
  - Intercambiando de forma segura y secreta una clave de sesión con un algoritmo de cifra asimétrica (ECDHE)

# Integridad de la información (ISO)

- Integridad es la propiedad de salvaguardar la exactitud y completitud del activo información
- Tiene como propósito garantizar que la información no será alterada, eliminada o destruida por entidades no autorizadas, preservando la exactitud y completitud de la misma así como de los métodos utilizados para su procesamiento
- En la práctica, la integridad de la información se consigue aplicando técnicas de criptografía
  - Utilizando hashes para comprobar su exactitud y completitud (SHA2)
  - Utilizando firmas digitales para comprobar lo anterior, además de la autenticidad del emisor o firmante (ECDSA)

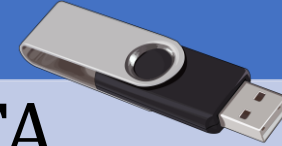
# Disponibilidad de la información (ISO)

- Disponibilidad es la propiedad o una característica de los activos, consistente en que las entidades o procesos autorizados tienen acceso a los mismos en el momento en que lo requieran
- Tiene como propósito asegurar que los usuarios autorizados puedan tener acceso a la información y a los medios asociados a ésta cada vez que lo requieran, garantizando que se trata de un activo disponible
- En la práctica, la disponibilidad se consigue mediante un sistema de gestión de máquinas y redes que permita conocer, administrar y minimizar los riesgos que atenten contra el acceso a la información
  - Utilizando protección de máquinas, fortificación de redes, controles de acceso, etc.

# Los objetivos de la CIA en tres frases

## INTEGRIDAD

1) LA INFORMACIÓN CORRECTA



## CONFIDENCIALIDAD

2) PARA LA PERSONA INDICADA



## DISPONIBILIDAD

3) EN EL MOMENTO ADECUADO



# Información en estado seguro o inseguro

- Posibles escenarios de **inseguridad**
- Respondamos SÍ o NO en un escenario de la información inseguro a estas 4 preguntas de expedientes académicos
  - **P1** ¿Puedes acceder al expediente de cualquier alumno?
  - **P2** ¿Es correcta la información de tu expediente y tus notas?
  - **P3** ¿Una nota del expediente puede ser modificada por cualquier persona?
  - **P4** ¿Dispones en cualquier momento de tu expediente para su consulta?

P1	P2	P3	P4
SÍ	SÍ	SÍ	SÍ
SÍ	SÍ	SÍ	NO
SÍ	SÍ	NO	SÍ
SÍ	SÍ	NO	NO
SÍ	NO	SÍ	SÍ
SÍ	NO	SÍ	NO
SÍ	NO	NO	SÍ
SÍ	NO	NO	NO
NO	SÍ	SÍ	SÍ
NO	SÍ	SÍ	NO
NO	SÍ	NO	SÍ
NO	NO	SÍ	SÍ
NO	NO	SÍ	NO
NO	NO	NO	SÍ
NO	NO	NO	NO



# Servicio de autenticación

- Proceso mediante el cual se verifica la identidad de un usuario
- Existen tres métodos de autenticación
  - Basados en algo **que se conoce**:
    - Una contraseña, una frase de paso, un código de entrada, etc.
  - Basados en algo **que se posee**:
    - Una tarjeta de identidad, una tarjeta inteligente o smartcard, un dispositivo USB o token, etc.
  - Basados en algo **que se es**:
    - Verificación de voz, huellas dactilares, patrones oculares, palma de la mano, etc.

# Servicio de control de acceso

- Medio para garantizar que el acceso a los activos está autorizado y restringido en función de los requisitos de seguridad y empresarial
- Por ejemplo LDAP Lightweight Directory Access Protocol, en el que un servidor o varios servidores distribuidos mantienen una base de datos con información sobre los usuarios
- La información incluye el mapeo entre un nombre de usuario y otros atributos/datos para controlar los derechos de acceso a distintos recursos
- Otros protocolos de autenticación:
  - CHAP, PAP, EAP, TACACS, RADIUS, KERBEROS, etc.

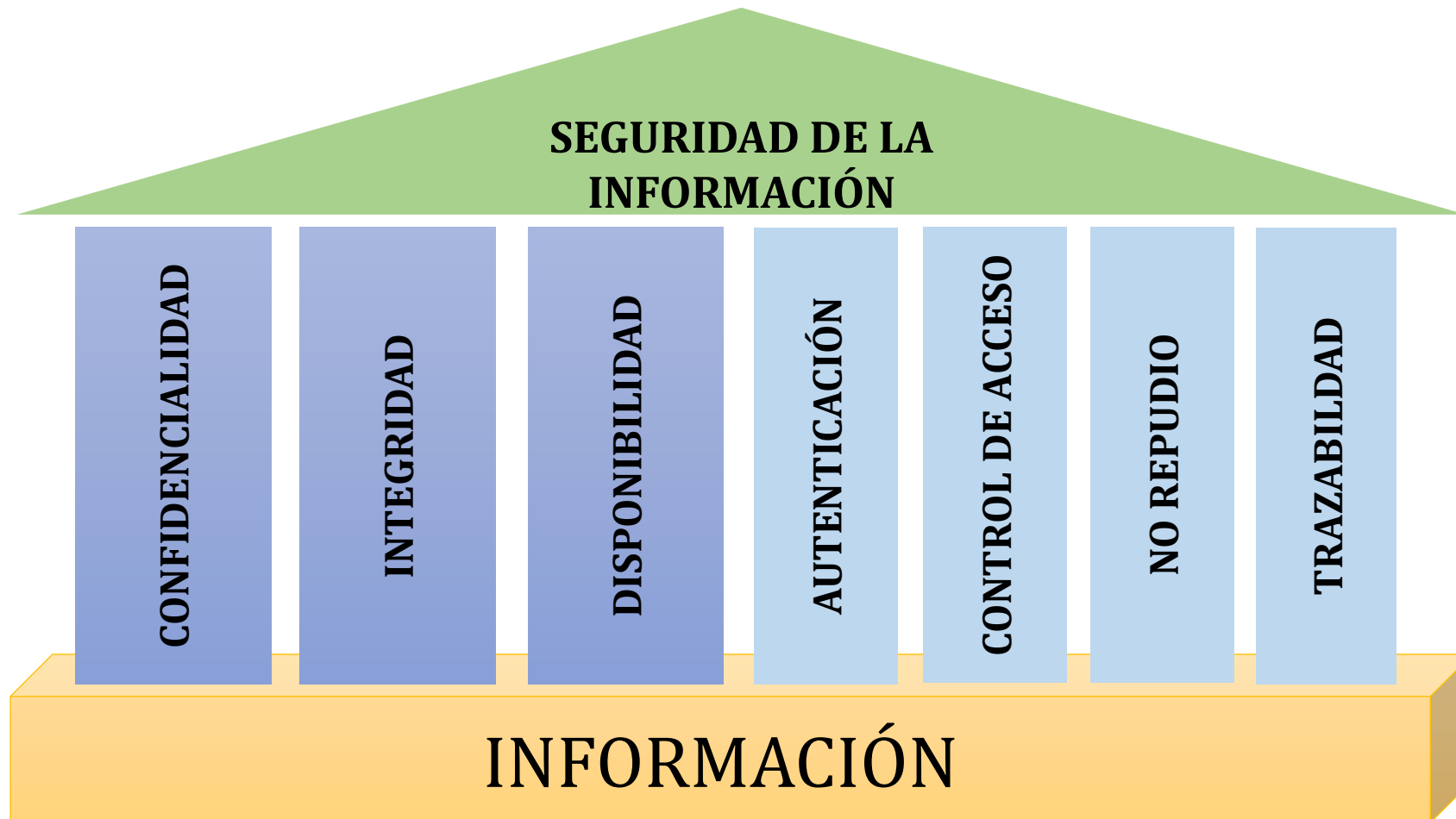
# Servicio de no repudio

- Capacidad de probar la ocurrencia de un evento o una acción reivindicada y sus entidades de origen, a fin de resolver las controversias sobre la ocurrencia, o no ocurrencia, del evento o acción y la participación de entidades en el evento
- No repudio en origen
  - El emisor no puede negar que envió el mensaje porque el destinatario tiene pruebas del envío
- No repudio en destino
  - El receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción

# Servicio de trazabilidad

- Creación, incorporación y conservación de la información sobre el movimiento y uso de documentos, en general de activos
- Conocimiento, en todo momento, de quién, cuándo, cómo y a qué se ha tenido acceso
- Capacidad de hacer un seguimiento del uso de los activos de información
  - Se basa en registros de trazas, por ejemplo logs
- Será muy importante en temas de informática forense, auditoría de máquina, etc.

# Los 7 pilares de la seguridad





# Más información en píldoras Thoth



[https://www.youtube.com/watch?v=KWAfVhy\\_GQ8](https://www.youtube.com/watch?v=KWAfVhy_GQ8)

# Conclusiones de la Lección 1.5

- La seguridad de la información descansa en tres principios básicos: la confidencialidad, la integridad y la disponibilidad de la información
- Una definición concisa:
  1. La información correcta (integridad)
  2. Para la persona o ente indicado (confidencialidad)
  3. En el momento adecuado (disponibilidad)
- Además, hay un conjunto de servicios que fortalecen a este activo: la autenticación, el control de acceso, el no repudio y la trazabilidad
- Estos 3 principios junto a los 4 servicios, conforman los 7 pilares en los que se fundamenta la seguridad de la información

# Lectura recomendada

- Authentication protocol / Protocolo ligero de acceso a directorios LDAP, Wikipedia
  - [https://en.wikipedia.org/wiki/Authentication\\_protocol](https://en.wikipedia.org/wiki/Authentication_protocol)
  - [https://es.wikipedia.org/wiki/Protocolo\\_ligero\\_de\\_acceso\\_a\\_directorios](https://es.wikipedia.org/wiki/Protocolo_ligero_de_acceso_a_directorios)
- Protocolos de Autenticación en Redes, UC3M, José María Sierra, 2015
  - <http://ocw.uc3m.es/ingenieria-informatica/seguridad-en-sistemas-distribuidos/material-de-clase-1/Tema2.pdf>
- Definiciones de autenticación, control de acceso, no repudio y trazabilidad
  - [https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias\\_Generales/401-glosario\\_abreviaturas/index.html?n=640.html](https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html?n=640.html)
- Guion píldora formativa Thoth nº 5, ¿Qué es la tríada CIA?, Jorge Ramió, 2014
  - <https://www.criptored.es/thoth/material/texto/pildora005.pdf>