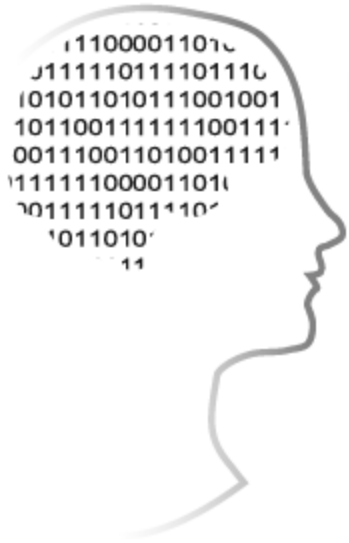


# Lección 4: Introducción a la seguridad en redes telemáticas

---



**intypedia**  
INFORMATION SECURITY ENCYCLOPEDIA

**Justo Carracedo Gallardo**  
carracedo@diatel.upm.es

**Universidad Politécnica de Madrid**  
Catedrático de Escuela Universitaria (EUITT)

# ¿Qué se entiende por seguridad en redes? (I)

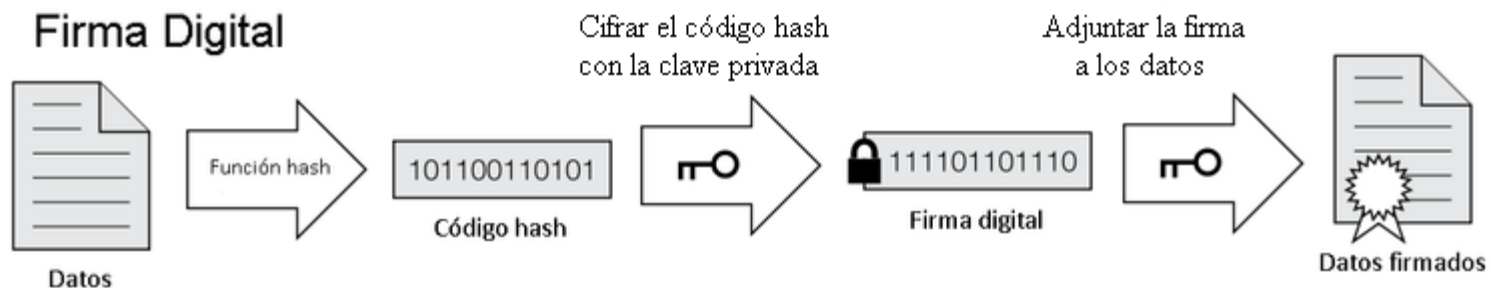
---

- **Un conjunto de técnicas** que tratan de *minimizar* la vulnerabilidad de los sistemas o de la información en ellos contenida.
- Se trata de conseguir que el coste de la consecución indebida de un recurso sea superior a su valor.
- **No existe la *seguridad total***: ante cualquier coraza de protección, siempre se podrá encontrar un elemento capaz de romperla.



# ¿Qué se entiende por seguridad en redes? (II)

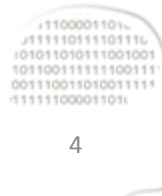
- El estado actual de **las tecnologías de seguridad** permite ofrecer en las redes telemáticas una **protección superior en varios órdenes de magnitud a la que se ofrece en el mundo ordinario** del intercambio de documentos en papel.



# Cómo proteger una red: **Mecanismos, Protocolos y Servicios de Seguridad (I)**

---

- Los ***Mecanismos de Seguridad*** se utilizan para construir protocolos de seguridad que facilitarán la prestación de servicios de seguridad.
- Los mecanismos de seguridad son los “**ladrillos**” que permiten, gracias a los servicios de seguridad, proteger las comunicaciones de los usuarios frente a los distintos ataques.



# Cómo proteger una red: **Mecanismos, Protocolos y Servicios de Seguridad (II)**

---

**Mecanismos => Protocolo => Servicio**

Los ***Mecanismos de Seguridad*** se apoyan principalmente en técnicas criptográficas. La mayoría de ellos son, por tanto, ***Mecanismos Criptográficos***.

La ***Criptografía*** es la base de apoyo de los servicios de seguridad, pero no más.



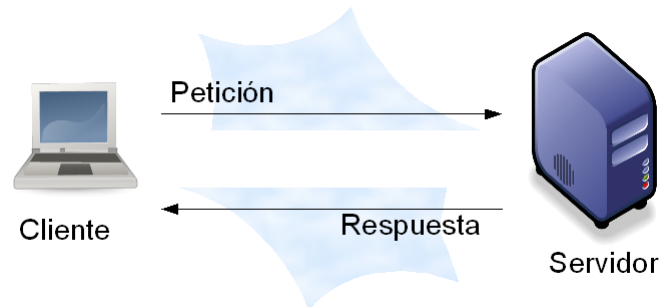
¡Lo que le interesa al usuario final son **los servicios!**



# Cómo proteger una red: Mecanismos, Protocolos y Servicios de Seguridad (III)

---

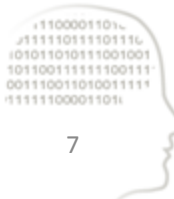
- Un **protocolo de seguridad** consiste en:
  - un conjunto de reglas y formatos que determinan el intercambio de piezas de información,
  - en el que intervienen dos o más entidades, y
  - está diseñado para conseguir que sean prestados a los usuarios determinados ***Servicios de Seguridad***.



# Cómo proteger una red: Mecanismos, Protocolos y Servicios de Seguridad (IV)

---

- Los **servicios de seguridad** protegen las comunicaciones de los usuarios frente a los distintos ataques.
  - **Ataques sobre la identidad de las entidades**
    - Interceptación de identidades
    - Suplantación de identidad (*masquerade*)
  - **Ataques sobre los servicios**
    - Negación del servicio
  - **Ataques sobre la información**
    - Revelación de datos
    - Manipulación de datos
    - Reenvío de datos
    - Repudio en envío y/o recepción de datos



# Servicios de seguridad más importantes (I)

---

- Autenticación de entidades
- Confidencialidad de datos
- Integridad de datos
- Control de acceso
- No repudio
- Disponibilidad
- Anonimato



# Servicios de seguridad más importantes (II)

---

- **Autenticación o autentificación (*Authentication*)**

Este servicio garantiza que una entidad comunicante es quien dice ser.

- **Confidencialidad de los datos (*Data confidentiality*)**

Proporciona protección de los datos para evitar que sean revelados accidental o deliberadamente a un usuario no autorizado.

- **Integridad de los datos (*Data integrity*)**

Este servicio garantiza al receptor de los datos que los datos recibidos coinciden con los enviados por el emisor, pudiendo detectar si se ha producido algún añadido, sustracción o cambio.



# Servicios de seguridad más importantes (III)

---

- **Control de acceso** (*Access Control*)

Sirve para evitar el uso no autorizado de los recursos de la red.  
*¿Quién puede hacer qué?*

- **Disponibilidad**

Propiedad de un sistema o recurso de estar accesible y utilizable a entidades autorizadas.

- **Anonimato**

Trata de mantener oculta la identidad de la persona que realiza una determinada operación telemática.

- Buzón de sugerencias/quejas.
- Encuestas.
- Votación electrónica.
- Dinero electrónico



# Servicios de seguridad más importantes (IV)

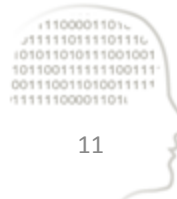
---

- **No repudio (*Non- repudiation*)**
  - **con prueba de origen**

El receptor del mensaje adquiere una prueba, demostrable ante terceros, del origen de los datos recibidos.
  - **con prueba de envío**

El receptor o el emisor del mensaje adquieren una prueba demostrable de la fecha y hora del envío.
  - **con prueba de entrega**

El emisor del mensaje adquiere una prueba, demostrable ante terceros, de que los datos han sido entregados al receptor adecuado.



# Atacantes... Hacker/Cracker

---

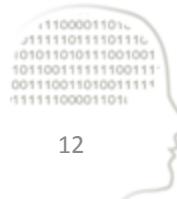
- **Conoce a tu enemigo**

Diversas formas de clasificar a los atacantes: por sus conocimientos, por sus intenciones, por el daño causado, etc.

- **Definición hacker/cracker (*jargon dictionary*)**

**Hacker:** persona especialista en una temática que disfruta explorándola por el placer de aprender y superar barreras. Aplicado a la informática son aquellas personas cuya habilidad para comprender los sistemas informáticos, su diseño y programación les permite dominarlos para un uso particular.

**Cracker:** Aplicado a la informática persona que irrumpe en un sistema informático alterando o dañando algún tipo de información o elemento. Habitualmente su motivación es económica.

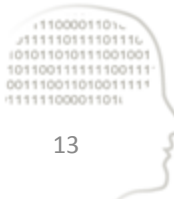


# Políticas de Seguridad

---

- La mejor forma de proteger una red telemática es mediante la **definición de políticas de actuación claras** (*políticas de seguridad*) y la **concienciación en seguridad informática**.

Habitualmente el eslabón más débil es el ser humano, por tanto se debe educar, entre otros, en evitar fallos derivados de la **ingeniería social**: Habilidad de los atacantes para hacer que otras personas trabajen en su beneficio, en muchos casos sin ser éstos conscientes del engaño al que están sometidos y por tanto vulnerando medidas de protección definidas.





# intypedia

INFORMATION SECURITY ENCYCLOPEDIA