# Seguridad y privacidad

## tratamiento de datos sensibles

Victoriano Giralt

Servicio Central de Informática
Universidad de Málaga

Aulario Juan López Peñalver
Universidad de Málaga
29 de mayo de 2012

There be dragons

# Índice

# Índice

# Índice

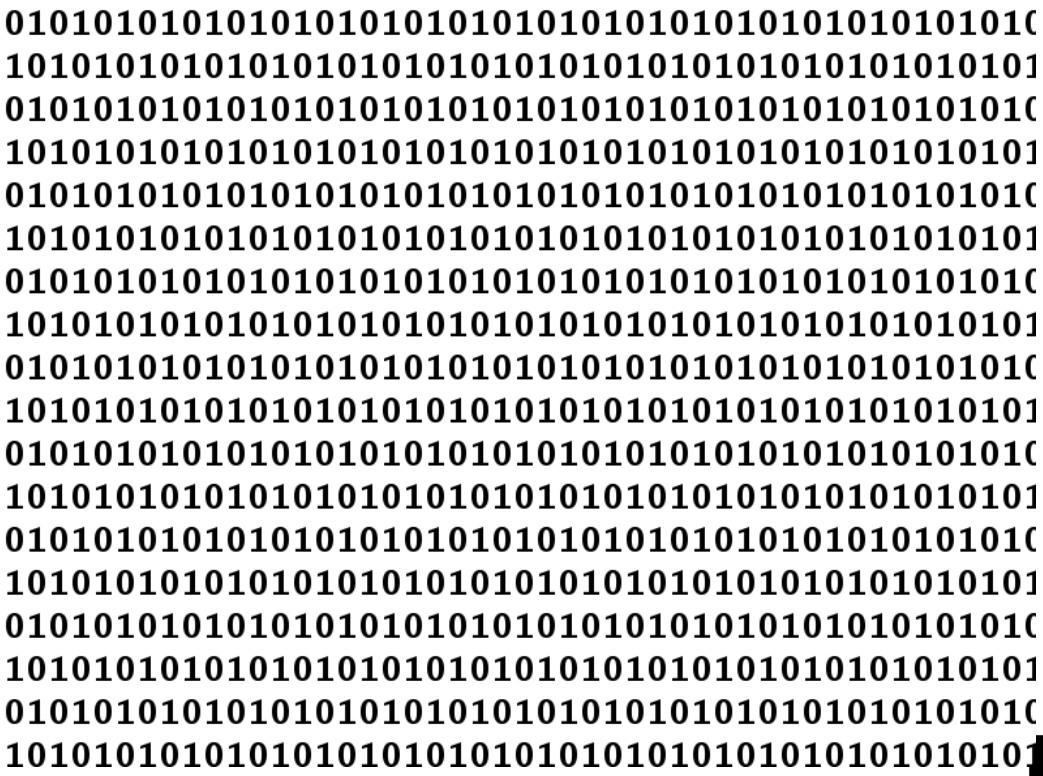
# Índice

# Índice

# Índice

# Información

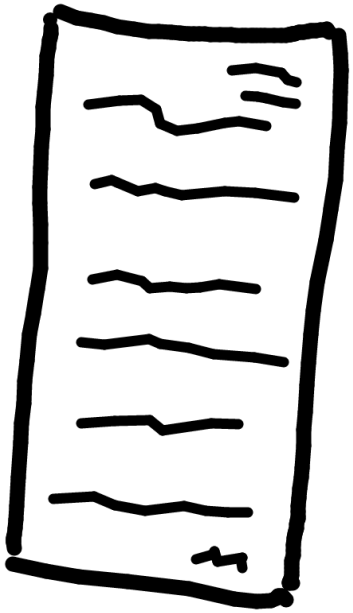
## en formato electrónico, es nuestro protagonista




SSEDIC Programme Partner

# Historia Clínica

alias *mucha información sobre alguien*



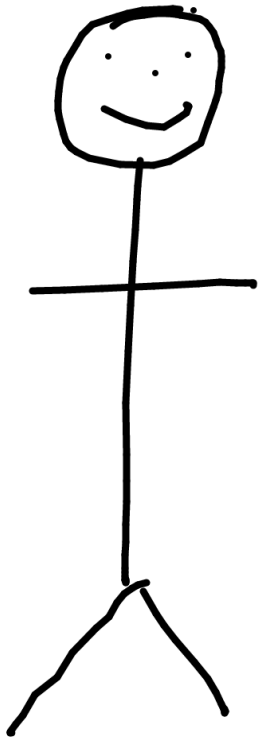
¡Hola! Soy *tu* historia clínica


SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

# Paciente

alias *cualquiera de nosotros*



¡Hola! soy *el* paciente


SSEDIC Programme Partner

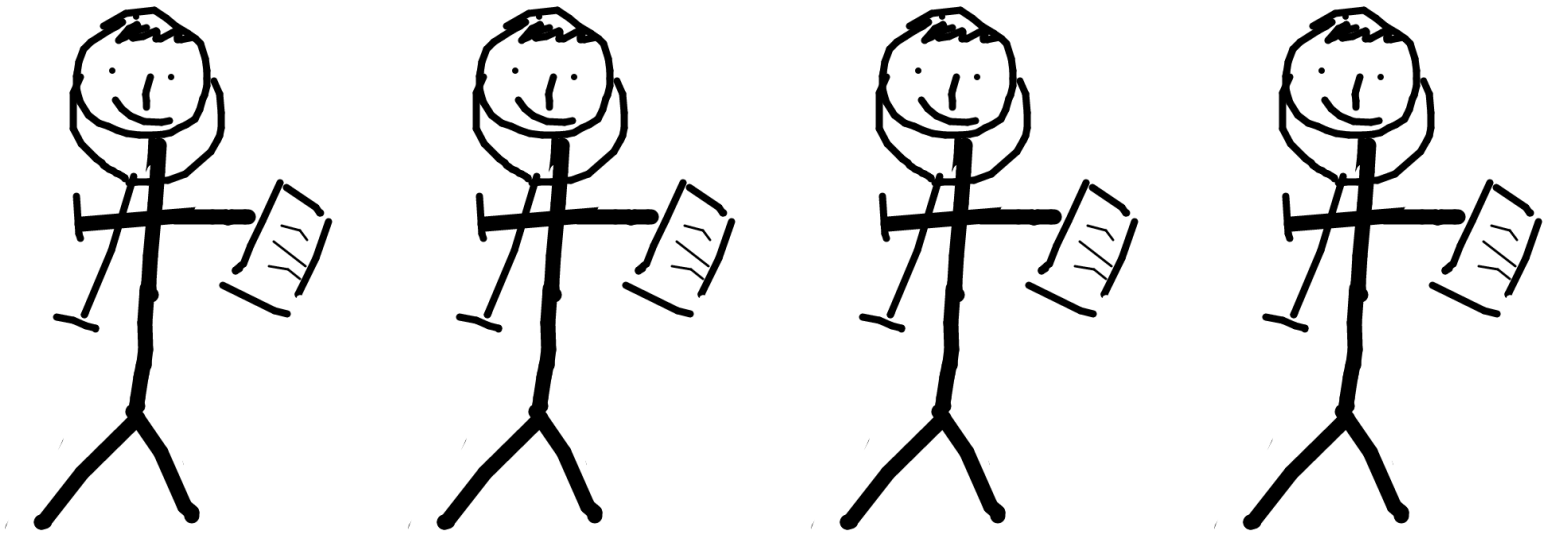
# Profesional de la salud

## alias *El* médico

¡Hola! soy *tu* médico

# Profesional de la salud

alias *El* médico



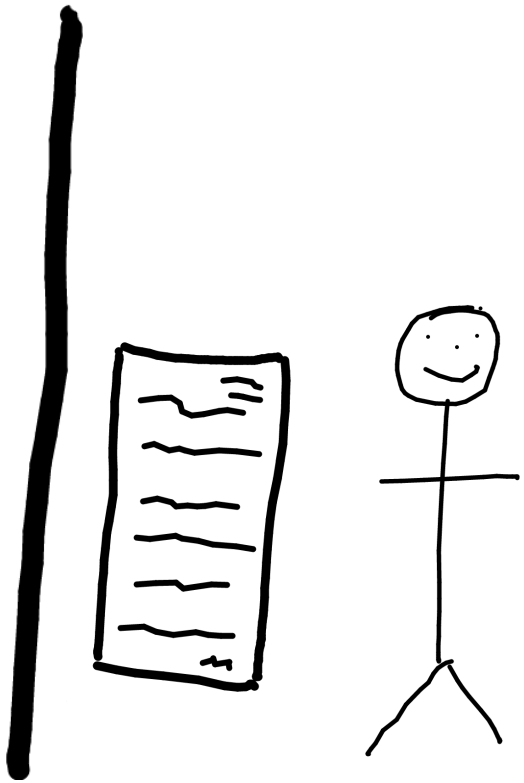
todos somos *tu* médico

# Proteger la información

## nuestro primer objetivo

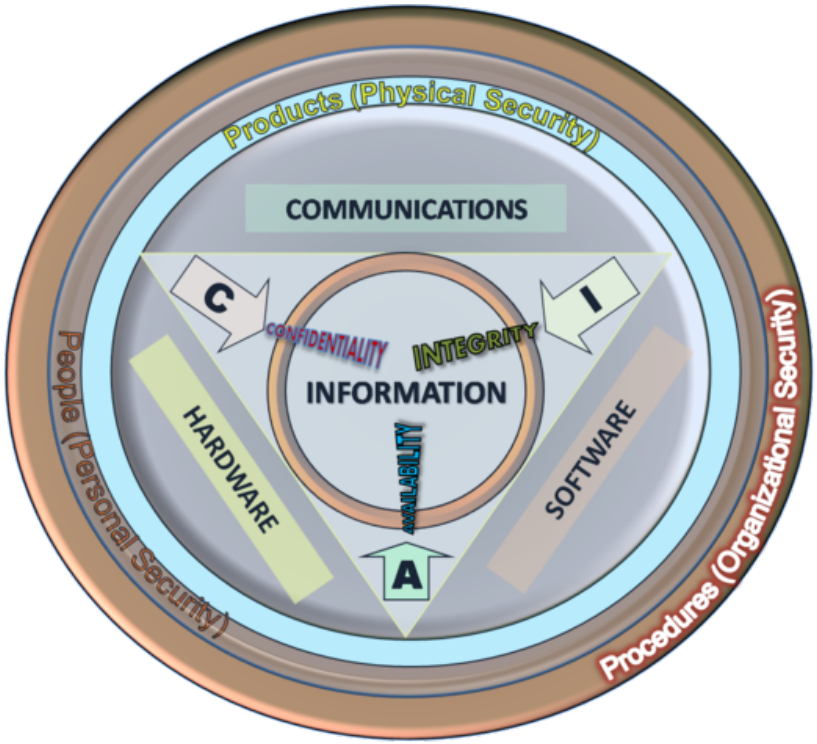
# Proteger al paciente

## nuestro segundo objetivo



# La seguridad

## es un estado, no un proceso



# La seguridad de la información

## caracterísitcas principales

1. Confidencialidad
2. Integridad
3. Disponibilidad
4. Autenticidad
5. No repudio


SSEDIC Programme Partner

# El eslabón más débil

## punto crítico en el proceso de seguridad

PEBKAC

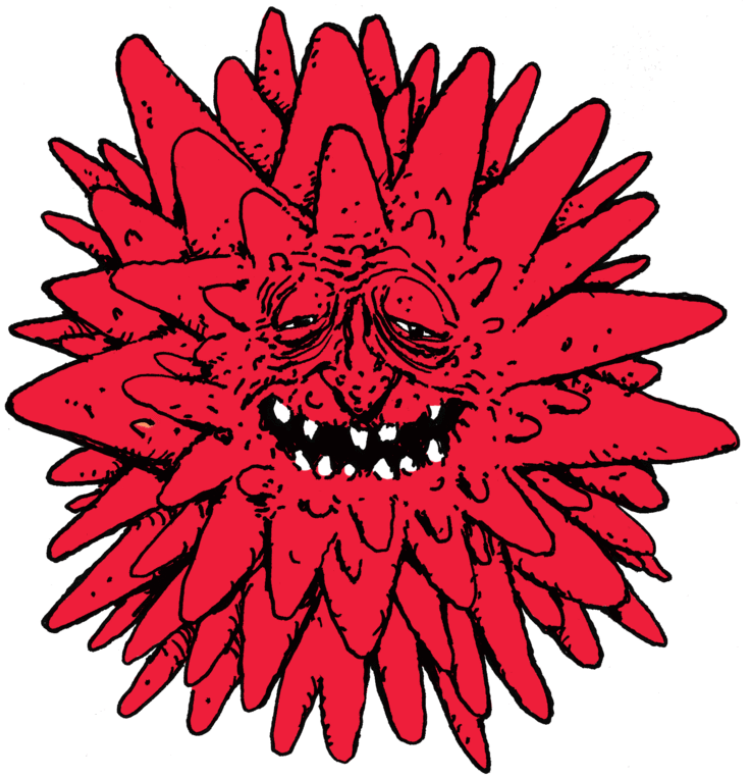
# Fugas de información

## el enemigo a batir



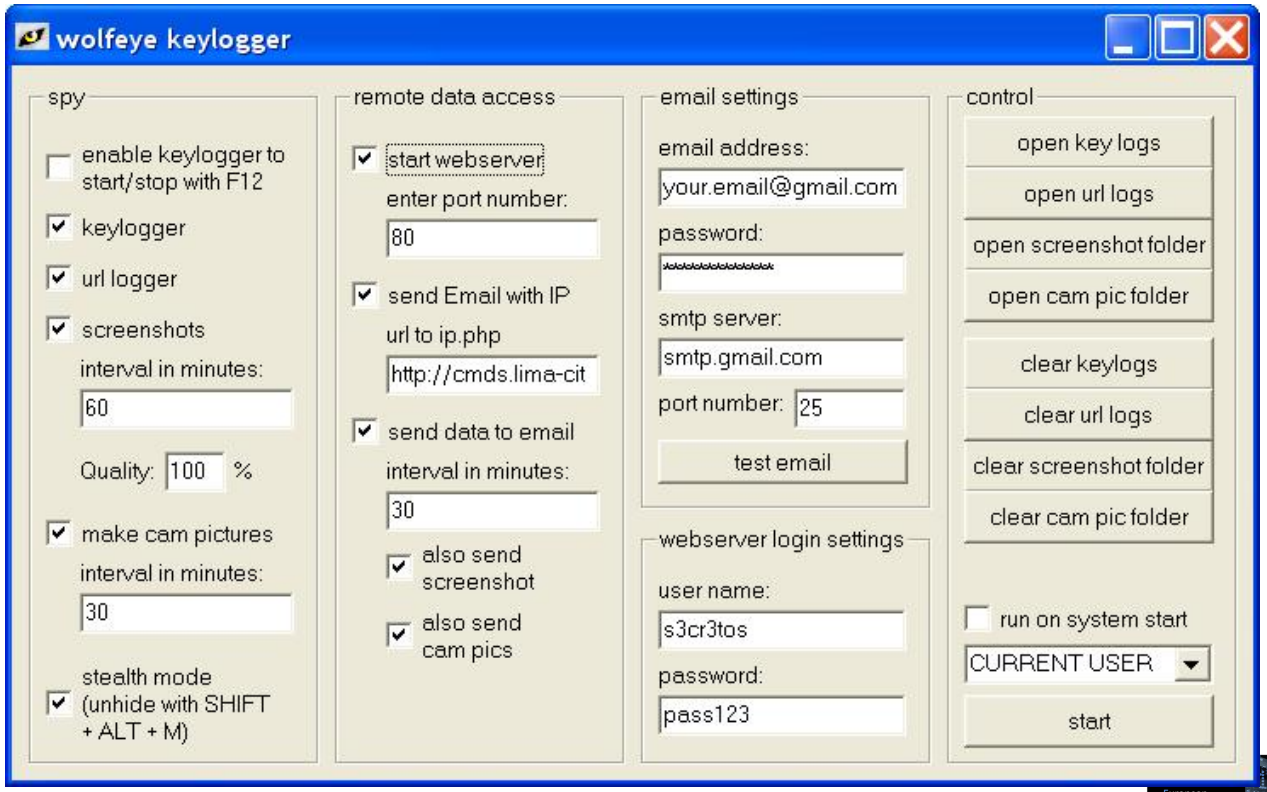
# Virus

## destructor de información



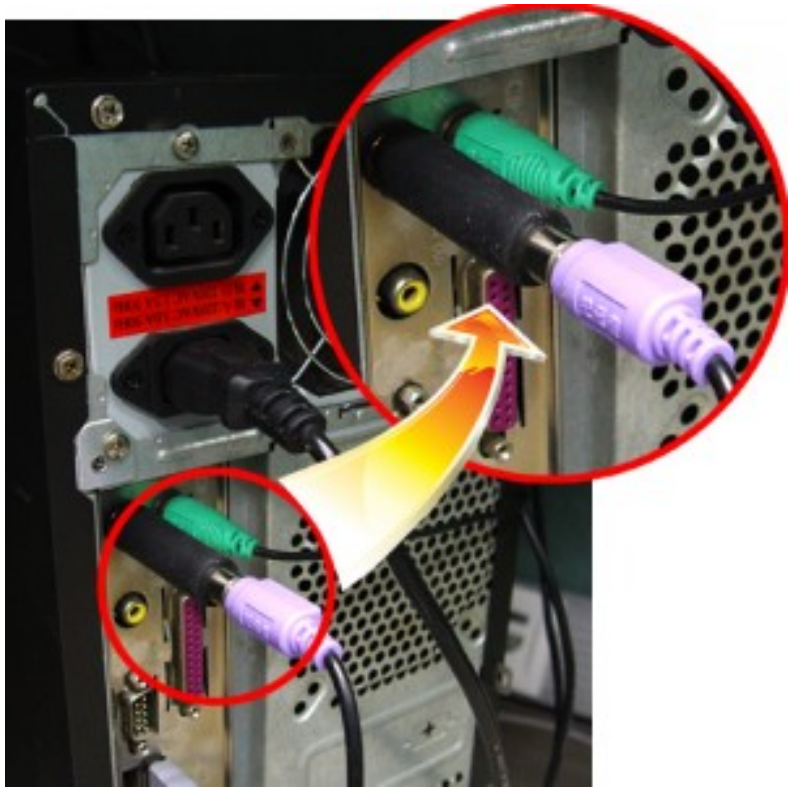
# Keyloggers

## el arma más peligrosa



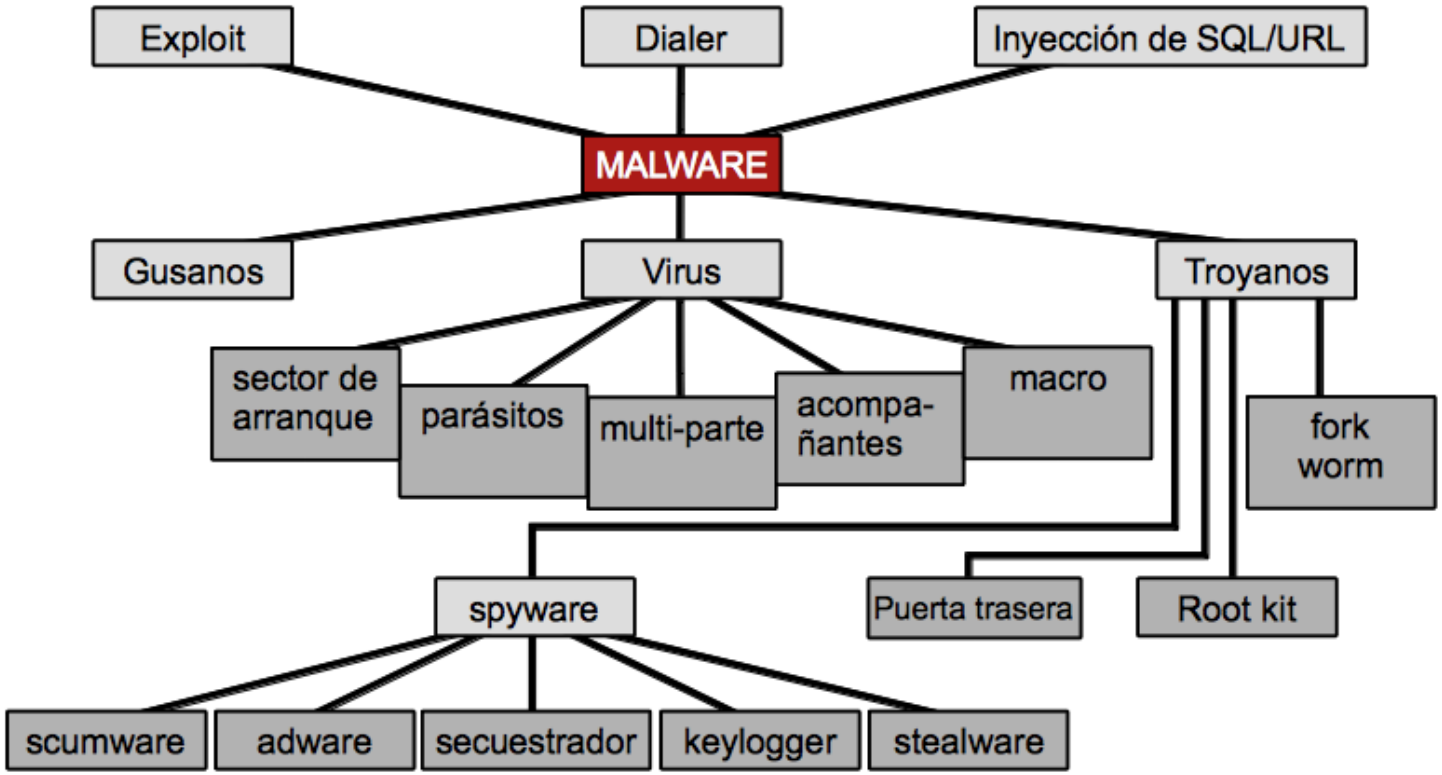
# Keyloggers

## el arma más peligrosa



# Genealogía de los bichos

## gran variedad de peligros y vectores



# Sabiduria e higiene

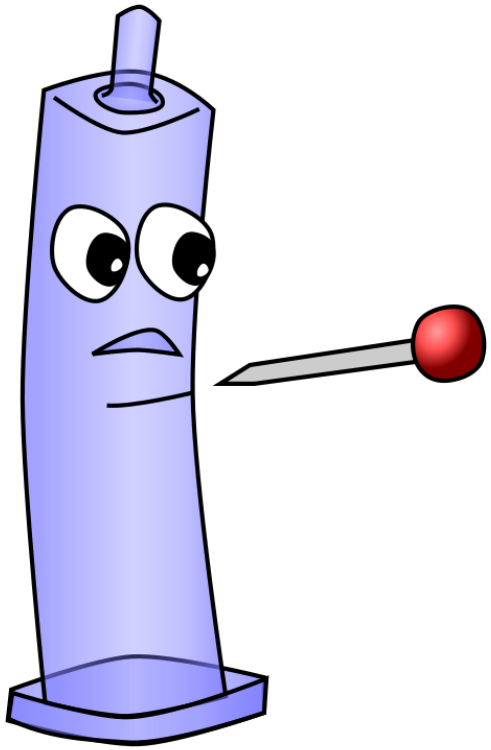
## reforcemos al eslabón débil

# Tratamiento

## antivirus y similares

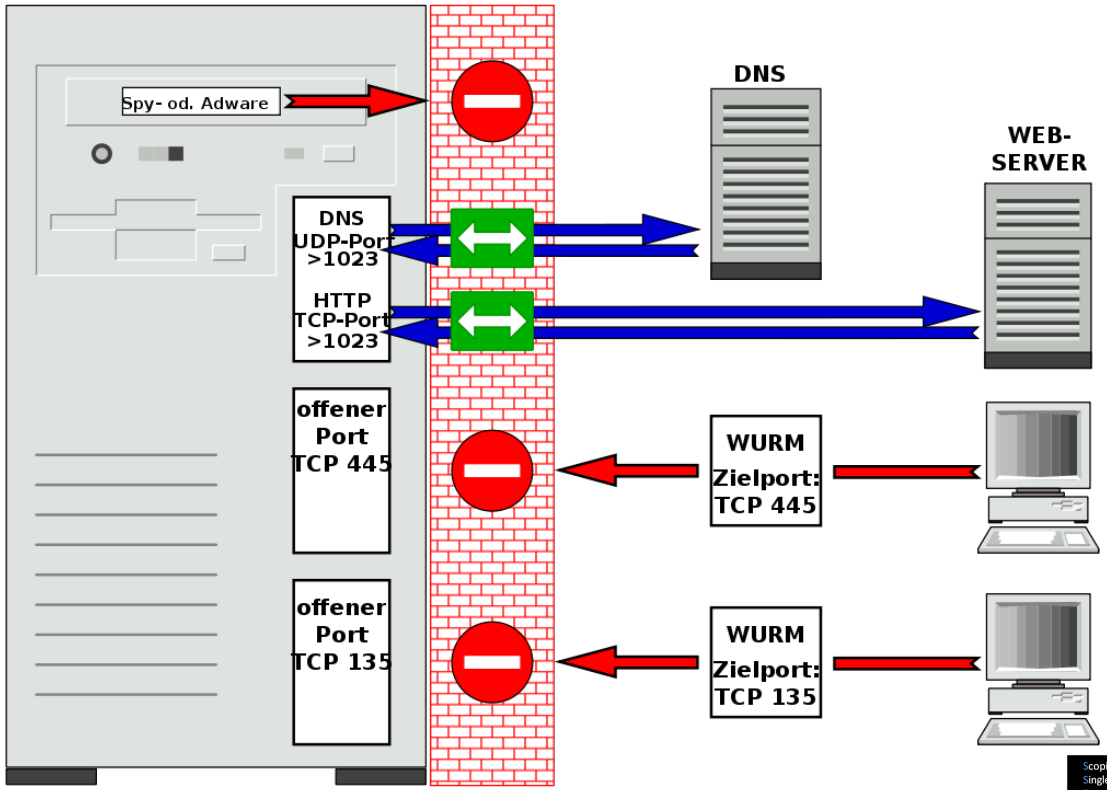
# Profilaxis

## antivirus y similares



# Profilaxis

## firewall personal



# Criptografía

## definiciones


SSEDIC Programme Partner

# Criptografía

## definiciones

Criptografía *(κριπτοσ γραφοσ)*

# Criptografía

## definiciones

Criptografía *(κριπτοσ γραφοσ)*

> *Ciencia de alterar la apariencia de los datos en un esfuerzo por mantenerlos seguros*


SSEDIC Programme Partner

# Criptografía

## definiciones

**Texto claro** Información que se desea proteger

**Texto cifrado** Información no inteligible

**Clave** Mapa que transforma el texto claro en el cifrado. De su tamaño depende la fortaleza del proceso


SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

# Criptografía

## definiciones

**Algoritmo criptográfico** Función matemática usada para cifrar y descifrar

**Esquema de cifrado** Cómo combinar texto, clave y algoritmo

**Función de dispersión** Obtiene la huella del texto claro


SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

# Una vía

## irreversible


SSEDIC Programme Partner

# Una vía

## irreversible

No es posible obtener el texto claro a partir del cifrado

```
$1$Bq28UJBA$1wY39esME6PIXGCdzNqg4.
```

# Simétrica

## un secreto entre dos

Emisor y receptor conocen la clave


SSEDIC Programme Partner

# Simétrica

## un secreto entre dos

Emisor y receptor conocen la clave

- Texto claro + clave = texto cifrado

# Simétrica

## un secreto entre dos

Emisor y receptor conocen la clave

- Texto claro + clave = texto cifrado
- Texto cifrado + clave = texto claro

# Simétrica

## un secreto entre dos

Es el método más antiguo,
ya lo usaban los judíos y Julio César

```
Inln phragb rfgb qry pvsenqb
```


SSEDIC Programme Partner

# Simétrica

## un secreto entre dos

Es el método más antiguo,
ya lo usaban los judíos y Julio César

```
ABCDEFGHIJKLMNOPQRSTUVXYZ
NOPQRSTUVWXYZABCDEFGHIKLM

Inln phragb rfgb qry pvsenqb
Vaya cuento esto del cifrado
```

# Simétrica

## un secreto entre dos

Pero, si la clave no es fuerte,
se puede descifrar por *fuerza bruta*

`Qnonyr neebm n yn mbeen ry nonq`


SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

# Simétrica

## un secreto entre dos

Pero, si la clave no es fuerte,
se puede descifrar por *fuerza bruta*

`Qnonyrneebmnynmbeenrynonq`


SSEDIC Programme Partner

# Simétrica

## un secreto entre dos

Pero, si la clave no es fuerte,
se puede descifrar por *fuerza bruta*

`Qnonyr neebm n yn mbeen ry nonq`


SSEDIC Programme Partner

# Simétrica

## un secreto entre dos

Pero, si la clave no es fuerte,
se puede descifrar por *fuerza bruta*

`Qnonyr neebm n yn mbeen ry nonq`

`Qeoeyr eeebm e ye mbeee ry eoeq`

# Simétrica

## un secreto entre dos

Pero, si la clave no es fuerte,
se puede descifrar por *fuerza bruta*

`Qnonyr neebm n yn mbeen ry nonq`

`Qaoayr aeebm a ya mbeea ry aoaq`


SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

# Simétrica

## un secreto entre dos

Pero, si la clave no es fuerte,
se puede descifrar por *fuerza bruta*

`Qnonyr neebm n yn mbeen ry nonq`

`Qaoayr arrbm a ya mbrra ry aoaq`

# Simétrica

## un secreto entre dos

Pero, si la clave no es fuerte,
se puede descifrar por *fuerza bruta*

`Qnonyr neebm n yn mbeen ry nonq`

`Qaoalr arrbm a la mbrra rl aoaq`


SSEDIC Programme Partner

# Simétrica

## un secreto entre dos

Pero, si la clave no es fuerte,
se puede descifrar por *fuerza bruta*

`Qnonyr neebm n yn mbeen ry nonq`

`Qaoale arrbm a la mbrra el aoaq`

# Simétrica

## un secreto entre dos

Pero, si la clave no es fuerte,
se puede descifrar por *fuerza bruta*

```
Qnonyr neebm n yn mbeen ry nonq

Qaoale arrbm a la mbrra el aoaq
Dabale arroz a la zorra el abad
```

# Asimétrica

## un secreto escondido y un secreto a voces

Conocida como criptografía de clave pública


SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

# Asimétrica

## un secreto escondido y un secreto a voces

Conocida como criptografía de clave pública

**Clave pública** Algo que debe ser muy conocido

**Clave privada** Lo que se debe proteger a toda costa

# Asimétrica

## un secreto escondido y un secreto a voces

Conocida como criptografía de clave pública

Clave pública Para que me puedan enviar mensajes cifrados

Clave privada Para descifrar lo que me envían

# Asimétrica

## un secreto escondido y un secreto a voces

Conocida como criptografía de clave pública

Clave pública Para que verifiquen lo que envío

Clave privada Para asegurar que lo envío yo

# Privacidad

## definiciones

del inglés *privacy*

1. *el estado o condición de estar libre de ser observado o molestado por otras personas*
2. *el estado de estar libre de la atención pública*

New Oxford American English Dictionary

SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

# Privacidad

## definiciones

### Privacidad

*Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión*

Diccionario de la Real Academia Española


SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

# Privacidad y criptografía

## proteger el mensaje

Gracias a la criptografia garantizamos el remitente

Firmo con mi clave privada Solo *yo* he podido firmar

Verifican con mi clave pública *Todos* pueden comprobarlo

# Privacidad y criptografía

## proteger el mensaje

Gracias a la criptografia garantizamos el destinatario y protegemos el contenido

Cifran con mi clave pública Solo *yo* podré leerlo

Descifro con mi clave privada *Nadie* puede *abirlo*


SSEDIC Programme Partner

# Almacenamiento

## todo un abanico para elegir

# Almacenamiento + criptografía =

## transporte seguro

# Correo-e + criptografía =

## mensajería segura



SSEDIC Programme Partner

# Gracias

## ¿Preguntas?

no se garantizan las respuestas


SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA