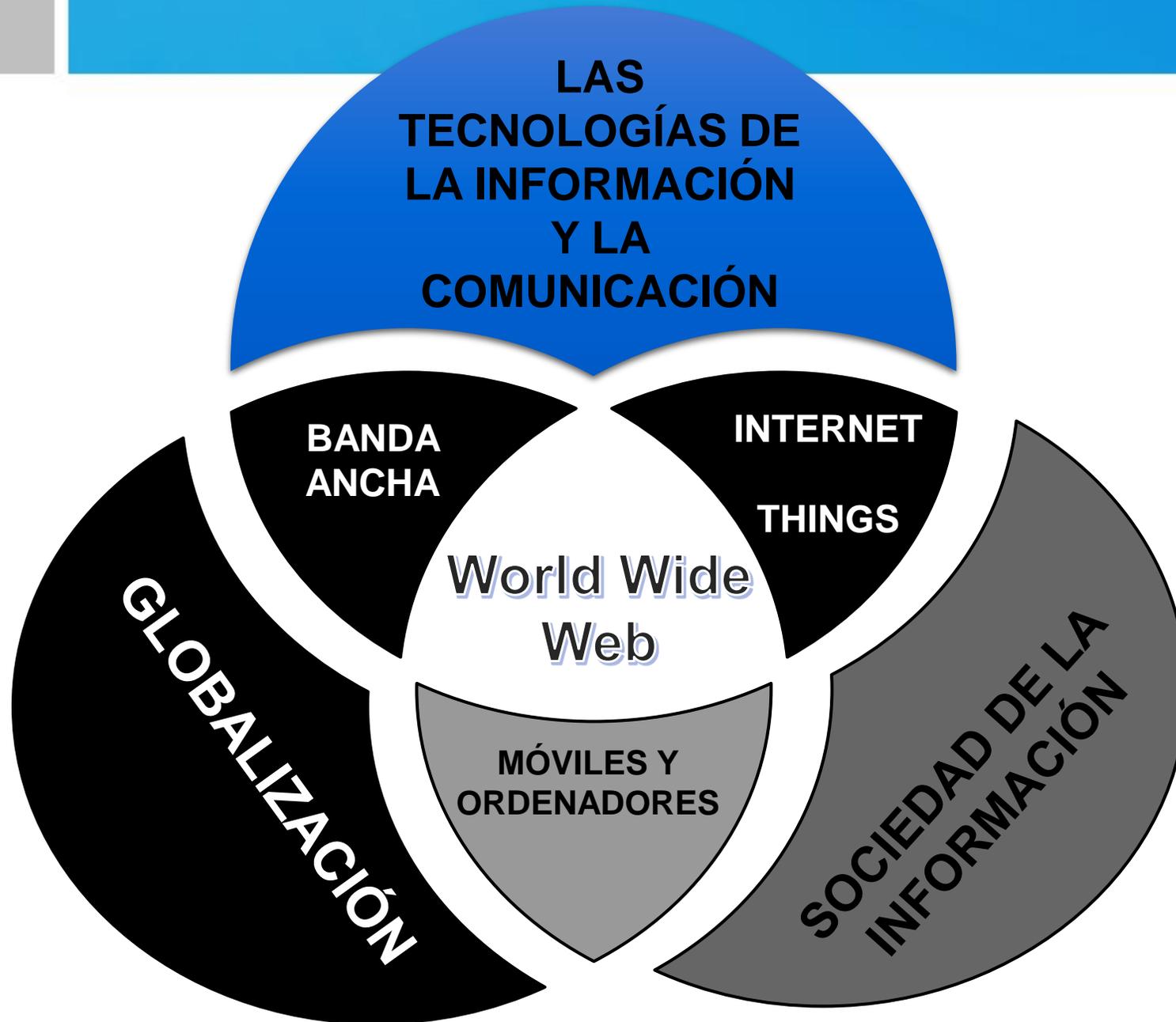


# Ciberseguridad

- 01. Concepto y Legislación
  - Causa de la ciberdelincuencia
  - Normativas de la Ciberseguridad





- La Ciberseguridad es un conjunto de herramientas y medidas de protección de los sistemas digitales

# Causas de la ciberdelincuencia

- Económicas
- Hacktivismo
- Espionaje industrial
  - gubernamental
  - particular
- Curiosidad, afán de sembrar caos

- **RGPD:** Responsabilidad proactiva, enfoque según riesgo desde un punto de vista europeo
- **Directiva NIS (Security of Network and Information Systems):** cooperación internacional a nivel UE. En cada país se designan CSIRTs (Computer Security Incident Response Teams)



## CSIRTs EN ESPAÑA

Entidades  
Públicas



**CCN** (Centro  
Criptográfico  
Nacional)

Particulares y  
Entidades Privadas



**INCIBE** (Instituto Nacional  
de **C**iberseguridad de  
España) ([www.incibe.es](http://www.incibe.es))

- 02. Evolución del virus a los ciberataques
  - Orígenes
  - Tipos
  - Desde 1990 hasta 2021

# Evolución de los ciberataques

1971: CREEPER- Primer virus informático en la red ARPANET.

1982: ELK CLONER- Primer virus en Apple II

1986: BRAIN- Virús para Pc IBM

1988: Viernes 13- Elimina todos los archivos cada viernes 13

**Periodo de baja implantación informática. Sobre todo tiene efecto en ámbitos militares, universitarios y de grandes empresas.**

# Evolución de los ciberataques

1998: CHERNOBIL- Infectó a ordenadores de todo el mundo, afectando al disco duro y al chip BIOS(Basic Input Output), localizado en la placa base, en la memoria ROM(Read Only Memory). Una vez apagado el ordenador la información sigue en la memoria.

1999: MELISSA- Difusión automática por mail.

**Periodo de incremento de la implantación informática. Empieza a ser un electrodoméstico más en los hogares. Juegos, trabajos y actividades privadas. Comienza el intercambio de mail, sustituyendo a la correspondencia tradicional. Las empresas comienzan a utilizar la página web como medio de comunicación con sus clientes.**

# Evolución de los ciberataques

2000: I love you- A través del mail infectó a millones de ordenadores.

2007: Italian Job- Infección de más de 10.00 webs italianas. Los visitantes de las webs extendían la infección.

2009: ZEUS: Ataque a Gobiernos, grandes instituciones y grandes corporaciones.

**Periodo de gran crecimiento en la implantación informática. Empieza a ser común la conectividad en las empresas y hogares por medio de WIFI. En 2007, comienza la interconexión de los terminales móviles (Blackberry y iPhone). Ecommerce y Redes Sociales empiezan su andadura.**

# Evolución de los ciberataques

2012: FLASHBACK- Troyano para Apple. Casi 1 millón de equipos infectados

2012: DROPBOX- Las contraseñas de más de 70 millones de usuarios se ven expuestas.

2013: CRYTOLOCKER: Primer ataque masivo de Ransomware.

2014: WIRELUCKER- Malaware para dispositivos con iOS (iPhone e iPad)

2014: WINDIGO- Servidores Linux redirigen el tráfico de 500.000 usuarios diarios a webs con malware

2015: XCODEGOSHT- La Apple Store se ve infectada por un código malicioso que infecta a más de 100 millones de usuarios.

# Evolución de los ciberataques

2016: MIRAI- Caída global de internet por varias horas. Miles de millones en pérdidas.

2016: HUMMINGBAD- Publicidad masiva en dispositivos Android. Más de 100 millones de terminales afectados.

2016: ACEDECEIVER: Robo de identidades en Apple.

2017: WANNACRY- Secuestro masivo de equipos informáticos en más de 150 países

**En 2020 llega la pandemia de Covid-19. Las casas comparten equipos informáticos para el desarrollo de actividades laborales y escolares. Muchas redes locales no están preparadas para esta situación inesperada y se producen ataques masivos.**

# EL CIBERCRIMEN SE MULTIPLICA



ALERTA

## Repunte de las campañas de phishing relacionadas con la pandemia COVID-19

Fecha de publicación: 19/03/2020

Nivel de peligrosidad: MUY ALTO

## Datos de 9 millones de clientes de easyJet se filtraron a causa de un ciberataque

La aerolínea británica low-cost fue víctima de un ciberataque que derivó en la filtración de datos personales de millones de clientes, entre ellos, detalles de más de 2000 tarjetas de crédito.



Juan Manuel Harán

19 May 2020 - 06:01PM

# EL CIBERCRIMEN SE MULTIPLICA

EUROPA

## Los ciberataques graves se duplicaron el año pasado en Europa en medio de la pandemia, según nuevas cifras

Por Nick Paton Walsh  
08:21 ET(12:21 GMT) 11 Junio, 2021



## Un ciberataque contra Phone House expone los datos bancarios de millones de clientes españoles

Afecta a los nombres, números de DNI, cuentas bancarias, emails, teléfonos, direcciones y fechas de nacimiento de 13 millones de clientes y trabajadores de la empresa

# EL CIBERCRIMEN SE MULTIPLICA

PORTADA | ECONOMÍA | EMPRESAS

España sufre 40.000 ciberataques diarios: administraciones y pymes, entre los objetivos más vulnerables

Alonso Trenado · Madrid  
21/06/2021 · 03:30h.

Un ciberataque a la "nube" pone en jaque a múltiples despachos profesionales

26 FEBRERO 2021

Un ciberataque a la nube pone en jaque a múltiples despachos profesionales de consecuencias incalculables

# EL CIBERCRIMEN SE MULTIPLICA

**El 'software' espía israelí Pegasus se usó en móviles de periodistas, activistas y empresarios de todo el mundo**

EFE NOTICIA 19.07.2021 - 03:01H



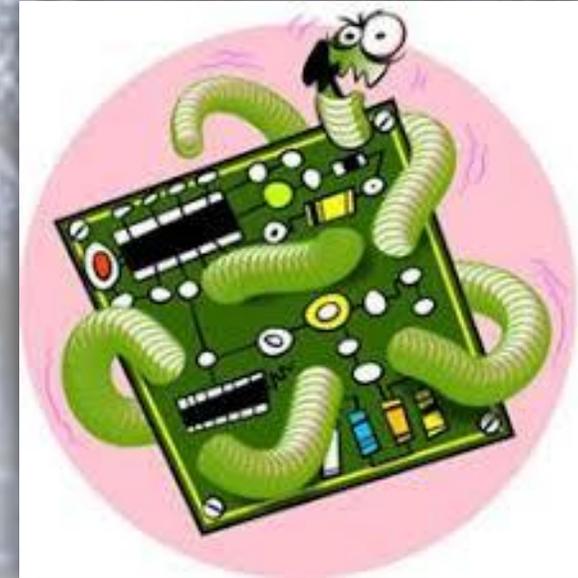
## TECNOLOGÍA

### Un ciberataque tumba los servicios de varios ayuntamientos de España

El servicio en la nube ASAC ha sufrido un ciberataque que ha dejado fuera de juego a ayuntamientos como el de Oviedo y a instituciones como el Tribunal de Cuentas

- 03. Diferentes ciberataques
  - Malware
  - Inteligencia Social
  - Otros ataques

- **VIRUS** -> Se autorreplican. Menos frecuentes hoy día. Provocan múltiples fallos de software



- **GUSANO** -> Se autorreplican y expanden a gran velocidad. Vehículo de entrada para otras clases de malware

**TROYANO** -> Se camuflan como software de confianza. Existen 4 tipos principales de troyanos:

**SCAREWARE** -> Bajo falsas advertencias de infección, se hace pasar por antivirus milagroso



Bancario



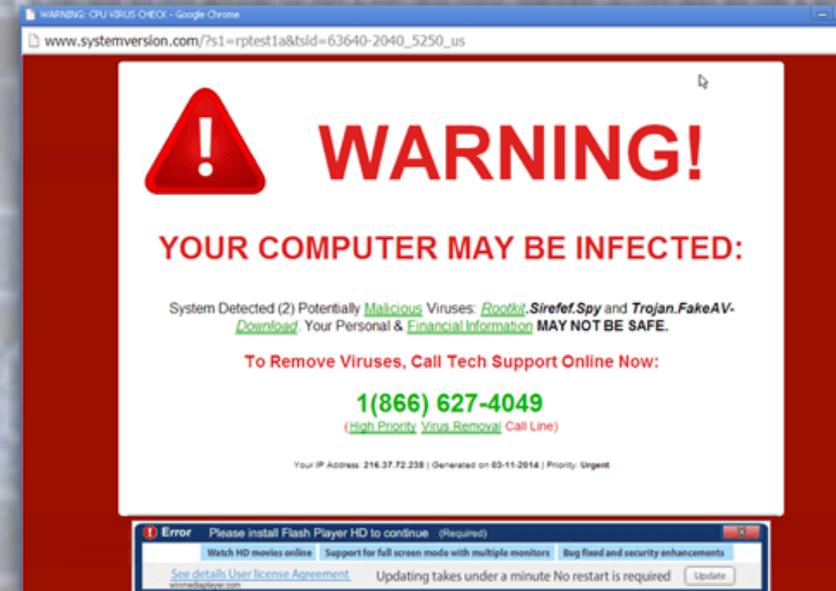
Backdoor/RAT



Zombie



Bomba de tiempo



**CRYPTOJACKING** -> Se aprovechan de ordenadores y móviles ajenos para minar criptomonedas



**SPYWARE** -> Keyloggers, cookies rastreadoras, spyware para móviles





```
usbcore: registered new driver hiddev
usbcore: registered new driver usbhid
drivers/usb/input/hid-core.c: v2.6:USB HID core driver
PNP: PS/2 Controller [PNP0303:KBC,PNP0F13:MOUSE] at 0x60,0x64 irq 1,12
serio: i8042 AUX port at 0x60,0x64 irq 12
serio: i8042 KBD port at 0x60,0x64 irq 1
mice: PS/2 mouse device common for all mice
md: md driver 0.90.3 MAX_MD_DEVS=256, MD_SB_DISKS=27
md: bitmap version 4.39
TCP bic registered
Initializing IPsec netlink socket
NET: Registered protocol family 1
NET: Registered protocol family 17
Using IPi No-Shortcut mode
Time: tsc clocksource has been installed.
ACPI: (supports S0 S1 S5)
md: Autodetecting RAID arrays.
md: autorun ...
md: ... autorun DONE.
RAMDISK: Compressed image found at block 0
Invalid compressed format (err=2)
VFS: Cannot open root device "<NULL>" or unknown
Please append a correct "root=" boot option
Kernel panic - not syncing: VFS: Unable to mount
-
```

➤ **ROOTKITS** -> Pasan inadvertidas con facilidad. Dan privilegios Root (administrador) y ocultan malware. Muy habituales en Linux



recopilación de la información completa de usted y contra usted será instruida una causa criminal.

**El monto de su multa es de €100 euros.**  
**La multa puede ser pagada con PaySafeCard o Ukash vouchers.**

Una vez pagada la multa y los medios monetarios serán traspasados a la cuenta del estado, su teléfono será desbloqueado y toda la información se puede descifrar en un plazo de 24 horas.

Después, usted tendrá que eliminar durante los 7 días todas las infracciones relacionadas con su teléfono. En caso de no eliminar las

IP: [REDACTED]  
País: Spain  
Región: [REDACTED]  
Ciudad: [REDACTED]

**¡ATENCIÓN! Su teléfono ha sido bloqueado por razones de seguridad vistos los motivos abajo detallados.**  
**Todas las acciones hechas en este teléfono,**

**RANSOMWARE** -> Encriptan la información y piden rescate en Bitcoins. Antiguamente lo pedían en Euros o Dólares Recientemente ha evolucionado a Ransomware de doble extorsión

You became victim of the PETYA RANSOMWARE!

The harddisks of your computer have been encrypted with an military grade encryption algorithm. There is no way to restore your data without a special key. You can purchase this key on the darknet page shown in step 2.

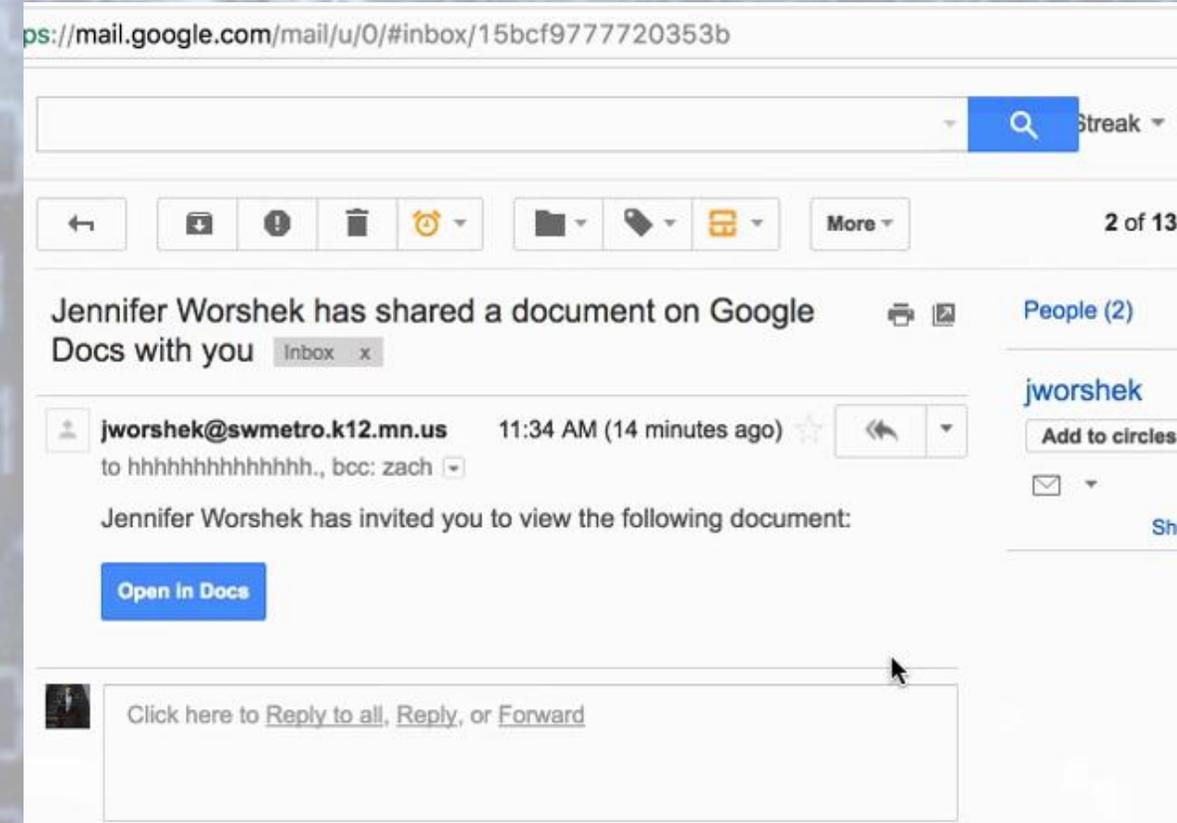
To purchase your key and restore your data, please follow these three easy steps:

1. Download the Tor Browser at "<https://www.torproject.org/>". If you need help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:  
[http://petya\[REDACTED\].onion/g](http://petya[REDACTED].onion/g)  
[http://petya\[REDACTED\].onion/g](http://petya[REDACTED].onion/g)
3. Enter your personal decryption code there:  
a6[REDACTED]  
nF[REDACTED]

If you already purchased your key, please enter it below.

Key: \_

- **PHISHING** -> Suplantación de identidad mediante estafas por correo, o SMS (smishing) o llamadas de voz (vishing)
- **SPEAR PHISHING** (personalizado)-> Whaling

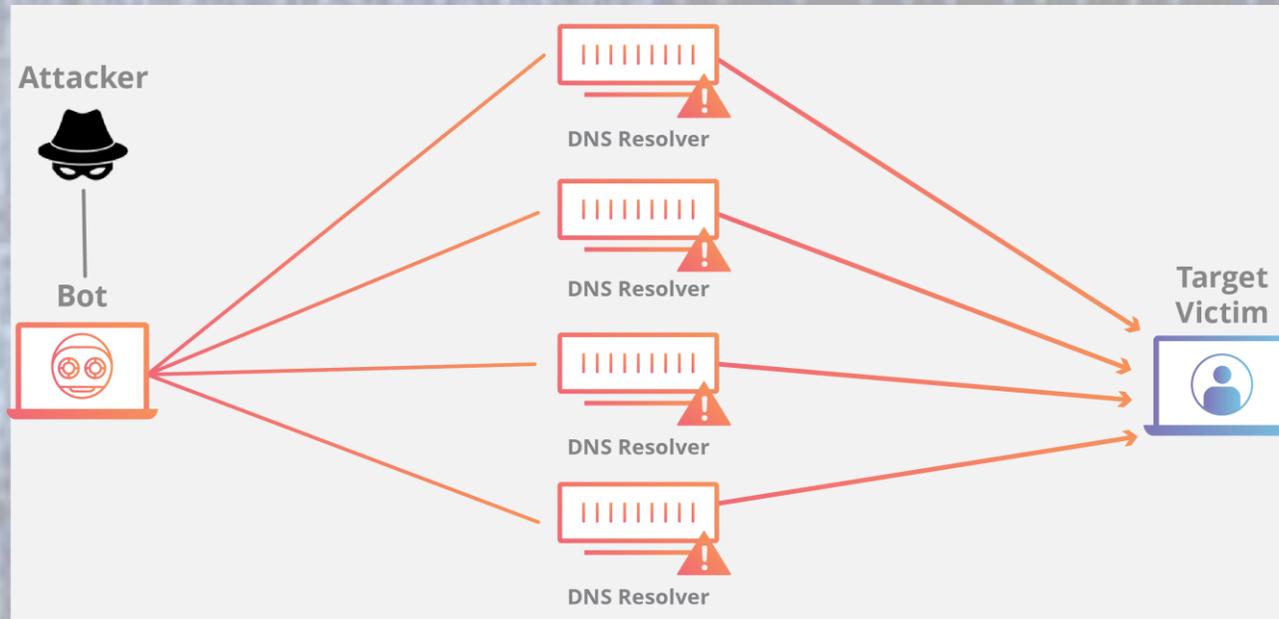
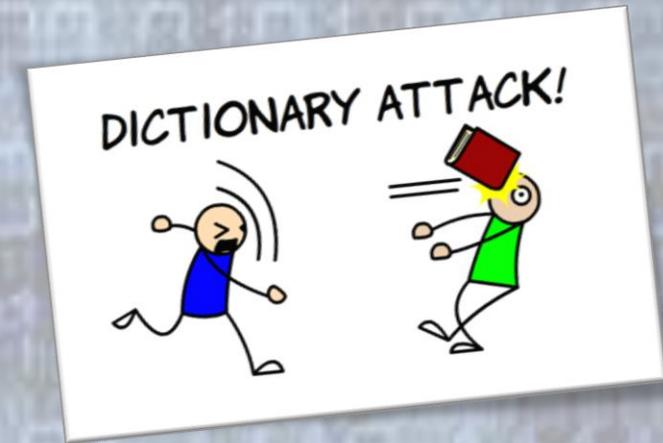


- **PHARMING** -> Redirección a webs clonadas para robar datos
- **MAN IN THE MIDDLE** -> Sniffer de paquetes en la misma WiFi



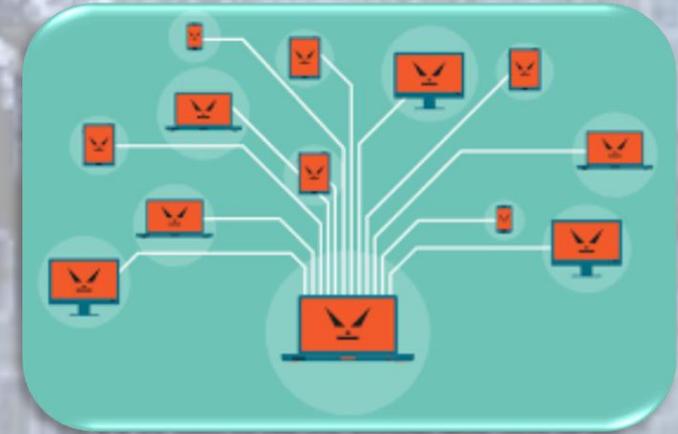
# Otras clases de ataques

- **DDoS** (Denegación de servicio)
- **FUERZA BRUTA** (Diccionario)



# Otras clases de ataques

- **SQL INJECTION** -> Acceso a la BBDD de una web
- **BOTNET** (Ejército Zombie)



# Caso Real

The screenshot shows a web browser window displaying the iCloud Mail interface. The address bar shows 'icloud.com/mail/'. The left sidebar contains navigation options for 'Buzones' (Inboxes) and 'Carpetas' (Folders). The main content area shows the 'Bandeja de entrada' (Inbox) with 9,600 messages. A prominent blue banner highlights an 'Mensaje Importante' (Important Message) from Enrique Ramos Dominguez, dated 17:28. The subject of the message is 'Alerta : N°307 CXS30701-ESP8306-XBM3070'. The message body contains the following text:

**Mensaje Importante** 17:28  
Para: Enrique Ramos Dominguez

**Alerta : N°307 CXS30701-ESP8306-XBM3070**

**Distinguido señor:**  
**Distinguida señora:**

Le informamos que Su firma electrónica ha sido revocada por motivos de seguridad.

**Hora de operación: 01/20/2022 05:28:05 pm**

A Partir de la fecha anterior, no puede realizar ninguna operación desde su Banca Online hasta que reactive su firma electrónica.

Si la operación no la hizo usted, ingrese al enlace de arriba y reactive su firma electrónica :

[Haga clic aquí](#) y verifique su identidad Cuenta

- En este sentido, debemos significarle que, si transcurridos veinte días naturales a partir de la fecha de la retención el citado organismo no nos ordena la suspensión del embargo, estaremos obligados a hacer efectivo el importe retenido.

The Windows taskbar at the bottom shows the search bar, system tray with icons for various applications, and the system clock displaying 18:50 on 20/01/2022.

- 04. Repercusiones de un ciberataque
  - Daños propios
  - Pérdida de Identidad
  - Pérdida de Información
  - Fraude
  - Paralización de la Actividad
  - Costes
  - Sanciones
  - Reclamación de Terceros
  - Pérdida reputacional

# Repercusiones de un ciberataque

Daños propios



Robos de identidad digital

- Credenciales,
- Certificados electrónicos
- Datos biométricos
- Etc.

# Pérdidas de información

## Repercusiones de un ciberataque



# Repercusiones de un ciberataque

Fraude/ extorsión  
cibernética

- **Ingeniería social y malware (principalmente ransomware)**

Paralización de  
actividad

- **Desde unos días hasta meses.**



# Repercusiones de un ciberataque

Gastos  
humanos

**INVESTIGACIÓN**

**RECUPERACIÓN**

**NOTIFICACIÓN**

**ASESORAMIENTO  
Y DEFENSA  
LEGAL**

**NUEVO  
PERSONAL**

**RELACIONES  
PÚBLICAS**

# Repercusiones de un ciberataque

## Sanciones administrativas

**•Plazo de 72 horas para notificar brecha a la AEPD. Sanciones desde 40.000 € y hasta 20 millones de euros o 4% de la facturación anual**

### 600.000€ de sanción por notificación tardía de una brecha de seguridad

Durante el presente mes de marzo, la Agencia Española de Protección de datos, ha emitido una resolución por la que acuerda sancionar a una aerolínea española de 600.000€ por la notificación tardía de una brecha de seguridad con más de 489.000 implicados, sin justificación válida para dicho retraso en la notificación.



The screenshot shows a Business Insider article. The header includes the Business Insider logo, navigation links for 'Economía', 'Tecnología', 'Estrategia', 'Política', and 'Más temas', a search icon, and a 'Suscríbete' button. The main headline reads: 'La AEPD ha impuesto más de 23 millones de euros en sanciones en lo que va de año, un 500% más de las multas que había propuesto entre 2018 y 2020'. Below the headline, the author 'Alberto R. Aguiar' and the date '14 may. 2021 6:00h.' are visible. Social media sharing icons for Facebook, Twitter, LinkedIn, and WhatsApp are located at the bottom right of the article preview.

# Repercusiones de un ciberataque

## Reclamaciones de terceros

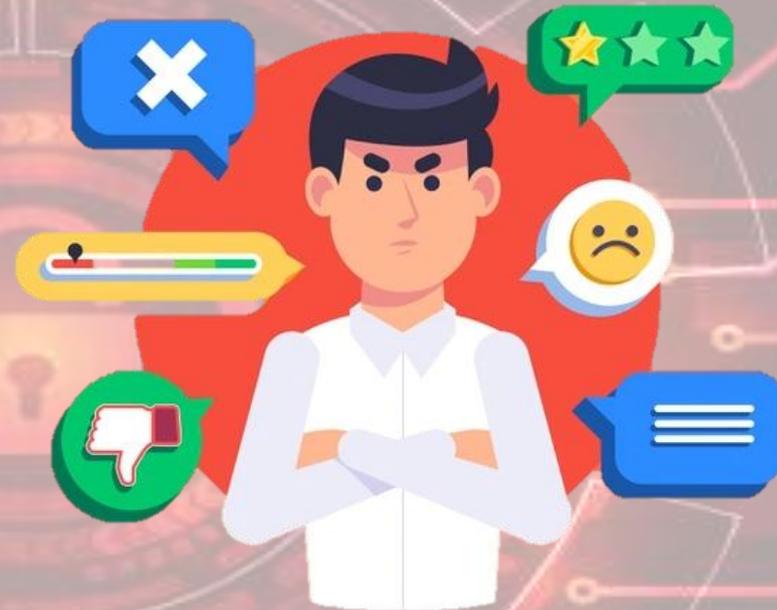
- Clientes, empleados y proveedores cuyos datos hayan sido expuestos



# Repercusiones de un ciberataque

## Daños reputacionales

- **Pérdida de confianza de clientes, proveedores e inversores**



# Repercusiones de un ciberataque

## Cierre de negocio

**6 de cada 10 PYMEs  
desaparece a los 6 meses de  
sufrir un ciberataque**



- 05. Prevención de un ciberataque
  - Software original y actualizado
  - Webs Http
  - Contraseñas
  - Back up

# ¿Cómo prevenir un ciberataque?

## 1) SOFTWARE ORIGINAL

- El software pirata presenta mayor cantidad de vulnerabilidades
- A menudo los cracks (activadores) contienen malware



## 2) MANTENER SOFTWARE ACTUALIZADO

- Sistema operativo, programas, aplicaciones, complementos, etc.

# ¿Cómo prevenir un ciberataque?

## 3) EVITAR WEBS HTTP



## 4) CONTRASEÑAS SEGURAS Y 2FA

- El 2FA no es infalible, aunque supone una capa extra de seguridad.



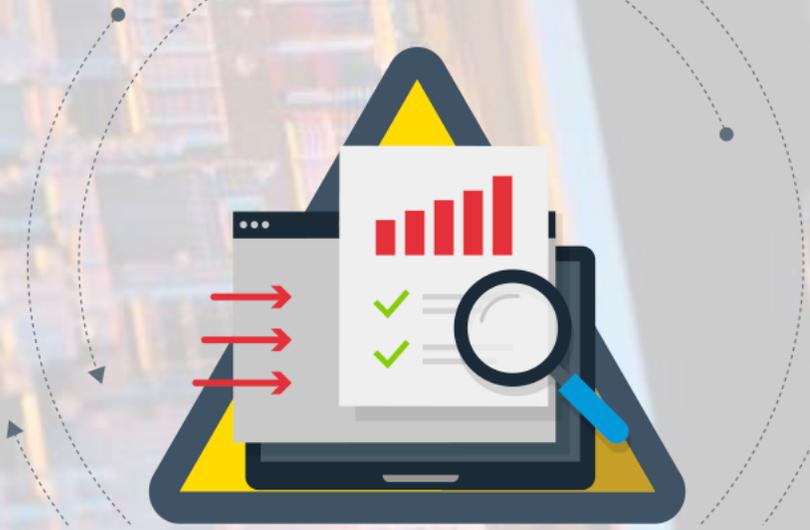
# ¿Cómo prevenir un ciberataque?

## 5) Correo electrónico

- **Desactivar descarga automática de archivos (desde aplicaciones)**
- **Descargar sólo archivos de confianza, y analizarlos antes de su apertura**
- **Evitar conectarse desde redes wifi públicas y/o sin seguridad WPA2. Preferible con datos móviles en tales casos**
- **Cifrar correos entrantes y salientes con protocolo TLS/SSL**
- **No hacer clic sobre enlaces de remitentes desconocidos o poco fiables**
- **Cerrar sesión al terminar (desde navegador)**

# ¿Cómo prevenir un ciberataque?

## 6) Análisis de vulnerabilidades (pentesting)



### **Pentesting**

Conoce tus debilidades para corregirlas



## 7) Antivirus

- Actualizado, correctamente configurado y realizar análisis periódicamente. Aplicable a sistemas operativos de escritorio y móviles

# ¿Cómo prevenir un ciberataque?

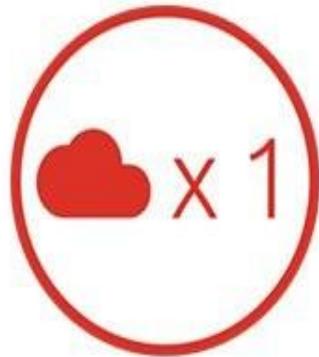
## 8) BACKUP: Regla 3-2-1



Crear **3** copias de los datos  
(1 original y dos secundarias)



Al menos **2** tipos de formatos de  
almacenamiento distintos



Amacena **1** fuera del  
lugar de trabajo

## 9) ALMACENAMIENTO EXTERNO:

- Deshabilitar la apertura automática
- Analizar antes de abrir
- Cifrar contenido sensible

# ¿Cómo prevenir un ciberataque?

## 10) REFORZAR SEGURIDAD ROUTER:

- Actualizar firmware
- Cambiar SSID y contraseña WiFi de fábrica
- Cambiar contraseña WiFi con asiduidad
- Cambiar credenciales predeterminados de acceso al router
- Establecer protocolo de seguridad WPA2-AES
- Configurar firewall



# ¿Cómo prevenir un ciberataque?

## 11) DESCARGAR SOFTWARE SÓLO DESDE FUENTES DE CONFIANZA

- Verificados por la propia Store del sistema operativo, o suministrado a través del propio fabricante/desarrollador

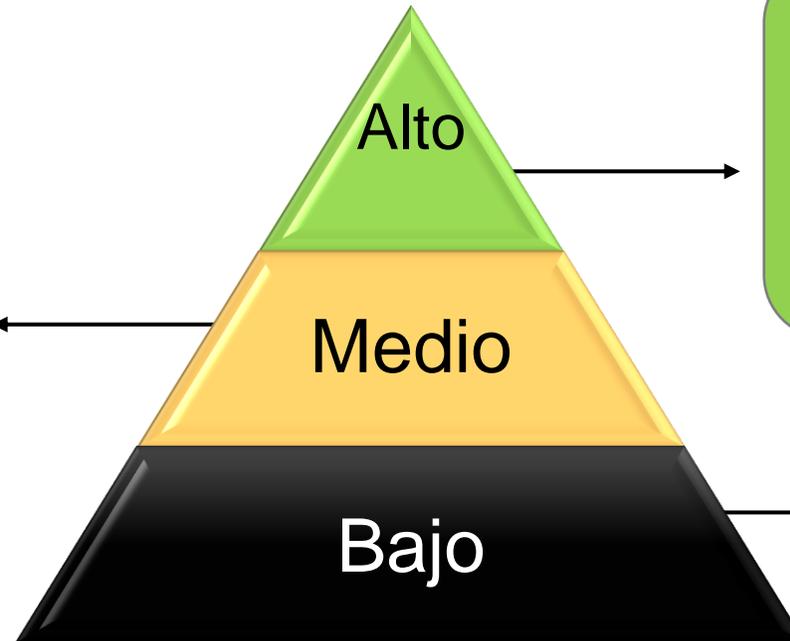
## 12) Formación



- 06. Gestión del incidente
  - Fases
  - Ciberseguro

# Grado de madurez cibernética en una empresa

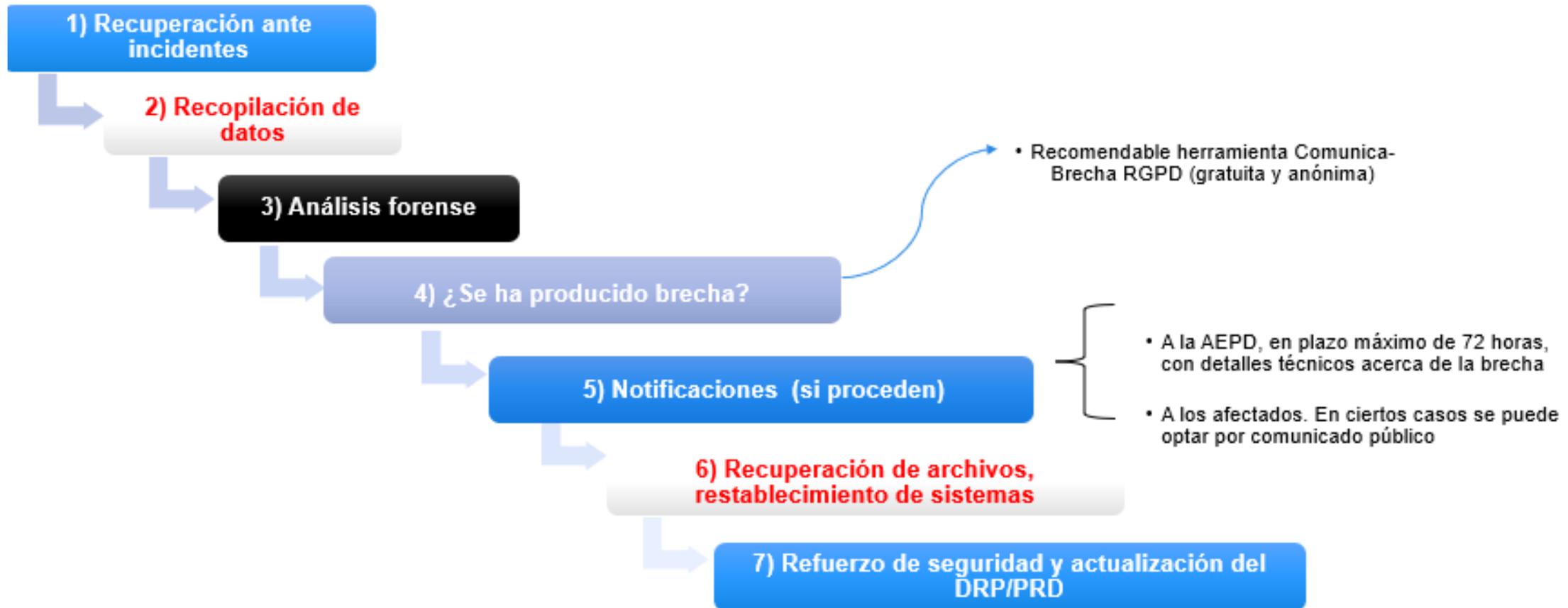
Combina con formación continua, pentesting frecuente y medidas de monitorización y detección de intrusiones



Incorpora Plan de Recuperación ante Desastres (actualizable) y continuidad de negocio. También incorpora ciberseguro

Sólo tecnología para prevención

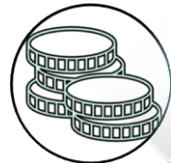
# FASES DE LA GESTIÓN TÉCNICA DE INCIDENTES



# COBERTURAS de CIBERSEGURO



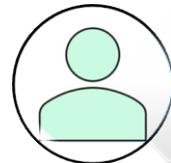
Gestión técnica de incidentes



-Gastos de defensa y fianzas



-Gastos de emergencia



-Daños propios



Fraude y extorsión cibernéticos

# COBERTURAS de CIBERSEGURO



-Sanciones  
administrativas



-Responsabilidad ante  
terceros



-Pérdidas de beneficios



-Restitución de imagen



-Etc.

# Datos de la AEPD 2022

Reclamaciones planteadas con mayor frecuencia	2020	2021	% relativo	Δ% anual
<b>TOP 10</b>	<b>7.727</b>	<b>10.840</b>	<b>78%</b>	<b>40%</b>
Servicios de Internet	1.602	2.220	16%	39%
Videovigilancia	1.189	1.736	12%	46%
Publicidad (excepto spam)	681	1.528	11%	124%
Ficheros de morosidad	1.510	1.284	9%	-15%
Reclamación de deudas	656	859	6%	31%
Administración pública	503	740	5%	47%
Sanidad	388	680	5%	75%
Comercios, transporte y hostelería	405	663	5%	64%
Entidades financieras/acreedoras	437	643	5%	47%
Publicidad a través de e-mail o teléfono móvil	356	487	4%	37%
<b>Otros</b>	<b>2.597</b>	<b>3.065</b>	<b>22%</b>	<b>18%</b>
<b>TOTAL</b>	<b>10.324</b>	<b>13.905</b>	<b>100%</b>	<b>35%</b>

MUCHAS GRACIAS POR SU ATENCION



**CONTACTO:**

**Enrique Ramos**

**Teléfono 664 670 785**

**Mail:**

**[eramos@recoletosconsultores.es](mailto:eramos@recoletosconsultores.es)**