

# Sistemas Informáticos

---

## UD 13. Seguridad Informática



*" El único sistema verdaderamente seguro es el que está apagado y desenchufado encerrado en una caja fuerte de titanio revestido, enterrado en un búnker de hormigón, y rodeado por gas nervioso y guardias armados muy bien remunerados. Incluso entonces, no apostaría mi vida por él."*

*Gene Spafford*

# ÍNDICE

1. Introducción a la Seguridad Informática.....	4
1.1. La sociedad de la información en que vivimos .....	4
1.2. Seguridad informática y seguridad de la información .....	4
1.3. Principios básicos de la seguridad de la información .....	5
1.4. Conceptos básicos en seguridad de la información.....	6
1.5. Tipos de amenazas y atacantes.....	6
1.6. El ciclo de vida de la seguridad informática.....	7
2. Clasificación de medidas de seguridad informática.....	10
2.1. Clasificación de medidas de seguridad .....	10
2.2. Seguridad física .....	10
2.3. Seguridad lógica .....	11
2.4. Seguridad activa .....	12
2.5. Seguridad pasiva .....	12
3. Software malicioso: medidas preventivas y paliativas .....	14
3.1. Software malicioso y su impacto actual.....	14
3.2. Clasificación del malware.....	14
3.2.1. Virus .....	15
3.2.2. Gusano .....	16
3.2.3. Troyano .....	17
3.2.4. Rootkit.....	17
3.2.5. Backdoor .....	17
3.2.6. Spyware.....	18
3.2.7. Adware .....	18
3.2.8. Hijackers.....	18
3.2.9. Dialers .....	19
3.2.10. Keyloggers.....	19
3.2.11. Stealers.....	19
3.2.12. Botnets .....	19
3.2.13. Rogueware .....	20
3.2.14. Ransomware .....	21
3.3. Medidas preventivas y paliativas .....	22
3.4. Pautas y prácticas seguras .....	23
4. Certificados digitales y firma digital.....	25
4.1. Criptografía de clave pública.....	25
4.2. Infraestructura de clave pública (PKI).....	26
4.2.1. Certificados digitales .....	27
4.2.2. Firma digital .....	32
4.3. Protocolos seguros: SSL/TLS y HTTPS.....	33

5.	Vulnerabilidades y ataques en redes informáticas .....	34
5.1.	Introducción a la seguridad en redes.....	34
5.2.	La seguridad heredada.....	34
5.3.	Ataques comunes en redes locales.....	35
5.3.1.	Man In The Middle.....	35
5.3.2.	Envenenamiento ARP.....	36
5.3.3.	Ataques al DHCP.....	37
5.3.4.	Ataques al DNS.....	38
5.3.5.	Ataques a SSL/TLS .....	40
5.4.	Ataques por correo electrónico y mensajería.....	40
5.5.	Seguridad perimetral: cortafuegos .....	44
6.	Seguridad en redes inalámbricas y redes privadas virtuales .....	47
6.1.	Seguridad en redes inalámbricas .....	47
6.1.1.	Mecanismos de cifrado en redes wifi .....	47
6.1.2.	Ataques a redes wifi.....	50
6.1.3.	Mecanismos de protección .....	53
6.2.	Redes privadas virtuales .....	55
7.	Alta disponibilidad en redes.....	57
7.1.	Alta disponibilidad .....	57
7.2.	Redundancia y tolerancia a fallos .....	57
7.2.1.	Redundancia.....	57
7.2.2.	Tolerancia a fallos .....	61
7.3.	Sistemas de clusters.....	61
7.3.1.	Clasificación de los clusters.....	62
7.4.	Balanceadores de carga .....	62
7.4.1.	Algoritmos de balanceo .....	63
7.4.2.	Topologías o modos de balanceo.....	63
7.5.	Redundancia en enrutadores.....	65
8.	Bibliografía .....	67

# 1. Introducción a la Seguridad Informática

## 1.1. La sociedad de la información en que vivimos

Actualmente vivimos en lo que se conoce como la Sociedad de la Información. Para cualquier organización - ya sea con ánimo de lucro o sin él, privada o pública - el activo más valioso es la información. Incluso cualquiera de nosotros, en nuestro ámbito particular, dependemos enormemente de la información que manejamos a diario para nuestras actividades.

Esta información lleva sufriendo un proceso de digitalización desde hace años y se está eliminando poco a poco el soporte papel, de forma que casi todos tenemos recibos en formato electrónico, hacemos la declaración de la renta de forma telemática y guardándola en pdf, tenemos nuestras fotos familiares en un disco duro o en la nube, o compramos entradas, libros o servicios a través de una pasarela de pago. Todo de manera digital.



Esto son pequeños ejemplos de nuestra vida cotidiana, pero las organizaciones y empresas van más allá. Muchos de sus canales de compra y venta, y por tanto, sus beneficios, son a través de Internet. Internet abre nuevas posibilidades de negocio para muchas empresas, que pueden globalizarse y llegar a vender sus productos y servicios a rincones del mundo donde no podrían llegar de otra forma.

La seguridad informática no es algo que debamos tomar a la ligera y todo el mundo deberíamos tener un mínimo de formación en este campo.

Muchas veces, es mejor aplicar el sentido común, que comenzar a aplicar medidas técnicas a lo loco (cortafuegos, antivirus, antiadware, etc) pensando que la tecnología nos puede proteger por sí sola. Gran parte de los incidentes de seguridad que nos ocurren, son debidos a fallos en la capa más vulnerable de todo el sistema: el factor humano.

De la misma manera que en la vida real no nos fiamos de algún desconocido que llame a la puerta haciéndose pasar por una inspección de gas de la que no nos han informado, tampoco deberíamos abrir correos electrónicos de extraños, aceptar desconocidos en redes sociales o conectarnos a wifi abiertas, por citar algunos ejemplos.

## 1.2. Seguridad informática y seguridad de la información

A continuación, definiremos los conceptos de seguridad de la información y seguridad informática:

### **Seguridad de la información**

Por seguridad de la información entendemos el conjunto de medidas y procedimientos, tanto humanos como técnicos, que permiten proteger la integridad, confidencialidad y disponibilidad de la información.

Este término, por tanto, es un concepto amplio que engloba medidas de seguridad que afectan a la información independientemente del tipo de ésta, soporte en el que se almacene, forma en que se transmita, etc.

## Seguridad informática

La seguridad informática, por su parte, es una rama de la seguridad de la información que trata de proteger la información que utiliza una infraestructura informática y de telecomunicaciones para ser almacenada, procesada o transmitida.

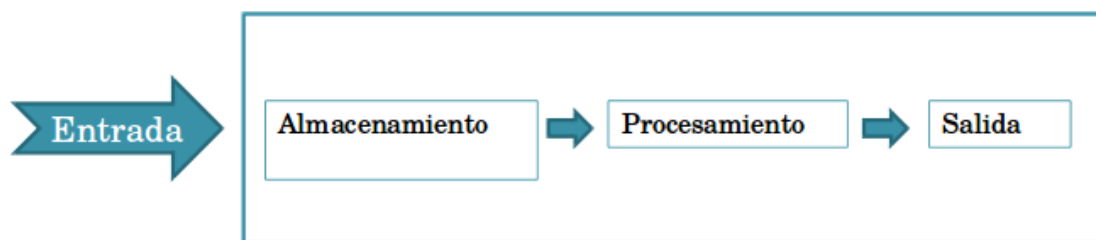
Mira este vídeo de Criptored (Red Temática Iberoamericana de Criptografía y Seguridad de la Información) donde se explican ambos conceptos claramente: <https://youtu.be/7MqTpfEreJ0>

Por tanto, podemos decir que la seguridad de la información es un concepto mucho más amplio, que engloba a la seguridad informática. O dicho de otra forma, la seguridad de la información se encarga de proteger el **sistema de información** de una organización y la seguridad informática, se encarga de proteger los **sistemas informáticos**, que son el soporte o infraestructura de ese sistema de información.

Un **sistema de información** es el conjunto de elementos organizados, relacionados y coordinados, para ayudar a una empresa u organización a conseguir sus objetivos. Dichos elementos pueden clasificarse en:

- **Recursos:** pueden ser físicos (ordenadores, periféricos, recursos no informáticos) y lógicos (S.O., aplicaciones...)
- **Equipo humano**
- **Información:** datos organizados que tienen significado para la organización
- **Procesos**

Por otra parte, un **sistema informático** está formado por un conjunto de elementos físicos (hardware, dispositivos, periféricos...), lógicos (sistema operativo., aplicaciones, protocolos...) y con frecuencia también elementos humanos y que permite a la organización crear, almacenar o procesar la información.



*Esquema simplificado de un sistema informático*

### 1.3. Principios básicos de la seguridad de la información

La organización **ISO/IEC**, en su norma **27000** define lo que son los tres principios básicos de la seguridad de la información, o lo que se conoce también como triada CIA: **confidencialidad**, **integridad** y **disponibilidad**. En el siguiente vídeo de criptored, se definen claramente esos tres principios básicos: [https://youtu.be/KWafVhy\\_GQ8](https://youtu.be/KWafVhy_GQ8)

Además de estos tres principios básicos, existen otros adicionales como son:

- **Autenticación:** consiste en verificar la identidad del usuario de la información como la de su creador
- **Control de acceso:** permite restringir los accesos a los recursos en función de los permisos asignados a cada usuario
- **No repudio:** relacionado con la autenticación, prueba la participación de ambas partes en una comunicación o transacción de tal forma que no se puede negar haber participado en ella. Puede ser:
  - En **origen:** el emisor no puede negar el envío. P.ej: presentación telemática del IRPF con el programa PADRE
  - En **destino:** el receptor no puede negar haber recibido la información pues el emisor tiene pruebas de la recepción
- **Trazabilidad:** es la capacidad de registro de las operaciones de un sistema informático, de manera que cualquier operación pueda ser rastreada hasta su origen. Nos va a permitir poder realizar un análisis forense de un incidente de seguridad

## 1.4. Conceptos básicos en seguridad de la información

En el campo de la seguridad de la información, se trabaja con una serie de términos y conceptos que conviene conocer. Destacamos los más importantes:

- **Activo:** recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.
- **Amenaza:** es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.
- **Impacto:** mide la consecuencia al materializarse una amenaza.
- **Riesgo:** mide la probabilidad de que produzca un incidente de seguridad en un activo, en un dominio o en toda la organización. El riesgo se relaciona con el impacto. El impacto mide lo que puede pasar. El riesgo lo que probablemente pase.
- **Vulnerabilidad:** debilidad inherente en cualquier sistema informático de ocurrencia de la materialización de una amenaza sobre un Activo. La vulnerabilidad se relaciona con la amenaza ya que un sistema puede ser más o menos vulnerable respecto a una amenaza.
- **Ataque:** evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.
- **Desastre o Contingencia:** interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras necesarias para la operación normal de un negocio.

En las empresas y organizaciones concienciadas con la seguridad de la información, antes de implantar un **sistema de gestión de la seguridad de la información (SGSI)**, hay que realizar un **análisis de riesgos e impactos** previo. En el siguiente vídeo de Intyedia, proyecto educativo de Criptored, queda bien claro: <https://youtu.be/EgiYIIJ8WnU>

## 1.5. Tipos de amenazas y atacantes

Una **amenaza** es un evento que puede desencadenar un incidente en la organización a consecuencia de una vulnerabilidad existente. Las vulnerabilidades suelen ocurrir por causas:

- **Tecnológicas**, debido a fallos inherentes en la tecnología.
- **De configuración**, debido a que los dispositivos, servidores, aplicaciones, etc., vienen con configuraciones inseguras por defecto o no han sido bien configurados por el administrador.
- **Políticas de seguridad**, porque la organización carece de ninguna política de seguridad o bien porque no son correctas o no se han actualizado con las nuevas amenazas que aparecen.

Los tipos de amenazas pueden ser:

- **Físicas**
- **Lógicas**
- **Pasivas**
- **Activas**

Las amenazas **físicas** y **ambientales** afectan a la parte física del sistema de información: instalaciones, hardware, control de acceso, etc. Son el **primer nivel** de seguridad a proteger.

Amenazas físicas o ambientales:

Robos, accesos a recintos no autorizados, sabotajes.  
Problemas en suministro eléctrico.  
Condiciones atmosféricas: temperatura, humedad, etc.  
Interferencias electromagnéticas.  
Desastres naturales.

Las amenazas **lógicas** afectan a la parte lógica: sistemas operativos (S.O.'s), aplicaciones y datos.

Amenazas lógicas:

La mayoría están relacionadas con el malware (software malicioso):

Virus  
Gusanos  
Troyanos y botnets  
Rootkits  
Exploits  
Rogueware y ransomware  
Puertas traseras  
Keyloggers, etc

Las amenazas **pasivas** o **escuchas**, suponen un intento de un atacante para obtener información relativa a una comunicación.

P. ej: capturar datos con un analizador de redes o sniffer como [wireshark](#)

Las amenazas **activas** son más peligrosas y su objetivo es la modificación de los datos transmitidos o la creación de transmisiones falsas.

P. ej: un ataque Man In The Middle (hombre en el medio, MITM) como el que podemos sufrir al conectarnos a una wifi abierta en una estación o aeropuerto. En un ataque MITM, el atacante generalmente suplanta al router de forma que el tráfico de la víctima pasa por el ordenador del atacante, pudiendo robar credenciales de acceso a servicios, como redes sociales o banca electrónica.

Detrás de muchas de estas amenazas - obviamente excepto los desastres naturales - se encuentra toda una taxonomía de atacantes, con fines lucrativos, de chantaje, activistas o simplemente de ego personal por el impacto del ataque realizado. Algunos de ellos son:

- **Hacker** (White hat)
- **Cracker** (Black Hat)
- **Grey Hat**
- **Lamer y Script Kiddies**
- **Phreaker**
- **Spammer**
- **Phisher**
- **Scammer**
- **Ciberterroristas**

## 1.6. El ciclo de vida de la seguridad informática

La **ISO/IEC 27001** define la seguridad como un **proceso de mejora continua**. La seguridad informática es un proceso que comienza en el momento en que se implanta en la organización, pero nunca acaba, ya que lo que hagamos hoy puede que no sirva para mañana. La tecnología avanza muy rápidamente y de la misma forma que aparecen nuevas funcionalidades y maneras de hacer las cosas, surgen como consecuencia nuevos vectores de ataques. Por tanto, si somos los responsables de seguridad de una organización, debemos estar continuamente aplicando las fases del ciclo de vida de la seguridad:



**Fases del ciclo de vida de la seguridad informática**

También se le conoce como el modelo **Plan-Do-Check-Act** (PDCA o ciclo Demming) y que consiste en las siguientes fases:

#### **Planificación (Plan)**

Establecer la política, objetivos, procesos y procedimientos relativos a la gestión del riesgo y mejorar la seguridad de la información de la organización para ofrecer resultados de acuerdo con las políticas y objetivos generales de la organización.

- Identificar lo que se quiere mejorar.
- Recopilar datos del proceso que se quiere mejorar.
- Analizar los datos recogidos.
- Establecer los objetivos de mejora.
- Detallar los resultados esperados.
- Definir los procesos necesarios conseguir los objetivos.

#### **Ejecución (Do)**

Implementar y gestionar el Sistema de Gestión de la Seguridad de la Información (SGSI) de acuerdo a su política, controles, procesos y procedimientos. En la medida de lo posible debería hacerse en un entorno de prueba para poder verificar sus resultados antes de implantarlo en el sistema real.

#### **Seguimiento (Check)**

Verificar, medir y revisar las prestaciones de los procesos del SGSI. Comprobar que las medidas adoptadas han surtido efecto, para ello se debe volver a recopilar datos y monitorizar el comportamiento del sistema.

#### **Mejora (Act)**

Adoptar acciones correctivas y preventivas basadas en auditorías y revisiones internas con el objetivo de mejorar el SGSI. Hace referencia a la actitud que se debe tomar después de los tres primeros pasos y dependerá de lo que haya ocurrido. En caso de haber ocurrido algún mal funcionamiento, se deberá repetir el ciclo de nuevo. Si el funcionamiento ha sido correcto, se instalarán las modificaciones en el sistema de manera definitiva.



La seguridad debe considerarse en toda organización como una **inversión** y no como un gasto. Desgraciadamente no muchas organizaciones se han dado cuenta de eso y es fácil ver hoy en día muchas empresas sin políticas de seguridad, sin planes de contingencia o continuidad de negocio ante desastres o incumpliendo la Ley Orgánica de Protección de Datos.

Muchas empresas reaccionan cuando han sufrido un incidente de seguridad y no tienen planes de acción de forma que lo dejan todo a la improvisación. No tener un SGSI implantado puede llevar a ocasionar muchas pérdidas económicas e incluso la reputación y la imagen de la empresa ante un incidente de seguridad con gran impacto y que pueda ser anunciado en los medios de comunicación, dando una mala publicidad a la empresa.

También es verdad es que empieza a haber un cambio de tendencia en el sector y las organizaciones empiezan a demandar profesionales en el campo de la seguridad informática.

Las organizaciones deben plantearse muy seriamente la necesidad de **formación** y **concienciación** de sus empleados en materia de seguridad informática, ya que el factor humano es muy importante a la hora de evitar incidentes. Muchos de los problemas se derivan por malas prácticas en los empleados y por desconocimiento de los peligros que acechan en Internet, donde la mayoría de ataques se realizan mediante [phishing](#) o [ingeniería social](#).

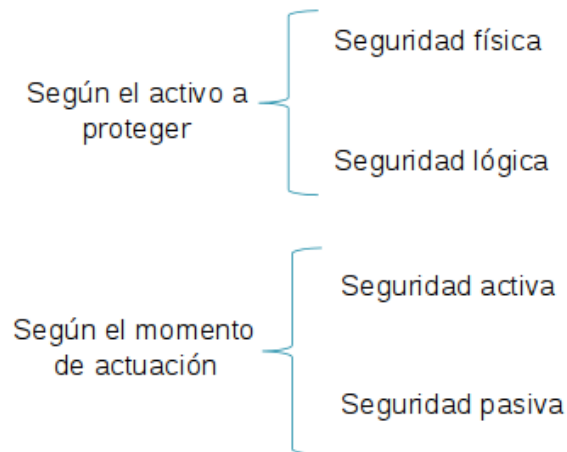


## 2. Clasificación de medidas de seguridad informática

### 2.1. Clasificación de medidas de seguridad

En esta unidad se estudiará la clasificación más habitual de las medidas que podemos aplicar en la seguridad de la información, como son la seguridad **física**, **lógica**, **activa** y **pasiva**.

Esta clasificación se hace atendiendo a dos criterios que se muestran en el siguiente esquema:



Todas las medidas de seguridad informática pueden clasificarse atendiendo a estos dos criterios. Por tanto tendremos medidas de seguridad física activa, física pasiva, lógica activa y lógica pasiva, como ya se verá. Incluso puede darse el caso que en un mismo criterio de clasificación, haya medidas de ambos tipos simultáneamente, como por ejemplo activa y pasiva a la vez.

### 2.2. Seguridad física

Las medidas de **seguridad física** tratan de proteger los **activos tangibles** y **físicos** de la organización, así como a las personas. Así pues, en la seguridad física podemos tener medidas para protegernos o minimizar el impacto ante las siguientes amenazas:

Amenaza	Medidas de seguridad
Incendios	Mobiliario ignífugo, muros y paredes cortafuegos, extintores...
Inundaciones	Evitar ubicación en plantas bajas, impermeabilizar paredes y techos...
Robos	Cámaras de seguridad, vigilantes, códigos de seguridad...
Señales electromagnéticas	Evitar ubicación en lugar con gran radiación, proteger de las emisiones mediante filtros o cableado especial...
Apagones	SAI, estabilizadores, grupos electrógenos
Sobrecargas eléctricas	SAI profesionales con filtros para evitar picos de tensión
Desastres naturales	Contactar con la Agencia Estatal de Meteorología, CPD's de respaldo...

Además, en las medidas de seguridad física y sobre todo, en las grandes organizaciones, entrarían todas las medidas de diseño, ubicación y acondicionamiento de lo que se conoce como **Centros de Procesamiento de Datos** (CPD), **Centros de Cálculo** o **Centros de Datos** (Data Centers), que son salas o edificios donde se ubican todos recursos físicos, lógicos y humanos necesarios para la organización, realización y control de las actividades informáticas de una empresa.

En las siguientes imágenes, se pueden observar algunas de las medidas en los centros de datos, como los **suelos técnicos, falsos techos**, los sistemas de **acondicionamiento ambiental** para controlar, la humedad, el calor o el polvo o los **SAI** y **grupos electrógenos** para proporcionar electricidad ante un fallo del suministro eléctrico:



Observa el siguiente vídeo (en inglés) sobre los CPD's de Google: <https://youtu.be/zRwPSFpLX8I>

Si deseas ampliar más información sobre los centros de datos de Google, lo puedes hacer en este enlace:  
[Centros de datos de Google](#)

### 2.3. Seguridad lógica

La **seguridad lógica** protege los activos **intangibles** de la organización, como son el **software**, los **datos** o los **procesos**, así como de los **accesos no autorizados** a los sistemas informáticos. Por tanto, en la seguridad lógica podemos tener medidas para protegernos o minimizar el impacto ante las siguientes amenazas:

Amenaza	Medidas de seguridad
Robos	Cifrar la información almacenada, utilizar contraseñas, sistemas biométricos...
Pérdida de información	Copias de seguridad, sistemas tolerantes a fallos, discos redundantes RAID...
Pérdida de integridad	Programas de chequeo del equipo, firma digital, herramientas de integridad...
Software malicioso	Antimalware (antivirus, antirootkit, etc.)
Ataques red	Firewall, programas de monitorización, servidores proxys, detectores de intrusos...
Accesos no autorizados	Contraseñas, listas de control de acceso, cifrar documentos...

La seguridad lógica es la rama más importante de la seguridad informática porque es la que se centra en proteger principalmente los datos y por tanto, la información que es el activo más importante de una organización. Por tanto, la mayoría de aplicaciones prácticas que veremos en este curso, entran dentro de esta categoría.

Un sistema con discos redundantes RAID, que recuperan el sistema ante el fallo hardware de un disco duro, ¿es seguridad física o lógica?

Aunque pueda parecer que el recuperar un sistema informático ante el fallo de un disco - que es un componente físico - sea seguridad física, realmente es lógica. El objetivo del RAID es proteger los datos que contienen, no los discos en sí. Muy importante tener en cuenta que tener un sistema RAID no es suficiente para proteger los datos. será necesario pues, contar con un buen sistema de copias de seguridad para tener salvaguardados los datos de la organización en el caso de un borrado accidental de los discos RAID, por citar un ejemplo de incidente de seguridad. En este caso, el RAID no nos protege de la pérdida de datos.

## 2.4. Seguridad activa

Por **seguridad activa** se entienden aquellas medidas que **previenen** e intentan evitar los daños en los sistemas informáticos. Son **medidas preventivas**. Para saber si una medida es seguridad activa o pasiva, hay que pensar si el incidente de seguridad ha ocurrido o no. Si se ha prevenido el incidente y no ha ocurrido gracias a las medidas de seguridad implantadas, se trata de seguridad activa. Si el incidente ya ha ocurrido y la medida minimiza el impacto del incidente o permite recuperar al sistema del fallo, se trata de seguridad pasiva.

Esta clasificación es comparable a las medidas de seguridad en los vehículos. Por ejemplo un ABS o ESP son ejemplos de medidas de seguridad activa pues intentan evitar el accidente, mientras que un arco de seguridad, un airbag o un cinturón de seguridad son medidas de seguridad pasiva pues intentan minimizar los daños una vez producido el accidente.

Como medidas o técnicas de seguridad activa en seguridad informática podemos citar los siguientes ejemplos:

Técnica	Amenaza de la que previene
Contraseña	Acceso al sistema o aplicaciones por parte de personas no autorizadas
Permisos en ficheros	Acceso a ficheros por parte de personal no autorizado
Cifrado	Accesos no autorizados a información confidencial
Antivirus	Virus informáticos y en general, aplicaciones maliciosas
Certificados digitales	Ataques a la integridad y autenticidad de los datos
Cuotas de disco	Fallo del sistema por agotamiento del espacio en disco

## 2.5. Seguridad pasiva

Por **seguridad pasiva**, se entienden aquellas medidas que se aplican **después** de ocurrir un incidente de seguridad e intenta **minimizar** el impacto del mismo. Son medidas **correctoras** o **paliativas**. Por tanto el objetivo de esta medida no es evitar el incidente o la amenaza, que en algunos casos es imposible hacerlos, pero sí poder recuperar el sistema a su estado de funcionamiento anterior.

En la seguridad pasiva cabe destacar todas las medidas de **redundancia** y **alta disponibilidad** (HA, High Availability) sobre todo en centros de datos críticos, como pueden ser:

- Suministro eléctrico o conexión a Internet con más de un proveedor
- Fuentes de alimentación dobles
- Conmutadores y routers redundantes
- Cableado y tarjetas de red redundantes

Otros ejemplos de medidas de seguridad pasiva más habituales pueden ser:

Técnica	Cómo minimiza el impacto
Discos redundantes	Restaura información de los otros discos en caso de fallo
Sistemas de ficheros tolerantes a fallos	Previene inconsistencia de datos en caso de apagones
SAI/UPS	Suministra energía al sistema en caso de un corte
Copias de seguridad	Recupera información en caso de pérdida o robo de información
Firma digital	Detecta un ataque a la integridad y autenticidad de los datos
Extintores, muros y paredes cortafuegos	Minimiza y palia los daños provocados por un incendio

¿Un sistema de vigilantes de seguridad con cámaras que graban, es seguridad activa o pasiva?

Analizándolo bien, este sistema es de seguridad activa y pasiva. De seguridad activa, porque la presencia de los vigilantes y las cámaras puede evitar que un intruso entre en el recinto protegido. De seguridad pasiva, porque en caso que los intrusos burlen el sistema de seguridad tras un despiste de los vigilantes, usando la información de las cámaras de seguridad y una vez ocurrido el incidente, se podría identificar a los delincuentes, detenerlos y recuperar el botín, siendo bajo ese punto de vista una medida paliativa.

### 3. Software malicioso: medidas preventivas y paliativas

#### 3.1. Software malicioso y su impacto actual

##### Definición de malware

Por **malware** entendemos todo el software malicioso, intrusivo o molesto, generalmente con fines dañinos para el sistema informático que lo ejecuta.

En muchas ocasiones se usa el término **virus** incorrectamente, sobre todo en los medios de comunicación, para referirse a todos los tipos de malware, incluyendo los verdaderos virus que son un tipo específico de software malicioso.

Mira este vídeo de Intypedia, donde se hace un breve recorrido del malware y su clasificación:

<https://youtu.be/NPsjN8AvNQM>

El malware (o mal llamado por los medios de forma genérica, virus) empezó hace algunas décadas pero no tenía los objetivos que tiene hoy en día. Eran más bien pruebas de concepto para demostrar los fallos que había en los sistemas o para demostrar las habilidades del creador. Muchos eran más bien inocentes e inofensivos.

El **primer virus informático** estaba diseñado para la máquina IBM Serie 360. Fue llamado **Creeper**, creado en 1972. Este programa emitía periódicamente en la pantalla el mensaje: «I'm a creeper... catch me if you can!» (¡Soy una enredadera... agárrame si tú puedes!). Para eliminar este problema se creó el primer programa antivirus denominado Reaper (cortadora).

Sin embargo, el primer virus informático moderno, aparece el 13 de noviembre de 1983, Fred Cohen, un estudiante de la universidad de California del Sur concibió un experimento que sería presentado en un seminario semanal sobre seguridad informática. La idea era simple: diseñar un programa de cómputo que pudiera modificar otros programas para incluir en ellos una copia de sí mismos. Estas copias podrían a su vez modificar nuevos programas, y de esta manera proseguir con su propagación y expansión.

En la actualidad el malware es un lucrativo "negocio" que permite a los cibercriminales tener ingresos entre 3000 y 6000 euros diarios (según Eugene Karspersky) y al cabo del año puede suponer un volumen de dinero equivalente al que gastan los americanos en comida rápida al año (según un análisis de EMC). Con el malware los criminales roban datos de tarjetas de crédito, datos personales para hacer extorsiones y chantajes, roban bitcoins de monederos electrónicos, construyen redes zombie que luego alquilan al mejor postor, realizan ataques a páginas de gobiernos o empresas contratados por otros, etc.

En el siguiente documental titulado **Amenaza Cyber** emitido en el programa En Portada de RTVE, se muestran datos escalofriantes acerca del malware y todo el crimen organizado a su alrededor: <https://www.rtve.es/play/videos/en-portada/amenaza-cyber-ciber-ciberguerra-ciberseguridad/1543800/>

#### 3.2. Clasificación del malware

Casi de manera análoga a la biología y los virus del mundo real, en el mundo informático existe una taxonomía muy desarrollada de tipos de malware.

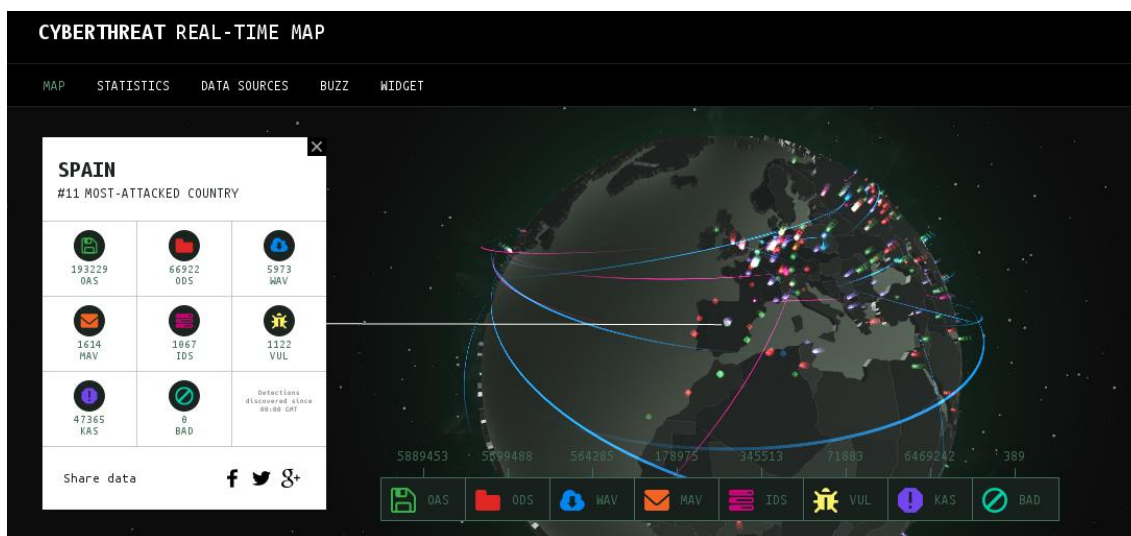
En este punto vamos a ver algunos de los tipos más destacados de software malicioso, sin pretender extendernos excesivamente. Algunos de ellos son:

- Virus
- Gusanos
- Troyanos
- Rootkits
- Dialers
- Spyware
- Rogueware
- Ransomware
- APT

Hay que señalar que hoy en día es raro encontrar un espécimen que se clasifique en un solo tipo, por tanto más que de malware, se suele hablar a veces de **suites maliciosas**. Por ejemplo es fácil encontrar un troyano, que además tiene una puerta trasera y un keylogger para capturar contraseñas.

## Mapa mundial de malware de Kaspersky

En la página web de Kaspersky, hay un mapa en 3D donde se puede ver el planeta y las amenazas por malware en tiempo real en todo el mundo, utilizando su software: <https://cybermap.kaspersky.com/>



### 3.2.1. Virus

#### Definición de virus

Un **virus** es un programa que al ejecutarse por **intervención humana**, se propaga infectando otros software ejecutables dentro de la misma computadora.

La característica principal de un virus es que se **adjunta** a otro ejecutable modificándolo, por ejemplo, el Word.

Los virus suelen tener una **funcionalidad maliciosa** como por ejemplo, borrar o modificar archivos, si bien es verdad que en sus orígenes eran más bien aplicaciones molestas.

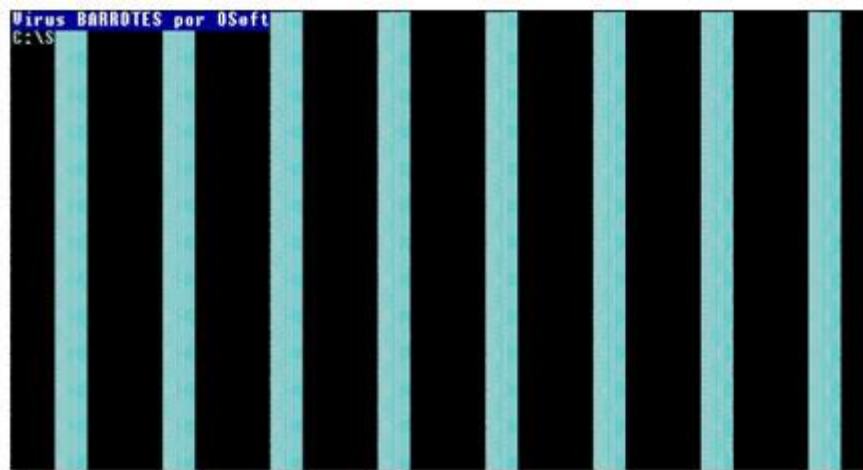
Es uno de los primeros tipos de malware que existió, antes de que se usara Internet en los hogares. Se propagaban como ejecutables modificados en los disquetes que se usaban en las antiguas disqueteras de los primeros ordenadores domésticos, ahora ya en desuso.

Actualmente se propagan como adjuntos a correos (el usuario debe ejecutar o abrir el adjunto), o a través de redes P2P o IRC, o aprovechando vulnerabilidades de aplicaciones o a través de los discos externos como pendrives. Este tipo de malware es muy común hoy en día.

#### Ejemplos de virus

¿Quién no recuerda el virus **Barrotes**? Fue desarrollado por un programador español y mostraba unas franjas verticales simulando ser barrotes. El virus se activaba el día 5 de enero, reescribiendo el sector de arranque (MBR).

En principio, una de las últimas variantes de Barrotes pretendía borrar los datos del disco cada día 22, pero por un error de programación, lo hacía cada día 34 (lo que nunca ocurría), convirtiéndolo en un virus poco peligroso.



*Virus barrotes en ejecución*

### 3.2.2. Gusano

#### Definición de gusano

Un **gusano** o worm es un malware que tiene la propiedad de duplicarse a sí mismo, bien en la memoria de un ordenador o bien propagándose a otros equipos a través de la red.

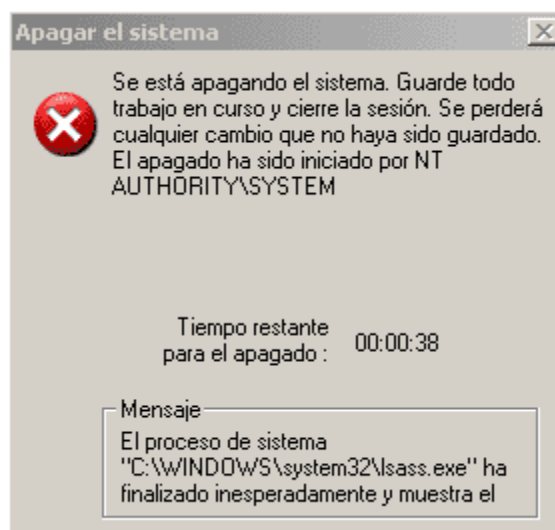
Los gusanos utilizan para propagarse servicios o funcionalidades de un sistema operativo que en muchas ocasiones son desconocidos por el usuario. Por ejemplo: gusanos Sasser y Blaster.

A diferencia de un virus, un gusano **no precisa alterar** los archivos de programas **ni requiere ejecución manual** de la víctima necesariamente, sino que reside en la memoria y se duplica a sí mismo. Casi siempre causan problemas de rendimiento en el equipo o en la red (aunque sea simplemente consumiendo ancho de banda).

Los gusanos usan la red para enviar copias de sí mismos a otros equipos y son capaces de llevar esto a cabo sin intervención del usuario propagándose, utilizando Internet, basándose en diversos métodos, como correo electrónico, IRC o redes de intercambio P2P entre otros.

#### Ejemplos de gusanos

El malware **Sasser** apareció en mayo de 2004 y es un gusano que explota un agujero de seguridad del proceso LSASS de Windows (*Autoridad de seguridad local*). La aparición del primer virus en explotar el fallo de seguridad en LSASS de Windows se produjo apenas dos semanas después de que se publicara el fallo y se lanzaran los primeros parches correctivos. Windows NT 4.0, 2000, XP y (en menor grado) Windows Server 2003 estaban todos afectados.



*Gusano Sasser en ejecución*



### 3.2.3. Troyano

#### Definición de troyano

Es un software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo pero al ejecutarlo ocasiona daños al sistema o instala otras aplicaciones maliciosas.

El término troyano proviene de la historia del caballo de Troya mencionado en la Odisea de Homero. En la mayoría de los casos crean una puerta trasera que permite la administración remota del equipo infectado. Son la base de las puertas traseras para crear redes botnet infectadas con ordenadores zombie.

Un troyano no es estrictamente un virus informático o un gusano, y la principal diferencia es que los troyanos no propagan la infección a otros sistemas por sí mismos.

#### Ejemplos de troyanos

Zeus o SpyEye son troyanos bancarios del tipo DIY ("hágalo usted mismo") muy popular. Su nivel de sofisticación es la punta de lanza del malware actual. Sus últimas versiones incorporan la infección del móvil con sistema operativo Android o Blackberry cuando se usa el SMS como segundo canal de autenticación de algunos bancos. Así, el troyano tiene el control sobre los dos dispositivos involucrados en la transacción. Además también tiene funciones de rootkit (que se verá más adelante) lo que permite ocultarlo de muchos antivirus.

Es habitual en estos troyanos crear una botnet, donde centenares de miles o millones de equipos infectados (zombies) son controlados remotamente desde un centro de mando y control (C&C)

### 3.2.4. Rootkit

#### Definición de rootkit

Un **rootkit** es un malware que modifica el sistema operativo de una computadora para permitir que permanezca **oculto** al usuario y a otros procesos como los antivirus.

Los rootkit evitan que un proceso malicioso sea visible en la lista de procesos del sistema o que sus ficheros sean visibles en el explorador de archivos, por tanto, consiguen ocultar cualquier indicio de que el ordenador está infectado por un malware.

**Originalmente**, un rootkit en el mundo Unix era un conjunto de herramientas instaladas por un atacante en el que había obtenido acceso como root (de ahí el nombre). Actualmente, el término es usado más generalmente para referirse a las técnicas de ocultación de un programa malicioso.

Muchos troyanos bancarios como Zeus o SpyEye usan técnicas de rootkit para ocultarse.

Uno de los rootkits más famosos fue el que la empresa **Sony** incluyó dentro de la protección anticopia de algunos CDs de música. De esta manera el rootkit evitaba que el usuario hiciera copias con una grabadora de un CD de Sony Music, provocando un fallo en la grabación. El conocido investigador de seguridad **Mark Russinovich** (nacido en Salamanca curiosamente, quién lo diría) descubrió la existencia de este rootkit y causó una mala imagen en Sony, de una manera similar al caso Volkswagen.

### 3.2.5. Backdoor

#### Definición de Backdoor

Una **puerta trasera** o **backdoor** es un malware diseñado para eludir los procedimientos normales de acceso a un ordenador o dispositivo

Una vez que el sistema ha sido comprometido e infectado con el backdoor, una puerta trasera puede ser instalada para permitir un acceso remoto más fácil en futuras conexiones. Las puertas traseras también pueden ser instaladas previamente al software malicioso, para permitir la entrada de los atacantes. Para instalar puertas traseras los crackers pueden usar troyanos, gusanos u otros métodos, aunque el uso de troyanos es el más habitual.

### 3.2.6. Spyware

#### Definición de spyware

El **spyware** es un malware que recopila información de un equipo infectado y después reenvía esta información a una entidad externa sin el conocimiento o consentimiento del usuario del dispositivo u ordenador infectado

La palabra spyware deriva de la fusión de los términos inglés **spy** que significa espía, y **ware** que en este contexto, significa programa.

La función más habitual del spyware es la de recoger información sobre el usuario y enviarla a empresas publicitarias u otras organizaciones interesadas, pero también se han empleado en organismos oficiales para recopilar información contra sospechosos de delitos, como en el caso de la piratería de software. El spyware, por tanto, consume ancho de banda de nuestra conexión al estar continuamente enviando esa información del perfil y hábitos del usuario.

El spyware puede ser instalado en un ordenador mediante un virus, un troyano que se distribuye por correo electrónico, o bien puede estar oculto en la instalación de un programa aparentemente inocuo. Una característica habitual del spyware es que no se intenta replicar en otros ordenadores de forma automática, por lo que funciona como un gusano.

Es habitual que programas descargados de sitios no confiables o shareware pueden tener instaladores con spyware y otro tipo de malware.

### 3.2.7. Adware

#### Definición de adware

El **adware** es un malware que muestra **publicidad no deseada** en forma de ventanas emergentes (pop-up) en el equipo infectado

La palabra adware deriva de la fusión de los términos inglés **ad** que significa anuncio, y **ware** que en este contexto, significa programa.

La publicidad que muestra un adware aparece inesperadamente en el equipo y resulta muy molesta. Es habitual en muchos programas **shareware** y **gratuitos**, el usar el programa de forma gratuita a cambio de mostrar publicidad, en este caso el usuario consiente la publicidad al instalar el programa. Este tipo de adware no debería ser considerado malware, pero muchas veces los términos de uso no son completamente transparentes y ocultan lo que el programa realmente hace.

### 3.2.8. Hijackers

#### Definición de hijacker

Los **hijackers** son un tipo de malware que realizan cambios en la configuración del equipo infectado, como por ejemplo el buscador o la página de inicio del navegador

Por ejemplo, algunos cambian la página de inicio del navegador por páginas web de publicidad o pornográficas, otros redireccionan los resultados de los buscadores hacia anuncios de pago o páginas de phishing bancario.

El **pharming** es una técnica que suplanta al DNS o modificando el archivo hosts, para redirigir el dominio de una o varias páginas web a otra página web, muchas veces una web falsa que imita a la verdadera. Esta es una de las técnicas más usadas por los hijackers.

### 3.2.9. Dialers

#### Definición de dialer

Los **dialers** o **módem hijackers** es un tipo de malware que toma el control del módem telefónico y realizan una llamada a un número de teléfono de tarificación especial (80X, 90X) que son mucho más caras que una llamada local

La forma más habitual de infección suele ser en páginas web que ofrecen contenidos gratuitos pero que solo permiten el acceso mediante conexión telefónica. Suelen utilizar como señuelos videojuegos, salvapantallas, pornografía u otro tipo de material.

Actualmente la mayoría de las conexiones a Internet son mediante banda ancha (ADSL, DOCSIS, 4G, Wimax, etc) y no mediante módem telefónico o RDSI, lo cual hace que los dialers ya no tengan mucho sentido.

### 3.2.10. Keyloggers

#### Definición de keylogger

El keylogger es un malware que **monitoriza** todas las **pulsaciones del teclado** y las almacena para un posterior envío al creador del programa

La palabra viene de la unión de **key** (tecla) y **log** (registro).

Por ejemplo al introducir un número de tarjeta de crédito, el keylogger guarda el número, posteriormente lo envía al autor del programa (por email o con algún otro sistema a través de red) y este puede hacer pagos fraudulentos con esa tarjeta o vender los datos de esa tarjeta en la tiendas de tarjetas de crédito en el mercado negro.

La mayoría los keyloggers son usados para recopilar contraseñas de acceso, datos personales pero también pueden ser usados para espiar conversaciones de chat u otros fines.

### 3.2.11. Stealers

#### Definición de stealer

El **stealer** es un malware especializado en robar información privada o credenciales que se encuentra almacenada en el equipo

El nombre viene del inglés **steal**, que significa robar.

Si las contraseñas se encuentran guardadas en el equipo, de forma que el usuario no tiene que escribirlas, el keylogger no las recoge, eso lo hacen los stealers. Al ejecutarse comprueban los programas instalados en el equipo y si tienen contraseñas almacenadas, por ejemplo en los navegadores web o en clientes de mensajería instantánea, descifran esa información y la envían al creador del malware.

### 3.2.12. Botnets

#### Definición de botnet

Las **botnets** son redes de computadoras infectadas, también llamadas **zombies**, que pueden ser controladas a la vez por un individuo desde un centro de mando y control (C&C, de command and control) y realizan distintas tareas bajo las órdenes del creador de la botnet.

Este tipo de redes pueden ser usadas para el envío masivo de spam o para lanzar ataques de denegación de servicio distribuido (DDoS) contra organizaciones, empresas o gobierno como forma de extorsión o para impedir su correcto funcionamiento.

La ventaja que ofrece a los spammers el uso de ordenadores infectados es el anonimato, que les protege de la persecución policial.

En el mercado negro, los dueños de estas redes las alquilan para ofrecer servicios de spam, ataques, etc. A veces estas redes pueden llegar a controlar millones de dispositivos.

### Verificar si perteneces a una botnet

En la **Oficina de Seguridad del Internauta** (OSI), existe una aplicación web que permite comprobar si la dirección IP pública de tu conexión, está en un registro de actividad de botnet. De esta forma puedes saber si algún equipo de tu red, está siendo usado sin tu consentimiento para hacer actividades delictivas en el contexto de una botnet o red de ordenadores zombis.

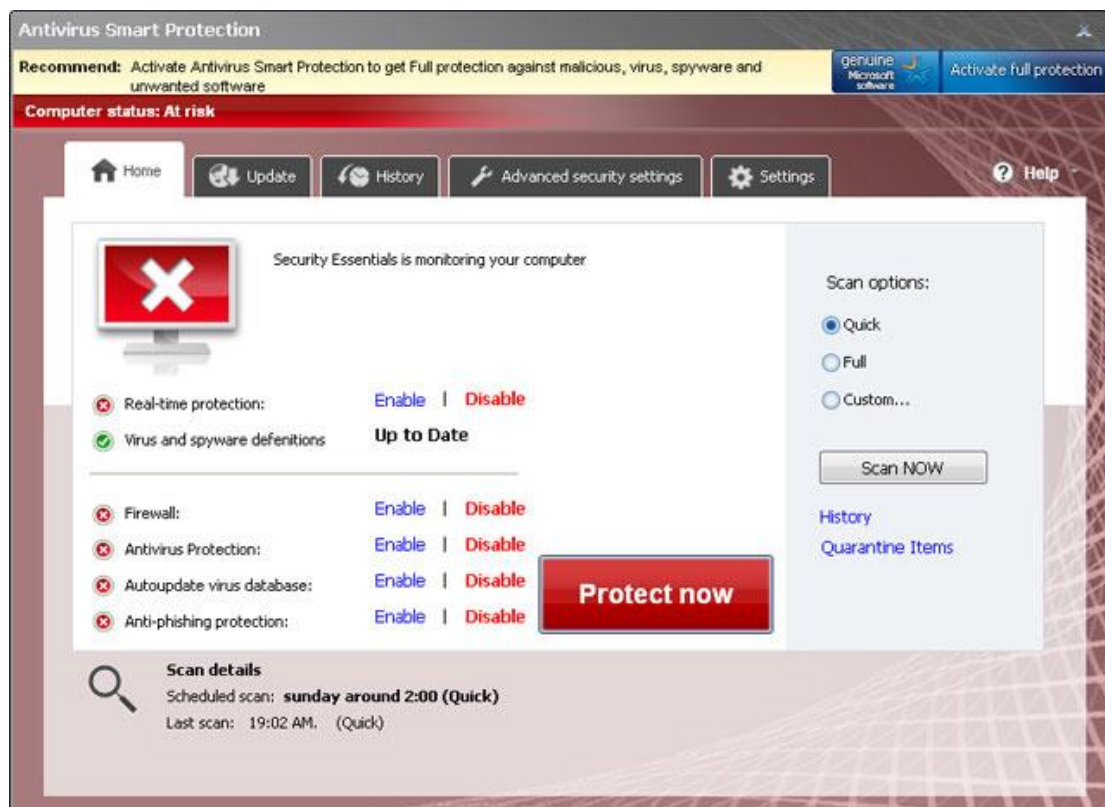
## 3.2.13. Rogueware

### Definición de rogueware

Un **rogueware** es un tipo de malware que engaña al usuario con el fin de robar dinero, inducir a compras u obtener información del usuario

Viene de la unión de las palabras **rogue** (pícaro, granuja) y **ware**.

Estos programas suelen tener éxito al provocar miedo al usuario para conseguir ser instalados. Por ejemplo, el rogueware puede hacer creer al usuario que el dispositivo está infectada por algún tipo de malware, esto induce al usuario a pagar por un software inútil o a instalar un software malicioso que supuestamente elimina las infecciones, pero el usuario no necesita ese software puesto que no está infectado realmente.



*Ejemplo de rogueware que se hace pasar por el antivirus de Microsoft*

### 3.2.14. Ransomware

#### Definición de ransomware

El **ransomware** es un tipo de malware que cifra los archivos del sistema informático para pedir posteriormente un **rescate** por los datos.

La palabra ransomware viene de la unión de **ransom** (rescate) y **ware**. Los ransomware, también se conocen con el nombre de **criptovirus** ya que cifran el disco duro o los archivos que contiene mediante algún tipo de criptografía, dejándolos inaccesibles.

Una característica común en casi todos ellos, es que aunque se pague, **nunca** se recibe la clave de descifrado, por lo tanto, las técnicas de seguridad pasiva como las **copias de seguridad actualizadas** son el mejor remedio ante un incidente de este tipo.

#### Ejemplos de ransomware

Hay dos casos muy conocidos que incluso han salido en las noticias en los medios de comunicación españoles: son el **virus de la policía** y el **virus de correos**.

El virus de la policía mostraba un mensaje con el logo de la policía nacional pidiendo pagar una multa por estar haciendo descargas ilegales. Se propagaba debido a una vulnerabilidad en Java:

**DIRECCIÓN GENERAL DE LA POLICÍA**  
**CUERPO NACIONAL DE POLICÍA**  
Guardia Civil

Apoyado y Protegido por   

**IP:** [REDACTED]  
**País:** [REDACTED]  
**Región:** [REDACTED]  
**Ciudad:** [REDACTED]  
**ISP:** [REDACTED]  
**Sistema Operativo:** Windows 7 (32-bit)  
**Nombre de Usuario:** Admin

**¡ATENCIÓN! Su OP (ordenador) está bloqueado debido a al menos una de las razones especificadas siguientes.**

Usted ha violado «el derecho de autor y los derechos conexos» (vídeo, música, software) y ha utilizado de una manera ilegal con la distribución de contenido los derechos de autor, infringiendo así el artículo 128 del Criminal Code del Reino de España.

El artículo 128 del Criminal Code prevé una multa 200 a 500 de los salarios mínimos o la privación de la libertad de 2 a 8 años.

Usted ha visto o distribuido el contenido prohibido pornográfico (porno infantil/Zoofilia y etc), violando así el artículo 202 del Criminal Code del Reino de España. El artículo 202 del Criminal Code prevé la privación de la libertad de 4 a 12 años.

El acceso ilegal al contenido prohibido se ha iniciado desde su OP (ordenador), o usted había sido...

El artículo 208 del Criminal Code prevé una multa hasta €100,000 y/o la privación de la libertad de 4 a 9 años.

Código PIN  Suma

1 2 3 4 5 6 7 8 9 0

Pagar PaySafeCard Pagar Ukash

**¿Dónde puedo comprar PaySafeCard?**

Puedes adquirir tu PaySafeCard en las siguientes redes: ePay (anteriormente Movilcarga y Telerecarga), NovaCaixaGalicia, CajaMar, EVO Banco, DisaShop, GMVending, kioscos de Red 30.000 y Canal Recargas de Telefónica. Otros cajeros: en los cajeros CajaMar, Caja Campo, Caja Albalat y Caja Casinos y en banca online de CajaMar. NovaCaixaGalicia: en los cajeros de NovaCaixaGalicia ([www.NovaGaliciaBanco.es](http://www.NovaGaliciaBanco.es)) y en su banca online.

El virus de correos llega por email, haciéndose pasar por Correos, solicitando que descarguemos un fichero para poder recoger un paquete:





Su paquete ha llegado a **20 de marzo**. 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.



CD 438685108339

[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 el est'a manteniendo en la cantidad de 7,55 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.

Condiciones y Términos del Servicio de localización de envíos

En ambos casos, la infección tiene éxito una vez más por el factor humano, como se comentó anteriormente. Por eso es tan imprescindible la concienciación y formación en los usuarios de Internet en buenas prácticas y desconfiar de cualquier mensaje sospechoso que llegue a nuestro correo.

### 3.3. Medidas preventivas y paliativas

Como medidas preventivas, además de las **buenas prácticas** que se comentarán más adelante y disponer siempre de **copias de seguridad** por lo que pueda pasar, en este punto nos ocuparemos de las herramientas que evitan que los sistemas se infecten con malware como son los antivirus, antispyware, antirootkit, etc. y que se conocen de forma más general como **herramientas antimalware**.

#### Antivirus

Los **antivirus** son programas cuyo objetivo es detectar y/o eliminar virus informáticos. Tienen por tanto doble función, **detección** y **prevención** antes de la infección y **curación** en caso de estar ya infectado. La aparición de sistemas operativos más avanzados e Internet y de nuevas técnicas de malware, ha hecho que los antivirus hayan evolucionado y sean capaces de reconocer otros tipos de malware, como spyware, rootkits, etc pasando a llamar **suites de seguridad** o más genéricamente antimalware.

Una suite de seguridad incluye entre otros: antivirus, antispyware, antirootkit, antiphishing, antispam, cortafuegos, filtro web, control parental, copia de seguridad, etc.

#### Mecanismos de detección y protección

Los programas antimalware combaten el malware de dos formas:

- Protección en **tiempo real** contra la instalación de malware en un ordenador. El software antimalware escanea todos los datos procedentes de la red en busca de malware y bloquea todo lo que suponga una amenaza.
- **Detectando** y **eliminando** malware que ya ha sido instalado en una computadora. Este tipo de protección es la más habitual. Se escanea el contenido del registro de Windows, los archivos del sistema operativo, la memoria y los programas instalados en el ordenador. Al terminar el escaneo muestran al usuario una lista con todas las amenazas encontradas y permiten escoger cuales eliminar. Algunos antivirus tienen la opción de guardar las amenazas encontradas en una zona segura llamada **cuarentena**.

Para detectar software malicioso, las herramientas antimalware usan varias técnicas:

- Comparación con **firmas**: se comparan los archivos sospechosos con una base de datos con las firmas de todo el malware conocido hasta la fecha. Estas bases de datos de firmas deben actualizarse periódicamente
- Métodos **heurísticos**: la heurística es el arte o ciencia del descubrimiento y en seguridad informática hace referencia a las técnicas para detectar virus de los que no se dispone firma en la base de datos. Este método busca secciones de código conocidas dentro de los archivos sospechosos, mediante la asignación de

probabilidades de aparición del código en muestras de malware ya confirmadas como tal, permitiendo detectar mutaciones y variaciones del malware.

- Detección por **comportamiento**: similar a la detección heurística pero en vez de buscar secciones de código, busca comportamientos maliciosos conocidos. Es una detección reactiva que sólo funciona una vez que el malware ha iniciado su ejecución.
- Ejecución controlada en **máquina virtual**: se ejecuta el presunto malware en una máquina virtual y se compara el estado de la máquina virtual antes y después de la ejecución. Se comprueba entonces qué archivos o procesos se han visto alterados y, en función de ello, se determina si el archivo es malicioso.

También es verdad que la labor que realizan las empresas antivirus es extremadamente difícil. Los desarrolladores de malware utilizan técnicas para **evitar su detección** como atacar o desactivar el antivirus, incluirse en la lista de programas permitidos por el antivirus aprovechando algún fallo de él, detectar que están en una máquina virtual y no hacer nada o cifrar u ofuscar parte del código son algunas de las técnicas.

### Antivirus personales y corporativos

Los **antivirus personales** son aplicaciones independientes que se instalan en un ordenador doméstico y se actualizan (motor y base de datos de firmas) a través de Internet. En muchas organizaciones se usan **antivirus corporativos** que dependen de un servidor en la empresa que contiene las actualizaciones y además recoge los informes y alertas de detección e infección de todos los ordenadores de la organización.

De esta forma, un administrador de red puede tener **centralizadas** todas las actualizaciones sin que todos los ordenadores cliente tengan que actualizarse de Internet gastando ancho de banda, así como toda la información relativa a malware detectado o eliminado en los clientes de la red. También se puede intervenir remotamente en los equipos en que se ha detectado una infección y no se ha podido eliminar.

### Ejemplos de antimalware

Hay una variada oferta de antivirus y antimalware en el mercado, algunos gratuitos y otros de pagos. Algunos de ellos son:

- |               |  |
|---------------|--|
| ○ Ad-Aware    | ○ Malwarebytes' Anti-Malware                       |
| ○ Avast!      | ○ McAfee   |
| ○ AVG         | ○ Microsoft Security Essentials y Windows Defender |
| ○ Avira       | ○ Norman   |
| ○ BitDefender | ○ Norton AntiVirus                                 |
| ○ ClamWin     | ○ Panda  |
| ○ ESET NOD32  | ○ Spybot - Search & Destroy                        |
| ○ HijackThis  | ○ SpywareBlaster                                   |
| ○ Kaspersky   | ○ VirusTotal                                       |

## 3.4. Pautas y prácticas seguras

No existe un sistema seguro al 100% pero podemos minimizar los riesgos llevando a cabo unas prácticas seguras que siempre se basan en el sentido común. Algunas de ellas son:

- Utilizar una buena política de contraseñas
- No instalar ni ejecutar servicios que no se utilicen en un servidor
- Instalar una buena suite de seguridad o antimalware
- Instalar un cortafuegos cuando sea necesario
- Mantener los sistemas actualizados:
  - Parches del sistema operativo y actualizaciones de aplicaciones críticas como el navegador
  - Firmas y motor de antivirus
- No abrir correos electrónicos de desconocidos ni ejecutar los adjuntos
- No facilitar datos personales, ni claves, ni códigos PIN solicitados por email u otro medio (SMA, teléfono, etc)
- No hacer caso de correos que pidan dinero por adelantado (siempre son estafas)
- No navegar por páginas web que sean sospechosas o no confiables o que ofrezcan regalos o promociones dudosas
- No fiarse de los acortadores de URL ni los códigos QR

- No reenviar cadenas de email
- Estar informado en cuestiones de seguridad:
  - Suscribirse a boletines de seguridad (Hispace, etc.)
  - Consultar páginas de información de seguridad (CERT, CSIRT)
- Concienciar y formar a los usuarios de la red en cuestiones de seguridad informática

Y recordar:





## 4. Certificados digitales y firma digital

### 4.1. Criptografía de clave pública

La criptografía es una herramienta utilizada desde hace muchos siglos. Los espartanos usaban un rudimentario método conocido como la **escítala** y el imperio romano usaba el conocido **método César** de desplazamiento o sustitución. Hoy por hoy ambos métodos son triviales de descifrar por cualquier iniciado en estos temas.

Pero es desde el siglo pasado donde ocurren los mayores avances en este campo, hasta el punto que podemos decir que ha habido un antes y un después pasando a denominarse criptografía clásica y moderna. Incluso hay hechos históricos que afectaron a grandes acontecimientos de la historia moderna, como conseguir que la segunda guerra mundial acabara dos años antes de lo previsto salvando la vida de millones de personas (según estimaciones de expertos) gracias al trabajo de **Sir Alan Turing** (considerado el padre de la informática) y su equipo en la mansión inglesa de **Bletchley Park**, rompiendo los códigos de la máquina de cifrado **Enigma** y **Lorenz** usadas por los nazis en la guerra.

En el siguiente breve vídeo del proyecto Criptored puedes ver esta distinción: <https://youtu.be/a3VYWMneK90>

A mediados de los años 70, la criptografía de **clave pública**, también conocida como de **clave asimétrica** viene a complementar la criptografía tradicional de cifrado simétrico y algunas de sus debilidades. Se conoce con este nombre porque la clave de cifrado es diferente a la de descifrado de forma que lo que se hace una clave, se deshace con la otra.

Cada participante en una comunicación - ya sea una persona o un sistema informático como un servidor web - utiliza un **par de claves**:

- Clave **pública**: se puede entregar o compartir con cualquier persona, ya que no es secreta. Incluso se puede publicar en páginas personales.
- Clave **privada**: el propietario debe guardarla a buen recaudo ya que no debe compartirse con nadie y como su nombre indica, es para uso privado de su poseedor.

La seguridad del sistema se basa por tanto en la seguridad de la clave privada y en que es computacionalmente "imposible", obtener la clave privada de una persona o servicio conociendo su pública. Cuando se habla de **computacionalmente imposible**, queremos decir que con la potencia actual de los ordenadores, se podría invertir decenas o cientos de años - en función de la fortaleza del algoritmo y de la longitud de las claves - en poder descubrir la clave privada.

El par de claves se generan mediante propiedades matemáticas de los números primos muy grandes. Esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.

Para cifrar a un destinatario, el remitente cifra el mensaje con clave pública del destinatario de forma que sólo el destinatario puede descifrar con su privada, pues es el único que la posee. De esta manera se logra la **confidencialidad** del envío del mensaje, ya que nadie salvo el destinatario puede descifrarlo.

Los sistemas de clave pública también permiten garantizar la **autenticación** y el **no repudio** mediante la firma digital. Al cifrar un documento con nuestra clave privada, cualquiera puede descifrarlo con nuestra pública. Lógicamente, este proceso no tiene sentido para la confidencialidad pues cualquiera puede ver su contenido, pero sirve para demostrar la autoría de un documento, pues sólo el poseedor de la clave privada, puede haberlo firmado.

El siguiente vídeo muestra de una forma más visual cómo funcionan los sistemas de cifra asimétrica: <https://youtu.be/On1clzor4x4>

#### ¿Qué sistema es mejor, el de clave simétrica o el de clave pública?

El siguiente breve vídeo de Criptored, compara los sistemas de cifra simétrica y asimétrica, concluyendo que ambos se complementan y tienen sus aplicaciones concretas de uso. Actualmente se utiliza en muchos escenarios la combinación de ambos, denominada **criptografía híbrida**, y que usamos a diario en nuestro navegador con el protocolo HTTPS cuando nos conectamos al banco, a redes sociales o a leer el correo electrónico vía web: <https://youtu.be/0qfOVm-dtcQ>

## 4.2. Infraestructura de clave pública (PKI)

Hemos visto en el punto anterior, que la criptografía de **clave pública** nos proporciona **autenticación, confidencialidad, integridad y no repudio**, necesarios hoy en día para garantizar una buena seguridad en la información. Como hemos visto, esto se consigue con un sistema de claves públicas y privadas que combinándolos adecuadamente nos proporcionan los servicios citados anteriormente.

Pero el principal problema que surge es la confianza. ¿Cómo puedo garantizar que la clave pública de un usuario es suya y no es la de un impostor? Cualquiera puede generar un par de claves y pretender ser otra persona. Aquí es donde entran en juego las **autoridades de certificación** (AC o CA, del inglés Certification Authority), que asumen la responsabilidad de autenticar la identidad de esa clave pública y que aparecerá en un documento electrónico llamado **certificado digital**.

Todo este conjunto de certificados, firmas digitales, autoridades de certificación y los procesos que intervienen, forman parte de lo que se conoce como **infraestructura de clave pública** que pasamos a definir a continuación.

### Infraestructura de clave pública

Por infraestructura de clave pública o **PKI** (Public Key Infrastructure) se entiende el conjunto de herramientas hardware, software, procesos y procedimientos legales que permiten crear, gestionar, almacenar, distribuir y revocar certificados digitales.

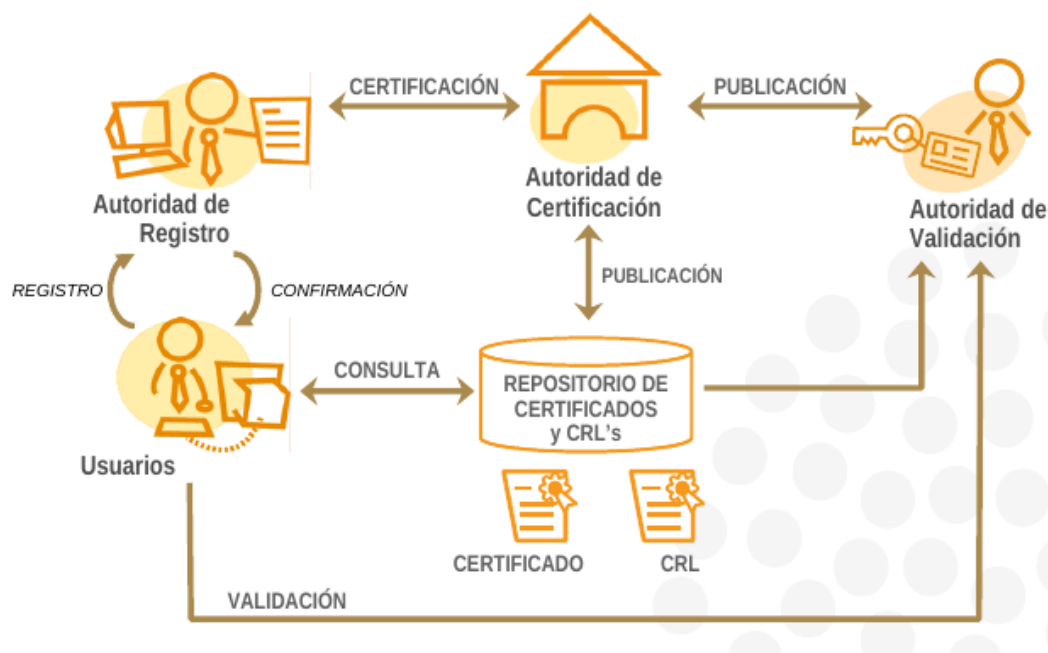
Este término incluye por tanto las autoridades de certificación y al resto de elementos que participan como los certificados digitales o los algoritmos de clave pública y firma digital en comunicaciones y transacciones electrónicas.

Hay que indicar también que para usar la firma digital y los algoritmos de clave pública, no es necesaria la PKI, como se ha podido ver en las prácticas del punto anterior.

Una infraestructura de clave pública consta de:

- **Autoridades de Certificación** (CAs) que llevan la gestión de los certificados
- **Autoridades de Registro** (RAs), que autorizan la asociación entre una clave pública y el titular de un certificado
- **Partes utilizadoras**, que verifican certificados y firmas
- **Repositorios** (Directorios), que almacenan y distribuyen certificados y estados de los mismos
- **Titulares de Certificados**, que son las entidades finales, usuarios o suscriptores de los certificados y por tanto a quien pertenecen
- **Autoridad de Validación** (opcional), que suministra información de forma online (en tiempo real) acerca del estado de un certificado

La siguiente ilustración muestra estos componentes y su relación:



### 4.2.1. Certificados digitales

Un elemento importante en la PKI son los **certificados digitales**, documentos electrónicos emitidos por autoridades de certificación (en adelante AC) que garantizan la identidad de un usuario o servicio electrónico como una página web.

Básicamente un certificado digital es una clave pública de un usuario o servicio, firmada digitalmente con la clave privada de una AC en la que confiamos, garantizando que esa clave pública es de quien dice ser. Por ejemplo, en el caso del DNI electrónico, la AC de la Policía Nacional firma digitalmente la clave pública del certificado ciudadano que está introducido en el chip de su DNI.

Un certificado digital por tanto es un **documento digital** mediante el cual un tercero confiable (una autoridad de certificación) garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública. Existen variados formatos para certificados digitales, los más comúnmente empleados se rigen por el estándar **UIT-T X.509**.

Los certificados digitales se usan para mayormente para:

- Firma digital de software o documentos
- Cifrar mensajes

Los certificados pueden ser de **varios tipos** según su uso:

- Personales
- Servidor
- Software
- Entidad de certificación

Los certificados también pueden clasificarse en función del **nivel de verificación** que se hace al concederlos por parte de la AC:

- **Clase 1:** corresponde a los certificados más fáciles de obtener e involucran pocas verificaciones de los datos que figuran en él: sólo el nombre y la dirección de correo electrónico del titular.
- **Clase 2:** se emiten para personas y para servidores o dispositivos y se realiza una mayor verificación de la identidad que en clase 1. Los certificados para personas de clase 2 resultan adecuados para las firmas digitales, el cifrado y el control de acceso electrónico en transacciones en las que la prueba de identidad basada en información de la base de datos de validación es suficiente. Los certificados de dispositivo o servidor de clase 2 resultan adecuados para la autenticación de servidores, la integridad de mensajes, software y el cifrado.
- **Clase 3:** se emiten a personas, organizaciones, servidores, dispositivos y administradores de AC y autoridades de certificados raíz. Los certificados individuales de clase 3 resultan adecuados para las firmas digitales, el cifrado y el control de acceso en transacciones donde se asegura la prueba de identidad. Los certificados de servidor de clase 3 resultan adecuados para la autenticación de servidor; la integridad de mensajes, software y cifrado. Dan un mayor nivel de confianza debido a que exigen un proceso de verificación presencial.

Otro tipo de clasificación de los certificados en función de la **validación** que se hace para la organización que lo solicita es:

- **Domain Validated (DV):** tienen el nivel más bajo de verificación porque sólo se comprueba que el dominio pertenece al solicitante. La confirmación por parte de la AC se hace enviando un email al correo que figura en la información de la base de datos whois del dominio registrado o bien enviando un archivo de verificación que el solicitante coloca en el sitio web para que la AC compruebe que le pertenece dicho dominio.
- **Organization Validated (OV):** tienen un nivel más alto de confianza porque además de comprobar el dominio, verifican la identidad de la organización a la que pertenece el dominio. El nombre de la organización también aparecerá en el certificado, dando confianza añadida de que tanto el sitio web como la compañía son de confianza. Suelen ser utilizados por empresas, gobiernos y otras entidades que desean proporcionar una capa adicional de confianza para sus visitantes.
- **Extended Validation (EV):** son los más seguros y confiables y a la vez los más caros porque requieren un proceso de validación mucho más complejo por parte de la AC y la solicitud de mucha documentación a la organización solicitante. Además de mostrar el nombre de la organización en el certificado, también aparecerá en **color verde** en la barra de direcciones, al lado del candado. Todos los bancos deberían usar certificados de este tipo, aunque desgraciadamente muchos no lo hacen, como es el caso del BBVA o Banco Santander por citar algunos ejemplos.



**Certificado de BBVA con validación OV únicamente y certificado Bankia con validación extendida y por tanto, de mayor confianza**

Los certificados pueden ir en varios **soportes** como por ejemplo:

- Fichero en disco duro, disquette o USB
- Tarjetas smartcard (como el DNI-e)
- tarjetas criptográficas
- token USB

Un certificado digital contiene **información** como:

- Número de versión
- Número de serie
- Nombre del emisor (AC)
- Nombre del sujeto
- Periodo de validez
- Clave pública del sujeto
- Método de verificación de la firma
- Firma digital del certificado por parte de la AC
- Extensiones de certificado

En la siguiente figura se pueden comprobar la información que contiene un certificado digital de un servidor web seguro (HTTPS) de un banco:

**Este certificado ha sido verificado para los siguientes usos:**

SSL Client Certificate

SSL Server Certificate

---

**Emitido para**

Nombre común (CN)	oi.bankia.es
Organización (O)	Bankia SA
Unidad organizativa (OU)	<No es parte de un certificado>
Número de serie	58:70:51:7A:72:B9:2B:BE:13:9F:59:E2:01:75:E3:E5

**Emitido por**

Nombre común (CN)	Symantec Class 3 EV SSL CA - G3
Organización (O)	Symantec Corporation
Unidad organizativa (OU)	Symantec Trust Network

**Periodo de validez**

Comienza el	29/09/15
Caduca el	29/12/16

**Huellas digitales**

Huella digital SHA-256	55:2A:70:3C:5D:70:C2:58:DE:55:6B:E0:AC:4F:6D:6A:11:98:47:2B:3C:05:55:86:02:17:1E:7A:CD:2E:D3:0F
Huella digital SHA1	93:D4:22:3B:33:E1:40:30:CB:59:9E:0B:3D:C4:4E:D9:1B:E0:E4:F0

Esta información puede obtenerse usando cualquier navegador. Por ejemplo en **Firefox**, pulsando Control + i (o bien Herramientas, Información de la página), pestaña Seguridad, botón ver certificado. También puede hacerse en el candado de la barra de direcciones. Desde **Chrome** puede hacerse haciendo clic en el candado de la barra de direcciones y después seleccionar Conexión, Datos del certificado. La siguiente imagen muestra la misma información desde Chrome:

**Este certificado se ha verificado para los siguientes usos:**

Certificado de servidor SSL

**Enviado a**

Nombre común (CN)	oi.bankia.es
Organización (O)	Bankia SA
Unidad organizativa (OU)	<No incluido en el certificado>
Número de serie	58:70:51:7A:72:B9:2B:BE:13:9F:59:E2:01:75:E3:E5

**Emitido por**

Nombre común (CN)	Symantec Class 3 EV SSL CA - G3
Organización (O)	Symantec Corporation
Unidad organizativa (OU)	Symantec Trust Network

**Periodo de validez**

Emitido el	29/9/15
Vencimiento el	29/12/16

**Huellas digitales**

Huella digital SHA-256	55 2A 70 3C 5D 70 C2 58 DE 55 6B E0 AC 4F 6D 6A 11 98 47 2B 3C 05 55 86 02 17 1E 7A CD 2E D3 0F
Huella digital SHA-1	93 D4 22 3B 33 E1 40 30 CB 59 9E 0B 3D C4 4E D9 1B E0 E4 F0

Los certificados digitales pueden encontrarse en varios **estados**:

- **Emitido**: se encuentra en vigencia y por tanto es válido.
- **Expirado**: ha finalizado su periodo de validez y es necesario renovarlo.
- **Revocado**: es un certificado que no es válido y ha sido incluido en una lista de revocación (CRL) debido a que la clave privada se ha visto comprometida o ha habido cambios en los datos asociados al certificado
- **Suspendido**: es una revocación temporal por las mismas razones que el revocado, pero es una situación reversible.

## Pasos para obtener un certificado

Como personas físicas o bien, para montar un servidor web seguro, podemos solicitar un certificado a una AC siguiendo los siguientes pasos:

1. El solicitante (persona física o una empresa) realiza una **solicitud** (CSR, Certificate Signing Request) enviando sus datos a la autoridad certificadora.
2. La Autoridad de Certificación verifica la identidad del solicitante de un certificado antes de su expedición, de forma presencial habitualmente.
3. Al expedir el certificado, la AC lo firma con su clave privada, garantizando su validez.
4. La AC envía al solicitante el certificado.
5. Los certificados suelen ser para personas físicas o para servidores (p.ej. https).

En algún momento del proceso, es necesario generar el par de claves (privada y pública) asociadas al solicitante. Hay dos opciones, siendo la segunda la más recomendable y usada:

1. **Método 1**: la autoridad al crear el certificado crea un par de claves:  
Clave privada: contenida en el propio certificado digital
  - Ni el usuario ni la CA deben proporcionar el certificado a otros
  - La CA no se queda con copia del certificado
  - Si se pierde, se debe pedir uno nuevoClave pública: guardada por la CA y proporcionada a todo el que la solicite
2. **Método 2**: para evitar que la CA pueda tener la clave privada el solicitante puede generar una petición de certificado (CSR) desde su ordenador, que enviará a la autoridad certificadora, y así no le envía su clave privada, que siempre la tendrá él en su ordenador

## Proceso de validación y verificación de un certificado

Los pasos que se siguen cuando una parte quiere validar el certificado que le envía la otra parte, como por ejemplo un navegador web cuando se conecta a una página web segura:

1. Conseguir el certificado de la otra parte.
2. Verificar la validez del certificado:
  - Dentro del período de validez
  - Certificado no revocado
  - Firma electrónica de la AC correcta
3. Verificar la firma digital del resumen o hash del mensaje con la clave pública del emisor.
4. El receptor debe estar en posesión de la clave pública de la AC (instalada en su navegador, por ejemplo), con lo que podrá comprobar la firma electrónica de la AC del certificado.

## Autoridad de Certificación

La AC es una entidad **fiable** y **reconocida** regional o mundialmente, encargada de garantizar de forma unívoca y segura la identidad asociada a una clave pública. Realiza las siguientes tareas:

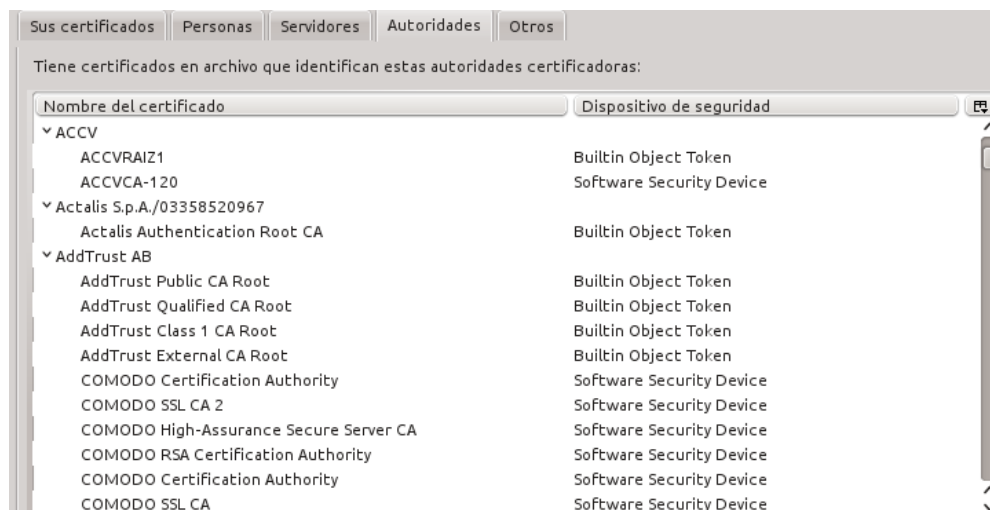
- Recibe y procesa peticiones de certificados (CSR) de los usuarios finales.
- Consulta con una Autoridad de Registro para determinar si acepta o rechaza la petición de certificado
- Emite el certificado
- Gestiona Listas de Revocación de Certificados (CRLs)
- Renueva certificados
- Proporciona:
  - Servicios de backup y archivo seguro de claves de cifrado
  - Infraestructura de seguridad para la confianza, políticas de operación segura e información de auditoría.

Algunas de las principales autoridades certificadoras son:

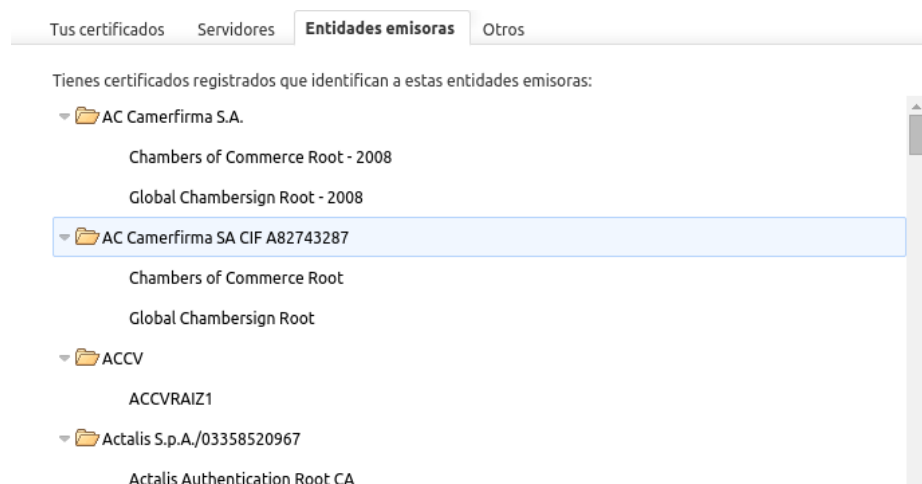
- **Internacionales:** Verisign, GlobalSign, Thawte Certification, Comodo, etc
- En **España:** FNMT, ACCV (GVA), Edicom, etc.

Cualquiera puede crear su propia AC con el software adecuado (por ejemplo Openssl). El problema es generar reputación y confianza por el resto para ser incluido en los repositorios de AC, como las que vienen de serie en nuestro navegador.

Se pueden consultar las AC de nuestro ordenador, dependiendo del software que utilicemos. Por ejemplo en el navegador **Firefox** se pueden consultar desde menú Preferencias, Avanzado, Certificados, botón Ver certificados, pestaña Autoridades:



Desde **Chrome**, podemos hacerlo desde menú Configuración, Mostrar opciones avanzadas, botón Administrar certificados, pestaña Entidades Emisoras:



### 4.2.2. Firma digital

La firma digital se usa para **autenticar** el origen de los datos y asegurar la integridad del mensaje. Su finalidad **no** es proporcionar **confidencialidad** ya que no se utiliza para cifrar los documentos completos si no un resumen del mensaje con una función hash, de esta forma las entidades pueden asegurar el origen de los datos.

Este tipo de firma electrónica está siendo adoptada progresivamente como una firma con **validez jurídica**. Por ejemplo, la firma digital de la declaración de la renta presentada telemáticamente por Internet, se realiza mediante este sistema.

Como ya se estudió en la unidad didáctica 2, la función hash es un algoritmo matemático que permite calcular un valor resumen (message digest) de los datos a ser firmados digitalmente. No es reversible, es decir, no es posible, a partir del valor resumen, calcular los datos originales. Algunos ejemplos de algoritmos de hash son SHA, MD4, MD5, etc.

La firma digital proporciona pues los siguientes **servicios**:

- **Autenticidad**
- **Integridad**
- **No repudio**

#### Funcionamiento de la firma digital

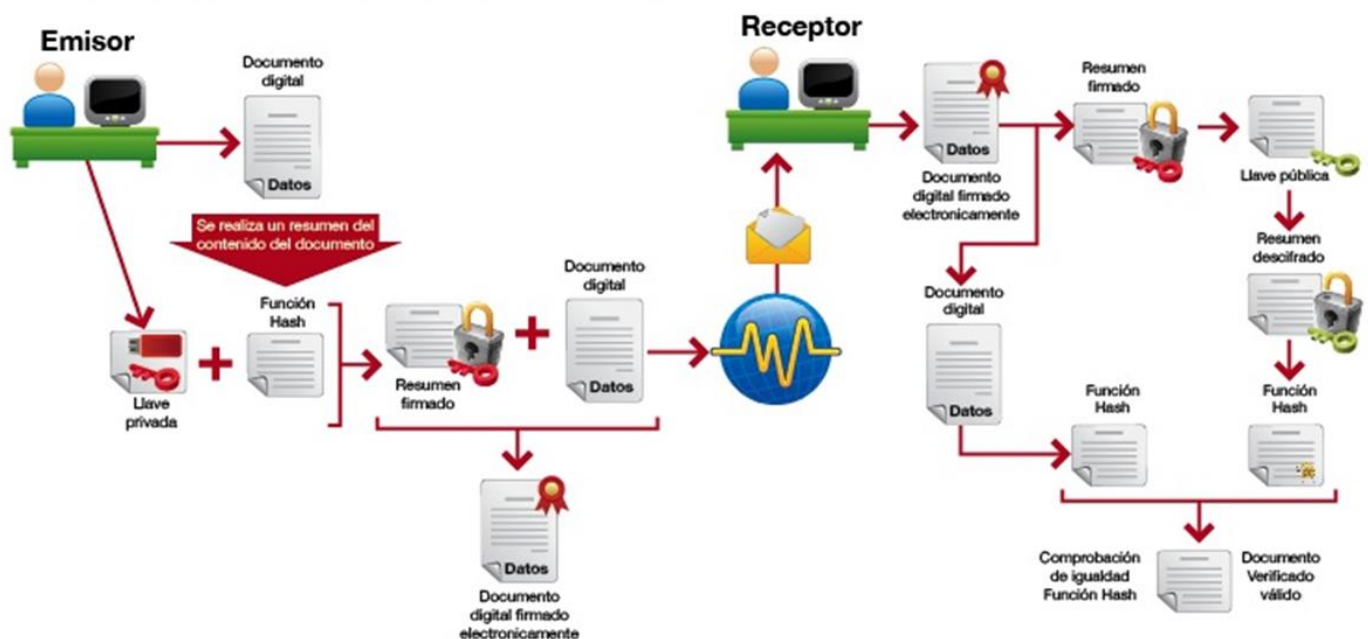
La firma digital de un documento es el resultado de realizar el siguiente proceso:

1. Aplicar una función **hash**, a su contenido generando así un resumen irreversible.
2. Aplicar el **algoritmo de firma** (como RSA o DSA y en el que se emplea la clave privada) al resumen, generando así la firma digital.

El destinatario, al recibir el mensaje:

1. Calcula de nuevo el resumen mediante la misma función hash.
2. Descifra la firma utilizando la clave pública del emisor y aplicando el mismo algoritmo de firma.
3. Si ambos resúmenes coinciden, la firma es válida

En la siguiente figura, se ilustra el proceso de la firma digital:





## Aplicaciones de la firma digital

Como ya se ha citado, actualmente la firma digital es un reemplazo de la firma manuscrita hasta el punto que tiene completa validez legal. Algunas de las aplicaciones más destacables de la firma digital son:

- o Mensajes con autenticidad asegurada
- o Mensajes sin posibilidad de repudio
- o Contratos comerciales electrónicos
- o Factura Electrónica
- o Desmaterialización de documentos
- o Transacciones comerciales electrónicas
- o Invitación electrónica
- o Dinero electrónico
- o Notificaciones judiciales electrónicas
- o Voto electrónico
- o Decretos ejecutivos (gobierno)
- o Créditos de seguridad social
- o Contratación pública
- o Sellado de tiempo

### 4.3. Protocolos seguros: SSL/TLS y HTTPS

**SSL** (Secure Sockets Layer) y **TLS** (Transport Layer Security) son una serie de protocolos que permiten dar seguridad a los protocolos de capa de aplicación que no la poseen de forma nativa, protegiendo de esta manera servicios como las aplicaciones web, el correo electrónico, la transferencia de archivos o la voz sobre IP.

De esta forma, protocolos como HTTP, SMTP/POP3 o FTP pasan a denominarse HTTPS, SMTPS, POP3S o FTPS cuando usan SSL/TLS por debajo. SSL/TLS ofrece cifrado híbrido al combinar algoritmos de clave pública con algoritmos de clave simétrica. La clave simétrica se usa para cifrar las comunicaciones entre ambos extremos, y para intercambiarse dicha clave de sesión, se usa la criptografía de clave pública.

Como ya se comentó anteriormente en la unidad, el cifrado simétrico es mucho más rápido y necesita menor carga computacional que el cifrado asimétrico. Sin embargo éste último es ideal para asegurar la integridad y la autenticación de los datos, así como para el intercambio seguro de claves.

SSL es el protocolo más antiguo y fue desarrollado por **Netscape** a mediados de los 90. En este protocolo han ido basándose las siguientes versiones que han ido mejorando fallos de seguridad hasta llegar al protocolo TLS, que es una versión mejorada de su antecesor SSL.

TLS actualmente va por la versión **1.3** y es el protocolo que se recomienda usar en navegador y servidores web, debido a los fallos de seguridad de SSL que han ido publicándose recientemente. SSL llegó hasta la versión 3 y se desaconseja su uso por las razones expuestas anteriormente.

Ambos protocolos han sido fundamentales para el auge del comercio electrónico, las compras seguras y la administración telemática al proporcionar seguridad en estos servicios al utilizar una red de transporte insegura como es Internet.

En el siguiente vídeo de Intypedia, puedes ver una introducción al protocolo SSL/TLS así como su funcionamiento: <https://youtu.be/pOeWmStBOYY>



## 5. Vulnerabilidades y ataques en redes informáticas

## 5.1. Introducción a la seguridad en redes

En la unidad anterior hemos visto como el malware es una de las principales amenazas que pueden sufrir tanto las organizaciones y empresas como los usuarios de ordenadores y dispositivos electrónicos de todo el mundo. Y esto es debido a que supone un negocio muy lucrativo para los desarrolladores de malware, que en muchos casos son bandas y mafias organizadas que distribuyen el software malicioso por todo el mundo obteniendo pingües beneficios.

También vimos que no sólo debemos confiar en la tecnología para protegernos usando herramientas como los antivirus o los cortafuegos, sino que es fundamental la formación y concienciación en el uso de las nuevas tecnologías. Si pensamos que sólo la tecnología va a protegernos, vamos muy mal encaminados ya que los cibercriminales van por delante de muchas de estas herramientas de seguridad.

Esto es más cierto cuando usamos redes habitualmente, como la red de nuestro instituto o empresa o las peligrosas wifi abiertas que podemos encontrar en muchos lugares como estaciones de tren, aeropuertos, cafeterías, grandes superficies, etc.

En esta unidad aprenderemos que, a pesar de tener nuestro sistema actualizado con antivirus y cortafuegos, podemos ser víctimas también de ataques simplemente por el hecho de estar conectados a una red local, como la de cualquier hotel, aeropuerto o cafetería.

En el siguiente vídeo de Intypedia puedes ver una breve introducción a la seguridad en redes:

<https://youtu.be/74DIEMJsXBw>

## El 70% de los ataques son internos

¿Sabías que en según datos analizados por grandes empresas como Cisco Systems, la mayoría de ataques son causados por usuarios internos? Empleados descontentos o despedidos, o alumnos que quieren obtener algún beneficio como acceso a exámenes son algunos ejemplos...

## 5.2. La seguridad heredada

Estamos acostumbrados a escuchar a los políticos en los medios de comunicación expresiones como la "herencia recibida". Sin pretender entrar en temas políticos, en seguridad informática podemos hablar en los mismos términos.

Cuando en los años 70 se inventaron tecnologías como Ethernet o la pila de protocolos TCP/IP, que se han impuesto ambas como estándares de facto en todo el mundo, nadie pensó el impacto que iban a tener en el futuro y que en unos años todo el mundo se conectaría a una red mundial de redes llamada Internet utilizando estas tecnologías.

Las redes y los protocolos que se usan en ellas fueran concebidas para usar en ámbitos académicos y militares. Nadie pensaba en el mal uso que se podían hacer de ellas aprovechando las carencias de seguridad con las que se crearon y que desgraciadamente, están siendo aprovechadas por los atacantes.



**Imagen de Robert Kahn y Vinton Cerf, creadores de los protocolos TCP/IP**

### 5.3. Ataques comunes en redes locales

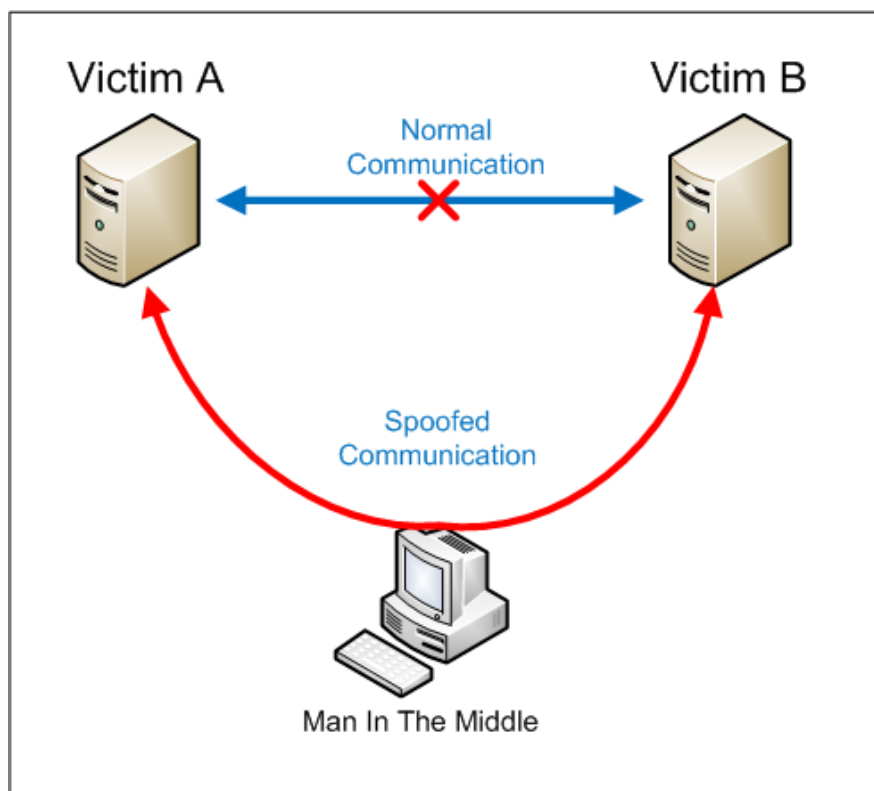
En esta sección citaremos algunos de los ataques más comunes y frecuentes que podemos sufrir como usuarios de una red local, como la red cableada o inalámbrica de cualquier lugar en el que estemos conectados, como estación de tren, aeropuerto, hotel o cafetería.

Hay que indicar que todos los ataques citados en esta sección, se aplican igualmente a las redes inalámbricas, pero éstas tendrán un apartado especial debido a las consideraciones especiales que hay que tener para proteger el acceso a estas redes.

#### 5.3.1. Man In The Middle

Los ataques **MITM** (Man In The Middle) es una clasificación de ataques bajo la que se pueden agrupar las técnicas que permiten que un atacante se introduzca en medio de una comunicación entre dos víctimas, de forma que se puede interceptar, modificar, espiar o destruir la comunicación.

Es habitual ponerse en el camino entre el router de acceso a Internet y la víctima. De esta forma el atacante tiene acceso a las comunicaciones en ambos sentidos: de la víctima a Internet y de Internet a la víctima. De ahí deriva el nombre de los ataques MITM (hombre en el medio):



**Figura que ilustra la interceptación de la comunicación que realiza el atacante**

### 5.3.2. Envenenamiento ARP

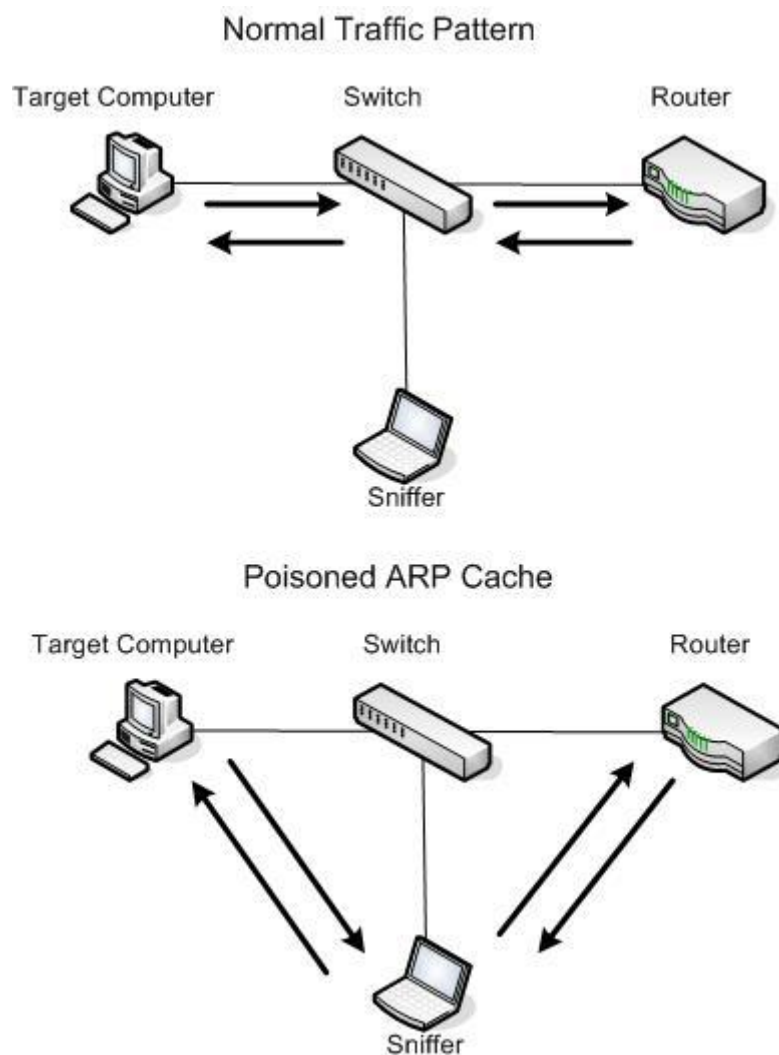
#### Protocolo ARP

El ARP es un protocolo de IPv4 que permite a un ordenador o dispositivo, conocer la dirección física de nivel 2 (**MAC**) de otro ordenador o dispositivo con el que quiere comunicarse en la **misma** red local. El ordenador origen conoce la IP de destino y hace una petición ARP por la red para que el equipo destino conteste con su dirección MAC, siendo guardada después durante un tiempo en una memoria caché en el ordenador que realiza la consulta.

El ataque de envenenamiento ARP o **ARP Poison** o **ARP Spoofing** es uno de los ataques MITM más habituales que podemos sufrir por el hecho de estar conectado a una red local, ya sea cableada o inalámbrica. El **objetivo**, como en todos los MITM, es meterse en la comunicación de una víctima con otro destino - como Internet -y de esta forma poder modificar la información, robar credenciales o hacer una denegación de servicio.

Ataca al protocolo **ARP**, y el principal problema es que este protocolo, fundamental es cualquier red IPv4 actual, no se diseñó pensando en que nadie falsificaría su información y por tanto podemos decir que funciona en la gran mayoría de redes a las que nos conectamos, a no ser que tengan mecanismos de defensa.

Para que este ataque tenga éxito, se realiza la **falsificación** de la dirección MAC de ambas partes mediante el protocolo ARP, para de esta forma recibir el tráfico de la víctima y del destino. Es habitual falsificar la dirección MAC del router para la víctima y la dirección de la víctima para el router. De esta forma, la víctima piensa que el router es el equipo del atacante (su dirección MAC) y el router piensa que la víctima es el equipo del atacante, de esta forma se captura el tráfico en ambas direcciones: de la víctima a Internet y de Internet a la víctima.



*Figura que ilustra el proceso del ARP Poison*

## Herramientas para ARP spoofing

Muchas son las herramientas disponibles en Internet al alcance de cualquiera y que pueden ser usadas fácilmente para realizar este ataque: arpspoof, ettercap, Caín & Abel, etc. son algunas de ellas. Muchas vienen de serie en distribuciones GNU/Linux para auditorías de seguridad, como el conocido **Kali Linux**, reemplazo del anterior Backtrack.

## Contramedidas

Algunas de las medidas que podemos usar para protegernos, bien detectando el ataque o evitándolo son:

- **Entradas ARP estáticas** en todos los equipos del aula: de esta forma, la asociación IP-MAC que realiza ARP en la tabla o caché arp es fijada por el administrador y prevalece ante cualquier intento de falsificación. Este procedimiento es eficaz pero muy laborioso, pues hay que hacerlo en todos los equipos o en la imagen de clonación del aula. [Cómo modificar la tabla ARP en varios sistemas](#)
- **Inspección ARP** en conmutadores/AP: esta es una de las mejores soluciones pero necesitamos conmutadores o puntos de acceso que soporten estas tecnologías como Cisco DAI, D-Link ARP spoofing prevention, arp-patrol ...Lo que hacen es monitorizar el protocolo ARP y rechazar las tramas maliciosas
- **Monitorización pasiva** con herramientas como detectores de intrusos, arpwatch, arpalert...
- **Monitorización activa** con herramientas como Marmita, Xarp, Patriot-NG, ettercap ...
- **Aislamiento de clientes** en puntos de acceso wifi: los puntos de acceso tienen que soportar esta función, pero además del ataque evitan la comunicación directa entre ordenadores en la red wifi, lo cual puede ser una funcionalidad requerida.
- **Secure ARP** - MACSec (802.1AE): es un estándar de firma digital similar a IPSec que se está usando en los servidores de Data Centers. Todas las tramas ethernet van firmadas de forma que no es posible suplantar la MAC de nadie.

### 5.3.3. Ataques al DHCP

#### Protocolo DHCP

El protocolo **DHCP** (Dynamic Host Configuration Protocol) permite asignar la configuración básica de IP a los ordenadores o dispositivos conectados a una red local. Asigna de manera automática la dirección IP, la máscara, la puerta de enlace o router, los DNS, el nombre de dominio y muchas más opciones. Es un protocolo fundamental en las redes actuales ya que evita que los usuarios tengan que asignar la configuración manual, con los posibles problemas de duplicidad de direcciones en la misma red.

Este protocolo, que funciona tanto para IPv4 e IPv6, también fue creado sin tener en mente la seguridad. En esta sección veremos algunos de los ataques que puede sufrir este protocolo y algunas contramedidas que podemos usar.

#### DHCP Starvation

El **DHCP starvation** o agotamiento DHCP es un ataque que persigue agotar todo el rango de direcciones IP asignables por el servidor de forma que éste deja de servir direcciones y por tanto no contesta a las peticiones de asignación. Por tanto consiste en una **denegación de servicio** (DoS) al DHCP.

El ataque consiste en realizar sucesivas peticiones con direcciones MAC falseadas desde el ordenador del atacante, de forma que el servidor asigna todas las direcciones IP disponibles y se agota el rango.

## Rogue DHCP

El **rogue DHCP** o falso DHCP, es una técnica que consiste en montar un servidor DHCP **no autorizado** en la red. Su objetivo es modificar la configuración IP de los equipos de la red, ya que éstos no validan al servidor DHCP. Principalmente se cambia la puerta de enlace y los servidores DNS para que apunten al atacante, con lo que se consigue hacer MITM y DNS Spoofing (ya veremos lo que es).

Con este ataque podemos asignar puertas de enlace inexistentes provocando un DoS o lo que es peor, asignar como puerta de enlace el ordenador del atacante que funciona como un router. De esta forma todo el tráfico pasa por él, pudiendo capturarlo o modificarlo.

El ataque rogue DHCP se suele realizar después de un DHCP Starvation, para asegurarse de que el servidor DHCP legítimo no funciona al tener agotado el rango.

## DHCP ACK Injection

En vez de montar un servidor DHCP falso, se realiza un seguimiento de las peticiones DHCP (DHCP Request) de los clientes de la red y se contesta con una confirmación (DHCP ACK) con los parámetros de configuración (gateway, dns, etc) manipulados.

Sin embargo la respuesta ACK del servidor legítimo podría llegar antes que la del atacante por tanto es un ataque no tiene un 100% de fiabilidad desde el punto de vista del atacante.

## Contramedidas

Algunas contramedidas que podemos usar ante estos ataques son:

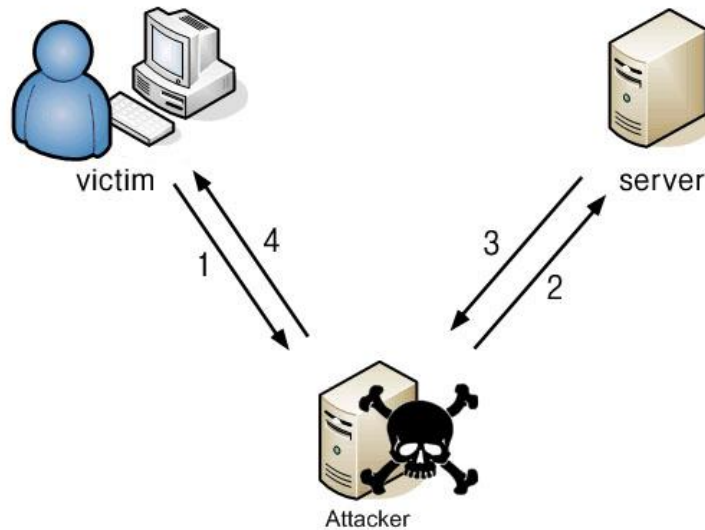
- **Habilitar port-security** en los puertos del switch: esta técnica permite asociar una MAC o un grupo de MAC conocidas, de forma que ante un intento de falsificar la MAC para solicitar una nueva dirección IP, se bloquea el puerto. Esta técnica sin embargo no vale para todos los ataques y además debemos tener conmutadores gestionables con esta función.
- **Habilitar protección DHCP** en los conmutadores y router: esta característica actualmente no la soportan muchos routers y conmutadores. Por tanto, es necesario tener equipamiento que soporte esta funcionalidad como por ejemplo:
  - Cisco: **DHCP Snooping**
  - D-Link: **DHCP Server Screening**
- **Monitorización activa**: la solución más viable por coste es detectar y alertar ante un servidor DHCP no autorizado con herramientas software como **dhcp\_probe**, que es una herramienta para GNU/Linux que puede instalarse en un servidor de la red y nos avisa cuando aparece un servidor DHCP no legítimo.

## 5.3.4. Ataques al DNS

### Protocolo DNS

El protocolo **DNS** (Domain Name System) es un servicio que permite fundamentalmente conocer la dirección IP asociada a un nombre de dominio. Esta es su principal función pero tiene muchas más como la resolución inversa de nombres, información de un dominio, servidores de correo o de nombres asociados a un dominio, registros de verificación de servidores de correo, etc.

El DNS es otro de los servicios críticos de Internet y candidato a sufrir muchos ataques. Cuando nos conectamos al banco a través de Internet, nuestro navegador hace una consulta DNS para saber a qué dirección IP debe conectarse. Ya sabemos que los ordenadores y dispositivos móviles no entienden de letras y tienen que resolver los nombres como [www.mibanco.com](http://www.mibanco.com). Si la respuesta del servidor DNS es manipulada y se nos envía la dirección IP del servidor de un atacante con una copia exacta de la página web del banco, nos podrían robar las credenciales de acceso si no advertimos que es una página falsa.



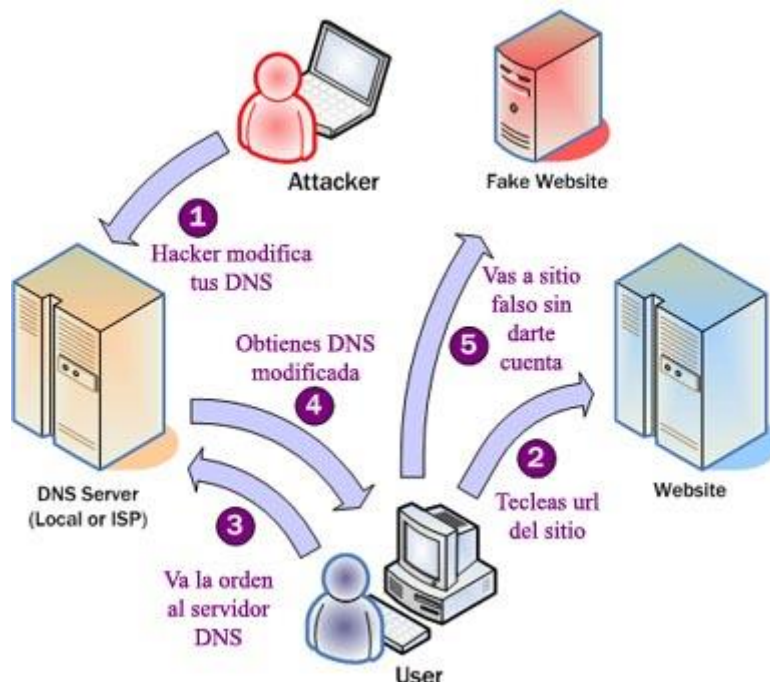
**DNS spoofing realizado por un atacante con un MITM**

## DNS Spoofing

El DNS Spoofing es una técnica que permite manipular las respuestas de un servidor DNS legítimo, mediante un ataque MITM previo para dirigir el tráfico DNS de la víctima hacia el atacante. La forma de evitarlo es mediante las contramedidas de MITM explicadas anteriormente. En la figura anterior se puede ver cómo funciona el mecanismo de DNS spoofing.

## DNS Poison

El envenenamiento DNS es un ataque mucho más peligroso ya que el ataque se realiza contra los servidores DNS que tenemos configurados en nuestro ordenador o dispositivos, de forma que no podemos saber si no podemos controlar o evitar el ataque. La siguiente figura ilustra el proceso:



En este caso, cuando hacemos la consulta al servidor DNS legítimo y éste ha sido atacado, nos puede proporcionar la información que ha introducido el atacante en la caché del servidor DNS.

Por eso es fundamental que los administradores de los servidores DNS deban estar al tanto de cualquier vulnerabilidad asociada al DNS que usan y actualizarlos convenientemente.



## DNSSEC

Una técnica que garantiza que la respuesta de un servidor DNS es legítima, es usar firma digital entre los servidores DNS, de tal forma que no sería posible corromper la caché de un servidor DNS legítimo con las respuestas falsas de un servidor atacante.

DNSSEC son unas extensiones de seguridad para el DNS y que funciona precisamente así, mediante criptografía de clave pública, garantizando la autenticidad de las respuestas al estar firmadas digitalmente por el otro servidor.

Sin embargo, a pesar de ser totalmente efectivo contra el DNS Poison, DNSSEC no está implantándose lo que debiera debida a su complejidad técnica, que requiere que toda la cadena de respuestas de servidores estén firmadas. Poco a poco, los dominios de primer nivel están implantando DNSSEC, pero es un proceso que va a un ritmo muy lento, similar a la implantación de IPv6, que hace años que debería haber sustituido a IPv4 por el problema del agotamiento de direcciones IPv4.

### 5.3.5. Ataques a SSL/TLS

**SSL/TLS** son los protocolos que se usan para cifrar las comunicaciones cuando se utiliza HTTPS en el navegador, que se suele reconocer por la aparición del candado al lado de la barra de direcciones.

## 5.4. Ataques por correo electrónico y mensajería

El correo electrónico es uno de los servicios de mensajería en red más usados desde los orígenes de Internet hace más de 45 años. De hecho ya se usaba en el año 1961 en el MIT, anteriormente a la creación de Internet.

Desgraciadamente, el correo electrónico es uno de los servicios más utilizados con fines maliciosos como el spam, las estafas o los hoax, y muchas veces el objetivo detrás de estos mensajes es la distribución masiva de malware para realizar delitos informáticos de todo tipo. Hasta hace pocos años, los datos decían que cerca del 95% del tráfico mundial de correo electrónico se usa para fines ilícitos como el spam.

[Cerca de un 95% del correo electrónico es spam según un estudio en EEUU](#)

El éxito de todas estas técnicas consiste en el envío masivo de mensajes. Por ejemplo, si se envían 20 millones de mensajes y sólo el 1% de los destinatarios pican, se habrá conseguido que 200.000 personas se infecten con malware, se hayan robado sus credenciales bancarias o caigan en una estafa.

En esta sección veremos algunos de los problemas más comunes asociados con este servicio.

### Spam

El **spam** son los mensajes de correo-e no solicitados, generalmente de tipo publicitario y enviados en cantidades masivas. Generalmente el medio más utilizado es el correo, aunque hay otros tipos de spam como en los grupos de noticias, mensajería instantánea, SMS, redes sociales, wikis, foros, pop-up's, voip, etc. El nombre proviene de la 2ª guerra mundial, cuando los soldados recibían comida enlatada con carne (Spiced Ham).

El spam está tipificado como delito con su sanción correspondiente en la LSSICE (Ley de Servicios de la Sociedad de la Información y Comercio electrónico).

Generalmente los **spammers** (que así se llaman los que usan esta técnica para sus fines) usan servidores de correo mal configurados (open-relay), ordenadores zombie o bien cuentas de correo comprometidas para realizar el envío masivo de correos.

Algunas técnicas para evitar el spam son [SPF](#) o [DomainKeys](#)

Sabías que...

Aunque el origen del spam no está del todo claro, hay fuentes que datan su origen el 3 de mayo de 1978, cuando 393 empleados de ARPANET, la red predecesora de lo que sería Internet, recibían un correo de la compañía de ordenadores DEC invitándoles al lanzamiento de un nuevo producto.



## Hoax y cadenas

Un **hoax** o bulo es un mensaje de correo electrónico con contenido falso o engañoso y normalmente distribuido en cadena. Algunos informan sobre virus desastrosos, niños enfermos o desaparecidos, otros contienen fórmulas para hacerse millonario o crean cadenas de la suerte como las que existen por correo postal.

Las cadenas y los hoax tienen muchas similitudes y los objetivos que se persiguen con ambos son los mismos: captar direcciones de correo para usarse como spam o saturar la red y los servidores de correo.



*Hoax enviado por whatsapp sobre un falso problema de salud del Papa*

### Sabías que ...

En diciembre de 1994, se envía el primer hoax masivo, que tenía como asunto Good Times. El contenido de este correo era:

"¡Cuidado! Si llega un mensaje titulado 'Good Times', simplemente leyéndolo, el virus malicioso actúa y puede borrar todos los contenidos del disco duro"

Hoy en día hay bulos a diario. Por ejemplo, son varias ya las veces que se ha repetido el bulo de un niño que necesitaba sangre en el hospital La Fe de Valencia. En estos casos se aprovechan de la buena voluntad de la gente para ayudar a un niño necesitado:

[La Fe alerta de un email fraudulento que pide sangre AB para un niño](#)

## Scam

El **scam** o estafa es una variante del spam en el que se produce una estafa y por tanto, pérdida monetaria por parte de la víctima que sufre el scam.

Hay muchísimas variantes pero casi todos estos mensajes se identifican porque suelen estar mal traducidos y acaban pidiendo **dinero por adelantado**, lo que nunca debe hacerse.

El scam también se aplica a sitios web que tienen como intención ofrecer un producto o servicio que en realidad es falso, por tanto una estafa, así como redes sociales o páginas de encuentros.

Un tipo común de mensajes de este tipo, son los que se conocen como cartas o [estafas nigerianas](#). Consiste en engañar al incauto con una supuesta fortuna (inexistente por supuesto) y persuadirlo para que pague una suma de dinero por adelantado, como condición para acceder a la supuesta fortuna. Las sumas solicitadas, aunque elevadas, son pequeñas comparadas con la fortuna que las víctimas esperan recibir. Son una versión actual del [timo de la estampita](#) o del [cuento del tío](#).

## Phishing, vishing y smishing

Todos ellos utilizan la **ingeniería social**, que consiste en aprovecharse de la ingenuidad del usuario y convencerlo de que realice una determinada acción, como enviar su usuario y contraseña o la información de su tarjeta de crédito.

El **phishing** es una comunicación falsa por correo electrónico, haciéndose pasar generalmente por un banco solicitando el usuario y contraseña del cliente del banco por alguna razón, como un problema en los sistemas informáticos de la entidad.

En el **vishing**, se solicita mediante un correo electrónico que el usuario actualice su información personal o que resuelva un problema relacionado con su tarjeta de crédito mediante una llamada telefónica. Cuando la víctima llama, una grabación se hace pasar por el banco y le solicita información personal, como su usuario y contraseña o el número y pin de su tarjeta de crédito. También se usan llamadas automatizadas mediante VoIP (lo que es fácil de hacer con software como Asterisk) haciéndose pasar por el banco y pidiendo los datos de la tarjeta de crédito y el pin en algún momento.

El **smishing** es una variante del phishing pero usando los SMS de la telefonía móvil.

Las víctimas reciben SMS con mensajes como:

*"Estamos confirmando que se ha dado de alta para un servicio de citas. Se le cobrará 2 dólares al día a menos que cancele su petición: [www.?????.com](#)."*

*"El cheque es preparado para usted. Favor gracias de llamarnos para completar las informaciones al número ??????"*  
(nótese que parece que el texto está traducido por algún traductor online).

*"Hola. Anoche lo pasé muy bien contigo. Favor llámame al ?????? para quedar"*

Cuando visitan la dirección web, las víctimas son incitadas o forzadas a descargar algún programa que suele ser malware.

## Spear phishing

Caso real: una persona que había hecho una reserva de un hotel en Londres a través de una conocida web de reserva de hoteles recibió un correo personalizado con su nombre de la empresa de reservas online (con el logo y toda la imagen corporativa) indicando que el hotel solicitaba el pago por adelantado y proporcionaban una cuenta bancaria para la transferencia.

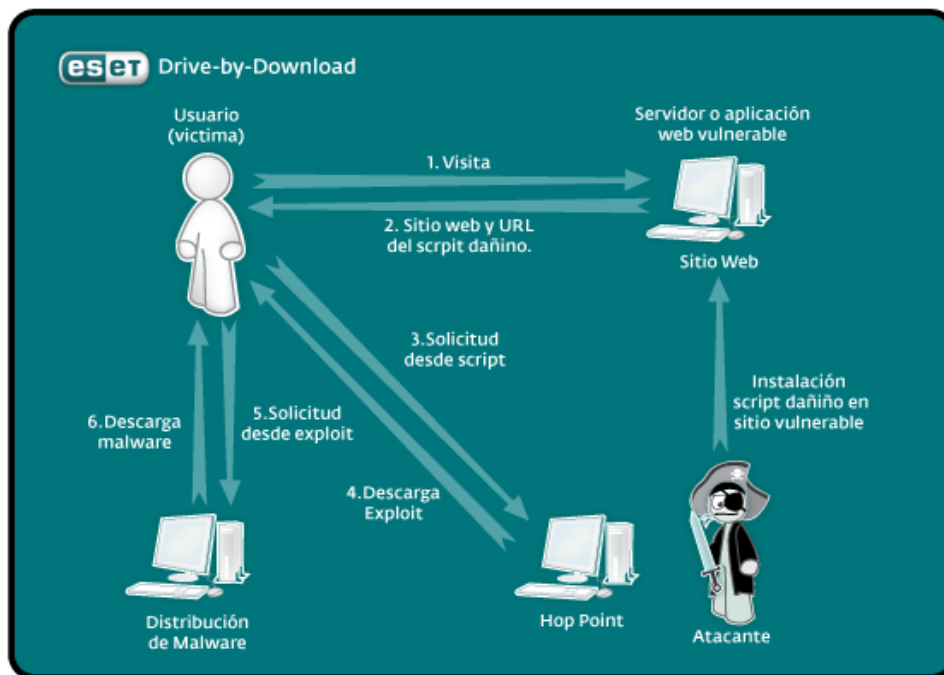
Días más tarde esta persona confirmó que había habido un ataque en la web de reservas y habían obtenido datos de reserva. Los atacantes se dedicaron a enviar mensajes falsos personalizados a las víctimas, para cobrar por adelantado las reservas de los hoteles. Por tanto, cuando se reciben mensajes de este tipo, no hay que pagar lo que se nos pide y sí ponerse en contacto con la empresa.

Esta técnica de enviar mensajes falsos personalizados con ingeniería social se conoce como **spear phishing**. El spear phishing también se usa para introducir APT en las organizaciones, con el objetivo de espiar o robar información secreta y confidencial.

## Drive by download

Es una técnica que los ciberdelincuentes utilizan para propagar malware gracias al aprovechamiento de vulnerabilidades existentes en diferentes sitios web, las cuales una vez explotadas, permiten la inyección de código malicioso entre el código original del sitio. El objetivo es infectar de manera masiva los ordenadores de los usuarios desprevenidos con solo entrar a un sitio web comprometido.

Para redireccionar a las víctimas a estos sitios, se utilizan los sistemas de mensajería comentados anteriormente.



**Imagen que ilustra el proceso, cortesía de ESET**

El proceso de infección mediante esta técnica se puede resumir así, una vez el atacante ha infectado la página web vulnerable con un script:

1. La víctima realiza una consulta al sitio comprometido tras haber recibido algún mensaje por alguna vía.
2. El sitio web consultado devuelve la petición que contiene embebido en su código el script dañino previamente inyectado por el atacante.
3. Una vez que el script se descarga en el sistema de la víctima, establece una conexión pero a otro servidor, denominado Hop Point, desde el cual descarga otros scripts maliciosos que contienen diversos exploits.
4. Cada uno de estos exploits tienen el objetivo de comprobar la existencia de vulnerabilidades que puedan ser explotadas en el equipo víctima.
5. En caso de encontrar alguna vulnerabilidad, se ejecutará una instrucción que invoca la descarga de un archivo ejecutable (el malware) desde otro servidor o desde el mismo Hop Point.
6. Se infecta el equipo de la víctima.

## Recomendaciones

Para evitar o minimizar los problemas derivados de todas estas técnicas ampliamente utilizadas hoy en día se recomienda:

- No descargar adjuntos de correos sospechosos
- Analizar todos los adjuntos
- Activar el bloqueo de phishing que llevan de serie navegadores como Firefox (Preferencias, Seguridad, Bloquear sitios ...) o Chrome (Opciones, Privacidad, Habilitar protección contra phishing)
- No hacer caso de correos de bancos o servicios pidiendo contraseñas
- No dar dinero por adelantado en ningún correo que así nos lo soliciten (excepto compras por Internet, lógicamente)
- Rechazar ofertas y reclamos sospechosos (ganador de un premio, herencia, etc.)
- No fiarse de los acortadores de URL ni los códigos QR
- No reenviar cadenas de email

## 5.5. Seguridad perimetral: cortafuegos

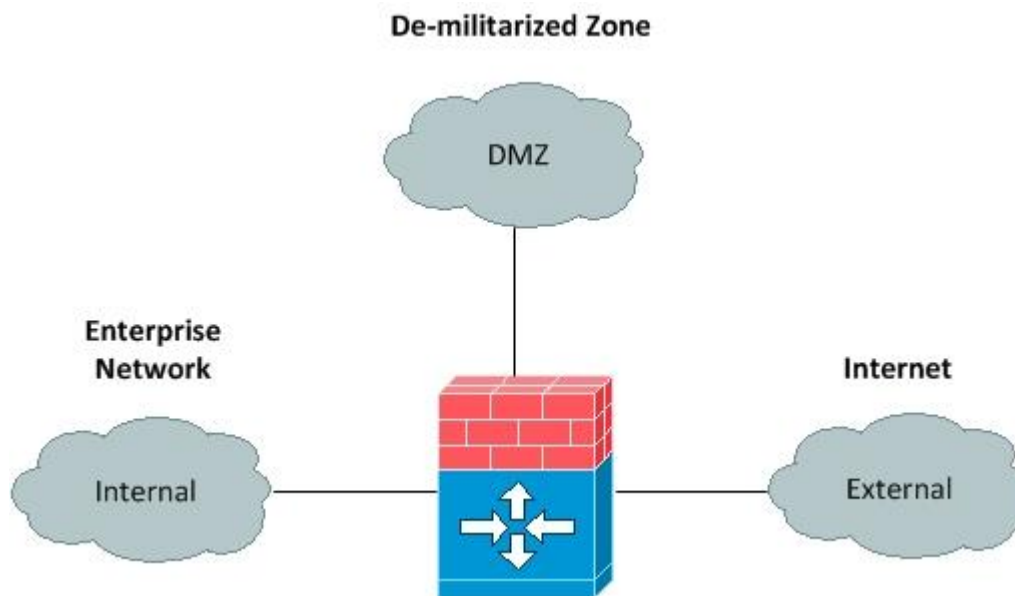
### Seguridad perimetral

Por **seguridad perimetral** entendemos el conjunto de métodos y técnicas para proteger una red informática y que se basan en el establecimiento de recursos de seguridad en el perímetro externo de la red y en diferentes niveles.

El **perímetro de una red** corporativa son los límites entre la red de la organización y las redes a las que ella se interconecta, como por ejemplo Internet. El perímetro de la red es la primera zona a proteger debido a la posibilidad de ataques desde las redes externas a la organización, No obstante, muchos ataques provienen de usuarios internos y hay que proteger la red también de estos ataques,

En el perímetro de la red se suelen definir **niveles de confianza**, permitiendo el acceso de determinados usuarios internos o externos a determinados servicios, y denegando cualquier tipo de acceso a otros. La seguridad perimetral también define **zonas** o áreas donde la seguridad se trata en bloque:

- **Red interna:** red donde se ubican los usuarios internos
- **Red externa:** generalmente es la red Internet
- **Extranet:** zona de acceso de proveedores o empleados
- **DMZ** o zona desmilitarizada: zona donde se ubican los servidores con acceso externo



**Firewall con tres zonas: interna, DMZ e internet**

### Cortafuegos

Un **cortafuegos** o **firewall** es un dispositivo software o hardware que forma parte de un sistema o red y que está diseñado para proteger dicho sistema o red bloqueando los accesos no autorizados y permitiendo sólo los autorizados, cumpliendo con las directrices definidas en la política de seguridad de la organización.

Los cortafuegos pueden ser implementados en hardware, software o una combinación de ambos.

**Todo** el tráfico que entra o salga de la red pasa a través del cortafuegos, que lo examina y bloquea aquél tráfico que no cumple los criterios de seguridad especificados en la política. Un cortafuegos en el perímetro no es suficiente, es conveniente combinarlo con otros sistemas como los detectores de intrusos (IDS/IPS) o los dispositivos de gestión unificada de amenazas (UTM)

## Políticas de acceso en cortafuegos

Hay dos políticas básicas en la configuración de un cortafuegos:

- **Política restrictiva:** Se deniega todo el tráfico excepto el que está explícitamente permitido. Por tanto hay que habilitar expresamente el tráfico de los servicios que se necesiten.
- **Política permisiva:** Se permite todo el tráfico excepto el que esté explícitamente denegado. Cada servicio potencialmente peligroso necesitará ser aislado básicamente caso por caso, mientras que el resto del tráfico no será filtrado

La restrictiva es la más segura, ya que es más difícil permitir por error tráfico potencialmente peligroso pero a la vez es la que más problemas y más carga administrativa puede exigir al administrador. La política permisiva es menos segura ya que es posible que no se haya contemplado algún caso de tráfico peligroso y sea permitido por omisión.

## Tipos de cortafuegos

- **Cortafuegos personales:** son cortafuegos generalmente software que se instalan en una máquina con el fin de protegerla a ella exclusivamente. Son típicos en entornos domésticos y también en entornos empresariales, sobre todo en los servidores ubicados en la DMZ, para "endurecer" todavía más su seguridad. Un ejemplo es el firewall que viene de serie con los sistemas Windows y también iptables en los sistemas GNU/Linux. También hay firewalls de terceros como Zone Alarm o Comodo Pro.
- **Cortafuegos perimetrales:** Son los cortafuegos más habituales en entornos empresariales. Se ubican en el perímetro de la red, esto es, la frontera entre la red interna y la red externa o Internet. Es muy común instalar cortafuegos hardware o dedicados como los ASA o PIX de Cisco Systems, aunque también se usan mucho los cortafuegos por software. Por razones de seguridad, es conveniente que sean equipos dedicados para esa función y con un S.O. propietario que no sea muy conocido para evitar vulnerabilidades de los S.O. más extendidos.

En función de la **capa del modelo OSI** en que actúan pueden ser:

- De **filtrado de paquetes:** También llamados cortafuegos sin estado, filtran el tráfico mirando únicamente direcciones ip de origen y destino, puertos TCP/UDP origen y destino o protocolo usado, pero sin llevar un seguimiento de conexiones o si forman parte de una secuencia anterior (estado). Funcionan a nivel de red y transporte (capas 3 y 4 del modelo OSI) como filtro de paquetes IP. A menudo en este tipo de cortafuegos se permiten filtrados según campos de nivel de enlace de datos como la dirección MAC.
- De **aplicación:** También llamados pasarelas de nivel de aplicación (ALG, Application Level Gateway) o proxys de aplicación. Actúan sobre la capa de aplicación del modelo OSI. Entienden las aplicaciones y protocolos para los que están diseñados (por ejemplo: FTP, DNS o HTTP) y permiten detectar si un protocolo no deseado se coló a través de un puerto no estándar o si se está abusando de un protocolo de forma perjudicial. Ejemplo: si una organización quiere bloquear el tráfico web relacionado con una palabra en concreto, puede habilitarse el filtrado de contenido para bloquear esa palabra en particular. Es mucho más seguro y fiable cuando se compara con un cortafuegos de filtrado de paquetes, ya que repercute en las siete capas del modelo de referencia OSI, aunque también es más lento. Un ejemplo de cortafuegos de aplicación es ISA Server o Forefront TMG de Microsoft.
- De **estado:** Este tipo de cortafuegos permite llevar un seguimiento de cada paquete individual y asignarlo a una sesión o conexión previa. Esta tecnología se conoce generalmente como la inspección de estado de paquetes, ya que mantiene registros de todas las conexiones que pasan por el cortafuegos, siendo capaz de determinar si un paquete indica el inicio de una nueva conexión, es parte de una conexión existente, o es un paquete erróneo. también se conoce como seguimiento de conexiones (connection tracking). Este tipo de cortafuegos puede ayudar a prevenir ataques contra conexiones en curso o ciertos ataques de denegación de servicio. Iptables/Netfilter es un ejemplo de cortafuegos de estado

En este vídeo de Intrypedia puede aprender más sobre los cortafuegos y otros dispositivos como los UTM:

<https://youtu.be/sxg1nq17Xj4>

## Cortafuegos de Windows











Todos los sistemas operativos de Microsoft más recientes, incluyen de serie una aplicación cortafuegos que además viene activada de serie. Uno de los principales problemas que presenta, es que no permite las solicitudes de echo entrante (ping), lo cual muchas veces presta a confusión porque parece que la máquina no funcione en la red cuando no responde al ping, sobretodo en prácticas de redes. Lo que no se recomienda nunca es deshabilitar el firewall, sino cambiar su configuración para permitir que funcione el ping hacia la máquina, como se indica más abajo.

Los siguientes enlaces, muestran algunas funciones interesantes del firewall de Windows, como por ejemplo activar o desactivarlo (sólo se recomienda si se va a usar otro firewall de terceros) o bloquear todo el tráfico entrante cuando estamos en redes inseguras, como redes wifi.

[Entendiendo las opciones del cortafuegos de Windows](#)

[Configuración del firewall con seguridad avanzada](#)

Una situación habitual que se presenta es dejar el firewall activado y permitir que funcione el ping (ICMP) de entrada. Para ellos hay que abrir firewall de Windows con seguridad avanzada (escribiendo "firewall" desde Inicio -> Buscar programas y archivos) y en reglas entrantes, habilitar las reglas que afectan al protocolo ICMP entrante tanto en IPv4 como en IPv6 si se desea, y en los tres perfiles dominio, privado y público. Los perfiles definen el tipo de red a la que estamos conectados (dominio, privado y público)

Reglas de entrada				
Nombre	Grupo	Perfil	Habilitado	
 Servicio de captura de SNMP (UDP de entrada)	Captura SNMP	Dominio	No	
 Archivos e impresoras compartidos (petición eco: ICMPv4 de entrada)	Compartir archivos e impresoras	Privado	Sí	
 Archivos e impresoras compartidos (petición eco: ICMPv4 de entrada)	Compartir archivos e impresoras	Público	Sí	
 Archivos e impresoras compartidos (petición eco: ICMPv4 de entrada)	Compartir archivos e impresoras	Dominio	Sí	
 Archivos e impresoras compartidos (petición eco: ICMPv6 de entrada)	Compartir archivos e impresoras	Dominio	Sí	
 Archivos e impresoras compartidos (petición eco: ICMPv6 de entrada)	Compartir archivos e impresoras	Público	Sí	
 Archivos e impresoras compartidos (petición eco: ICMPv6 de entrada)	Compartir archivos e impresoras	Privado	Sí	
 Compartir archivos e impresoras (datagrama NB de entrada)	Compartir archivos e impresoras	Privado	Sí	
 Compartir archivos e impresoras (datagrama NB de entrada)	Compartir archivos e impresoras	Dominio	No	
 Compartir archivos e impresoras (datagrama NB de entrada)	Compartir archivos e impresoras	Público	No	



## 6. Seguridad en redes inalámbricas y redes privadas virtuales

### 6.1. Seguridad en redes inalámbricas

Las redes inalámbricas se utilizan cada vez más actualmente, superando ya en uso a las cableadas. Eso es debido a la reducción de costes que supone no necesitar una infraestructura de cable y por la movilidad que permite a los usuarios desplazarse por una organización con sus portátiles o dispositivos móviles como smartphones o tabletas.

Todos los ataques que se han explicado anteriormente en el curso, son igualmente válidos en la redes wifi. Sin embargo, las redes inalámbricas presentan nuevos vectores de ataque que no existen en las redes cableadas y que aparecen por el mero hecho de que los datos circulan libremente por el aire, pudiendo ser escuchados por cualquiera.

Además de los problemas típicos de falta de cobertura, interferencia con puntos de acceso (AP) cercanos en el mismo canal o presencia de inhibidores de frecuencia, están los problemas de seguridad en el acceso y que se estudiarán en este punto.



La redes wifi mejoran la movilidad y los costes de las redes cableadas pero a costa de la seguridad

#### 6.1.1. Mecanismos de cifrado en redes wifi

##### WEP

**Wired Equivalent Privacy** fue el primer mecanismo de protección wifi, que como todo el mundo ya sabe a estas alturas, es completamente inseguro y se desaconseja su utilización en cualquier entorno.

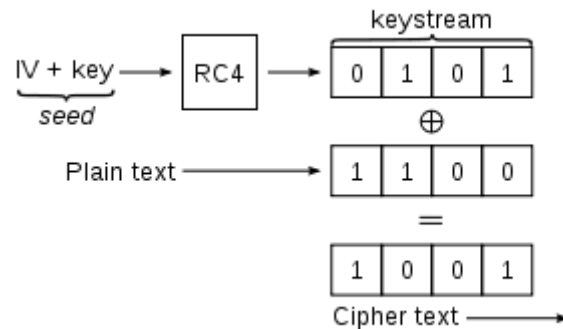
Algunas de sus características son:

- Utiliza una contraseña estática compartida de 40 o 104 bits que se combina con 24 bits del vector de inicialización IV.
- Algunos fabricantes amplían la clave, y en algunos casos el IV también, a una longitud de 128 o 232 bits (se llamó WEP2), pero no aporta una mejora real a la seguridad.
- Usa el algoritmo de cifrado de flujo (stream cipher) RC4.
- A través de la clave WEP más el IV, se genera un keystream que se combina con la trama usando una XOR bit a bit, produciendo la trama cifrada.
- No numera las tramas por tanto es vulnerable a ataques de replay (reinyectar la misma trama muchas veces en la red), así es que con inyección de paquetes se obtiene clave WEP en pocos minutos.

La principal debilidad de WEP es usar RC4 con claves estáticas que no cambian, a pesar de usar los IV. Mediante un ataque estadístico con criptoanálisis, herramientas como **aircrack-ng** pueden romper una clave WEP inyectando y capturando tráfico durante pocos minutos.

Previo a la creación del estándar 802.11i que incluye a WPA como protocolo de acceso, se desarrolló una variante de WEP llamado **WEP dinámico**, que sentó las bases de lo que sería WPA con sus claves dinámicas que cambian cada pocos minutos. En WEP dinámico, cada dispositivo usa dos claves: una de asignación y una predeterminada. La de asignación protege las tramas unidifusión. La clave predeterminada es compartida por todos los clientes para proteger las tramas de difusión y multidifusión.

Además de los conocidos ataques de replay contra WEP, existen programas como WlanDecrypter que pueden descubrir la clave WEP de redes con SSID tipo WLAN\_XX generando un diccionario breve de posibles combinaciones.



#### Esquema de funcionamiento de WEP con el algoritmo RC4

El mecanismo de **asociación en WEP** funciona en dos modos:

##### Modo "open":

- No existe autenticación, configuración por defecto en los puntos de acceso
- Cualquier dispositivo wifi puede asociarse
- Para descifrar y generar tráfico válido, se necesita la clave

##### Modo "shared":

- Existe autenticación y se necesita la clave WEP para asociarse
- Paradójicamente es más inseguro que el método open
- El handshake (tramas que se usan para asociarse entre AP y dispositivo) se puede capturar y descifrar la clave fácilmente

## WPA

**WPA** es el estándar de cifrado recomendado en las redes actuales y a ser posible en su versión WPA2. WPA y WPA2 surgen para mejorar la baja seguridad de WEP. WPA surgió primero como solución temporal. Algunas de sus características son:

- más económico que WPA2
- no necesita actualizar el hardware (router y tarjeta)
- vectores de inicialización mayores que WEP (48 bits)
- números de secuencia en cada trama
- integridad en tramas MIC (MICHAEL)
- utiliza claves dinámicas RC4 que van cambiando (TKIP)

**WPA2** mejora sustancialmente a WPA en lo siguiente:

- soporta completamente la norma 802.11i
- utiliza el cifrado simétrico AES (CCMP) mucho más robusto que RC4 y que necesita más potencia de cálculo
- puede usar TKIP pero se recomienda AES



- necesita actualización hardware del equipamiento. Los routers o dispositivos más viejos sólo soportan WEP y WPA pero no WPA2 con AES
- tiene el modo personal (PSK o clave precompartida) y enterprise (EAP/802.1X con servidor RADIUS)

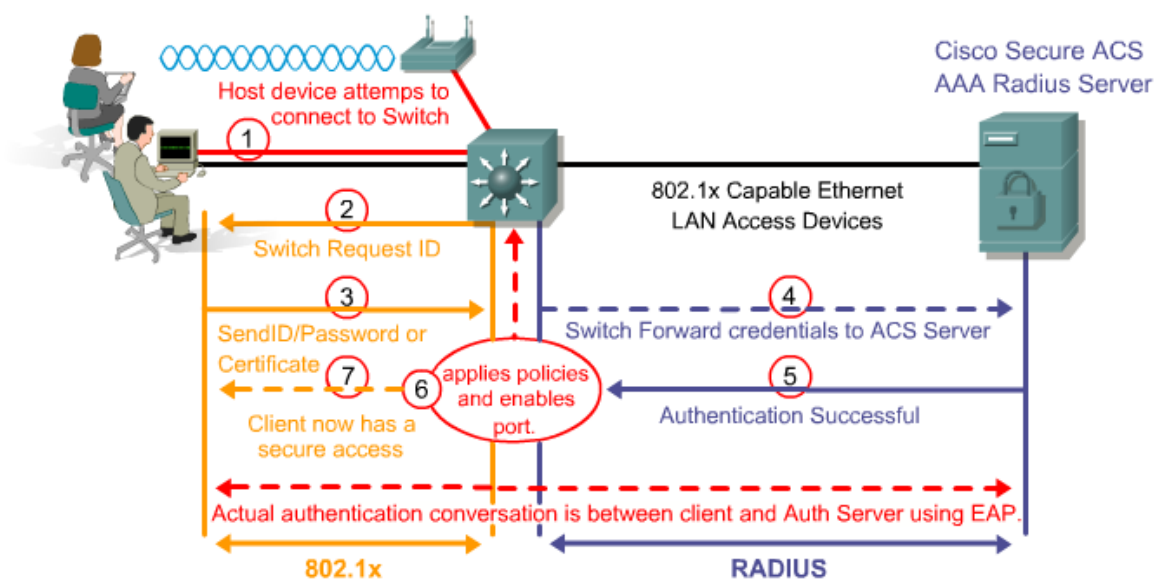
Sin embargo, WPA2 si se configura inadecuadamente, también es vulnerable a ataques:

- **Contraseña maestra WPA/WPA2 débil:** si la contraseña elegida para WPA no es robusta, puede romperse con diccionarios o fuerza bruta. Tan sólo hay que capturar el handshake (protocolo de asociación de un cliente wifi a la red) e intentar averiguar la contraseña con alguno de estos métodos.
- **Configuraciones por defecto:** si no cambiamos la contraseña WPA y el nombre de la wifi que viene por defecto en el router de un proveedor de Internet, se puede obtener la clave WPA si el router del fabricante con muchas de las aplicaciones que hay disponibles por Internet, incluso para móviles. Esto es debido a que algunos fabricantes implementan algoritmos de generación de la contraseña por defecto que son débiles y sencillos de adivinar mediante ingeniería inversa, a partir de los valores del BSSID (MAC del AP), nombre de la wifi y contraseña por defecto.
- **WPS** (Wi-Fi protected setup): este sistema permite configurar clientes wifi de forma sencilla para gente no iniciada, con tan solo estar cerca del punto de acceso mediante mecanismos como NFC, USB, pulsando un botón en el router o introduciendo un PIN. El uso del pin es bastante habitual, pero existen vulnerabilidades en muchos routers y puntos de acceso inalámbricos de fabricantes en los que si está habilitada esta característica y aunque la contraseña maestra WPA sea realmente compleja, es posible averiguar el PIN de WPS en unas pocas horas (son 8 dígitos separados en dos bloques de 4). Si se averigua el PIN, se puede transferir la configuración de la red al cliente a través de este protocolo.

¿Qué es WPS y porqué debes deshabilitarlo?

## WPA Enterprise

Utilizar WPA/WPA2 con claves precompartidas (PSK) es una buena solución para escenarios con pocos usuarios, como en un domicilio particular. Pero cuando estamos en una organización con cientos de usuarios potenciales la solución más robusta es usar un sistema con WPA Enterprise con un servidor de autenticación [RADIUS](#). De esta manera cada usuario del sistema accede con su usuario y contraseña único e intransferible, en vez de una contraseña compartida para todos que finalmente todo el mundo intercambia y es conocida por todos disminuyendo la seguridad de la red al poder conectarse cualquiera.



**Esquema de un sistema Wi-Fi Enterprise con WPA + 802.1x + RADIUS**

Existen muchos tutoriales en Internet que explican cómo montar un servidor RADIUS con **freeradius** y una base de datos de usuarios LDAP o Active Directory, donde se almacenan todos los usuarios del sistema.

### 6.1.2. Ataques a redes wifi

A los ataques a redes cableadas que ya estudiamos en unidades previas, a las redes inalámbricas se le unen otros tipos de ataques. Podemos hacer una clasificación como la siguiente:

#### **Ataques usados en redes cableadas**

Funcionan en las redes inalámbricas, exactamente igual que en redes cableadas:

- MITM (con ARP, con ICMP Redirection, con DHCP o DNS Spoofing, etc)
- DHCP Starvation, Rogue DHCP
- DNS Spoofing, etc

#### **Ataques de acceso**

Serían los que atacan al sistema de acceso o asociación al AP, como por ejemplo:

- Asociación falsa
- Inyección de paquetes
- Fuerza bruta
- Ingeniería inversa
- Ataque WPS

#### **Ataques de denegación de servicio**

Serían los que atentan contra el funcionamiento y la disponibilidad de la red wifi:

- Interferencias electromagnéticas (vecinos, microondas, bluetooth, teléfonos DECT, etc)
- Inhibidores
- Desasociación de cliente

#### **Ataques a los propios clientes**

Serían los que atacan a los dispositivos wifi:

- Interferencias electromagnéticas (vecinos, microondas, bluetooth, teléfonos DECT, etc)
- Desasociación de clientes
- Puntos de acceso falsos (Rogue/Fake AP, Evil Twin)

### Ataques de acceso

Como se ha citado previamente, serían los que intentan romper al sistema de acceso o asociación al AP, intentado descubrir las credenciales de acceso. A continuación se cita brevemente las características más destacables de ellos:

#### **Ataque arpreplay**

- Ataque de acceso contra WEP
- Necesita asociación con el AP
- Se utiliza en combinación con airodump-ng y aircrack-ng
- Captura un paquete ARP, y lo reinyecta miles de veces para provocar que el AP genere más vectores de inicialización (IV)

## Ataque de fragmentación

- Ataque de acceso contra WEP
- Obtiene el PRGA xor (hasta 1500 bytes)
- El PRGA o keystream es el XOR del texto plano y cifrado que se usa para cifrar en RC4
- Ejemplo: 0011 (texto plano)+0110 (texto cifrado)=0101 (PRGA)
- Con el xor, se genera un paquete ARP con packetforge-ng y se reinyecta
- Requiere al menos un paquete de datos del AP
- Si funciona, es uno de los más rápidos

## Ataque chopchop

- Se usa cuando no hay clientes asociados
- Su objetivo es obtener el PRGA xor, como el ataque anterior
- Se genera un paquete ARP con packetforge-ng y se reinyecta
- Algunos AP's no son vulnerables
- Más lento que el ataque de fragmentación

## Ataque WEP por diccionario

- Se descifra la clave mediante fuerza bruta
- La clave es la combinación del BSSID y de XX
- Hace falta capturar un IV al menos
- Se utiliza la herramienta wlandecryption
- Una vez capturado el IV, el ataque se hace con :

```
aireplay-ng --w <diccionario> <fichero.cap>
```

## Ataque WPA por diccionario

- Se descifra la clave mediante fuerza bruta
- Hace falta al menos un cliente conectado
- Es necesario capturar el handshake entre cliente y AP
- Muchas veces no es inmediato capturarlo, hay que estar cerca del cliente y el AP
- En Internet existen enormes ficheros de diccionario (de varias decenas o centenas de gigas) con las combinaciones de los SSID más habituales y permutaciones de contraseñas
- Una vez capturado, el ataque se hace con :

```
aireplay-ng -a 2 -w <diccionario> <fichero.cap>
```

## Ingeniería inversa contra WPA

- Es un ataque contra punto de acceso vulnerables de distintos operadores
- Se descubre mediante ingeniería inversa el algoritmo de generación de claves por defecto de sus routers, que normalmente involucra la MAC (BSSID) y el nombre (SSID)
- Afecta a muchos tipos de SSID como WLAN\_XXXX, JAZZTEL\_XXXX, ONOXXXX, etc.

## Ataque WPS

Como ya se indicó en el punto 1.1, este sistema permite configurar clientes wifi de forma sencilla para gente no iniciada, con tan solo estar cerca del punto de acceso mediante mecanismos como NFC, USB, pulsando un botón en el router o introduciendo un PIN. El uso del pin es bastante habitual, pero existen vulnerabilidades en muchos routers y puntos de acceso inalámbricos de fabricantes en los que si está habilitada esta característica y aunque la contraseña maestra WPA sea realmente compleja, es posible averiguar el PIN de WPS en unas pocas horas (son 8 dígitos separados en dos bloques de 4). Si se averigua el PIN, se puede transferir la configuración de la red al cliente a través de este protocolo. Un ejemplo es la aplicación **Reaver-WPS** o **WPS Pin Generator** (disponible para móviles)

[Vulnerabilidad en WPS permite ataques de fuerza bruta en routers WiFi](#)

## Ataques DoS

Algunos ejemplos de ataques de denegación de servicio (DoS), ya sean intencionados o no, serían:

### Interferencias electromagnéticas

Pueden ocasionar interferencia a nuestra wifi:

- bluetooth
- hornos microondas
- teléfonos DECT
- inhibidores de frecuencia
- AP de vecinos en nuestro mismo canal

Pueden ser intencionadas con un emisor de Wifi en el mismo canal o accidentales por AP adyacentes en nuestro canal, por ello se recomienda usar la banda 5 GHz en 802.11n o 802.11ac si lo permite nuestro AP y tarjetas (que no sean 802.11n lite, pues trabajan en 2,4 Ghz)

### Desasociación de clientes

En estos ataques se fuerza continuamente a que un cliente se desasocie del AP inutilizando su conexión. El atacante se hace pasar por el AP, enviando paquetes de desasociación, por ejemplo usando la herramienta arpreplay-ng: `aireplay-ng --deauth`

## Ataques a clientes

### Desasociación de clientes

Además de ser un ataque DoS, la desasociación de clientes tiene más usos. Uno de ellos es forzar a que el cliente se vuelva a asociar enviando en claro el nombre del red (SSID, ESSID) en la trama de asociación que puede ser capturada por el atacante revelando el nombre de una wifi oculta.

La otra funcionalidad es obligar a que el cliente realice de nuevo el handshake WPA para asociarse al AP, para de esta manera una vez capturado y guardado, realizar un ataque de diccionario o fuerza bruta. Como ya se ha citado, en Internet existen enormes ficheros a modo de tablas rainbow (no son exactamente tablas rainbow, pero les llaman así en muchos sitios) con las combinaciones de contraseñas o SSID ya con su hash precalculado para de esta forma atacar más rápido. Si además se combina con el lenguaje CUDA de las potentes GPU, el tiempo se reduce considerablemente.

Por ello es importante no solo cambiar la contraseña por defecto WPA por una con al menos 20 caracteres alfanuméricos, sino también cambiar el nombre de la red (SSID).

### Puntos de acceso falsos

También conocido como **Rogue AP**, **Fake AP** o **Evil Twin**, consiste en instalar un punto de acceso falso cerca del cliente al que queremos atacando, simulando una de sus redes preferidas abiertas que aparece en su PNL (Preferred Network List). De esta manera el cliente podría conectarse de forma automática y el atacante situarse en medio de sus comunicaciones pudiendo interceptar sus comunicaciones.

Muchos puntos de acceso profesionales llevan **detección de Rogue AP** funcionando como detectores de intrusos inalámbricos (WDS).

Insights		Rogue Access Points					Page Size 10
Search		Last Seen 7 days					
↕ Name/SSID	↕ BSSID	↕ Channel	↕ Type	↕ Manufacturer	↕ Location	↕ Last Seen	
<hidden>	00:02:cf:b7:e1:7e	11 (ng)	encrypted	ZygateCo	near SA (salon actos)	2014/05/05 11:09:14	
AndroidAP1275	1c:66:aa:3e:22:de	6 (ng)	encrypted	SamsungE	near TO (taller optica)	2014/04/30 20:04:33	
HTC Portable Hotspot 8FBA	50:2e:5c:d7:5b:36	6 (ng)	encrypted		near TO (taller optica)	2014/05/02 17:01:00	
Lenovo A850	6e:5f:1c:60:0f:ac	1 (ng)	encrypted		near SA (salon actos)	2014/05/03 23:29:59	
ONOCASA	c4:3d:c7:3f:15:af	11 (ng)	encrypted	Netgear	near 2B (aula 2B4)	2014/05/05 08:33:25	
ONO6A05	04:a1:51:06:6a:05	1 (ng)	encrypted	Netgear	near SA (salon actos)	2014/05/05 11:09:41	
vodafoneCFDC	72:6b:d3:6e:cf:dc	4 (ng)	encrypted		near SA (salon actos)	2014/05/04 15:33:09	
Orange-3CA5	88:03:55:89:3c:a7	1 (ng)	encrypted	Arcadyan	near SA (salon actos)	2014/05/03 10:53:44	
VodafoneDB8C	74:31:70:f0:db:8c	1 (ng)	encrypted	Arcadyan	near SA (salon actos)	2014/05/05 05:26:57	
ONOE679	5c:35:3b:52:f5:49	1 (ng)	encrypted	CompalBr	near SA (salon actos)	2014/05/05 11:09:43	
21 - 30 / 90							

### Detector de puntos de acceso falsos del fabricante Ubiquity

Aunque este tipo de ataque es fácil realizarlo con un AP y un portátil con las herramientas necesarias, existen a la venta dispositivos para realizar este tipo de ataques de forma muy sencilla, como por ejemplo el **Pineapple**.

## 6.1.3. Mecanismos de protección

### Falsas medidas de seguridad

Cuando se habla de seguridad en redes inalámbricas, muchas veces se dan algunas recomendaciones que en absoluto mejoran la seguridad y producen al usuario una falsa sensación de protección ante acceso no autorizados. Conviene pues, conocerlas para que no perdamos el tiempo en aplicarlas. Estas falsas medidas son:

- **Utilizar WEP** como sistema de cifrado: WEP es el primer sistema que se implantó para dotar de protección a las redes wifi y actualmente es posible romper cualquier red wifi protegida con WEP en cuestión de pocos minutos, con técnicas como la inyección de paquetes, el modo monitor para capturar tramas y una herramienta de criptoanálisis como **aircrack-ng** o **wepcrack**. Todas estas herramientas se encuentran disponibles en Internet e incluso hay asistentes en algunas distribuciones de auditoría que permiten hacer el proceso sin ser experto. WEP utiliza un algoritmo de cifrado llamado RC4 cuya implementación para redes wifi está rota desde hace muchos años. Por tanto, no se recomienda su uso.
- **Usar filtrado de MAC** en el AP: muchos puntos de acceso y routers inalámbricos tienen la opción de sólo permitir el acceso a la red wifi a determinados dispositivos usando la dirección física MAC de su tarjeta de red. Es muy fácil ver las direcciones MAC asociadas a un punto de acceso con software de monitorización como **airodump-ng** y cambiar la MAC de la tarjeta wifi del atacante desde cualquier sistema operativo. Por tanto, no se recomienda usar esta técnica porque es muy fácil saltársela con pocos conocimientos de redes.
- **Deshabilitar el anuncio de la red**, también como conocido como difusión o broadcast del **SSID** (Service Set Identifier): todos los puntos de acceso por defecto envían tramas "beacon" con el nombre de la wifi cada 100 milisegundos. De esta forma podemos ver las redes a nuestro alrededor. Si deshabilitamos esta función en el router, nadie puede ver el nombre de nuestra red y conectarse. Pero de nuevo, con herramientas como **airodump-ng** pueden verse las MAC asociadas a un AP dado (aparece su BSSID, que es la MAC del AP) y el nombre de la red aparece como **<hidden>** (oculto). Después, es fácil lanzar un ataque de **desautenticación** contra el cliente asociado haciéndose pasar por el AP, con lo que se fuerza a que el cliente vuelva a asociarse automáticamente y en este momento, el cliente envía el nombre de la wifi (SSID) en la trama de conexión, que es capturada por el atacante. Este proceso se hace en cuestión de pocos segundos.

```
Terminal
File Edit View Terminal Tabs Help

[02:34:54] Tested 627489 keys (got 55118 IVs)

KB    depth  byte(vote)
0     0/ 1     FC(78080) E7(66304) 5B(62976) A8(62720) 2A(62464)
1     0/ 1     81(72960) 45(64512) 3F(63744) 1C(62720) 3A(62208)
2     0/ 2     A2(66560) A6(66560) 0C(64768) E0(64256) ED(64256)
3     0/ 1     C8(79616) 3C(66816) B0(64000) D7(64000) 55(63488)
4     0/ 2     9B(65280) 4F(64256) 36(63232) 7D(63232) 7F(63232)
5     0/ 1     B3(76288) 50(66560) 13(66304) 3F(65280) 87(65280)
6     0/ 1     2E(72192) D4(64256) 8C(63744) 9B(63488) 0B(63232)
7     0/ 1     1A(72704) 6D(66304) 16(64768) 53(64768) D3(64768)
8     0/ 2     4A(68352) 7D(66816) 38(65536) 9D(65024) 96(64512)
9     0/ 1     14(68608) C8(64000) 09(63488) EF(63488) 47(62976)
10    0/ 1     50(67328) 59(67328) 0D(66304) B4(66048) EE(66048)
11    1/ 1     16(66048) 34(65280) BD(64256) D0(64256) 49(63488)
12    1/ 2     AA(64444) B9(63700) 36(63220) C7(62420) 1D(62368)

KEY FOUND! [ FC:81:A2:C8:9B:B3:2E:1A:00:14:C9:8F:AA ]
Decrypted correctly: 100%

[root@debian:koosha]#
```

*Imagen de aircrack-ng en acción rompiendo una clave WEP*

## Herramientas libres de auditoría

Todas las herramientas de auditoría wireless que se han comentado anteriormente, vienen de serie en muchas distribuciones GNU/Linux como Wifislax, Wifiway, nUbuntu, Backtrack o Kali Linux. De todas ellas cabe destacar **Kali Linux**, porque es la más actualizada y personalmente opino que es la mejor distribución para seguridad, con muchas herramientas de pentesting, inyección SQL, análisis de aplicaciones web, análisis forense, etc.

## Recomendaciones para Wi-Fi

A continuación, se citan las recomendaciones más destacables en materia de redes inalámbricas:

- **WPA PSK:** En caso de no querer aventurarse en montar un RADIUS con gestión centralizada de usuarios en LDAP, Samba, Active Directory, etc. se recomienda usar WPA2 con AES en la medida de lo posible y una clave compleja. Los expertos en seguridad han revelado que una clave PSK de 20 caracteres alfanuméricos se podría romper por fuerza bruta usando toda la capacidad de cómputo del planeta en una media de unos 100 años. Las vulnerabilidades de WPA vienen por usar contraseñas débiles, por no cambiar la contraseña ni el nombre de la wifi por defecto o por tener activo WPS. En cualquier caso, no recomiendo WPA PSK en una empresa con cientos de usuarios porque al final, esa contraseña es conocida por todos, incluso por gente ajena a la empresa, por tanto es como no tener contraseña. Si hay algún ataque, no es posible identificar al usuario porque es la misma contraseña para todos.
- **WPA Enterprise:** Ya se han comentado las ventajas de este sistema. El problema es la curva de aprendizaje necesaria para gente no experimentada y que es más complejo de administrar un RADIUS o un LDAP/Active Directory.
- **No conectarse a redes abiertas** bajo ningún concepto ni montar soluciones como portales cautivos abiertos. En las redes wifi abiertas puede conectarse cualquiera que disponga de las herramientas necesarias para hacer ataques MITM (las hay incluso apps para móviles como dSploit, zAnti, Wifikill, etc). Los portales cautivos como los de los hoteles, aeropuertos, cafeterías, etc. que muestran una página web de identificación una vez nos conectamos (portal cautivo) son extremadamente fáciles de saltar con los conocimientos adecuados, a no ser que protejan con algún sistema como claves WPA. Por tanto, no se recomienda la instalación de un portal cautivo abierto con autenticación web pues es fácil atacar el sistema y a los usuarios, así como evitar la autenticación.

- **Eliminar las redes abiertas de la lista de redes preferidas**, de esta forma, al borrarlas de la lista de nuestro dispositivo, un atacante cerca de nosotros no puede averiguar las redes abiertas a las que nos hemos conectado y crear una red que se llame igual. A esta técnica se le conoce como Rogue AP o Evil Twin. De esta forma nuestro dispositivo se conectaría automáticamente y el atacante podría espiar nuestras comunicaciones.
- **Deshabilitar WPS**, por las razones expuestas anteriormente. Existen herramientas como **reaver**, que permite atacar este protocolo.
- **Cambiar contraseñas** WPA y nombre de la red **por defecto**.

Para finalizar, puedes ver las recomendaciones de seguridad de este vídeo de Intypedia, en la línea de las que se han comentado aquí: <https://youtu.be/rhJAJ1TdNyg>

## Mecanismos de protección adicionales (modo paranoico)

A continuación se citan algunas medidas que pueden ser recomendables, si bien se pierde algo de funcionalidad en muchas ocasiones al activarlas:

- Deshabilitar DHCP en el router o punto de acceso wifi
- Limitar número de clientes asociados
- Modificar la potencia y direccionalidad de la señal (cambiar antena o usar antena windsurfer)
- Aislar comunicación entre clientes
- Instalar un firewall en el perímetro entre red cableada e inalámbrica
- Utilizar entradas ARP estáticas

## 6.2. Redes privadas virtuales

### Red privada virtual

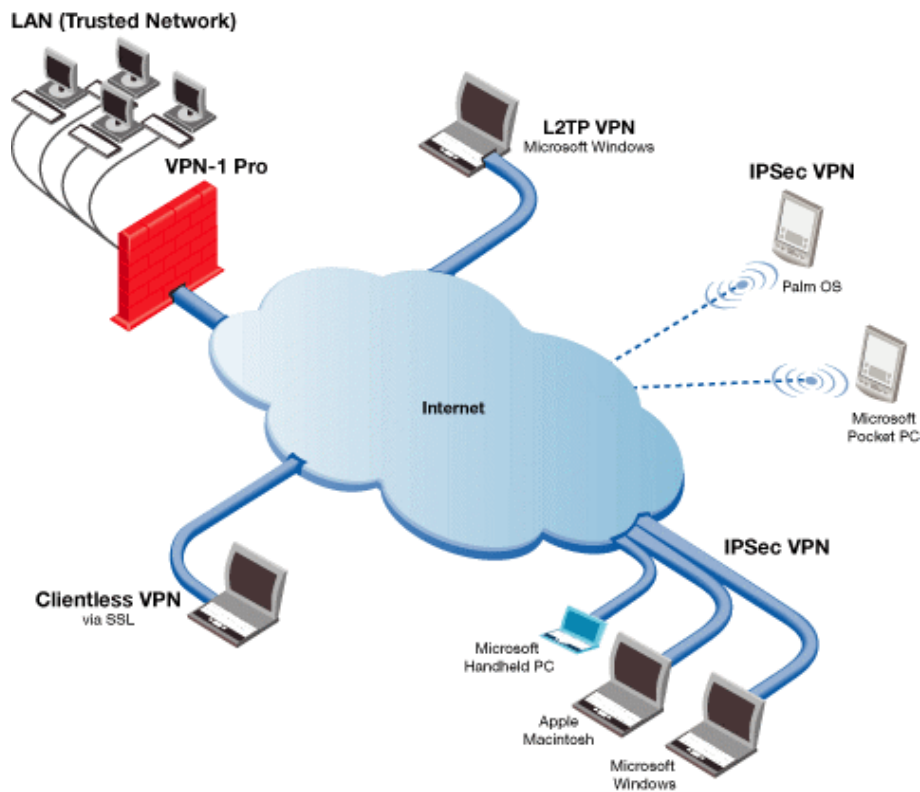
Una **red privada virtual** (VPN, Virtual Private Network) es una red privada que se configura sobre una red física subyacente, generalmente de ámbito público e insegura.

Aunque en la mayoría de los escenarios, una VPN se implanta sobre una red pública insegura, en algunos casos puede hacerse sobre una red privada que carece de las garantías suficientes para proporcionar una comunicación segura.

El principal objetivo de una VPN es **proporcionar seguridad**, garantizando la confidencialidad e integridad de las comunicaciones, pero en ocasiones una VPN se establece para lograr una comunicación entre dos extremos que de otra manera no sería posible y no tiene que utilizar cifrado obligatoriamente.

El uso más común es conectar dos o más redes LAN remotas a través de una red pública e insegura como es Internet. Pero hace años, cuando WPA se estaba desarrollando, era habitual usar VPN sobre una red wifi privada para proporcionarle la seguridad de la que carece WEP.





**Diferentes tecnologías de VPN**

Es importante hacer la distinción entre **Red Privada** y **Red Privada Virtual**: la primera utiliza líneas alquiladas para formar toda la Red Privada. La VPN lo que hace es crear un túnel entre los dos puntos a conectar utilizando infraestructura pública.

Tampoco debe confundirse con las **VLAN** (Red Local Virtual). Una VLAN se configura en una red local de una organización para separar los usuarios en subredes por función o departamento y no utiliza técnicas de túneles ni una red pública para comunicarse, por tanto, es una forma de crear segmentos de red virtuales

### Ventajas de las VPN

Las VPN presentan algunas claras ventajas frente a otras opciones como las líneas dedicadas. Algunas de ellas son:

- Seguridad
- Bajo coste económico frente a las líneas dedicadas
- Fácil escalabilidad cuando la red necesita crecer
- Movilidad de los clientes de la VPN
- Existen muchas tecnologías disponibles, tanto libres como propietarias

### Desventajas de las VPN

Sin embargo, no todo son ventajas. Las VPN presentan algunos problemas como los siguientes:

- Los derivados de las red pública subyacente como:
  - Calidad de servicio
  - Latencias
  - Pérdida de paquetes
  - Desconexiones
- Sobrecarga por encapsulación
- Sobrecarga por cifrado
- Interoperatividad entre nodos diferentes

## 7. Alta disponibilidad en redes

### 7.1. Alta disponibilidad

La **disponibilidad de la información** es uno de los servicios que brinda la seguridad de la información, y garantiza que la información está accesible a los usuarios autorizados siempre que lo requieran. La alta disponibilidad se enmarca dentro de las medidas de la **seguridad pasiva**. Es decir, son medidas correctoras, que no pretenden evitar un incidente o un fallo en el sistema, pero sí recuperar el sistema de forma que no haya una parada de los servicios.

Todos sabemos que hay ciertos sucesos que no podemos evitar, como el fallo de un disco por el desgaste, pero podemos conseguir que el sistema sea tolerante a fallos si tenemos implementado algunos de los niveles RAID que proporcionan redundancia de datos.

En este apartado se pretende hacer una introducción al mundo de la alta disponibilidad.

#### Alta disponibilidad

Por **alta disponibilidad** entendemos los procesos o técnicas para garantizar un grado muy alto de continuidad operacional en un sistema de información durante un tiempo de medición dado.

Para que un sistema se considere de alta disponibilidad debe estar funcionando sin interrupciones durante un alto porcentaje del tiempo, como por ejemplo el **99,99%** del tiempo o incluso el **99,999%**. Esto es lo que se conoce como a regla de los **cuatro nueves** o los **cinco nueves** respectivamente.

En la regla de los cuatro nueves (99,99%) implica una parada de 0,01% del año, que son 52,6 minutos al año

En la regla de los cinco nueves (99,999%) implica una parada de 0,001% del año, que son 5,26 minutos al año, la décima parte del caso anterior

Hay que indicar que no debe confundirse el tiempo de funcionamiento de un sistema, con su disponibilidad. Un sistema puede estar funcionando y no ser disponible, por tanto a la hora de realizar mediciones de disponibilidad, hay que comprobar que el sistema o el servicio se comportan adecuadamente. Un ejemplo sería un servidor de una aplicación web que está funcionando, pero temporalmente se ha perdido la conexión a la base de datos por un error en el gestor de base de datos. En ese caso, si comprobamos que el servidor web está escuchando en el puerto 80 solamente, no estamos haciendo bien la medición.

### 7.2. Redundancia y tolerancia a fallos

#### 7.2.1. Redundancia

La alta disponibilidad generalmente se consigue mediante la **redundancia** de elementos del sistema informático, como servidores, fuentes de alimentación, RAID, sistema eléctrico, red de datos, etc.

La redundancia consiste en **duplicar** las veces que sean necesarias, los componentes de un sistema informático para proporcionar alta disponibilidad y como mecanismo de seguridad pasiva que permite recuperar al sistema del fallo de un componente. Por tanto no basta con redundar, sino configurar el sistema para que sea **tolerante a fallos** y que pueda recuperarse ante el fallo de un elemento del sistema informático.



### ***Redundancia en un servicio que permite recuperar el sistema ante un fallo***

El **grado** de redundancia de un sistema, dependerá de su importancia y del dinero que perdamos cuando el sistema no está disponible por un fallo. A mayor redundancia en todos los niveles, más disponibilidad pero mayor **coste**. No merecerá la pena invertir en redundancia, si la inversión necesaria para tener un sistema redundante cuesta más de lo que perderíamos en dinero, reputación y horas de trabajo, si el sistema fallara. Los fallos siempre pueden ocurrir, pero existen técnicas y configuraciones para tener sistemas redundantes tolerantes a fallos y que puedan seguir funcionando a pesar de un fallo.

Los **fallos de un sistema informático** pueden ocurrir:

- En el propio servidor
- En el software
- En los discos
- En las fuentes de alimentación
- En las tarjetas de red
- En la infraestructura:
  - electrónica de red
  - acceso a internet
  - sistema eléctrico, etc.

En este sentido, podemos aplicar técnicas de redundancia en distintas partes del sistema, como por ejemplo:

### **Redundancia en los componentes**

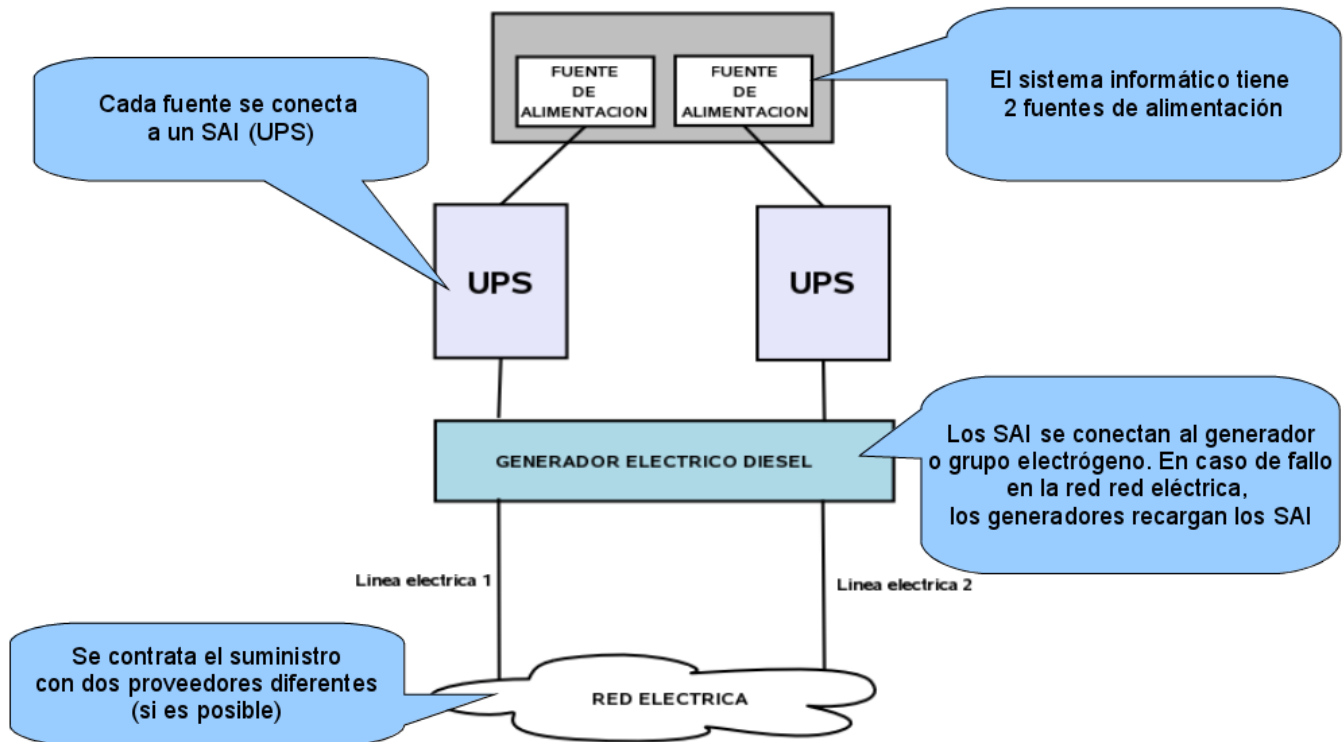
- Almacenamiento:
  - Sistemas DAS RAID por hardware o software
  - Sistemas RAID por red (p.ej. software DRBD)
  - Redes SAN con almacenamiento centralizado y/o virtualizado
- Tarjetas de red: varias tarjetas o una tarjeta multipuerto funcionando en alta disponibilidad (activo/pasivo) o bien con balanceo (Etherchannel, LACP, etc.)
- Fuentes de alimentación redundantes

## Redundancia en el suministro eléctrico

En este caso, se suele contratar el suministro con dos proveedores, aunque en muchas zonas de España es sólo una empresa la distribuidora por lo tanto no existe esa posibilidad de redundancia real.

Otra técnica son las fuentes de alimentación redundantes, en que cada fuente se conecta a una línea de alimentación diferente en los centros de datos. Estas fuentes además se suelen poder cambiar en caliente (hotswap).

Además de estas técnicas, están los grupos electrógenos, baterías y SAI/UPS, ya estudiados en el curso.



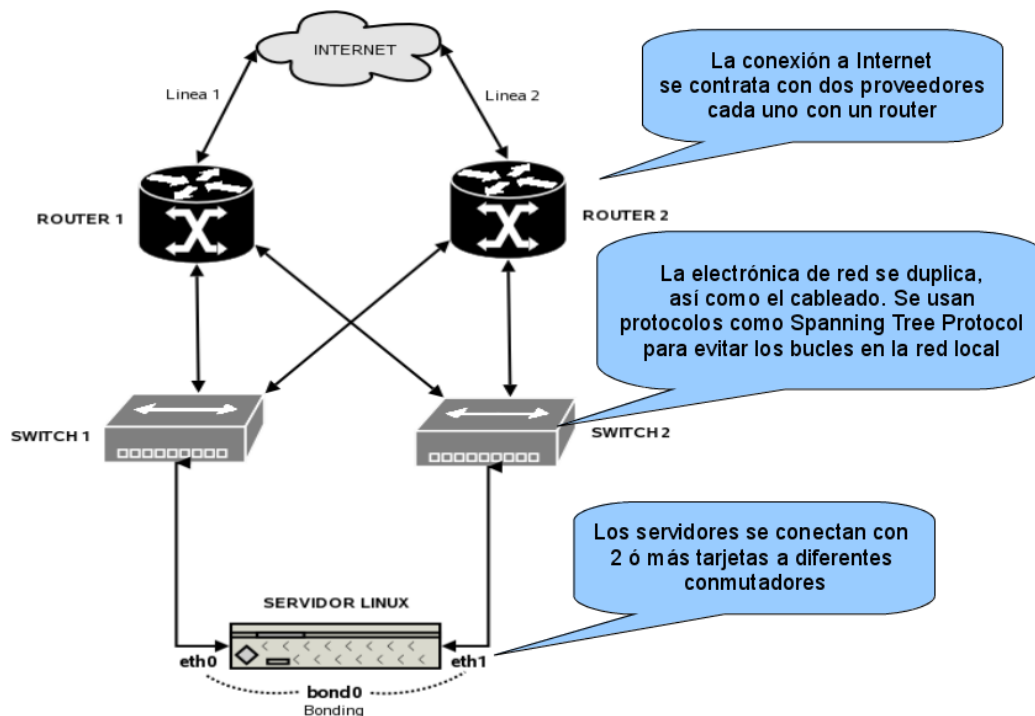
## **Esquema de un suministro eléctrico redundando en un centro de datos**

### Redundancia en la red de datos

En la infraestructura de red, se duplican la electrónica de red:

- Routers
- Conmutadores
- Cableado de la LAN
- Líneas de conexión WAN (Internet, red corporativa, etc.)

Aunque tengamos redundancia en los componentes de servidor y en el suministro eléctrico, un conmutador o switch pueden ser un punto de fallo en la red, por ello es necesario duplicar los elementos críticos.



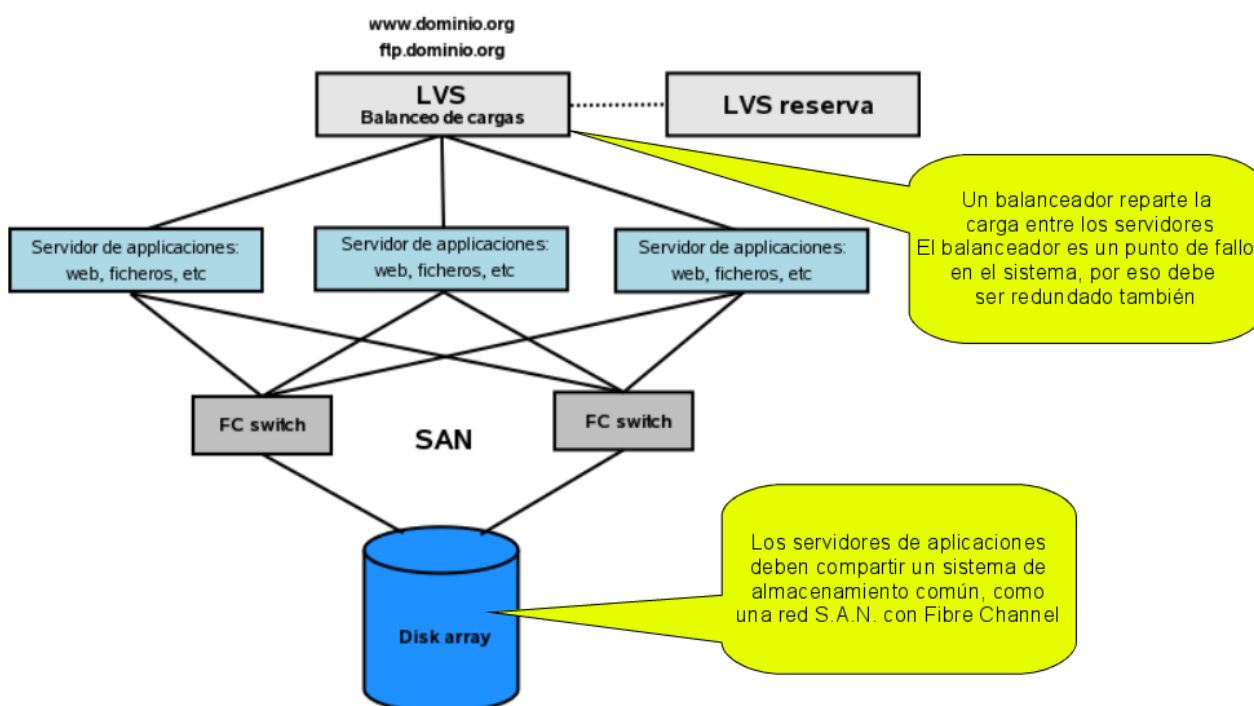
*Esquema de redundancia en la red de datos*

### Redundancia en los servidores

Un servidor, aunque tenga sus componentes redundados, puede fallar completamente y constituye un único punto de fallo del sistema. Existen distintos tipos de configuraciones de redundancia y alta disponibilidad en servidores, como los **clusters** o las **granjas de servidores**, que se estudiarán más adelante.

Los **clusters** son un grupo de servidores que funcionan como uno sólo. Los servidores del cluster se denominan nodos y el cluster se puede administrar de forma única como si fuera un solo servidor.

Las **granjas** son un grupo de servidores que ofrecen generalmente uno o más servicios en alta disponibilidad con balanceo de carga. Un dispositivo llamado **balanceador**, reparte la carga de la aplicación entre los nodos de un cluster o una granja de servidores usando diferentes algoritmos de balanceo.



*Esquema de un balanceador en HA conectado a una granja de servidores*

## 7.2.2. Tolerancia a fallos

Las aplicaciones y servicios corporativos cada vez son más críticos y necesitan de sistemas tolerantes a fallos y con capacidad de recuperación.

La **tolerancia a fallos** es la capacidad que tiene un sistema para continuar funcionando correctamente, a pesar del fallo de alguno de sus elementos. Un concepto muy relacionado con la tolerancia a fallos es la **conmutación por error** o **failover**, que se produce cuando las funciones de un componente del sistema (CPU, servidor, disco, red, etc.) son asumidos por componentes secundarios del sistema cuando el componente principal no está disponible ya sea debido a un fallo o por un tiempo de inactividad programado. El failover obviamente debe producirse de forma **automática** por el sistema, y no de forma manual, y además avisar a los administradores de que se ha producido esta situación, pues en la mayoría de los casos, un segundo fallo podría dejar el sistema inutilizable.

Se definen tres conceptos muy importantes y que suelen verse en las especificaciones técnicas de los fabricantes y son el **MTTF**, **MTBF** y **MTTR**

### MTTF, MTBF y MTTR

**MTTF** (Mean Time To Failure) es el tiempo medio que se espera que el sistema funcione antes del **primer fallo**.

**MTBF** (Mean Time Between Failure) es el tiempo medio entre **dos averías consecutivas** del sistema.

**MTTR** (Mean Time To Repair) es el tiempo medio de **recuperación** de un sistema cuando ocurre un fallo.

A partir de la definición de estos tres parámetros, se define la disponibilidad como:

$$\text{Disponibilidad} = \text{MTTF} / (\text{MTTF} + \text{MTTR})$$

## 7.3. Sistemas de clusters

En los sistemas informáticos de misión crítica y/o de alto rendimiento es habitual configurar un **cluster** de servidores.

### Definición de cluster

Un **cluster** es un conjunto de computadores interconectados por una red de alta velocidad, a los que se les llama nodos y generalmente juntos en una zona geográfica, que funcionan como uno sólo, proporcionando tolerancia a fallos y alta disponibilidad.

Los nodos del cluster se **monitorizan** entre ellos detectando cuales están activos y cuales inactivos, exigiéndose un **quórum**, que es el número mínimo de nodos funcionando para que el cluster se considere activo. En caso de no alcanzarse el quórum, el cluster no arranca sus servicios. Un cluster tiene como mínimo dos nodos, pudiendo ser un número mucho más elevado en entornos críticos y de alto rendimiento.

### Imágenes de clusters



### Ejemplos reales de clusters

Algunos de ejemplos de clusters con un número elevado de nodos son:

- Cluster realizado en 2004 con 70 consolas PS2 con GNU/Linux en la Universidad de Illinois
- Cluster [Beowulf](#)
- Cluster del departamento de informática de la [universidad de Valencia](#) creado en 2008

### 7.3.1. Clasificación de los clusters

Atendiendo al **modo de funcionamiento** pueden ser de tipo:

- **activo/pasivo**: un nodo activo y el resto a la espera de un fallo del nodo activo
- **activo/activo**: todos los nodos en activo
- **combinación** de ambos, es decir, determinados nodos en activo y el resto esperando

También pueden clasificarse atendiendo a su **objetivo**, en clusters de:

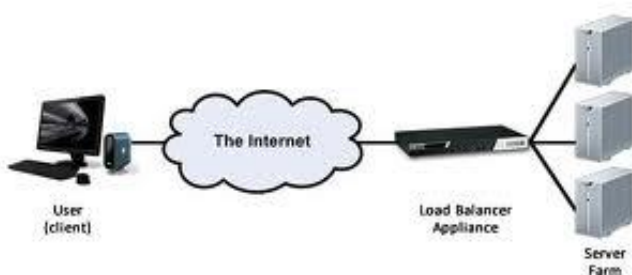
- **Alto rendimiento** (HP, High Performance), para tareas de mucha capacidad computacional durante poco tiempo. Generalmente los nodos del cluster ejecutan un software en paralelo. Se miden en FLOPS (operaciones de coma flotante/seg).
- **Alta eficiencia** (HT, High Throughput), para realizar tareas independientes de mucha carga computacional durante períodos largos de tiempo como meses o años. Ej: grid computing, proyecto SETI. Se miden en tareas completadas por tiempo.
- **Alta disponibilidad** (HA, High Availability), para entornos críticos que requieran una disponibilidad elevada independientemente del rendimiento o eficiencia. Aquí entrarían también los balanceadores de carga.

Los clusters pueden ser de distintos **niveles**, destacando los siguientes:

- A nivel de **aplicación o servicio**: la misma aplicación o servicio instalado en todos los nodos del cluster funciona en alta disponibilidad. P.ej: Oracle RAC, SQL Server, Web Sphere, Apache Hadoop, etc.
- A nivel de **sistema operativo**: todo el sistema operativo (y no determinado servicio o aplicación) funciona en modo cluster. Son los más complejos de configurar.

### 7.4. Balanceadores de carga

Los **balanceadores de carga** (SLB, Server Load Balancer) se usan en un tipo especial de cluster, que son las **granjas de servidores**. El balanceador (generalmente dos balanceadores en alta disponibilidad) recibe las peticiones de un servicio a una **IP virtual de servicio** (VIP) y mediante un algoritmo de balanceo, decide a qué servidor pasar la petición para que la procese.

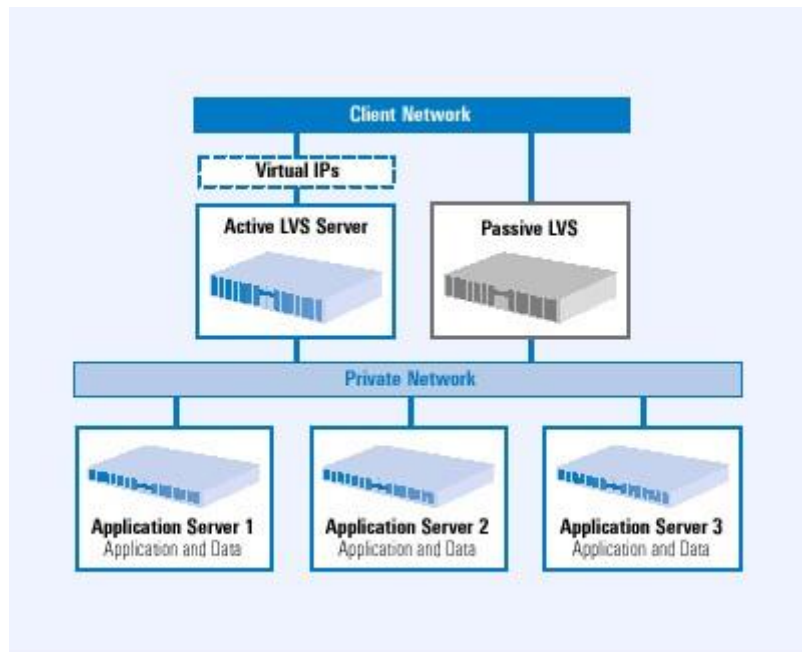


#### Esquema de un SLB conectado a una granja de servidores

El balanceador o balanceadores, que se conectan con los servidores con una red generalmente privada, va repartiendo la carga entre los distintos nodos de la granja de servidores en función del algoritmo de balanceo y del estado de los mismos.

Para que el SLB no sea un **punto de fallo único** en el sistema, se configuran generalmente dos SLB mediante el protocolo **VRRP** para tener la VIP del servicio del balanceador en alta disponibilidad, si el SLB principal cae. El protocolo VRRP es un protocolo de redundancia para enrutadores, y que estudiaremos en la siguiente sección.





*Esquema de un cluster de balanceadores en activo/pasivo*

### 7.4.1. Algoritmos de balanceo

Algunos de los algoritmos más usados en los SLB son:

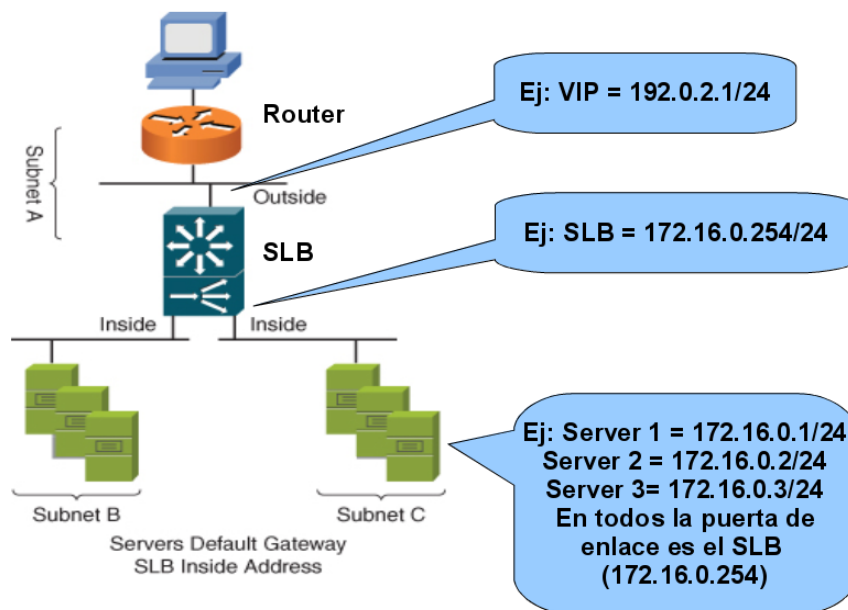
- **RR** (Round Robin): distribuye de forma circular enviando cada petición al siguiente servidor, hasta volver a repetir el ciclo: servidor 1, 2, 3, 1, 2, 3, 1, 2, 3, etc
- **WRR** (Round Robin ponderado): donde hay nodos que reciben más peticiones en función de su peso. Los servidores con igual peso reciben el mismo número de peticiones
- **LC** (Least Connection): más peticiones a servidores con menos peticiones actuales
- **WLC** (Weighted Least Connection): es como el LC, pero asignando un peso a cada servidor. Asigna más peticiones a servidores con menos trabajos y relativo al peso del servidor
- **LL** (Least Load): más peticiones a servidores con menor carga actual
- **DH** (Destination Hashing): se hace un hash de destino, de forma que para determinada url siempre se envía la petición al mismo servidor
- **SH** (Source Hashing): se hace un hash de origen de forma que para determinado cliente, siempre se le asocia el mismo servidor
- **SED** (Shortest Expected Delay): se asigna la petición al servidor con el menor retardo esperado
- **NQ** (Never Queue): se asigna la petición al primer servidor libre que haya, en vez de esperar al más rápido. Si todos están ocupados, usa el SED

### 7.4.2. Topologías o modos de balanceo

A la hora de desplegar una granja de servidores con balanceadores de carga, hay diferentes modos o topologías de interconexión del balanceador con los nodos de la granja. Algunos ejemplos son:

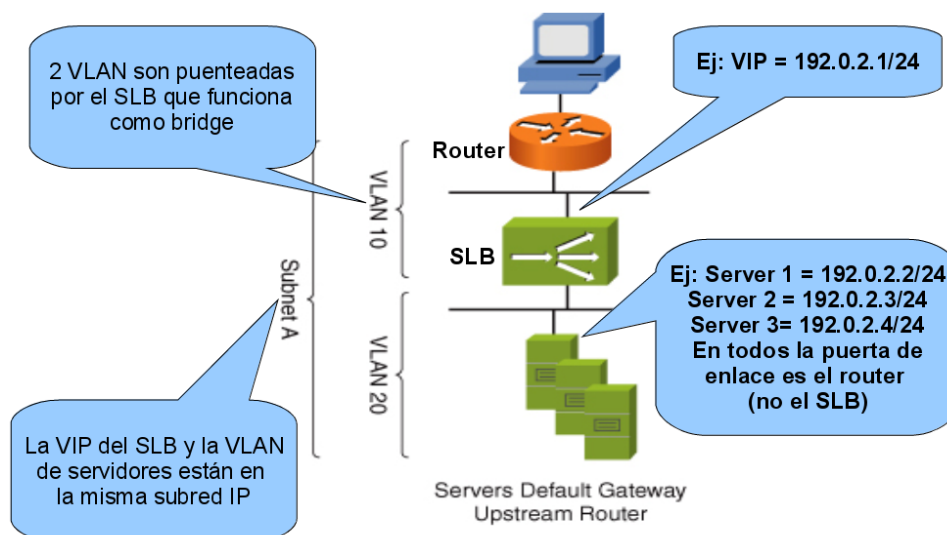
## Router mode

En el modo enrutado, el balanceador o SLB se comporta como un router, enrutando entre la VIP pública del servicio y la red interna de los servidores. La VIP del servicio está en una subred **diferente** a la subred de los servidores. En la siguiente figura se puede apreciar este modo:



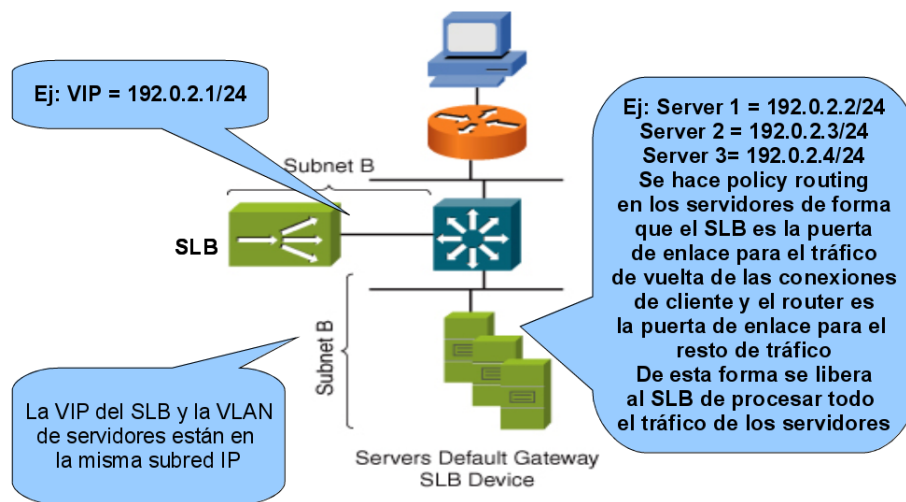
## Bridge mode

El el modo puente también llamado **inline**, el SLB funciona en modo transparente haciendo funciones de puente y su VIP está en la misma subred que los servidores. El SLB se encuentra físicamente en el camino entre el cliente y el servidor. En la siguiente figura se aprecia este modo:



### One-armed o two-armed mode

En el modo one o two-armed, también conocido como **offline**, el SLB no se encuentra físicamente en el camino entre el cliente y el servidor, de forma que el servidor puede saltarse el SLB para otros servicios como la administración remota de los servidores, transferencia de archivos, etc. descargando de esta manera al SLB de ese tráfico. Si el SLB hace de puente es one-armed y si hace de router es two-armed. La siguiente figura muestra este modo:



## 7.5. Redundancia en enrutadores

La redundancia en enrutadores permite que la puerta de enlace de una red se configure en alta disponibilidad, de forma que si un router cae, el servicio se garantiza. Estos sistemas funcionan mediante dos o más routers que comparten una **IP virtual (VIP)** que es la que configuran los clientes como **puerta de enlace**. Estos sistemas también se aplican para los balanceadores en alta disponibilidad.

El servicio puede ser **activo/pasivo**, donde sólo un router funciona y el resto espera, o bien **activo/activo** donde todos los routers funcionan a la vez balanceando la carga de los usuarios de la LAN.

Los fabricantes de routers y balanceadores, pueden usar diferentes protocolos de redundancia, pero los más habituales son:

### HSRP y VRRP

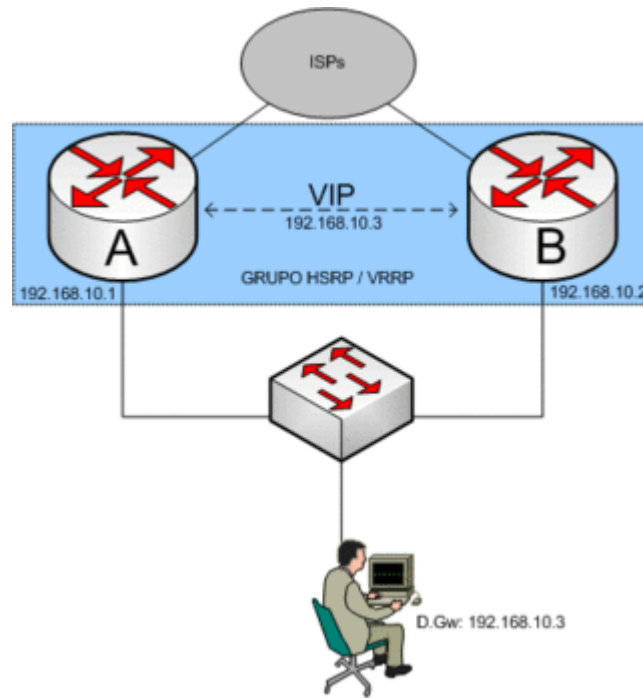
**HSRP** (Hot Standby Router Protocol) es un protocolo propietario de **Cisco Systems** que funciona únicamente entre los routers y conmutadores de nivel 3 de esta marca. Este protocolo evita la existencia de puntos de fallo únicos en la red mediante técnicas de redundancia y comprobación del estado de los routers.

Este protocolo funciona eligiendo un router **maestro** dentro del cluster, siendo el resto routers de **backup**. El router maestro es el router con la **prioridad más alta** configurada por el administrador de la red.

En caso de un fallo en el router maestro o alguna de sus interfaces configuradas, el router maestro baja su prioridad y el router de backup con mayor prioridad asume la VIP y pasa a ser la puerta de enlace de la red local.

**VRRP** (Virtual Router Redundancy Protocol) es un protocolo **estándar** creado a partir de HSRP y funciona de manera muy similar. Al ser un estándar funciona en la mayoría de routers y sistemas operativos como GNU/Linux.

En la siguiente figura se puede ver un esquema del funcionamiento de HSRP/VRRP:

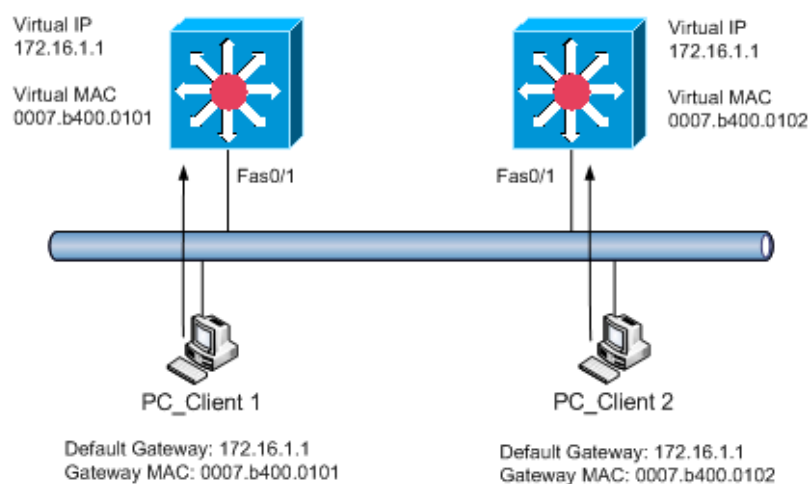


## GLBP

**GLBP** (Gateway Load Balancing Protocol) es un protocolo propietario de **Cisco Systems** que funciona únicamente entre los routers y conmutadores de nivel 3 de esta marca. Este protocolo también evita la existencia de puntos de fallo únicos en la red mediante técnicas de redundancia y comprobación del estado de los routers como hace HSRP, pero su principal diferencia es que trabaja en modo **activo/activo**, balanceando la carga entre todos los routers del cluster.

En este protocolo, todos los routers usan una MAC virtual, además de su MAC real. En un cluster, se elige un AVG (Active Virtual Gateway) como el router principal. Él es el responsable de contestar a las peticiones ARP de los clientes, para obtener la MAC del router. Cada vez, el AVG responde con la MAC virtual de cada uno de los routers (AVF, Active Virtual Forwarder) incluyéndose a sí mismo. De esta manera se produce un balanceo a nivel de puerta de enlace porque cada cliente usará un router diferente.

En la siguiente figura se muestra el esquema de funcionamiento:



## 8. Bibliografía

- ONRUBIA, R. (2018). Curso Seguridad Informática. Cefire.