

## Módulo 13. Introducción á Seguridade Informática

A [seguridade informática](#) é a disciplina da Ciencia Informática que se ocupa de definir e deseñar o conxunto de medidas destinadas a [protexer](#), tanto os [equipos informáticos](#) como a [información](#) contida neles.

Estas medidas están compostas polas diferentes normas, procedementos, políticas, protocolos, técnicas, métodos e ferramentas, que están encamiñadas a protexer hardware, software, información e persoas ante calquera tipo de ameaza.

Se non podes visualizar o seguinte vídeo, fai clic na ligazón [Conceptos Básicos sobre la Seguridad de la Información](#).

### Sistema de Información e Sistema Informático

Aínda que no momento actual é moi difícil imaxinar calquera actividade humana na que non se utilice un sistema informático, primeiramente, debemos definir qué se entende, conceptualmente por:

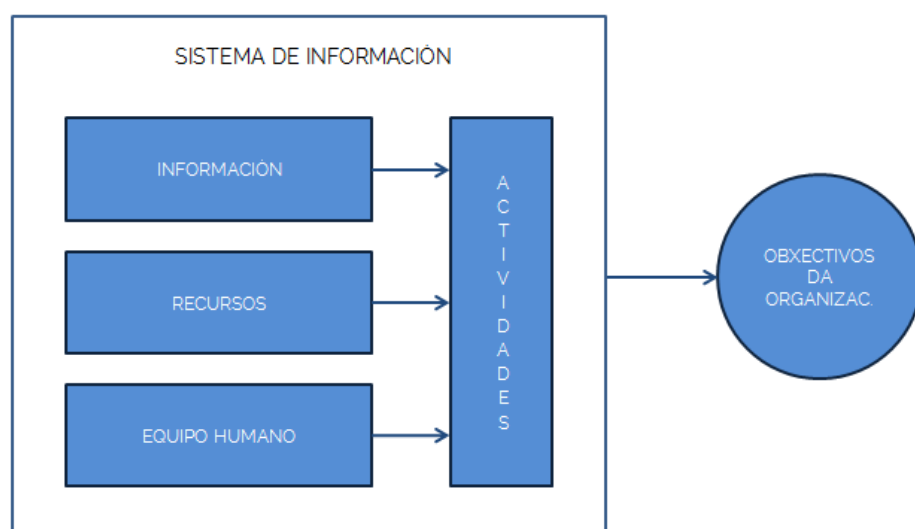
- Sistema de Información e
- Sistema Informático.

### Sistema de Información

Un [sistema de información](#) é un conxunto de elementos organizados, relacionados e coordinados entre sí, encargados de facilitar o funcionamento global dunha organización.

Estes elementos son:

- [Recursos](#): poden ser físicos (ex. un archivador, un ordenador...), e lóxicos (ex. normas, software...).
- [Equipo humano](#): as diferentes persoas que traballan nunha organización.
- [Información](#): conxunto de datos organizados que teñen un significado e importancia para a organización, os cales poden estar contidos en calquera tipo de soporte (papel, bases de datos ordenadores...).
- [Actividades](#) ou [procesos](#): que se realizan na organización, relacionadas ou non coa informática.

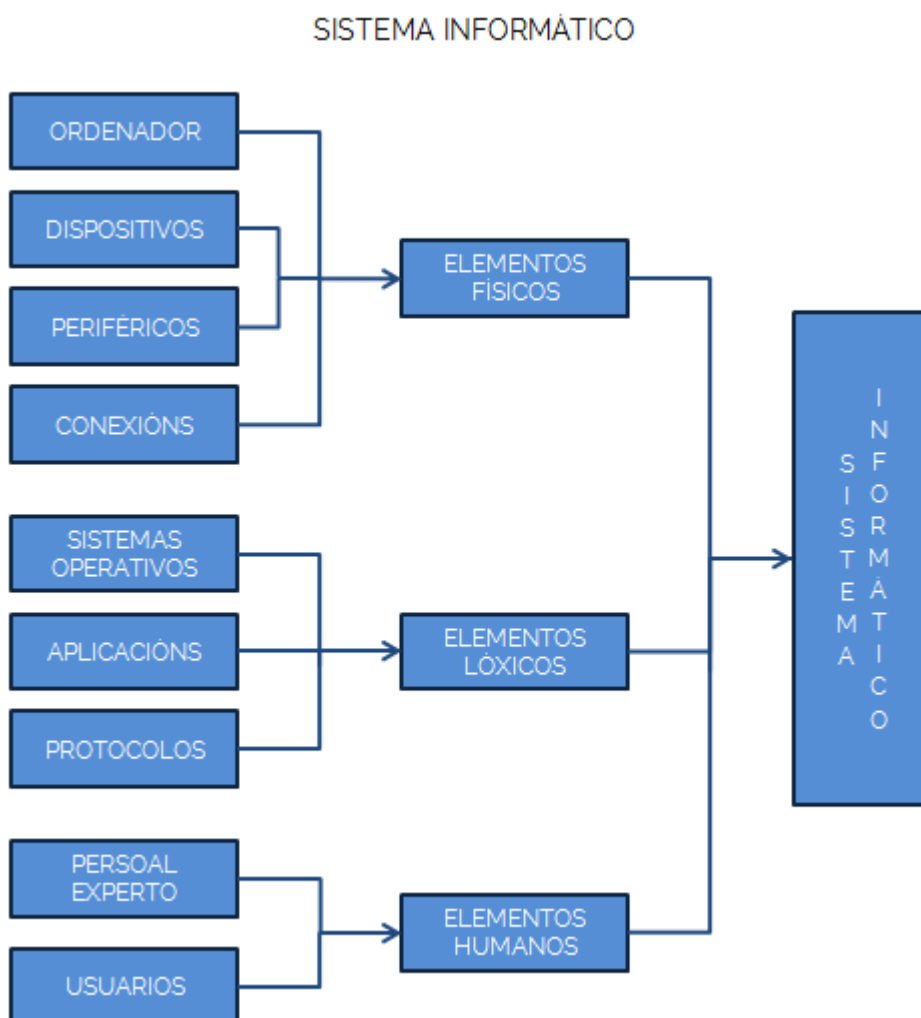


Vexamos como flúe a información na nosa empresa, dende que un cliente entra no noso local, ata que sae del (con ou sen o produto ou servizo desexado). Vai xerarse un movemento de información, por exemplo pedido do cliente; o vendedor xera o pedido e manda unha copia a almacén para ser servido (probablemente comproba que o cliente teña crédito); en almacén compróbase que exista en stock o produto e nese caso asígnallo ao pedido; elabórase un recibo que se achega ao pedido e se remite tamén a facturación; facturación xera a factura de acordo ás condicións de venta e por fin remata o proceso co envío ou a entrega no mesmo momento, segundo o caso.

Toda a información recolectada, elaborada, distribuída e almacenada (datos dos clientes, provedores, produtos vendidos, facturas), xunto cos procesos que manipulan esa información (comprobación de crédito, comprobación e asignación pedido, xenerar un pedido, enviar unha copia a almacén, etc.) conforman o **SISTEMA DE INFORMACIÓN** da empresa.

## Sistema Informático

Un **Sistema Informático** é un sistema constituído por un conxunto de hardware, software e persoal informático, que permite almacenar e procesar datos.



O **Hardware** inclúe:

- Ordenadores
- Calquera tipo de dispositivo informático

O **software** inclúe:

- [Sistema operativo](#),
  - [firmware](#) e
  - aplicacións informáticas
- [Personal informático](#) que inclúe:
- Persoal técnico que crean e manteñen o sistema (analistas, programadores, operadores...)
  - Usuarios que utilizan o sistema informático

Polo tanto podemos dicir que un [Sistema de Información Informático](#) é un subconxunto dos [Sistemas de Información](#) en xeral, aínda que hoxe en día nos resulte practicamente imposible pensar nun sistema de información no que o compoñente informático non sexa imprescindible, e por iso, estes dous termos se utilizan indistintamente cando na realidade **NON** son sinónimos.

## **Aproximación ao concepto de Seguridade**

Un [Sistema Informático nunca será totalmente seguro](#) e, por moitas medidas de seguridade que se apliquen, sempre se manterá un marxe de risco.

Para establecer un [sistema de seguridade fiable](#), deben coñecerse:

- Cales son os [elementos](#) que compoñen o sistema.
- Cales son os [perigos](#) que afectan ao sistema, accidentais ou provocados
- Cales son as [medidas](#) que se deberían adoptar para coñecer, previr, impedir, reducir ou controlar os riscos potenciais.

Tras o estudo dos riscos e a implantación de medidas, debe facerse un [seguimento periódico](#), revisando e actualizando as medidas adoptadas.

Todos os elementos que participan nun sistema de información poden verse afectados por fallos de seguridade, pero é a [información](#) o [recurso máis vulnerable e valioso](#). O hardware pode ser comprado de novo, o software, tamén reinstalado, pero a información danada ou roubada non é recuperable, o que pode ocasionar danos importantes sobre a organización, non só económicos, tamén sobre a imaxe da organización e mesmo, prexudicar a persoas.

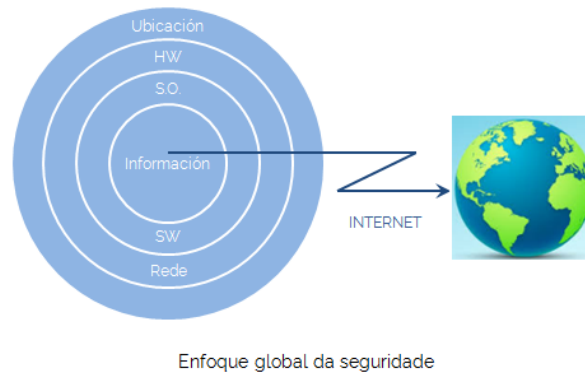
É importante ter en conta que a [maioría das fallas de seguridade se deben ao factor humano](#).

## **Enfoque global da seguridade**

A información é o núcleo de todo sistema de información. Para protexer as súas propiedades de integridade, dispoñibilidade e confidencialidade é necesario ter en conta os niveis que a envolven para poder dotalos de mecanismos e servizos de seguridade.

Dende o exterior ata chegar á información, pódense definir estes niveis:

- A [ubicación física](#), edificio, planta ou estancias, despacho ou oficina, por ser o lugar físico no que se atopan ubicados os demais niveis.
- [Hardware](#) e os compoñentes da rede que se atopan no interior do entorno físico, por conter, soportar e distribuír a información.
- O [sistema operativo](#) e todo o [software](#), para xestionar a información.
- A [conexión a internet](#), por ser a vía de contacto entre o sistema de información e o exterior.
- A [información](#).



## Tipos de seguridade: Activa e Pasiva

Inicialmente, debemos distinguir entre dous tipos de seguridade:

- Seguridade **Activa**: comprende o conxunto de defensas ou medidas que teñen coma obxectivo o reducir os riscos que ameazan ao sistema.  
Exemplos: impedir o acceso á información a aqueles usuarios non autorizados introducindo a política de utilización de nomes de usuario e contrasinais, evitar a entrada de virus instalando un antivirus, impedir a lectura non autorizada de mensaxes mediante a encriptación, etc.
- Seguridade **Pasiva**: Está formada polas medidas que se implantan unha vez producido o incidente de seguridade, minimizar a súa repercusión e facilitar a recuperación do sistema.  
Exemplo: manter ao día as copias de seguridade dos datos.

## Obxectivos

A **Seguridade Informática** ten que asegurar que os recursos dun sistema informático son utilizados da forma na que se determinou, e que o acceso á información que neles se contén, así como a súa modificación, e mesmo borrado, unicamente pode ser realizada por aqueles usuarios que se atopen autorizados e, sempre, dentro dos límites da súa autorización.

Ademais, podemos identificar varios obxectivos:

- **Detectar** todos os posibles problemas e ameazas á seguridade, xestionando e minimizando os riscos.
- **Garantir** que os recursos físicos e lóxicos son utilizados para aquelas funcións que se determinaron.
- **Previr** un incidente de seguridade, física ou lóxica, minimizando os danos, limitando as perdas e, se é o caso, recuperando o sistema no menor tempo posible.
- **Cumprir** co marco normativo e legal vixente.

**SEGURIDADE INFORMÁTICA**  
**"O QUE NON ESTÁ PERMITIDO**  
**DEBE ESTAR PROHIBIDO"**

SISTEMA DE SEGURIDADE = **TECNOLOXÍA + ORGANIZACIÓN**



## Propiedades dun sistema informático seguro

Os danos producidos pola [falta de seguridade](#), poden causar responsabilidades de carácter [penal](#), [perdas económicas](#) e, moito máis importantes, de [credibilidade](#) e [prestixio](#) da organización.

A orixe destes danos pode ser:

- [Fortuíta](#): erros cometidos polos usuarios, accidentes, cortes de fluído eléctrico, avarías do sistema, catástrofes naturais, etc.
- [Fraudulenta](#): danos causados por software malicioso, intrusos, ou mesmo por algún membro do persoal con acceso ao sistema, roubo, accidentes provocados, etc.

### Integridade

Este [principio](#) garante a [autenticidade](#) e [precisión da información](#) sen importar o momento no que se solicita, é dicir, unha [garantía de que os datos non foron alterados nin destruídos de xeito non autorizado](#).

Para evitar este tipo de riscos, débese dotar ao sistema de mecanismos que preveñan e detecten o momento no que se produce unha falla de integridade, tratando de resolver os erros descubertos.

Por exemplo, se un usuario, interno ou externo á organización, accede e modifica certa información cando non debería ter acceso a esta, se di que viola a integridade da información.

### Confidencialidade

A [información](#) ou os datos estarán [unicamente ao alcance do coñecemento das persoas ou entidades autorizadas](#), nos momentos autorizados e cos métodos autorizados.

Para previr erros de [confidencialidade](#), debe ser deseñado un [control de accesos ao sistema](#), é dicir, quen pode acceder, a qué parte do sistema pode acceder, en qué momento pode acceder, e para realizar qué operacións pode acceder.

Imaxínade que ocorrería se facemos unha compra por Internet e os datos das nosas contas bancarias, o noso nome de usuario e contrasinal non navegasen encriptados e calquera puidera lelos sen problema?

### Dispoñibilidade

A información debe estar dispoñible para os usuarios cando estes a necesiten.

Esta [característica](#) está asociada á [fiabilidade técnica dos compoñentes do sistema informático](#).

Débense aplicar medidas que protexan a información, así como crear copias de seguridade e mecanismos para restaurar os datos que, ben accidental ou ben intencionadamente, se destruíron ou danaron.

Como resumo, podemos dicir que:

[SEGURIDADE INFORMÁTICA](#) é o conxunto de procedementos,  
estratexias e ferramentas que permiten garantir a  
[Integridade](#), [Confidencialidade](#) e [Dispoñibilidade](#) da Información.

### Análise de riscos

No momento de [dotar de seguridade a un sistema informático](#), debemos ter en conta:

- todos os [elementos que o compoñen](#),
- analizar o [nivel de vulnerabilidade](#) de cada un deles ante determinadas ameazas e
- valorar o [impacto que un ataque podería causar](#) en todo sistema,

E todo isto tendo sempre en conta as máximas de que [a cadea sempre rompe polo eslabón máis débil](#) e que este, soe ser o humano.

## Activos

### [Ocultar](#)

Son os [recursos](#) que pertencen ao propio sistema de información ou que están relacionados con este. A presenza dos activos facilita o funcionamento da organización e a consecución de seus obxectivos.

Ao estudar estes activos hai que ter en conta sempre as [interrelacións](#) que se manteñen entre eles e o seu grao de influencia, é dicir, cómo pode afectar a un activo o dano que se poda producir noutro.

Estes activos poden ser clasificados en:

- [Datos](#)
- [Software](#)
- [Hardware](#)
- [Redes](#)
- [Soportes](#)
- [Instalacións](#)
- [Persoal](#)
- [Servizos](#)

Mostramos a definición de cada un deles:

## Datos

### [Ocultar](#)

## Retroalimentación

- Constitúen o [núcleo de toda organización](#), de tal xeito que se considera que o [resto dos activos están ao servizo da protección deles](#). Os datos son o maior activo dunha organización, e o funcionamento e supervivencia desta depende, absolutamente, da súa correcta utilización.
- Xeralmente se atopan [organizados en bases de datos](#) e almacenados en soportes de diferente tipo, e poden clasificarse en diferentes categorías, económicas, fiscais, de recursos humanos, provedores, legais, etc.
- [Cada tipo de dato debe ter un estudo do risco propio](#), pola diferente repercusión que o seu deterioro ou perda poda causar, como por exemplo os que afectan á intimidade das persoas ou outros de carácter confidencial.

## Software

Está constituído polos [sistemas operativos](#) e o conxunto de [aplicacións](#) instaladas nos equipos dun sistema de información que reciben e xestionan, ou transforman, os datos para obter algún fin.

## Hardware

Trátase dos equipos, servidores e ordenadores que conteñen as aplicacións e permiten o seu funcionamento, á vez que almacenan os datos do sistema de información.

Tamén se incorporan neste grupo os diferentes periféricos e elementos accesorios que aseguran o correcto funcionamento do resto dos equipos ao servir de medio de transmisión dos datos, por exemplo os routers, cable módems, sistemas de alimentación ininterrumpida (SAI), cableado de datos, cableado eléctrico, etc.

### Redes

Comprende as diferentes vías de comunicación e transmisión de datos, dende as redes locais da organización, pasando polas metropolitanas ou mesmo internet.

### Soportes

Este grupo incorpora todos aqueles medios de almacenamento onde se alberga a información durante diferentes períodos de tempo, sexan estes dvd's, cd's, discos duros externos de almacenamento, dispositivos usb, etc.

### Instalacións

Os lugares que albergan aos sistemas. Normalmente trátase de oficinas, despachos, locais, edificios, ademais das posibles ubicacións móbiles coma poden ser vehículos, furgonetas, etc.

### Persoal

Nesta categoría debemos incorporar a todo o conxunto de persoas que interactúan co sistema de información independentemente do seu rol no mesmo.

É aquí onde se produce a maior cantidade de fallas de seguridade, non na tecnoloxía.

### Servizos

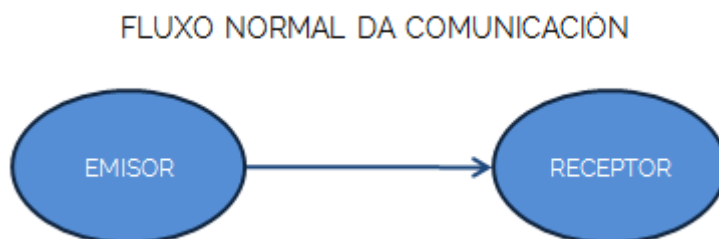
Calquera tipo de servizos que a organización presta aos clientes ou usuarios, teñen cabida neste apartado.

### Ameazas

Enténdese por ameaza, a presenza dun ou máis **factores** de diferente índole, por exemplo persoas, máquinas, procesos, etc, que, de ter a oportunidade, **atacarían** ao **sistema** aproveitando algunha vulnerabilidade e producindo danos.

Podémonos atopar con moitos tipos de ameaza, dende as físicas como interrupcións de enerxía eléctrica, fallas do hardware, riscos ambientais, ata os erros intencionados dalgún usuario, pasando pola introdución no sistema de software malicioso, virus, troianos, etc., ou mesmo o roubo, destrución ou modificación de información.

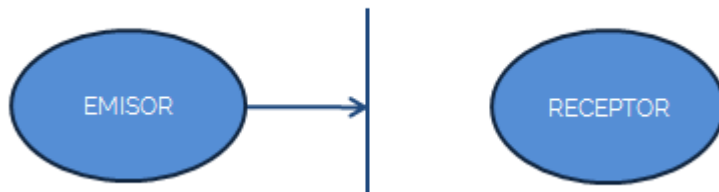
O **proceso de comunicación** mantén un fluxo como o que se mostra na seguinte figura:



Podemos categorizar as ameazas segundo diferentes criterios.

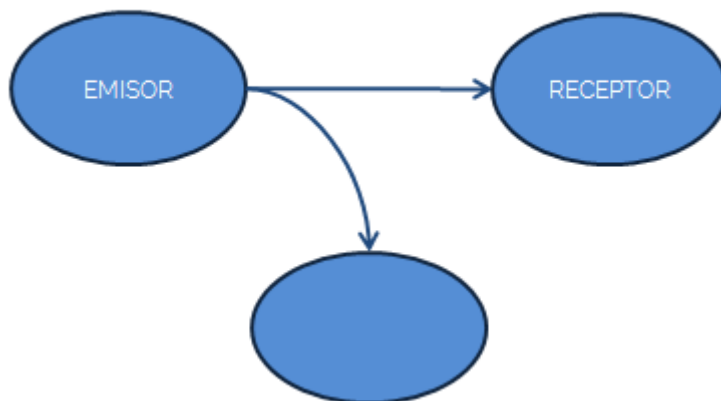
- Se temos en conta o **tipo de alteración**, **dano** ou **intervención** que poderían producir sobre a información. Distinguimos:
  - **De interrupción**  
O obxectivo desta ameaza é deshabilitar o acceso á información, por exemplo, destruindo compoñentes físicos como podería ser un disco duro, bloqueando o acceso aos datos ou mesmo cortando ou saturando as canles de comunicación.

#### INTERRUPCIÓN



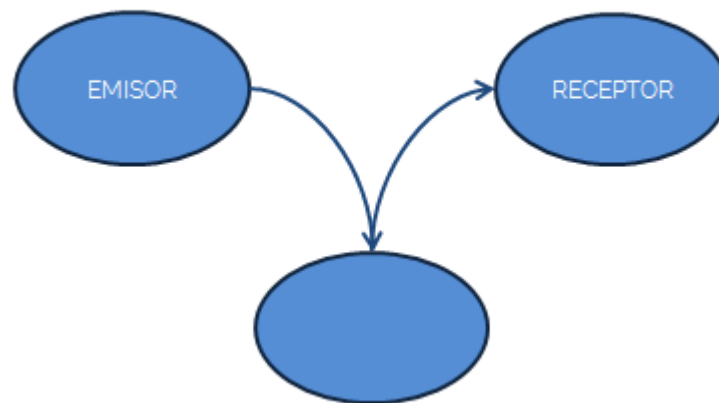
- **De interceptación**  
Persoas, programas ou equipos non autorizados poderían acceder a un determinado recurso do sistema e captar información confidencial, xa sexan datos, programas, identidades, etc.

#### INTERCEPTACIÓN



- **De modificación**  
De igual xeito que no caso anterior, persoas, programas ou equipos non autorizados, non soamente accederían aos programas e datos do sistema, senon que ademais, os modificarían. Por exemplo, modificar a resposta enviada a un usuario conectado, ou ben alterar o comportamento dunha aplicación instalada.

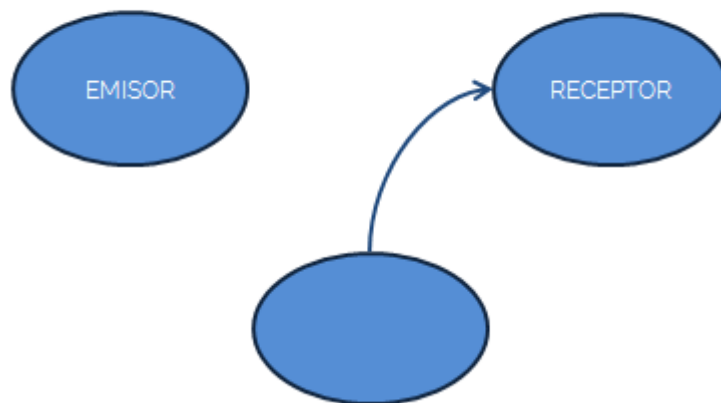
### MODIFICACIÓN



- **De creación ou fabricación**

Neste caso sería agregada certa información falsa no conxunto da información do sistema.

### CREACIÓN OU FABRICACIÓN



- Segundo a **orixe das ameazas**, estas se clasifican en:

- **Accidentais**

Onde se categorizan os accidentes meteorolóxicos, incendios, inundacións, fallas nos equipos, nas redes, nos sistemas operativos, no software, erros humanos, etc.

- **Intencionadas**

Son debidas sempre á acción humana, como pode tratarse da introdución de software malicioso, malware, aínda que penetre no sistema por algún procedemento automático, a intrusión informática que, xeralmente se inicia coa introdución de malware, etc.

Estas ameazas intencionadas poden ter a súa orixe tanto no exterior como no interior da organización.

## Vulnerabilidades

Unha **vulnerabilidade** é a **probabilidade de que unha ameaza se materialice contra un activo**.

Non todos os activos son vulnerables ás mesmas ameazas, por exemplo, os datos son vulnerables á acción dos hackers, mentres que unha instalación eléctrica é vulnerable a un cortocircuíto.

Recomendámosche tamén ver: [Corrixidas vulnerabilidades Drupal](#)

## Riscos

Un risco é a [probabilidade de que se materialice ou non unha ameaza aproveitando unha vulnerabilidade](#).

Non é un risco unha ameaza cando non hai vulnerabilidade, nin unha vulnerabilidade cando non existe ameaza.

Unha organización pode, [ante un determinado risco](#), optar por unha das [alternativas](#) seguintes:

- [Eliminalo](#), aplicando medidas
- [Transferilo](#), contratando un seguro, por exemplo.
- [Mitigalo](#), aplicando medidas.
- [Aceptalo](#) ou [asumilo](#), non facendo nada, por exemplo, cando o custe de aplicación das medidas supera ao de reparación do dano, ou ben cando o perxuício esperado non ten valor algún

## Ataques

Un [ataque](#) é unha [ameaza materializada](#).

En función do impacto causado nos activos, clasificaremos os ataques en:

- [Activos](#): se modifican, danan, suprimen ou agregan información, ou ben bloquean ou saturan as canles de comunicación.
- [Pasivos](#): cando se accede sen autorización aos datos contidos no sistema. Son os máis difíciles de detectar.

Un ataque tamén se pode clasificar como:

- [Directo](#): é producido dende o atacante directamente.
- [Indirecto](#): incorpora recursos ou persoas intermediarias.

## Impactos

A [consecuencia](#) da materialización [dunha ou varias ameazas](#) sobre un ou varios activos aproveitando as vulnerabilidades do sistema.

Non deixa de ser o [dano causado por un ataque](#).

Poden ser categorizados como:

- [Cuantitativos](#): se os perxuícios se poden cuantificar economicamente.
- [Cualitativos](#): supoñen danos non cuantificables, como poderían ser os causados contra os dereitos fundamentais das persoas.

## Control de riscos

Unha vez realizada a análise dos riscos, tense que determinar cales serán os servizos que necesitamos para conseguir un sistema seguro, co cal, para poder proporcionar eses servizos, debemos dotar ao sistema dos mecanismos correspondentes.

## Mecanismos de seguridade

Segundo a función que desenvolvan, os mecanismos de seguridade poden clasificarse en:

- **Preventivos**: actúan antes de que se produza o ataque, a súa misión é evitalo.
- **Detectores**: actúan cando o ataque se ten producido e antes de que cause danos no sistema.
- **Correctores**: actúan despois do ataque e de que se produzan os danos, a súa misión é a de corrixir as consecuencias do dano.

A elección de mecanismos de seguridade depende de cada sistema de información, da súa función, das posibilidades económicas da organización e, ante todo, de cales sexan os riscos aos que poda estar exposto o sistema.

## Seguridade lóxica

Os mecanismos e ferramentas de seguridade lóxica teñen coma obxectivo a **protección dixital da información** dunha maneira directa.

- **Control de acceso**
- **Cifrado de datos, encriptación**
- **Antivirus**
- **Devasa ou firewall**
- **Firma dixital**
- **Certificados dixitais**

### Control de acceso

Básicamente mediante nomes de usuario e contrasinais *ou mediante outros métodos que estudaremos nun tema posterior*.

### Cifrado de datos, encriptación

- Os **datos** son **enmascarados cunha clave especial** creada mediante un algoritmo de encriptación.
- **Emisor e receptor** son **coñecedores da clave** e, á chegada da mensaxe se produce o descifrado.
- O cifrado de datos **fortalece a confidencialidade**.

### Antivirus

- **Detectan e impiden a entrada de virus** e outro software malicioso.
- No caso de **infección** teñen a **capacidade de eliminalos** e de **corrixir os danos** causados no sistema.
- **Preventivo, detector e corrector**.

Protexe a [integridade](#) da información.

#### Devasa ou firewall

- Trátase dun ou varios [dispositivos software](#), [hardware](#) ou [mixtos](#), que [permiten](#), [denegan](#) ou [restrinxen o acceso ao sistema](#).
- [Protexe a integridade](#) da información.

#### Firma dixital

- Utilízase para a [transmisión de mensaxes](#), así como na [xestión de documentos electrónicos](#).
- A súa finalidade é [identificar de forma segura á persoa ou ao equipo](#) que se fai responsable da mensaxe ou do documento.
- [Protexe a integridade](#) e a [confidencialidade](#) da información

#### Certificados dixitais

- Son documentos dixitais mediante os que unha [entidade autorizada garante que unha persoa ou entidade é quen di ser](#), sendo avalado este feito pola verificación da súa clave pública.
- [Protexe a integridade](#) e a [confidencialidade](#) da información.

## Seguridade na wifi

As redes sen fíos, wi-fi, necesitan precaucións adicionais para a súa protección:

- Usar un [SSID](#), Service Set Identifier (Identificador de pertenza a unha rede)
- [Protección](#) da rede mediante [claves encriptadas WEP](#), Wired Equivalent Privacy, ou ben [WPA](#), Wifi Protected Access

## Seguridade Física

A seguridade física identifica as tarefas e mecanismos físicos que teñen coma obxectivo a protección do sistema e a información, dos perigos físicos e lóxicos.

- [Respaldo de datos](#): gardar copias de seguridade da información do sistema en lugar seguro.

Relacionado coa [Dispoñibilidade](#)

- [Dispositivos físicos de protección](#) como poden ser detectores de fumes, devasas por hardware, alarmas contra intrusos, sistemas de alimentación ininterrompida (SAI), pararraios ou mecanismos de protección contra instalacións.



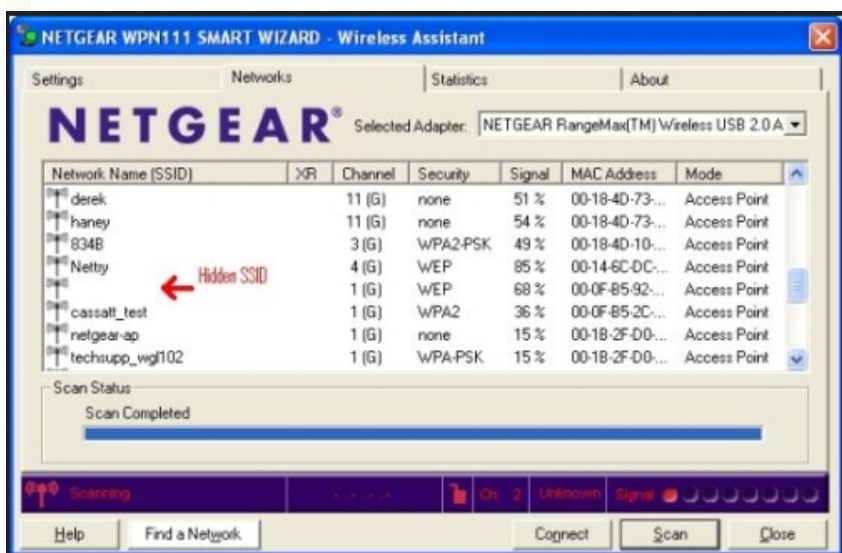
En canto as persoas, acceso restrinxido ás instalacións mediante calquera dispositivo que discrimine a entrada de persoal a determinadas zoas.

- [Filtrado de direccións MAC](#), Media Access Control (é unha dirección física que identifica cada dispositivo de forma única).

Usar un SSID, Service Set Identifier

#### SSID

- Darlle un nome á rede, preferiblemente un que non chame a atención de terceiros que detecten esta rede entre todas as dispoñibles.
- Cambiar con certa frecuencia o SSID.
- Ocultalo (Hidden), para que non se vexa o nome da rede cando buscamos redes sen fíos ás que conectarnos, de xeito que só poda acceder quen saiba o nome desa rede.



Imaxe derivada por [Gabriel Ferreiro](#), [Ana Veloso](#). [CC BY-SA](#), da orixinal [SSID](#). [CC BY-SA](#)

#### WEP vs WPA

Protección da rede mediante claves encriptadas WEP, Wired Equivalent Privacy, ou ben WPA, Wifi Protected Access

#### WEP vs WPA

- A clave WEP consume máis recursos e tamén é máis doadamente descifráble que a WPA, e debería ser cambiada con frecuencia.
- A WPA ten encriptación dinámica, sendo moito máis segura que a anterior.
- Hoxe en día utilízase fundamentalmente a versión 2 de WPA, WPA2 que é unha versión certificada e actualizada de WPA, que a fai máis segura.
- De todos os xeitos debemos cambiar o contrasinal de acceso á rede con frecuencia.

## Filtrado MAC

### Filtrado de direccións MAC, Media Access Control

#### Filtrado MAC

- É un mecanismo de acceso ao sistema mediante direccións físicas das tarxetas de rede, polo que unicamente se admiten determinados equipos, aqueles que teñen a dirección MAC correspondente con unha das cargadas na táboa de asignacións do router sen fíos.
- Pode resultar laborioso de configurar, non sendo de todo infalible, pois pode ser disfrazada a dirección MAC real.



**Gateway** VoIP Status - Network - Advanced - Firewall - Parental Control - Wireless

Radio  
Primary Network  
**Access Control**  
Advanced  
Bridging  
WMM

**Wireless**

**802.11 Access Control** : This page allows the configuration of the Access Control to the AP as well as status on the connected clients.

---

Administration  (Allow or Deny Access to Administration Web Page from PC connected over Wifi.)

Web Page Access

Wireless Interface

MAC Restrict Mode

MAC Addresses

|                      |                      |
|----------------------|----------------------|
| BC:85:56:12:FE:14    | <input type="text"/> |
| 74:2F:68:BD:FB:24    | <input type="text"/> |
| 74:2F:68:15:CD:31    | <input type="text"/> |
| <input type="text"/> | <input type="text"/> |
| <input type="text"/> | <input type="text"/> |
| <input type="text"/> | <input type="text"/> |
| <input type="text"/> | <input type="text"/> |
| <input type="text"/> | <input type="text"/> |

Connected Clients

| MAC Address       | Age(s) | RSSI(dBm) | Type | IP Addr      | Host Name |
|-------------------|--------|-----------|------|--------------|-----------|
| BC:85:56:B1:59:23 | 0      | -84       | 11g  | 192.168.0.13 |           |
| 74:2F:68:4C:92:61 | 1      | -82       | 11g  | 192.168.0.17 |           |
| C0:C9:76:87:96:D0 | 40     | 0         | 11g  | ERROR        | ERROR     |
| 98:FE:94:A1:88:A7 | 15     | -39       | 11g  | ERROR        | ERROR     |

© - Thomson - 2007

## Módulo 14. Seguridade na contorna física

- Unha das medidas máis importantes e, ás veces máis esquecidas, é aquela que fai referencia á contorna física de traballo.
- Esta **contorna** refírese á **ubicación física** (sala, conxunto de salas ou oficinas e edificios no que se atopan situados os **equipos e sistemas informáticos**, os **sistemas de rede** e os correspondentes **periféricos**.



- O **edificio** conta cunhas instalacións que todo persoa que instale os sistemas informáticos debe coñecer, para poder verificar que cumpren coas **normas de seguridade** e, no seu caso, solicitar a **reparación co fin de evitar posibles riscos futuros** sobre o hardware, software e información.
- Se descoidamos as instalacións físicas, de pouco pode servir as grandes medidas de nivel lóxico que podemos ter implantadas. Temos presente algún caso no que grandes multinacionais tiñan implantados moitas e moi boas medidas de seguridade lóxica, pero un simple lume no recinto dos servidores botou a perder meses de traballo. Por outro lado, ás bandas criminais moitas veces lles é máis rendible realizar un asalto físico que un lóxico.

## Seguridade pasiva

- A **seguridade pasiva** está composta polo conxunto de medidas que se implementan co fin de **minimizar a repercusión** dun **incidente** de seguridade e poder permitir a **recuperación** do **sistema**. Este tipo de **medidas** son **CORRECTIVAS**.
- Un exemplo clásico e moi claro de seguridade pasiva, pero non referente á ciencia informática, son os mecanismos que se incorporan aos vehículos para ser activados en caso de colisión, os cintos de seguridade, os airbag, repousacabezas, etc.
- Este tipo de seguridade aplícase aos elementos físicos do sistema de información, nas salas, oficinas e edificios onde se atopan situados, pois todos eses elementos poden sufrir incidentes de seguridade e deben ter especificadas medidas de reparación e recuperación.
- Os mecanismos e servizos que proporcionan seguridade pasiva a un sistema de información poden ser de tipo físico e de tipo lóxico.

## Seguridade activa

- Fai referencia aos diferentes mecanismos e procedementos que permiten **previr** e **detectar** **riscos** para a seguridade do sistema. Este tipo de **medidas** son **PREVENTIVAS**.
- Se utilizamos o mesmo símil que na seguridade pasiva, os mecanismos de seguridade activa nun vehículo poderían ser os freos, os espellos retrovisores ou os avisadores acústicos de colisión.
- Ao igual que na seguridade pasiva, os mecanismos de seguridade activa se aplican á parte física e á lóxica do sistema, podendo ser físicos e lóxicos.

## Seguridade física e lóxica

- Definiremos **seguridade física** a aquelas **medidas** de **seguridade** que teñen que ver coa **protección** dos **elementos físicos** dunha organización, como podería tratarse do hardware e a ubicación física, salas, oficinas e edificios que o albergan.
- A **seguridade lóxica** defínese como toda medida de seguridade relacionada coa **protección** do **software** e dos sistemas operativos, é dicir, a **protección** directa dos **datos** e da **información** da organización.
- Existen unhas medidas de seguridade, físicas e lóxicas, elementais, que todo sistema de información debe cumprir, independentemente do seu tamaño pero, a medida que a organización se fai máis grande, tanto a cantidade de información como a tipoloxía dos datos que deben ser protexidos atópanse máis comprometidos, co que as medidas deben adaptarse á mesma medida.

## Acceso de persoas ao recinto

- O **espazo** no que se atopa o **hardware** debe contar con diferentes **restricións de acceso** a persoas, en función do impacto que tería sobre o roubo ou deterioro dos equipos e, sobre todo, a da información.
- A **ubicación física** na que se atopen os **servidores**, debe ter a **máxima protección** dentro do conxunto de espazos no que se concentra todo o hardware do sistema.
- As restricións de acceso de persoas debe ser máis ou menos forte en relación á importancia dos datos que se custodian, do valor dos equipos e do impacto que pode supoñer para a organización a perda de material ou información.
- O control de acceso das persoas pódese realizar con sistemas moi diversos, podémonos atopar con compañías que ocupan edificios enteiros co sistema informático distribuído por plantas e usan uniformes de distinta cor para o persoal que pode ter acceso a cada planta.
- Tamén podemos ter unha tarxeta magnética personalizada e con acceso restrinxido por zoas, así como vídeo vixilancia, vixilantes xurados, biometría, etc.
- Todas as **medidas** relacionadas co control de acceso teñen **carácter preventivo** pero, **en caso de incidencias**, **teñen tamén carácter correctivo**. Como exemplo podemos ter a do vixiante diante dun monitor que pode impedir o acceso dunha persoa a unha zona determinada á que non está autorizada pero, no caso de

que pase ese control e se produza un ataque, esa persoa podería ser identificada mediante as gravacións da cámara.

### Instalación eléctrica

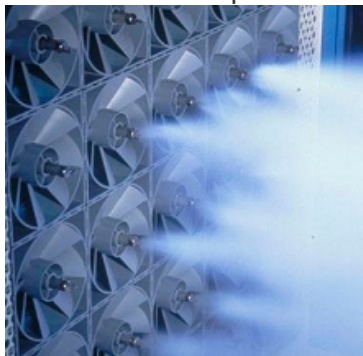
- Un punto clave no funcionamento dos equipos dun sistema informático é a **corrente eléctrica**, polo que tamén ten a mesma importancia ao falar de seguridade.
- Debemos ver a **rede eléctrica** dende dous puntos de vista, a **externa**, que pertence á compañía eléctrica, e a **interna**, propiedade da entidade.
- Sobre a primeira, **rede eléctrica externa**, unha das poucas cousas que poderemos facer é **ocultar o cabreado externo**, sempre co permiso da compañía eléctrica.
- En cambio, é sobre a **rede interna** onde deberemos ter en conta máis aspectos, entre os que se poden citar:
- Contratar a **potencia suficiente** para facer funcionar todo o sistema sen riscos de cortes de subministro por exceso de consumo.
- Instalar o **cabreado** que cumpra os **estándares de calidade** necesaria para esta actividade.
- Configuración correcta das **tomas de terra**.
- **Comprobación periódica** do correcto funcionamento dos **magneto-térmicos** e **diferenciais**.
- Pero, se por calquera circunstancia unha zona da instalación deixa de funcionar, podería poñer en perigo a integridade da información. Unha das medidas para minimizar os danos consiste na **segmentación por sectores**, para que un accidente afecte ao menor número posible de elementos.
- Por outra parte, débense instalar outros dispositivos e mecanismos que sirvan como recursos provisionais ata que a avaría sexa emendada, por exemplo, os **GRUPOS ELECTRÓXENOS**, os **SISTEMAS DE ALIMENTACIÓN ININTERROMPIDA (SAI)** e o **ALUMEADO DE EMERXENCIA**.

### Temperatura

- O **funcionamento idóneo** dos ordenadores é a **baixa temperatura**, sendo a ideal a que se atopa **entre os 15°C e os 25°C**, podendo chegar a picos de 10°C e 32°C.
- Os ordenadores terminais están sendo utilizados polos usuarios, pero os **servidores** ao non requirir presenza humana constante, **poden ser ubicados nunha zoa de especial climatización**, as denominadas **salas frías**, na que **a temperatura, segundo os estándares internacionais, debe ser de 22,3°C**.

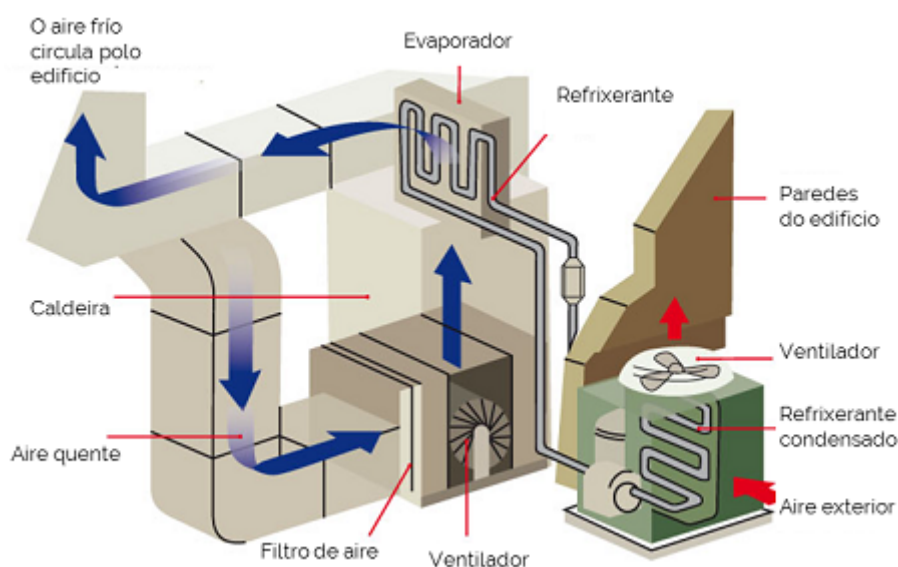
### Humidade ambiental

- A **humidade relativa** do aire que asegura un **funcionamento óptimo dos ordenadores e servidores**, se atopa no **rango do 40-50%**.
- As **persoas aportan humidade** ao aire, mentres que os **equipos electrónicos a reducen**.
- Debido a esta cuestión, faise necesaria a instalación de **humidificadores** e **deshumidificadores** de aire nas zonas que o requiran, ou ben **sistemas mixtos** que realicen esta función ata acadar o grao de humidade relativa necesario para o bon funcionamento dos equipos.



## Purificación do aire

- As **partículas de po** que se manteñen no aire son un grande **inimigo** para os **equipos informáticos**. Co tempo se incrustan nos disipadores e cobren os circuítos, tapando as vías necesarias de refrixeración, o que fai que os compoñentes electrónicos, principalmente o procesador, se quente, deteriore ou se chegue a fundir. Outras veces esas mesmas partículas de po poden conter materiais metálicos, sendo condutoras de electricidade, o que pode chegar a provocar cortocircuitos.
- Para permitir a aireación dos equipos, é conveniente un sistema de ventilación natural, aínda que este leva consigo multitude de partículas, po, fibras, polen, fume, pelo, etc., facéndose necesario limpalo con **PURIFICADORES DE AIRE**.
- En zonas moi sensibles dos datacenter, onde se ubican os servidores do core do negocio, faise necesario o illamento integral da sala contra o po, fibras e outras partículas.
- A pureza do aire se pode controlar mediante a instalación de **DETECTORES DE GASES**, que detectan e miden o monóxido de carbono, oxíxeno, metano, sulfuro de hidróxeno, etc.





## Auga

- A **auga** é outro dos grandes **inimigos** do **equipamento electrónico**, unha inundación pola rotura de tubarías no interior do edificio, ou pola entrada de auga da chuvia, tería consecuencias nefastas sobre todo o equipamento.
- Os baños e as saídas de auga débense situar a determinada distancia das salas que alberguen os sistemas e contar con sistemas de desviación e absorción da auga en caso de escapas accidentais e roturas.
- Por outra banda, a ubicación física do equipamento hardware debe ser afastada das ventás e non estar apoiada directamente no chan.
- O mercado dispón de detectores de líquidos que se poden instalar no chan e en paredes e teitos para detectar fugas de auga, da mesma planta o da superior.

## Incendios

- As **medidas** de **seguridade pasiva** contra **incendios** comprende, principalmente:
  - a instalación de **barreiras** contra a propagación de lume,
  - a existencia de **vías de evacuación** de persoas e
  - os **sistemas de extinción**.
- Será a **seguridade activa**, a que debe contar coas medidas necesarias para evitar os incendios fortuítos ou provocados, e con todos os sistemas de **detección de fume, chamas e calor**.
- Xeralmente, un incendio que se produce nas áreas de ordenadores, se debe a problemas co sistema eléctrico e, o problema que pode causar no hardware débese, non tanto a propia chama, máis ben ao deterioro dos circuítos pola calor e o fume.

### Muros devasas

Os muros devasa separan edificios e zonas dentro dos edificios. O seu obxectivo é impedir que o lume se propague a zonas colindantes durante un período de tempo máis ou menos longo, reducindo os danos e os riscos para as persoas.

Estas barreiras son construídas á vez que os edificios, dende os cimentos até superar a cuberta, están feitos de material ignífugo, non inflamable e de grande resistencia á calor, os cales deben conter o lume durante varias horas, o tempo suficiente para que se poida extinguir.

Con respecto ás portas, existen no mercado comportas devasa que son coladas nas saídas dos condutos de ventilación e aire acondicionado para ser pechados de forma automática ou manual para evitar que se propague o lume, o fume e os gases a outras seccións.

### Muro devasa



## Detector de incendios

Trátase de diferentes dispositivos que se instalan, xeralmente, no teito ou na parte máis alta dos muros das habitacións, os puntos cara os que se despraza o fume.

Débense instalar tantos puntos de detección de fume como posibles focos de risco de incendio estimemos que existen na instalación, tendo en conta tamén a distancia do fume que detecta, aproximadamente 7 metros. Estarán conectados a unha central de alarma que mostrará visualmente qué detector se activou, acción que se realiza cando percibe un aumento porcentual considerable na presenza de fume ou partículas de combustión.

Podemos atopar no mercado, diferentes detectores:

ÓPTICOS

IÓNICOS

DE TEMPERATURA OU TÉRMICOS

POR EXTRACCIÓN DE FUME

VESDA

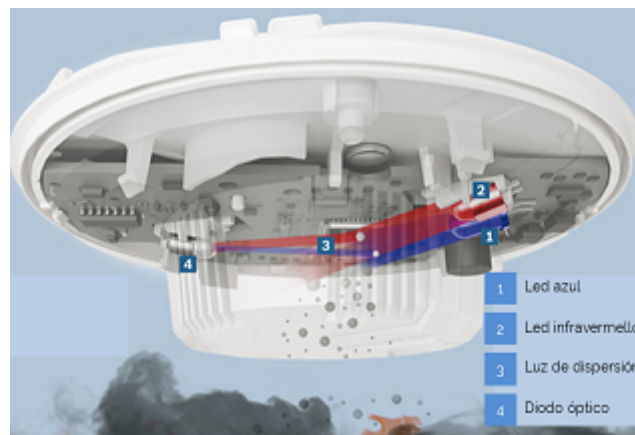
## Tipos de detectores de incendios

Imos mostrarvos, a nivel curiosidade, as características destes detectores.

### Ópticos

Están dotados de tecnoloxía fotoelétrica, xerando un feixe de raios luminosos. Cando o fume penetra no detector de fumes, se escurece o feixe de luz e se activa o sinal de perigo.

### Detector óptico



O máis moderno dos sistemas fotoelétricos emite raios láser e pode chegar a ser cen veces máis rápido que os sistemas ópticos simples.

### Detector óptico



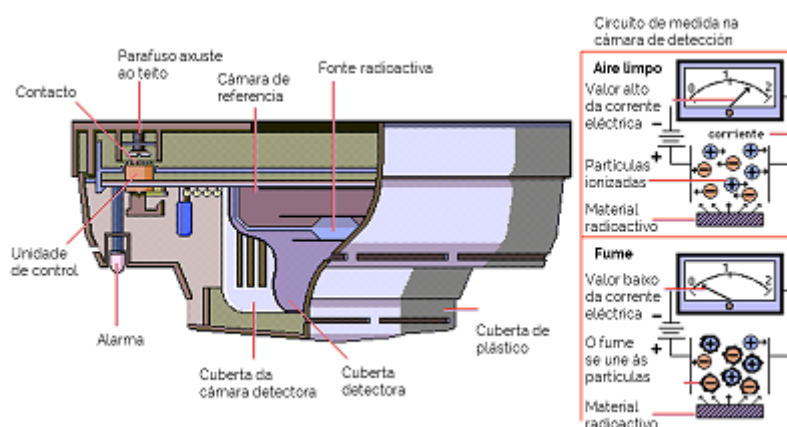


## Iónicos

Perciben as partículas procedentes da combustión de materiais. Ao penetrar o fume nas rendixas do detector, a ionización do aire se fai menor co que se corta a pequena corrente eléctrica que se produce entre os seus eléctrodos, o que activa o sinal acústico que avisa do perigo de incendio.

É un aparato radioactivo, dispón dunha cámara de americio 241 e que, baixo un funcionamento normal non representa risco para as persoas, pero necesita revisións periódicas por persoal especializado.

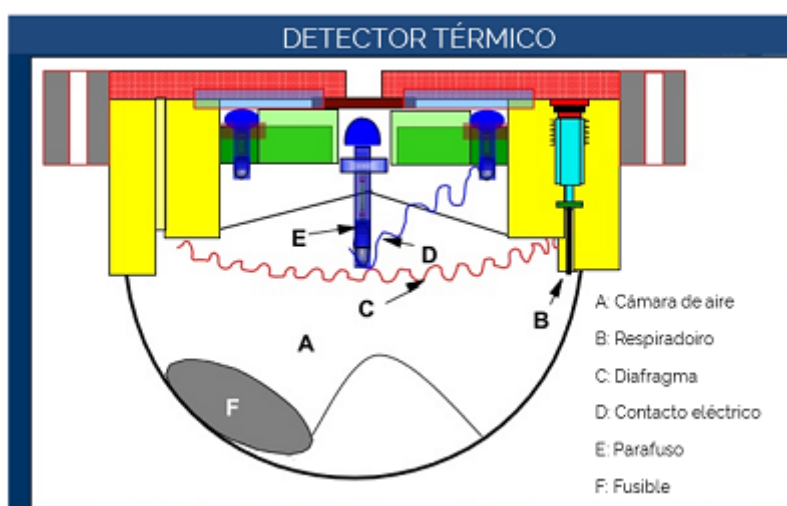
### Detector iónico



## Térmicos

DE TEMPERATURA OU TÉRMICOS. Están programados para avisar dos cambios bruscos de temperatura no recinto ou para que disparen a alarma a partir dunha temperatura determinada.

### Detector térmico



## Extracción de fume

Son dispositivos que extraen o aire de forma continua por unha serie de condutos. Cando o aire está enrarecido, a partir dun patrón de aire predeterminado, prodúcese unha alarma.

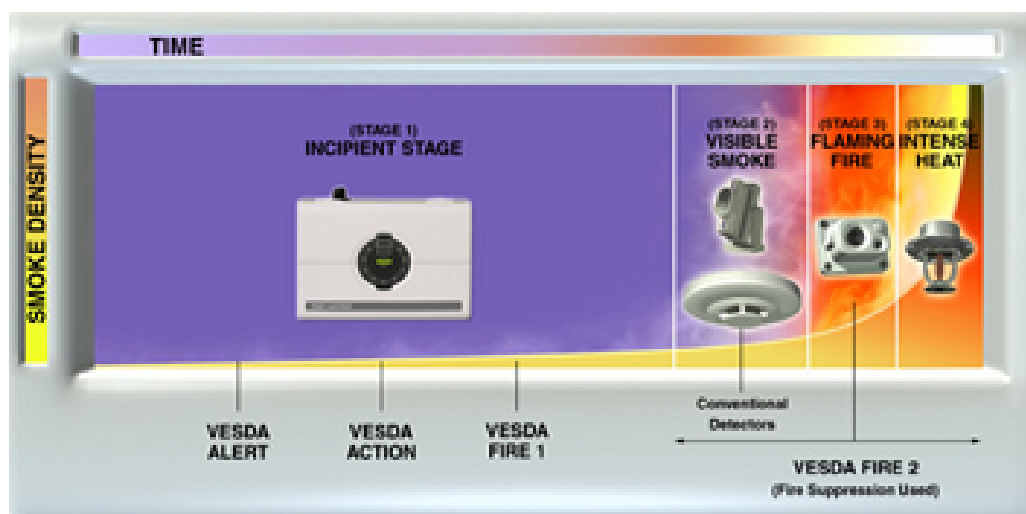
É un dos extractores máis costosos polo tipo de instalación que necesita para o seu funcionamento.  
Extracción fume



Vesda

Existen uns aparatos detectores moi avanzados, denominados, Very Early Smoke Detection Apparatus, VESDA, que teñen a capacidade de detectar a densidade do fume e determinar en qué fase se está a producir o incendio, dende un estado do fume aínda non perceptible.

Detector Vesda



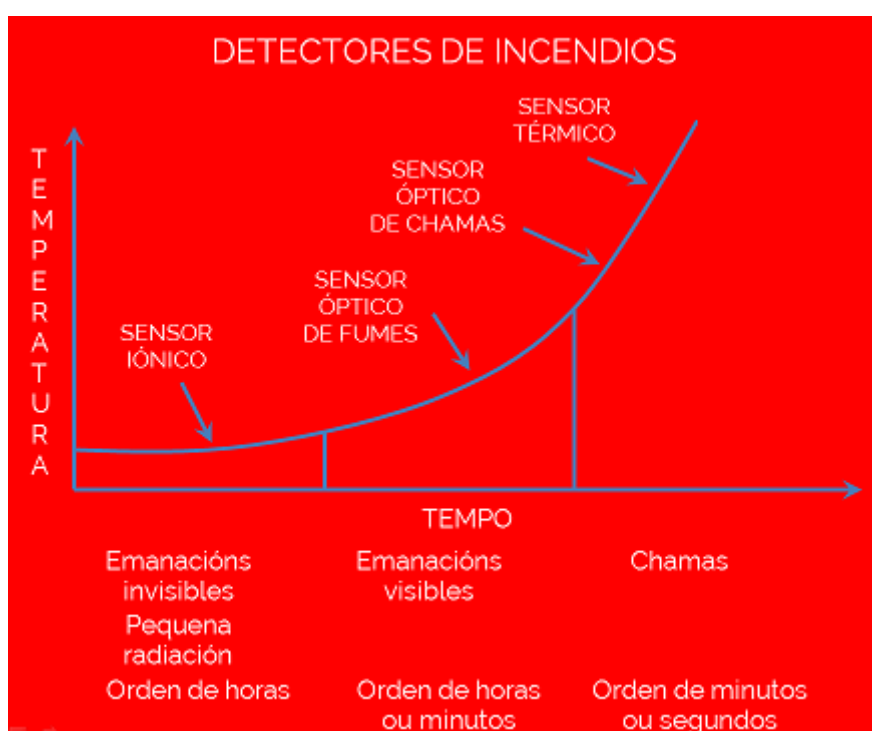
Conclusións

Podemos ver nas dúas imaxes seguintes, unha pequena comparativa dos detectores máis habituais do mercado.

Comparativa sensores

|                                                                                   |                                                                                                             |                                                                                           |                                                                                                       |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| <b>Sensor Fotoeléctrico</b><br>Feixe de luz de detección<br>Feixe de chama lenta  | <b>Sensor Térmico</b><br>Detección de temperatura<br>Criterio de aumento de temperatura ou temperatura fixa | <b>Sensor Iónico</b><br>Detección por condutividade do aire<br>Detección por chama rápida | <b>Sensor de Fume</b><br>Detección e control de propagación do fume en condutos de aire acondicionado |
|  |                            |         |                    |

Comparativa sensores



### Extintores

Existen varias clases de extintores en consideración ao peso e tipo de carga. Podemos atopar diferentes equipos portátiles dende 1 Kg até chegar aos 250 Kg, que están provistos de rodas ou carriño para o seu desprazamento. A cuestión principal é conseguir o tipo de extinto conveniente a cada espazo físico que cumpra coa normativa legal.

Un lume se clasifica en categorías, dependendo do material combustible ao que afecta. Estes tipos de lume non se atopan estandarizados a nivel mundial, existindo variacións dun país ao outro en relación á súa denominación, simboloxía e material combustible ao que afectan.

Na seguinte figura mostramos a clasificación dos lumes e o tipo de extintor axeitado para facerlle fronte:

### Extintores

| EXTINTOR<br>TIPO DE LUME  |                                                                                                               | EXTINTOR |                |            |                     |       |                    |
|---------------------------|---------------------------------------------------------------------------------------------------------------|----------|----------------|------------|---------------------|-------|--------------------|
|                           |                                                                                                               | AUGA     | ESFUMA QUÍMICA | POLVO SECO | ANHIDRIDO CARBÓNICO | HALÓN | ACETATO DE POTASIO |
| <b>A</b><br>SÓLIDOS       | O lume que se produce sobre material combustible sólido: madeira, papel, plástico, que forma brasas ao arder. | SÍ       | SÍ             | SÍ         | NON                 | SÍ    | NON                |
| <b>B</b><br>LÍQUIDOS      | O que queimaría líquidos altamente inflamables, como graxas, aceites, gasolina, alcohol.                      | NON      | SÍ             | SÍ         | SÍ                  | SÍ    | NON                |
| <b>C</b><br>GASES         | Sobre gases inflamables como butano, gas natural, propano...                                                  | NON      | NON            | SÍ         | SÍ                  | SÍ    | NON                |
| <b>D</b><br>METAIS ESP.   | O que queimaría metais especiais combustíbeis, como o sodio, magnesio, potasio, que arden a alta temperatura. | NON      | NON            | NON        | NON                 | NON   | SÍ                 |
| <b>E</b><br>RISCO ELECTR. | Risco de electrocución, afecta a materiais que conducen, producen ou almacenan enerxía eléctrica.             | NON      | NON            | SÍ         | SÍ                  | SÍ    | SÍ                 |
| <b>K</b><br>GRAXAS        | O que afecta a graxas vexetais, como os utilizados en cocinas.                                                | NON      | NON            | NON        | NON                 | NON   | SÍ                 |

EXTINTORES E TIPOS DE LUME

### Vías de evacuación

As vías de evacuación e as saídas de emerxencia para casos de incendio deberán estar debidamente sinalizadas e iluminadas, así como constar no plan de emerxencias da organización.

Vía de evacuación Vía de evacuación Vía de evacuación



### Seguros

A contratación de un ou varios seguros de riscos, compensará economicamente e minimizará as perdas por desastres ocorridos na organización, como poderían ser os incendios, inundacións, roubo, fallos eléctricos, po ambiental, etc.

### Exemplo de Contorna física dun centro de proceso de datos

Un CPD ou Centro de Proceso de Datos, en inglés Data Center, consiste nun ou varios locais, unha planta ou un edificio completo que alberga o sistema principal de redes, ordenadores e recursos asociados, que teñen como fin o procesar toda a información dunha empresa ou organización.

O obxectivo principal dun cpd é a protección da integridade, confidencialidade e

dispoñibilidade da información. Neste cometido velarán polo disposto na corresponde normativa legal.

No que respecta á contorna física, contarán con todas as medidas de seguridade que se foron enumerando neste documento, xunto con outras máis específicas.

CPD Google



Exemplo de Estrutura dun CPD

O chan debe contar con moi alta capacidade de carga.

Dobre chan para evitar riscos de electrocución e inundación

Construción antisísmica

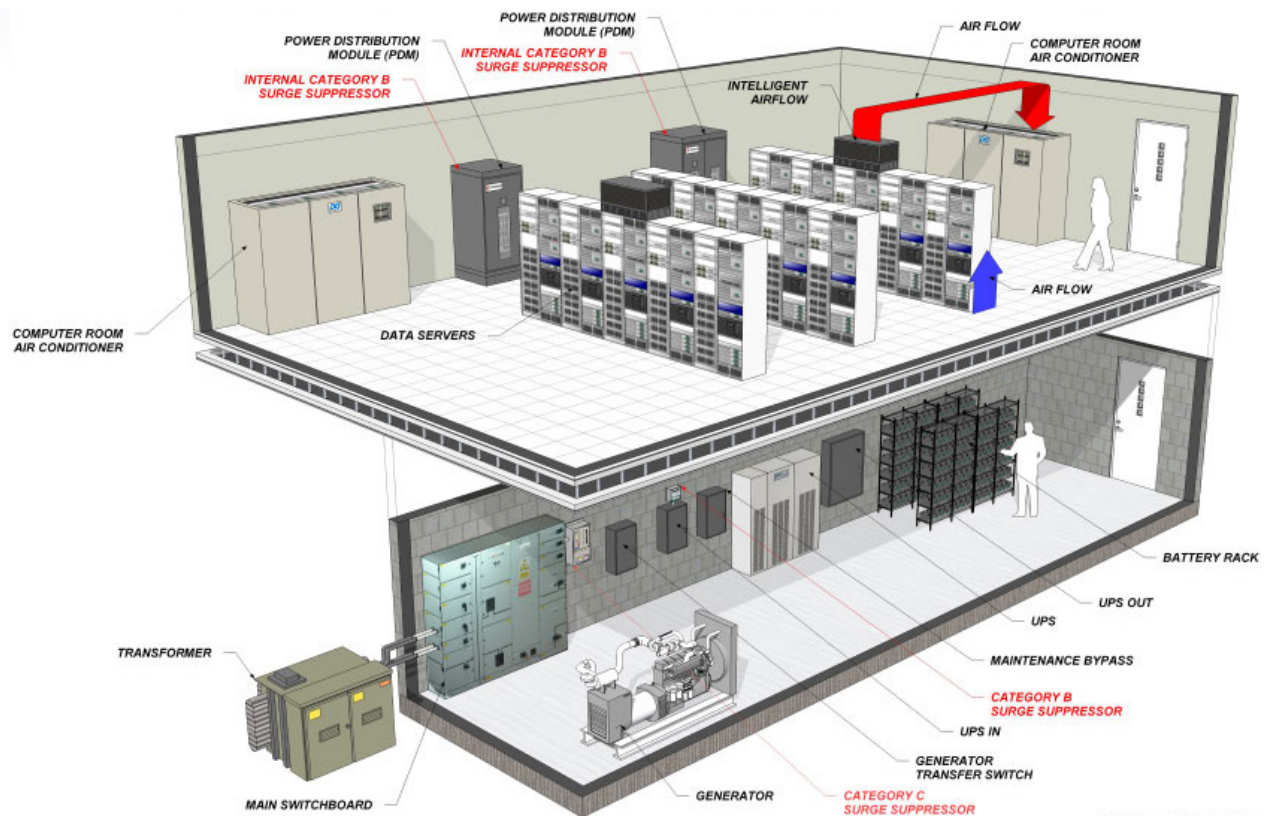
Paredes con tratamento ignífugo e antipo

Illamento térmico en muros e ventás

Sala fría, a zona máis protexida de todo o datacenter, na que se ubican os elementos máis protexidos de todo o sistema, con acceso restrinxido e vestimenta especial, para non traspasar ao aire fibras da roupa nin pelo.

Estrutura data center





## Módulo 15. Seguridade no hardware

Neste tema comentaremos todos os aspectos que consideramos relevantes en relación á [seguridade no hardware](#).

Un dos grandes esforzos na protección do sistema é o referente ao hardware, debido a que, se protexemos este elemento, manteremos a salvo os datos, é dicir a información.

Teremos en conta a protección fronte a terremotos e tormentas eléctricas, veremos cómo realizar un mantemento axeitado e protexeremos todos os sistemas fronte a cortes de electricidade, xa sexan breves como prolongados, en función dos requisitos da nosa instalación.

### Seguridade activa

Entre os compoñentes e ferramentas que aseguran de forma activa o hardware, atópanse:

- Sistemas de alimentación ininterrompida
- Regletas protectoras
- Grupos electrógenos

### Sistemas de alimentación ininterrompida

- Os sistemas de alimentación ininterrompida, máis comunmente denominados [SAI](#) ou en inglés, *uninterruptible power supply* ([UPS](#)), son un elemento básico na protección do hardware.
- A pesar do seu nome, os SAI non serven para seguir traballando durante un corte de electricidade prolongado, unicamente [subministra enerxía ao ordenador ou a outro periférico durante un tempo limitado, o que nos permitiría gardar os datos necesarios e apagar o sistema con seguridade](#), ademais de [protexelos ante as anomalías do subministrador eléctrico](#).



### Tipos de SAI

Os sai categorízanse en tres tipoloxías:

- SAI stand by ou offline
- SAI interactivo ou inline
- SAI online

## SAI stand by ou offline

Soen utilizarse en ordenadores persoais, proporciona a protección máis básica:

- Fallos de alimentación
- Caídas de tensión
- Picos de corrente, sobretensión e subtensión



## SAI interactivo ou inline

De tipo medio, ofrece máis protección que o anterior, pero a batería dura menos que no anterior debido que o equipo a protexer toma corrente con máis frecuencia. Ademais dos tres fallos da corrente do anterior, ofrece protección contra:

- Infratensións prolongadas
- Sobretensións prolongadas



## SAI online

Traballa constantemente proporcionando a súa propia corrente, independentemente da que circula pola rede normal, co que as baterías se gastan antes. É o tipo de SAI que se usa nos datacenter e, proporciona protección sobre todos os problemas da corrente eléctrica, é dicir, ademais das do tipo anterior:

- Distorsións na onda da liña
- Variacións nas frecuencias
- Microcortes
- Distorsión armónica



## Cuestións a considerar



- As baterías do SAI conteñen unha carga elevada, debe ser manexado coa máxima precaución, seguindo sempre as instrucións do fabricante.
- A práctica maioría deles incorporan software e drivers para a monitorización do seu funcionamento..
- As baterías teñen un tempo de vida útil determinado e, progresivamente, van perdendo capacidade de rexeneración, é conveniente cambialas en función das instrucións do fabricante.

### Regletas protectoras

- As regletas protectoras son, na maior parte dos casos, unha solución alcanzable para o problema das subidas de tensión.
- Non son comparables aos SAI, pois non protexen dos cortes de subministro, pero poden ser útiles para [protexer o hardware por un importe módico, da acción de raios de tormentas eléctricas, baixadas e subidas de tensión ou ruído eléctrico](#).
- Poden incorporar un interruptor xeral e un mando a distancia para apagalas e aforrar a enerxía que consumen os equipos en estado de repouso.



### Grupos electróxenos

- Un grupo electróxeno é unha [pequena maquinaria que xera electricidade](#) mediante un motor de combustión interna.
- Este tipo de máquinas [se emprega en lugares onde é vital seguir traballando independentemente das condicións eléctricas](#), por exemplo nas zonas críticas dos hospitais, en aeroportos, onde é imprescindible non ter cortes do subministro eléctrico.
- Cando se produce un corte de enerxía eléctrica, por exemplo nun datacenter, os SAI interveñen en primeiro lugar pero, inmediatamente se inicia o arranque automático dos grupos electróxenos, para proporcionar a tensión suficiente para manter os equipos en marcha.
- No mercado podemos atopar multitude de equipamento electróxeno, dende pequenos motores con arranque manual para pequenos centros de traballo e situacións de emerxencia non habituais, até chegar a grandes grupos electróxenos que dan cobertura as grandes infraestruturas que comentabamos anteriormente, quirófanos de hospitais, torres de control de aeroporto, situacións de emerxencia, inundacións, etc.



## Monitorización do hardware

- A **monitorización do hardware** úsase para **comprobar o correcto funcionamento** do sistema e a detección de erros nos compoñentes físicos, como pode ser a temperatura da CPU, a velocidade de xiro dos ventiladores, etc.
- Para lograr este cometido, contaremos con diferentes medios, tanto software como hardware

## Método hardware

- Podemos comprobar o funcionamento dun compoñente medindo as magnitudes eléctricas dos elementos que forman parte do sistema.
- Nalgúns casos pode resultar unha tarefa complicada pero, noutros como a fonte de alimentación, resulta sinxela e será a mellor forma de comprobar que todo funciona correctamente.
- Usaremos para estas tarefas un polímetro, instrumento que nos permite coñecer a corrente dun determinado dispositivo. A maior parte dos modelos inclúen unha roda que permite seleccionar a magnitude que se vai medir.



- Por outra banda é imprescindible realizar inspeccións visuais de forma periódica para recoñecer o estado do hardware e poder augurar futuros problemas ou avarías. Por exemplo, ruídos estraños, pezas mal instaladas, en mal estado ou mesmo acumulación de sucidade, que non son detectadas mediante software, serán fonte próxima de avarías.

## Método software

- A **monitorización do hardware a través** de determinados **programas** é o método máis utilizado.
- No mercado se poden atopar cada vez máis solucións, tanto de software gatuíto como ferramentas de pago moi completas, que ofrecen información importante que pode ser de moita utilidade, non só na detección de erros, tamén á hora de comprobar o rendemento do noso ordenador e, extrapolando, do sistema informático da organización.
- Existe moito software que analiza a utilización da CPU, a memoria RAM dispoñible, consumida e libre, o disco duro e o uso que facemos del, tamén a utilización da tarxeta gráfica e as características dos buses e dispositivos do ordenador.



- Algúns exemplos:
  - [Everest Ultimate Edition e AIDA64](#), ferramentas de diagnóstico de sistemas, orientado a usuarios domésticos. Realiza recoñecemento, visualización(Diagnosticar) dos compoñentes tanto hardware como software do sistema no que se está executando.
  - En [ticarte](#), podedes atopar enlaces a varias ferramentas, como [speccy](#), [HWinfo](#), ...
  - [PSENSOR](#), permite analizar a información proporcionada polos sensores do noso hardware. Podemos visualizar curvas de temperatura da gráfica (GPU) e do procesador (CPU), así como temperatura dos discos duros.
  - [HARDINFO](#), versión libre de AIDA64. Podedes visualizar tamén información en [Ubuntu-hardinfo](#).
  - [speedfan](#), monitoriza temperaturas, voltaxes,...

De todas estas ferramentas e outras do estilo, podedes atopar moita información e vídeos na web.



## Fixación dos compoñentes físicos

- Os [compoñentes físicos](#) dun ordenador e, por extrapolación, dun sistema, deben atoparse [perfectamente ordenados](#) e, sempre que sexa posible, fixalos fisicamente a un armazón.
- Un equipo electrónico produce vibracións, que poden afectar ao hardware, o disco duro, o lector de dvd, o ventilador da fonte de alimentación, son compoñentes que conteñen partes móbiles e que, ao funcionar, traspasan parte desa enerxía ao resto de pezas. Tamén existen conexións grandes, por exemplo o conector vga ou hdmi, que realizan grande presión sobre a tarxeta gráfica, chegando, co tempo, a deteriorarse e descolocarse da súa posición inicial.
- Estas situacións deben ser evitadas, pois acaban por provocar un mal funcionamento do equipo, así como un lugar de traballo non idóneo.
- Tamén debemos ter en conta os factores externos, que deben requirir atención especial, como poden ser os terremotos. En zonas de grande actividade sísmica, como por exemplo

Xapón, é conveniente anclar os equipos de forma segura en armarios especiais antisísmicos.

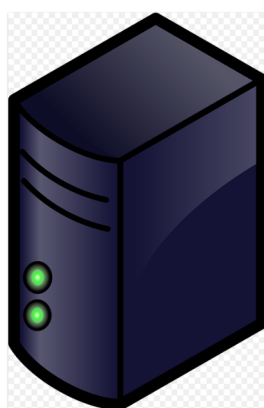
- É imprescindible manter os sistemas perfectamente ventilados e coas aberturas en perfecto estado de limpeza, en caso contrario poden quentarse en exceso e chegar a queimar, tanto o procesados como o disco duro, perdendo a información almacenada.
- Tamén teremos en conta que, se están de cara ao público, pode ser roubado, co que debemos tomar precaucións neste sentido, utilizando, por exemplo, cables e cerraduras de seguridade Kensington que, aínda non sendo un elemento definitorio de protección antirroubo, si ten efectos disuasorios.



## Outros compoñentes

Entre outros compoñentes de seguridade activa que podemos utilizar para a seguridade do hardware, podemos atopar:

- **Carcasas.**  
Son o recubrimento das interioridades de todo sistema. Podemos atopar moi variados tipos de carcasas, sinxelas e con moito deseño.
- **Maletín de transporte.**  
Maletín ou mochila con elementos de amortecemento que absorben impactos e garanten a seguridade do hardware durante o transporte. Son utilizados con dispositivos móbiles, ordenadores portátiles, tablets, etc., pero tamén existen versións para grandes equipos.



- **Refrixeración líquida.**  
Este tipo de refrixeración, utilizado sobre todo en superordenadores, son un recurso poderoso para baixar a temperatura e evitar problemas de quecemento.
- **Portátiles, teclado e rato resistentes á auga, po e golpes.**  
Utilizados en contornas industriais e climas extremos, protexen a información e software contida nos equipos dunha forma moi eficaz.

## Seguridade pasiva

- Non todas as vulnerabilidades poden ser cubertas por completo, polo que se mantén aberta a posibilidade dun ataque ao sistema coa súa conseguinte perda de información.
- É neste momento cando entran en acción as medidas de seguridade pasiva, que reducirán ou anularán o impacto do ataque.
- Entre as medidas de seguridade pasiva para a protección do hardware que se empregan con maior frecuencia, figuran:
  - Mecanismos de tolerancia a fallos
  - Renovación de equipos
  - Equipos de substitución

## Mecanismos de tolerancia a fallos

- A tolerancia a fallos é a capacidade dos sistemas de seguir funcionando a pesar da avería dalgún dos seus compoñentes.
- Adóitase dotar con este tipo de mecanismo a equipos que se consideran vitais, e dos que se espera un funcionamento continuo e sen fallos, por exemplo servidores de correo e de aplicacións. Non é habitual, nin aconsellable, atopalo en ordenadores de usuarios finais, debido ao alto custe que supón
- Os sistemas con mecanismos de tolerancia a fallos dispoñen de compoñentes duplicados, o que se denomina redundancia.
- A redundancia pode ser:
  - **Estática:** os compoñentes duplicados sempre se atopan activos e funcionando.
  - **Dinámica:** é o propio compoñente redundante, mediante outros sistemas, o que detecta o fallo e comeza a funcionar.
- Actualmente, todos os servidores contan con múltiples CPU e módulos de memoria RAM, traballando en conxunto para satisfacer as necesidades de demanda do servidor. Todas as pezas deste tipo de equipos poden ser cambiadas “en quente”, sen a necesidade de apagar o equipo para realizar as tarefas de mantemento e substitución de pezas.
- Tamén é moi habitual o atoparnos con sistemas que conteñen discos duros, fontes de alimentación e tarxetas de rede redundantes.

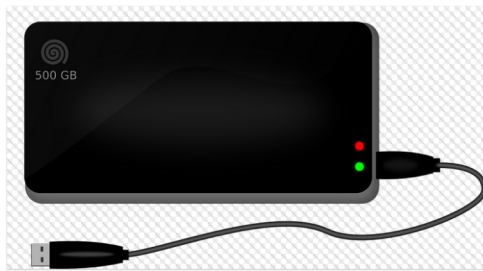


## Discos duros



A estas alturas, todos e todas nós estamos xa convencidos da importancia que teñen os nosos datos e a necesidade de asegurarnos de que non podemos permitírnos perdernos, incluso a nivel personal (fotos, traballos de aula...). Para iso podemos facer copias ou implementar sistemas que nos aseguren a conservación de toda esa información.

- Podemos empregar simplemente discos tanto internos como externos para facer copias de seguridade coa regularidade que se estime (diarios, semanais, mensuais...), en función da importancia dos datos a gardar.



- Para máis seguridade, pódese usar [RAID](#), Redundant Array of Independent Disk ou grupo redundante de discos independentes.
  - Son un conxunto de discos fisicamente independentes, entre os que se distribúen ou replican os datos.
  - Existen diferentes formas de implementar ou configurar estes discos, por exemplo combinado os discos de xeito que para o sistema operativo aparezan como un único disco, noutro caso crea copias exactas dun disco noutro (espello), pode ser que se configure de xeito que a información se vaia distribuindo entre todos os discos...



- Outra posibilidade é utilizar [NAS](#), Network Attached Storage, Almacenamiento conectado en Rede.
  - A misión principal dos NAS é servir como almacenamento externo e masivo, conectado por rede.
  - A aparencia externa dun NAS é a de unha pequena caixa que terá unhas dimensións que dependen das súas características finais, principalmente do número de discos duros que podemos utilizar nel.

- Ademais dos discos duros (que xeralmente se configuran en RAID), todos os NAS do mercado integran un pequeno ordenador, que como calquera computador utiliza o hardware básico: procesador e memoria RAM, entre outros.
- A súa instalación é moi sinxela, pódese realizar dende un PC de forma case automática, gracias ao programa que inclúe o NAS.

Se non podes visualizar o seguinte vídeo, fai clic en [NAS vs Disco con conexión ethernet](#)

### Fontes de alimentación

É habitual atopar un mínimo de dúas fontes de alimentación redundantes nos servidores, as cales son conectadas as redes diferentes subministradores de enerxía eléctrica.



### Renovación de equipos

- Unha das tarefas máis importantes que se debe ter en conta é unha [planificación rigorosa para a renovación do equipamento hardware](#).
- Cando falamos de renovación de equipos, non estamos incorporando neste apartado a substitución dun equipo que non funciona por un novo, realmente se trata de planificar o período de funcionamento de cada un dos equipos que adquirimos, temos que tratar de valorar a obsolescencia do noso sistema, que aínda segue a funcionar, pero que, en pouco tempo pode deixar de facelo ou, o que é máis importante, nas condicións axeitadas.
- Débense ter en conta diversos factores, entre eles, o custe do novo equipo, os de instalación e adecuación do resto de compoñentes ao novo hardware e os gastos para a actualización do software do novo equipo.

### Equipos de substitución

- Calquera empresa ou profesional cuxo traballo dependa do ordenador, non se pode permitir parar súa actividade por unha avaría.
- A posibilidade de contar cun equipo de substitución, é dicir, un ordenador para utilizar en caso de que o noso falle, adoita estar cuberto por un seguro ou unha cota extraordinaria de algunha compañía, ben de seguro, ben de servizos informáticos.
- Temos que ter en conta que, mentres o equipo é reparado, podemos seguir traballando coa información do mesmo, incorporando o disco duro nunha carcasa e utilizándoo no equipo temporal.



## Racks e armarios

- Os racks, supoñen unha medida de seguridade máis, serven para organizar de forma axeitada os dispositivos, favorecendo a colocación en zonas seguras e ben protexidas por sistemas antiincendios e con proteccións antisísmicas.
- Serven, ademais, para proporcionar a axeitada refrixeración dos sistemas, sendo tamén illantes acústicos.



- Poden colocarse en armarios ignífugos, o que aínda brinda máis seguridade.
- Os armarios ignífugos están equipados con sistemas que os protexen do lume. Están fabricados con materiais illantes, tanto do lume como do fume e de altas temperaturas, sendo un recurso imprescindible para manter a salvo as copias de seguridade.



## Módulo 16. Ameazas ao software

- Nos introduciremos neste tema nos aspectos que consideramos relevantes en relación ás [vulnerabilidades](#) que se poden atopar no [software](#), no conxunto de programas e aplicacións que fan posible que se poda levar a cabo calquera tarefa nun sistema informático.
- O software principal que nos atopamos nun sistema informático, é o [Sistema Operativo](#), o conxunto de programas e aplicacións que administra todos os recursos, internos e externos ao ordenador, así como os ficheiros e tarefas correspondentes.
- Tanto o [Sistema Operativo](#) como as diferentes [aplicacións](#) que están instaladas no meu equipo, e por conseguinte, a [información](#) gardada nel ou nalgún outro equipo da rede na que traballo, son [susceptibles de ameazas](#).

### Vulnerabilidade do software

- Partimos da máxima de que [todo o software é vulnerable](#).
- Ás veces contén [erros nas fases de deseño e desenvolvemento](#) do mesmo, e que non foron detectadas nin corrixis na fase de probas.
- Outras veces, debido a unha [defectuosa instalación ou configuración](#) deste software por parte do persoal técnico ou mesmo usuarios.

### Erros de programación

- Os [erros](#) cometidos [nas fases de deseño e desenvolvemento](#) do software, que non foron detectados nin corrixis a posteriori, soen denominarse [bugs](#) (insecto).
- Un erro no deseño dunha aplicación pode ser, por exemplo, gardar os usuarios e contrasinais dos usuarios, en lugares do sistema informático facilmente accesible ou sen codificar.
- No módulo 7, Deseño e realización de probas, vimos varios exemplos de erros software con consecuencias moi graves.
- Mostraremos aquí algún outro exemplo interesante:
  - [10 erros informáticos que provocaron catástrofes](#)
  - [Os cinco grandes erros da Historia do Software.](#)
  - [Cómo ganar miles de dólares cazando errores de software](#)

### Erros de instalación ou configuración

Este tipo de erros poden deberse a:

- unha [deficiente documentación](#) do software,
- a [falta de información cara os usuarios que o instalarán ou configurarán](#) ou, ás veces,
- unha tamén [deliberada configuración defectuosa](#).
- Algúns exemplos:
  - [Cómo solucionar problemas de errores de Windows installer](#)
  - [Outro error de instalación de Windows...](#)
  - [Solucionar problemas instalación Microsoft](#)

- [No se puede continuar con la instalación](#)
- [Cómo solucionar el bug que impide instalar software de terceros en Ubuntu](#)
- [Pronto se corregirá el error al instalar paquetes .deb de terceros desde GNOME Software en Ubuntu 16.04](#)

## Publicación de solucións ás vulnerabilidades

- Como se comentaba anteriormente, todo software pode conter erros de deseño ou desenvolvemento que poden, á súa vez, afectar á seguridade. Cando estes se detectan, a organización que o desenvolveu procede á súa corrección con novo software que o substitúe ou unha solución software para corrixir ese erro, algo que se denomina “[parche](#)”.
- Se non se aplican estas solucións ou parches tan pronto son publicadas, córrese o risco de manter a vulnerabilidade do noso sistema informático ante posibles entradas alleas.

## Descarga de software de fontes non fiables

- En internet podemos atopar moitos sitios web que ofertan software libre e gratuíto, e mesmo comercial, que podería parecer exactamente igual que o orixinal, pero que, polo xeral, contén pequenas aplicacións adicionais que poden pasar inadvertidas ao usuario, pero que pode [incorporar código malicioso](#) que pode poñer en perigo o sistema informático no que se instala.
- Por outra parte, tamén é posible atopar en fontes pouco fiables, anuncios de antivirus que, realmente, son virus, troyanos, gusanos ou programas espía.

## Efectos de ataques a código vulnerable

Un ataque producido por unha vulnerabilidade no código das aplicacións, afectará a unha ou máis propiedades da información, que analizamos en profundidade en módulos anteriores:

- Integridade
- Confidencialidade
- Dispoñibilidade

Deixa aberta vías a posibles atacantes para:

- Obter información sobre o sistema, de xeito oculto, sobre os equipos que o compoñen, datos de usuarios, sistemas operativos, aplicacións e bases de datos.
- Obter, copiar e divulgar información restrinxida
- Modificar ou borrar datos
- Impedir o acceso á información por parte de usuarios con permisos de acceso

## Ameazas sobre o software e a información

- O núcleo de todo sistema de información son os datos, se se accede ás bases de datos dunha organización, pódese obter información privilexiada de calquera organización e, se se lles causa algún tipo de dano, se lle causa á súa vez, un dano irreparable á empresa.
- Podemos contar innumerables ameazas ao software e á información, empezando polo eslavón máis débil da cadea, o persoal da organización. Moitas veces, pola falta de formación ou de preparación profesional, cometen descoidos ou negligencias que acaban poñendo en perigo á organización, co que, moitas veces é o persoal o utilizado de maneira inconsciente para acceder e atacar o sistema de información.
- Podemos tipificar as ameazas sobre a información en dous tipos:

- código malicioso e
- enxeñaría social.

## Código malicioso

O **código malicioso**, ou **malware**, é un programa que ten coma obxectivo introducirse e facer dano nun ordenador sen que o usuario o note.

Entre os obxectivos do malware, podemos comentar:

- Roubar información, datos persoais, contrasinais, números de conta
- Crear redes de ordenadores zombies, denominadas tamén botnet, para ser utilizados no envío masivo de spam, phishing, realizar ataques de denegación de servizo,...
- Cifrar o contido de determinados arquivos para solicitar o pago dunha cantidade para solventalo

## Virus

- É un código malicioso que ten coma **obxectivo alterar o funcionamento do ordenador sen o coñecemento do usuario**.
- Polo xeral, incorporan anacos de código infectado en arquivos executables, activándose os virus cando se executa ese arquivo. Nese momento, o virus, se aloxa na memoria RAM e se apodera dos servizos básicos do sistema operativo. Cando o usuario executa outro arquivo "executable", o virus aloxado na RAM o infecta tamén, para ir, desta forma, replicándose.
- Pode afectar ao funcionamento do software, hardware e ás propiedades da información, causando impacto, que pode abarcar dende leve a moi grave. Nestes momentos, as infeccións por virus son menos frecuentes que por gusanos ou troianos.

## Gusanos

- Realmente é un tipo de virus. As principais diferenzas entre gusano e virus é que, o gusano **non** necesita a intervención humana para ser propagado, faino automaticamente, non necesitado aloxarse en código anfitrión, é dicir **propágase de xeito autónomo, sen intervención dunha persoa que execute o arquivo infectado**. Soen apropiarse dos servizos encargados da transmisión de datos para controlalo.
- Polo xeral, os *gusanos* consumen moita memoria, facendo que os equipos non respondan axeitadamente.
- Un dos sistemas que utiliza o gusano para a súa **propagación** é enviarse a sí mesmo mediante **correo electrónico**, a aqueles contactos que se atopan no ordenador infectado. Moitos gusanos teñen, tamén, a capacidade de mutar, modificar automaticamente o seu propio código.

## troianos

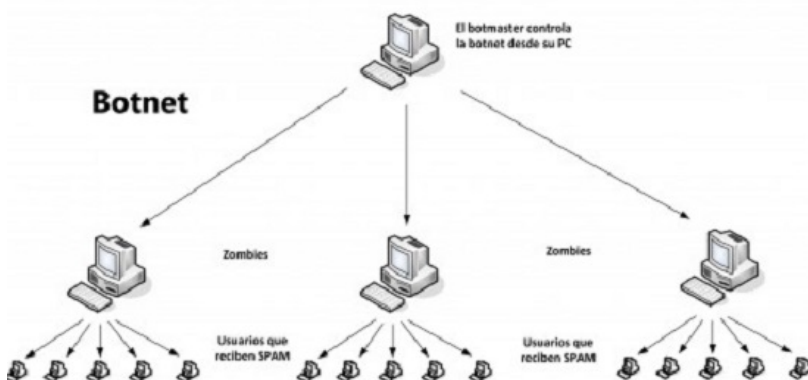
- Tamén son denominados **cabalos de Troia**, polo mito grego referente á Guerra de Troia, **un programa, aparentemente inofensivo, que ten unha función non desexada**.
- Son realmente un programa daniño con aparencia de software útil que pode acabar sendo unha grande ameaza contra o sistema informático.  
Nalgunhas ocasións son distribuídos como troianos outros tipos de virus como:

- **Portas traseiras:** modifican o sistema para permitir unha porta oculta de acceso ao mesmo, de xeito que o servidor toma posesión do equipo coma se fora propio, o que permite ter acceso a todos os recursos, programas, contrasinais, correo electrónico, unhas veces en modo vixilancia e, outras, para modificar a información e utilizala con fins non lícitos.
- **Keyloggers:** almacenan toda pulsación do teclado que realiza o usuario.
- **Spyware,** ou software espía: envía información do sistema ao exterior de forma automática.
- **Adware:** programas de publicidade que mostran anuncios, xeralmente mediante ventás emerxentes ou páxinas do navegador.

• Os equipos pódense infectar se executan algún programa non axeitado, con código maligno, xeralmente recibido por correo electrónico como adxunto ao mesmo ou ben, descargado de internet. Ás veces, tamén é posible que sexa instalado directamente no equipo por alguén con acceso físico ao mesmo.

### Bot malicioso

- Tamén son coñecidos como **robot web**. **Bot** é a **simplificación de robot**, trátase dun programa que **pretende emular o comportamento humano**.
- Moitos bots foron creados con fins lúdicos, por exemplo para manter un chat cunha persoa e, tomando como base as palabras que utilizaba, respondía ou preguntaba frases gramaticalmente correctas, xeralmente dun dicionario de frases que se incorporaba ao mesmo.
- Outros bots se utilizan como contrincantes ou compañeiros de xogo nalgúns programas que emulan xogos de mesa. Outros teñen como finalidade escribir poesía, artigos periodísticos ou blogs, etc.
- Tamén, os máis coñecidos e utilizados, son os bots de rastreo que utilizan os buscadores tipo Google ou Yahoo, e que teñen como finalidade detectar o movemento que se produce nos sitios web aos que enlazan e ofertan as novidades nas buscas dos usuarios.
- Os **bots maliciosos**, son realmente **troianos coa funcionalidade de porta traseira**, coa particularidade de que **se instalan** nos equipos vulnerables **mediante o sistema de rastreo en internet**. Unha vez infectado o equipo, o bot envía un sinal ao seu creador e o equipo empeza a formar parte dunha **botnet**, ou **rede de bots**.



- Aos bots se lles denomina **zombies**, pois cumpren as ordes que reciben dos ciberdelinquentes que os crearon.
- As tarefas que realiza un bot, de forma automática e transparente ao usuario, poden ser:
  - Reenviar spam e virus

- Roubar información, confidencial ou privada
- Enviar ordes de denegación de servizo a sitios web
- Facer clic automaticamente en anuncios publicitarios que pagan por cada clic efectuado. Quen se beneficia é o cibercriminoso que manexa a botnet e puxo o anuncio no seu sitio ou páxina web.

## Spyware

- É un código malicioso que, para instalarse nun ordenador, necesita a participación dun virus ou troiano, aínda que tamén pode estar oculto nos arquivos de instalación dun programa normal. O seu cometido é obter información acerca dos usuarios que utilizan ese ordenador. O obxectivo máis leve e máis común, é aportar eses datos a determinadas empresas de márketing online que, con posterioridade e por diferentes medios, correo electrónico, pop-ups, enviarán publicidade ao usuario sobre os temas que detectaron lles pode interesar.
- Estes programas espía poden indagar en toda a información existente no equipo, como listas de contactos, información recibida, enviada, por exemplo o dni, números de tarxetas de crédito, contas bancarias, domicilios, teléfonos, software que ten instalado, direccións ip, servidores de internet que utiliza, páxinas web que visita, tempo de permanencia nun sitio web, etc.
- Determinados programas espía poden causar danos tan importantes como a quebra de empresas por difundir información confidencial.
- Por outra parte, o spyware pode servir como sistema de detección de delitos cometidos a través de internet, é moi representativa a utilización pola Policía española de código malicioso incorporado a fotos de menores que permite identificar casos de corrupción de menores e pederastia.
- Os efectos que pode causar sobre un ordenador son moi variados, dende a utilización dalgún software instalado ou a aparición de xanelas emerxentes, ata a derivación dende unha páxina web legal a outra que é exactamente igual, pero ilegal.

## Virus de macro

- Tamén se denominan **macro virus**, son realmente un subtipo de virus que foron creados en macros inscritas en documentos, páxinas web, presentacións, etc. Se o ordenador da vítima abre un documento infectado, a macro pasará á biblioteca de macros da aplicación que a executa, co que a macro acabará por executarse nos diferentes documentos que se abran con esa aplicación.
- Os resultados da execución deste tipo de virus son moi variados, por exemplo, abrir un arquivo novo, auto-enviar o documento por correo electrónico a unha dirección definida na macro, realizar cálculos matemáticos erróneos, etc.

## Keylogger

- Son utilizados xeralmente para roubar contrasinais. Se inician co envío ao usuario de código malicioso que detecta as teclas que pulsa cando escribe o contrasinal, remitindo o mesmo ao usuario.
- Pode ser conseguido de igual forma mediante intrusión do código no ordenador do usuario, anotando todo o que vai atopando nos arquivos do mesmo.



## Enxeñaría social

- Unha **grande ameaza** sobre o software e a información é a **enxeñaría social**. Esta consiste en obter información a través das persoas que a utilizan. Non é necesario recorrer a programas complexos, código malicioso ou estratexias para entrar en sistemas informáticos utilizando portas traseiras e aproveitando as vulnerabilidades do software ou sistema operativo.



- Realmente consiste na utilización dos tradicionais e moi antigos métodos de engano e timo, pero utilizados a nivel informático, baseándose na natural tendencia humana a confiar, mantendo a máxima de que o ser humano é o eslavón máis débil da cadea, cando nos estamos a referir á seguridade dos sistemas de información.
- O **método principal** que se utiliza para este fraude é o **correo electrónico**, sendo os argumentos moi variados.
- En moitos casos, a **orixe** destas cadeas é unha persoa ou organización que se atopa interesada en **obter direccións** de correo electrónico **para**, posteriormente, **enviarlles spam**.
- Un email deste tipo multiplícase en progresión aritmética ou exponencial, co que tarde ou cedo, o **emisor** volve a recibilo, pero tendo xa **averiguados centos de direccións de email**.
- Outro dos seus obxectivos é **colapsar** os **servidores de correo**.

Se vos interesa este tema, invitámosvos a ler [Ingeniería social, eludiendo el "firewall humano"](#)  
Se non podes visualizar este vídeo, fai clic na seguinte ligazón [Estafas de impostores de negocios de soporte técnico](#)

Podedes atopar máis vídeos interesantes proporcionados pola [Federal Trade Commission](#), en [Vídeos y Multimedia](#)

## Correos millonarios

- Apelan á ambición das persoas por obter cartos de forma doada.
- Dende os primeiros que apareceron nos que se anunciaba que unha persoa morrera sen herdeiros e deixando unha moi importante fortuna, se seguías as instrucións do correo, ata os recentes correos da lotería dos nixerianos, que prometen entregar unha cantidade moi importante de cartos se facilitas unha conta corrente nun banco para que eles podan ingresar o premio da lotería gañada.

## Phishing

- Palavra parecida ao termo inglés de *pescar*, *fishing*, pero coa *p* de *password*.

- É un dos métodos máis frecuentes de recollida de contrasinais con fins de suplantación de identidade.

- Pode chegar a través dun **correo electrónico** de xente descoñecida ou de sitios web de pouca confianza pero, en ocasións, parece que provén de contactos coñecidos, bancos ou organismos oficiais. Por tratarse de correos de fontes de confianza, aumentas as posibilidades de que a vítima chegue a caer na trampa.

- Un exemplo típico é o de que a vítima recibe un correo electrónico de parte do director de seu banco no que lle comunica que o novo método de acceder á súa banca electrónica é pulsando sobre un enlace que lle envía e que, realmente, apunta a unha web fraudulenta con aparencia similar á real. O fin deste método é o de facerse co seu usuario e password reais das súas contas bancarias reais, para logo tentar operar con elas no seu nome.



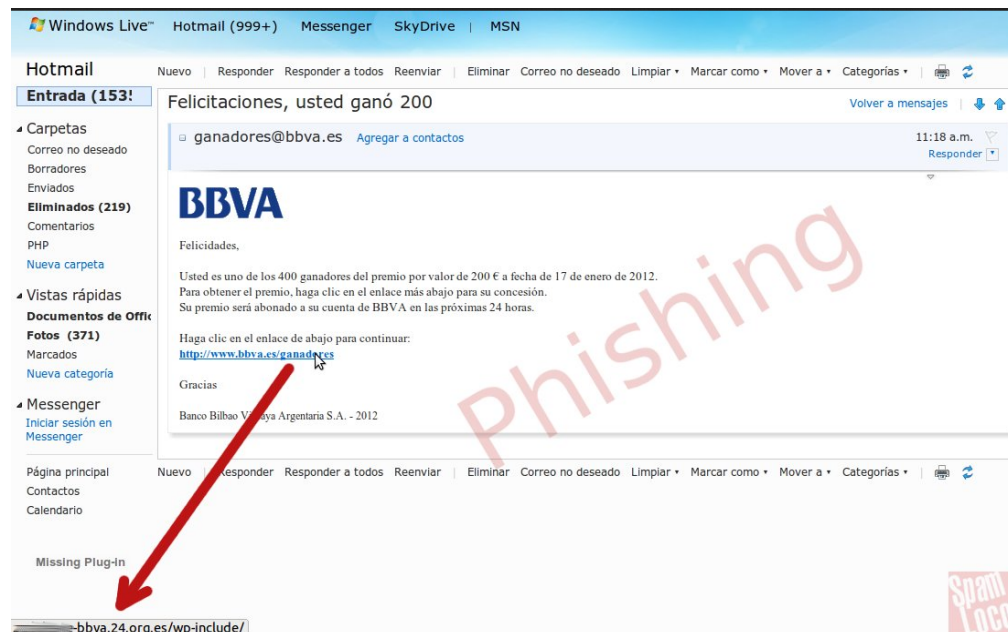
### Exemplos de Phishing

Mostramos algúns exemplos de casos claros e reais de phishing

Neste primeiro caso, unha páxina que trata de enganar, facéndose pasar por BBVA, solicita a introdución de información da tarxeta:

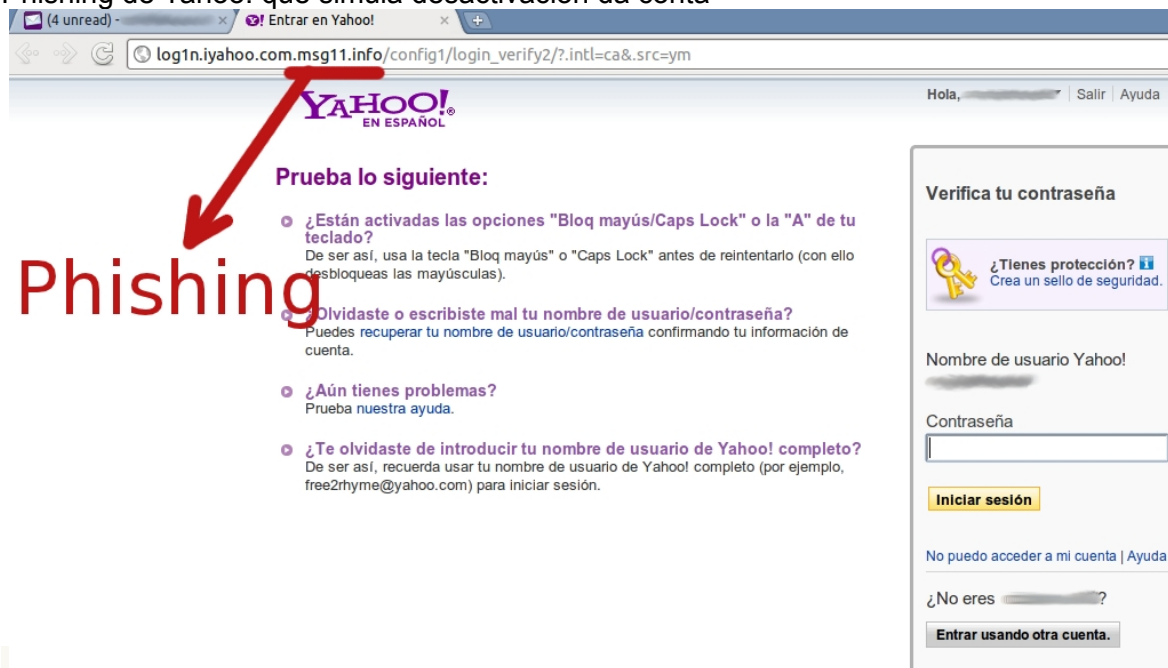
**Solicitan datos de la tarjeta para robarlos**

Correo falso que simula ser enviado polo banco:



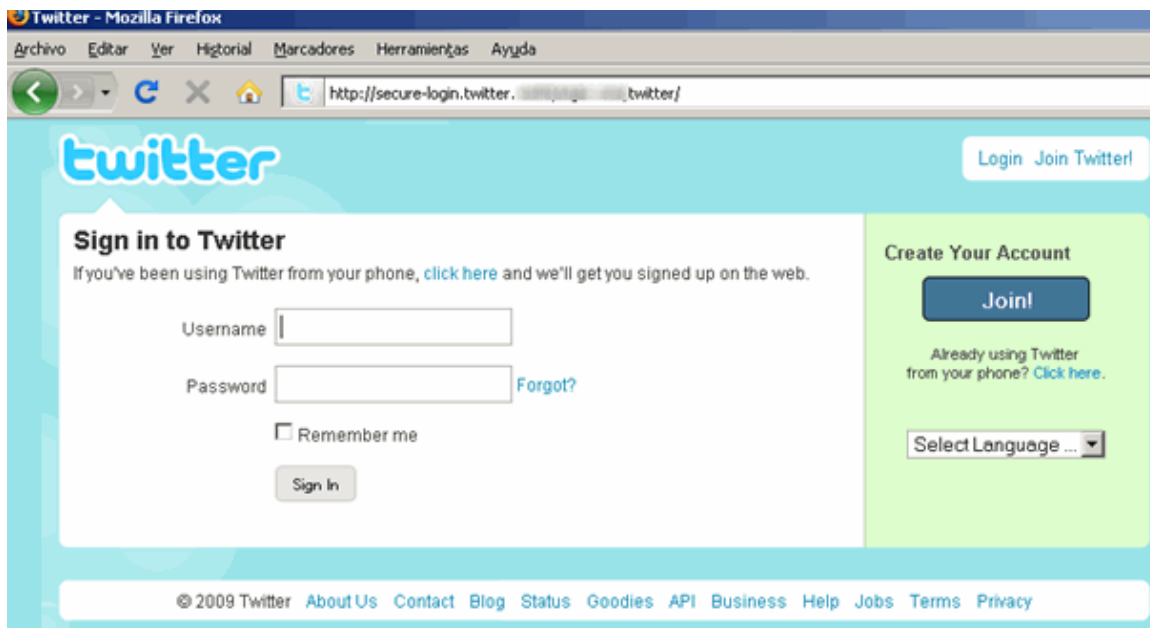
Phishing de Yahoo!

Phishing de Yahoo! que simula desactivación da conta



Phishing twitter

Trátase da clonación da páxina de autenticación para acceder ao perfil en Twitter:



## Intrusismo

O intruso informático selecciona sistemas informáticos ou servidores web para tomar o control dos mesmos mediante técnicas de [hacking](#), xeralmente utilizando a enxeñaría social de xeito remoto.

Dependendo dos coñecementos que teñan sobre técnicas de hacking e da acción que exerzan sobre as redes, servidores ou equipos que invaden, pódense derivar moitas definicións:

- Hacker
- Cracker
- Phreaker
- Script kiddie
- Newbie

## Hacker

- [Hacker](#) é realmente o nome xenérico que se da aos intrusos informáticos pero, na realidade, o hacker é o único que defende un código ético para as súas intrusións, chegando a ser definido, en diferentes situacións como [hacking ético](#).
- Chega a coñecer en profundidade as linguaxes de programación, as instrucións e protocolos de comunicación das redes de ordenadores para poder introducirse nelas con privilexios de administrador.
- O seu código ético inclúe o [non realizar dano sobre os equipos nos que consegue entrar, nin revelar a terceiros a información obtida](#), atopándose aínda cuestionada a ética ao entrar de forma non lícita na privacidade de persoas e entidades.

Se non podes visualizar o seguinte vídeo, fai clic na ligazón [Hacking y anonimato: para pasar un buen rato: Chema Alonso at TEDxRetiro](#)

**Curiosidade.** Fíxadevos neste artigo: [Telefónica nombra al 'hacker' Chema Alonso como jefe de datos](#)

## Cracker

- Utiliza as técnicas de hacking pero para [beneficio propio e causando dano nos sistemas nos que entra](#).
- Definimos a unha persoa como **cracker** cando:
  - Mediante [enxeñería inversa](#) realiza seriais, *keygens* e [cracks](#), que serven para modificar o comportamento, ampliar a funcionalidade etc. Por exemplo, pódense utilizar para saltarse restriccións, como que un programa deixe de funcionar nun determinado tempo, ou que só funcione se é instalado dende un CD orixinal.
  - Salta a seguridade dun [sistema informático](#) e toma o control do mesmo, obtén información, modifícaa, bórraa, etc.
- Podedes atopar na seguinte ligazón unha boa explicación sobre [qué é un Cracker e en que se diferencia dun Hacker](#)

## Phreaker

- Persoa con experiencia en redes de telecomunicación, tendo coma obxectivo os terminais e redes telefónicas.
- Polo tanto o [Phreaker](#) podemos dicir que é o [Hacker dos sistemas telefónicos](#), telefonía móvil, tecnoloxías inalámbricas e el Voz sobre IP (VoIP).
- Un phreaker é unha persoa que investiga os sistemas telefónicos, mediante o uso de tecnoloxía polo pracer de manipular un sistema tecnolóxicamente complexo e, en ocasións tamén para poder obter algún tipo de beneficio como chamadas gratuitas.

## Script kiddie

- É unha persoa que non ten coñecementos de técnicas de hacking, pero utiliza as ferramentas xeradas por expertos para realizar os seus ataques.
- Son os que realizan a maior parte de roubos de contrasinais e intromisións con danos.
- En xeral considérase que os script kiddies son inmaduros e perezosos, e definitivamente non son hackers. É un perfil non apreciado entre os restantes hackers. Ser un script kiddie non che traerá ningún recoñecemento na comunidade hacker.

## Newbie

Realmente son os hackers novatos, que se atopan en período de aprendizaxe das técnicas de hacking.

## Proceso de hacking

A aprendizaxe de técnicas de hacking require moito tempo e coñecementos profundos de todas as ferramentas necesarias para detectar vulnerabilidades, conseguir entrar nos sistemas e non deixar rastro.

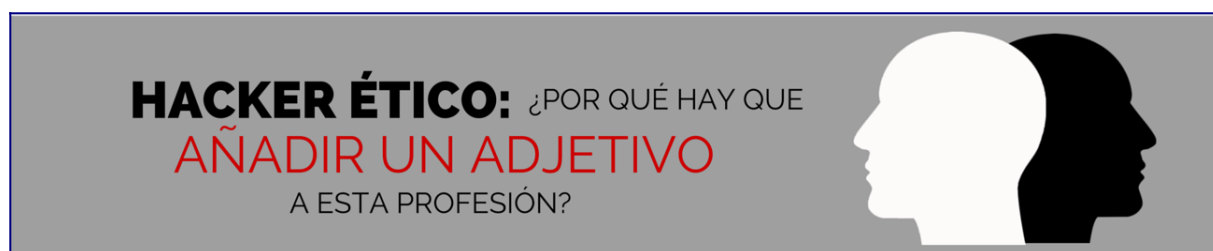
O proceso lóxico é similar ao seguinte:

- Decidir cal será a máquina obxectivo
- Obter información sobre o sistema obxectivo, portos abertos, equipos que compoñen a rede, as IPs privadas de cada ordenador, proveedor de acceso a internet.
- Detectar as medidas de seguridade e posibles vulnerabilidades
- Aproveitar as vulnerabilidades para acceder aos rexistros de contrasinais

- Facerse cunha conta de administrador, conseguindo o control total do sistema.
- Consegur manter o acceso ao sistema
- Manter o traballo metódico e prudente, de forma inadvertida para os administradores do equipo da vítima

## Ferramentas de hacking

- As ferramentas utilizadas para o acceso de hacking, independentemente dos fins que persiga son:
  - Comandos do sistema operativo
  - Ferramentas para escanear redes e sistemas
  - Ferramentas para manipular redes cabreadas e sen fíos
  - Ferramentas de auditoría de sistemas para detectar vulnerabilidades
  - Ferramentas de rastrexo de páxinas web
  - Ferramentas de ataque



- Dúas páxinas interesantes nas que podedes atopar información sobre ferramentas de Hacking:
  - [8 Aplicaciones Para Convertirse En Hacker](#)
  - [Algunas de las mejores herramientas de hacking de 2016](#)

## Contornas de risco

- Un sistema informático pode ser atacado directamente a través do correo electrónico, mensaxería instantánea, canles de chat ou dispositivos extraíbles...
- As vulnerabilidades do sistema informático son aproveitadas de xeito técnico, ou utilizando os usuarios que o manexan.

## Computación na nube

- A computación na nube é unha das características da Web 2.0. Son moitas as empresas que utilizan a nube para manter gardados os seus arquivos e datos en servidores de diversos provedores específicos, tanto no seu país de orixe como noutros países, próximos ou lonxanos, con [moi diferentes, e nalgúns casos inexistentes, leis de protección de datos](#).
- O almacenamento na nube permite non só facer realidade a posibilidade de mobilidade, gardando os nosos arquivos e permitinto acceder a eles dende calquera kugar do mundo, senón tamén traballar en documentos colaborando con outros usuarios e accedendo a eles dende os múltiples dispositivos que utilizamos.
- Estes grandes centros de datos [contan coas maiores medidas de seguridade redundante](#), física ou lóxica, e grandes medios humanos e técnicos, o que proporciona unha garantía de cara aos seus clientes.
- A oferta é moi ampla e todos os servizos ofrecen versións gratuitas cunha cantidade de espazo base. Entre a oferta que podemos atopar na actualidade para almacenamento na nube, citaremos [Dropbox](#), [Google Drive](#), [OneDrive](#), [Box](#), [iCloud](#), [MEGA](#), ...



- Os [intrusos](#) teñen entre os seus [principais obxectivos estes grandes centros de datos](#), os cales están continuamente recibindo ataques.

## Redes sociais

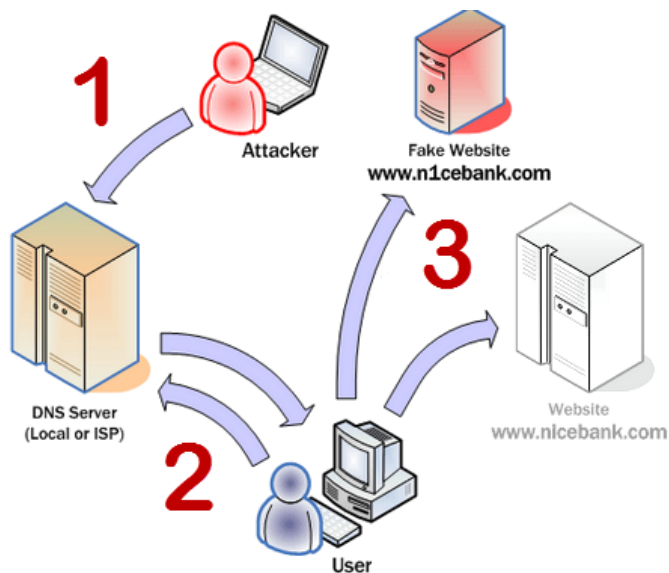
- A [redes sociais](#) son un medio idóneo para distribuír código malicioso pola grande cantidade de usuarios que as utilizan.
- Un dos [perigos](#) aos que se enfrontan é o do [roubo de identidade](#) e o [intercambio de código malicioso](#).
- Son as redes sociais [un dos obxectivos prioritarios dos intrusos](#), que manteñen o obxectivo de roubar datos persoais utilizando a enxeñaría social, de feito, unha das grandes preocupacións das organizacións é a excesiva publicación de información persoal dos seus empregados.

Se queres afondar neste tema, consulta

- [Peligros de las redes sociales](#)
- [Riesgos y peligros de las redes sociales en Internet](#)
- Artigo de La Opinión: [Esto es lo que debes saber para evitar ser víctima de robo de identidad](#)
- [Comisión Federal de Comercio. Robo de Identidad](#)
- [Robo de identidad](#)

## Servidores de dominio

- Os [servidores de dominio](#) son outro dos obxectivos dos intrusos.
- Cada equipo conectado directamente a Internet terá polo menos un enderezo IP específico. Pero os usuarios no queren traballar con enderezos numéricos, senón con nomes de dominio que poidan recordar máis facilmente, por exemplo [www.edu.xunta.es](#), e para asociar os dous enderezos naceu [DNS](#) (Sistema de Nombres de Dominio).
- [DNS](#) é como un sistema de preguntas e respostas. Cando escribimos un enderezo no navegador, por exemplo [www.edu.xunta.es](#), este preguntará aos servidores DNS cal é o enderezo IP, no noso caso devolverá como resposta [10.180.188.38](#) e despois xa poderá lanzar unha petición HTTP a ese enderezo IP para obter a páxina web correspondente.
- Existen distintas formas de atacar a un servidor DNS ou de conseguir que un equipo consulte cun servidor DNS que non sexa quen di ser. Por exemplo:
  - Atacando os servidores DNS, un intruso pode chegar a modificar a relación entre nome de dominio e ip e chegar a desviar o tráfico dirixido a unha páxina, cara outra, moitas veces de aparencia idéntica á orixinal para, ben utilizar técnicas de phishing sobre os usuarios que están a navegar sobre ela, ben solicitar un rescate á organización por recuperar o control da mesma. Esta técnica de enxeñaría social se denomina [pharming](#), moi relacionado co [phishing](#).



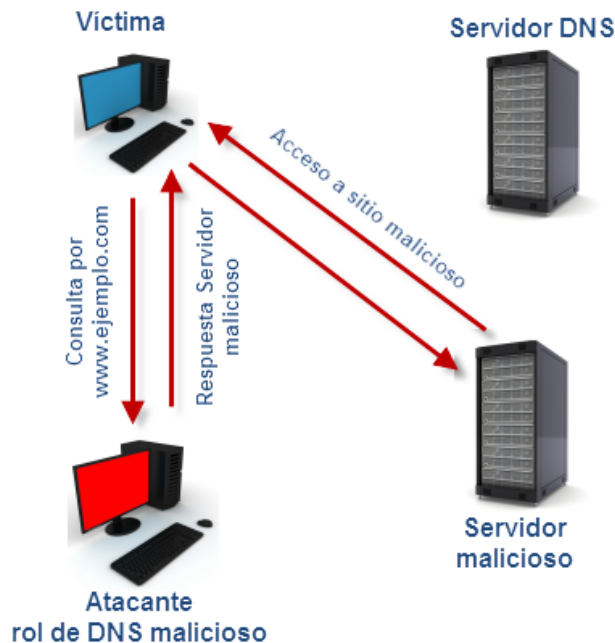
Imaxe derivada por [Gabriel Ferreiro](#), [Ana Veloso](#), [CC BY SA](#), da orixinal de [Wiki Ciberseguridad](#) [CC BY SA](#)

Mostramos a continuación un exemplo de Pharming (a primeira imaxe corresponde ao servidor web orixinal e a segunda, á do intruso). Podedes acceder á páxina web onde examinan este exemplo [Oficina de Seguridad del Internauta](#).



- Outra posibilidade é o [DNS spoofing](#) que consiste en alterar os enderezos IP dos servidores DNS aos que a vítima vai preguntar, de xeito que agora consultarán a outros "Servidores DNS maliciosos".

Podedes atopar información moi clara en [DNS Spoofing. ¿en qué consiste?](#)



## Páxinas web

O proceso de navegar por internet está cheo de perigos de infección por virus, gusanos, troianos, etc. Non é necesario entrar en páxinas non fiables, [calquera páxina web pode ser atacada por hackers e infectada con código malicioso](#), incorporando un risco grande a aqueles usuarios que navegan polas mesmas, descargando sen darse conta o código malicioso, risco que se mantén ata que os responsables da web se dan conta da infección e logran poñerlle freo.

## Redes p2p

- A definición deste concepto é unha [rede de ordenadores](#) que funciona sen necesidade de contar nin con clientes nin con servidores fixos, senón que son unha serie de nodos [con un comportamento igual entre sí](#). De ahí o nome de [rede de pares ou iguais](#).
- Isto quere dicir que actúan de maneira simultánea como clientes e servidores con respecto aos demais nodos que ten a rede. Este tipo de funcionamento permite o intercambio directo de información, en calquera formato, entre todas as computadoras interconectadas.
- Polo tanto [permiten descargar arquivos de outros usuarios](#) ao mesmo tempo que os [ceden para que outros os descarguen](#). Aínda que o seu uso se estendeu enormemente por toda a rede, non todo o mundo sabe que estes sistemas de intercambio de información [teñen os seus riscos](#).

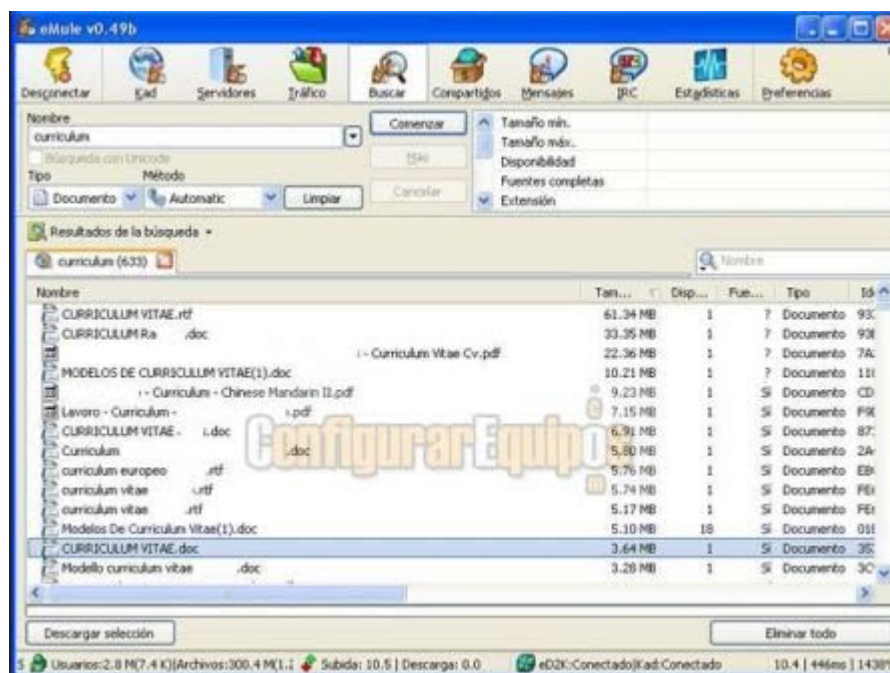


Se queres ler máis sobre P2P: [tecnología-fácil](#)

- Este sistema de intercambio de arquivos e información, é un dos grandes medios que se utilizan para **infectar código malicioso**, sendo relativamente sinxelo incorporar pequenos anacos de código entre a grande cantidade de información a intercambiar.

Se queres máis información sobre os seus riscos das redes P2P, podes acceder a [Hijos Digitales](#).

Exemplo de información privada á que se podería ter acceso, simplemente buscando a palabra currículum:



## Enderezos interesantes

Por último facilitámosvos algunhas ligazóns que nos parecen interesantes, con artigos ou vídeos relacionados coa seguridade na rede.

- [Pantallas amigas](#)
- [Comisión Federal de Comercio](#)
- [Magazcitur](#)
- [timos.info](#)
- [Secure&IT](#)
- [welivesecurity](#)

# Seguridade no software e na rede

Introducirémonos neste tema naquelas vulnerabilidades que afectan á seguridade do software e cales son as precaucións e medidas proactivas e reactivas que deben ser tomadas para evitar os danos que podan afectar á información que se mantén no sistema informático.

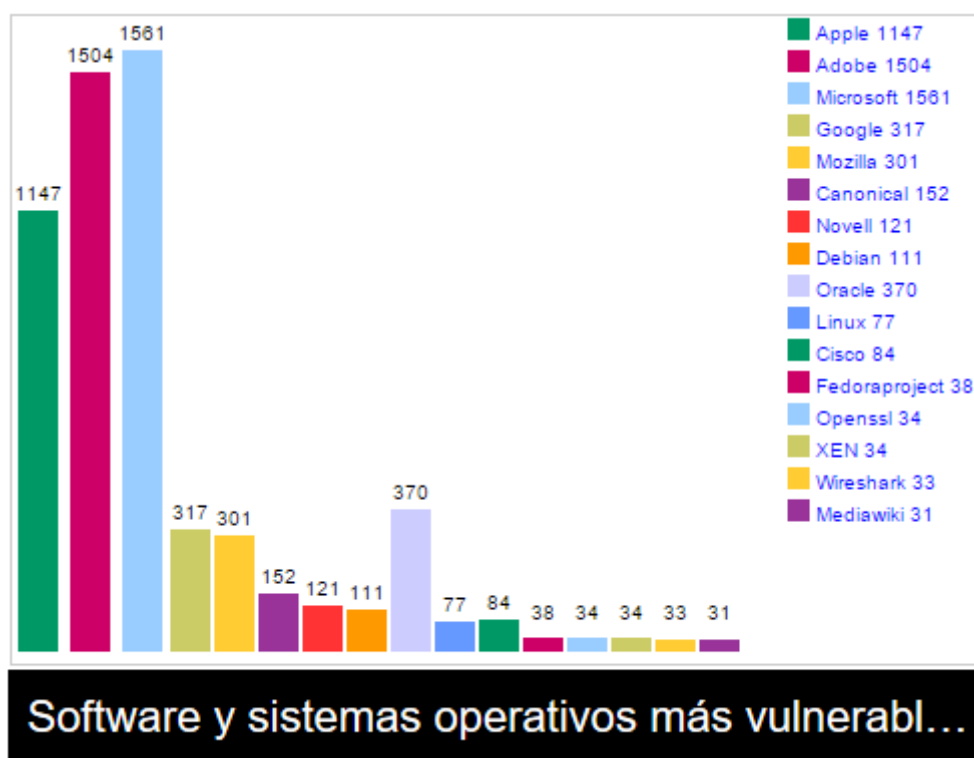
Estudaremos tamén cales son os medios de seguridade que se deben implementar nas redes de ordenadores para evitar ameazas á seguridade dos equipos informáticos e á información que conteñen.

A nivel resumido debemos ter tres elementos instalados e coa última versión en todos os nosos sistemas operativos:

- Antivirus potente con funcións de detección de programas espías "Spyware"
- Cortalumes, devasa ou firewall activado. Evitará ataques a nivel de redes.
- Últimas actualizacións do sistema operativo.

## Software e Sistemas Operativos con máis vulnerabilidades de 2015

Os resultados mostrados son recollidos por [CVE Details](#) e recopilados pola **National Vulnerability Database**, unha base de datos estadounidense que inclúe todo tipo de erros de seguridade, fallos de software e demais vulnerabilidades.



|    | Product Name                           | Vendor Name               | Product Type | Number of Vulnerabilities |
|----|----------------------------------------|---------------------------|--------------|---------------------------|
| 1  | <a href="#">Mac Os X</a>               | <a href="#">Apple</a>     | OS           | <a href="#">384</a>       |
| 2  | <a href="#">Iphone Os</a>              | <a href="#">Apple</a>     | OS           | <a href="#">375</a>       |
| 3  | <a href="#">Flash Player</a>           | <a href="#">Adobe</a>     | Application  | <a href="#">314</a>       |
| 4  | <a href="#">Air Sdk</a>                | <a href="#">Adobe</a>     | Application  | <a href="#">246</a>       |
| 5  | <a href="#">AIR</a>                    | <a href="#">Adobe</a>     | Application  | <a href="#">246</a>       |
| 6  | <a href="#">Air Sdk &amp; Compiler</a> | <a href="#">Adobe</a>     | Application  | <a href="#">246</a>       |
| 7  | <a href="#">Internet Explorer</a>      | <a href="#">Microsoft</a> | Application  | <a href="#">231</a>       |
| 8  | <a href="#">Chrome</a>                 | <a href="#">Google</a>    | Application  | <a href="#">187</a>       |
| 9  | <a href="#">Firefox</a>                | <a href="#">Mozilla</a>   | Application  | <a href="#">178</a>       |
| 10 | <a href="#">Windows Server 2012</a>    | <a href="#">Microsoft</a> | OS           | <a href="#">155</a>       |
| 11 | <a href="#">Ubuntu Linux</a>           | <a href="#">Canonical</a> | OS           | <a href="#">152</a>       |
| 12 | <a href="#">Windows 8.1</a>            | <a href="#">Microsoft</a> | OS           | <a href="#">151</a>       |
| 13 | <a href="#">Windows Server 2008</a>    | <a href="#">Microsoft</a> | OS           | <a href="#">149</a>       |
| 14 | <a href="#">Windows 7</a>              | <a href="#">Microsoft</a> | OS           | <a href="#">147</a>       |
| 15 | <a href="#">Windows 8</a>              | <a href="#">Microsoft</a> | OS           | <a href="#">146</a>       |
| 16 | <a href="#">Windows Rt 8.1</a>         | <a href="#">Microsoft</a> | OS           | <a href="#">139</a>       |
| 17 | <a href="#">Windows Rt</a>             | <a href="#">Microsoft</a> | OS           | <a href="#">138</a>       |
| 18 | <a href="#">Windows Vista</a>          | <a href="#">Microsoft</a> | OS           | <a href="#">135</a>       |
| 19 | <a href="#">Safari</a>                 | <a href="#">Apple</a>     | Application  | <a href="#">135</a>       |
| 20 | <a href="#">Android</a>                | <a href="#">Google</a>    | OS           | <a href="#">130</a>       |

## Recursos de seguridade no sistema operativo

As organizacións que desenvolven os [Sistemas Operativos](#) actuais, manteñen, cando se detectan vulnerabilidades, [os seus propios procesos de actualización e publicación de parches](#), diferentes medios polos que os usuarios dos mesmos poden:

- descargar o software para corrixir as mesmas, ou
- incorporarse aos procedementos automáticos para realizalo.

Algúns exemplos recentes

[Un fallo en Windows 10 permite acceder a los datos cifrados con BitLocker](#)

[El cifrado de Android está muy por detrás del que usa Apple en iOS](#)

[iOS y OS X ya tienen más vulnerabilidades que Windows](#)

[Las vulnerabilidades de Android más importantes en 2016](#)

[Cinco vulnerabilidades comunes de Linux para tener en cuenta](#)

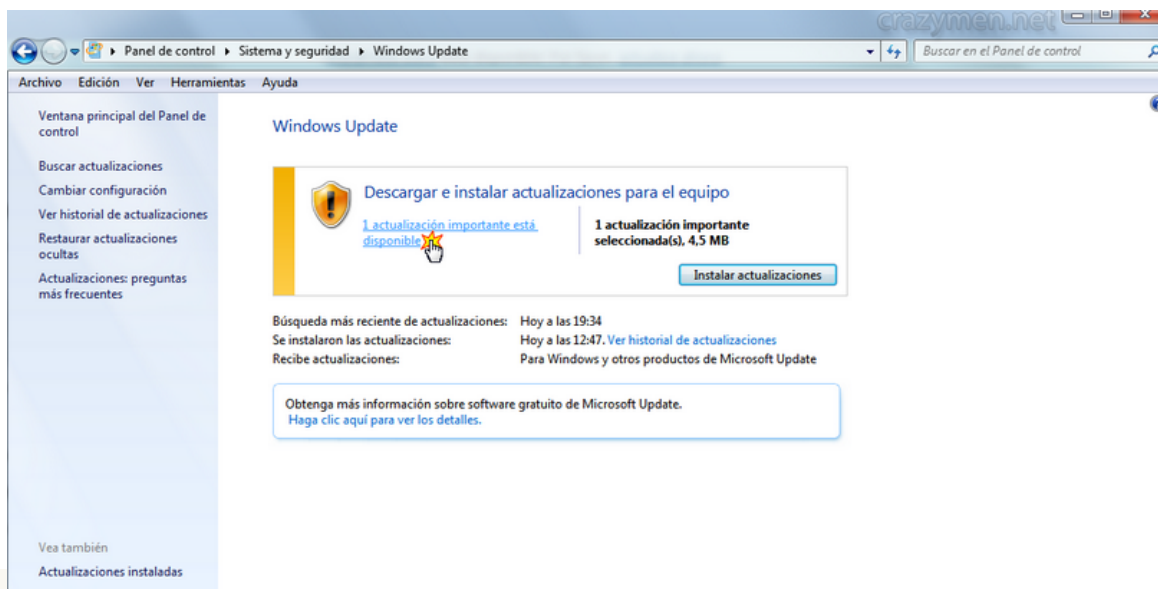
[Apple soluciona 173 vulnerabilidades](#)

Podedes atopar máis exemplos en [softzone](#)

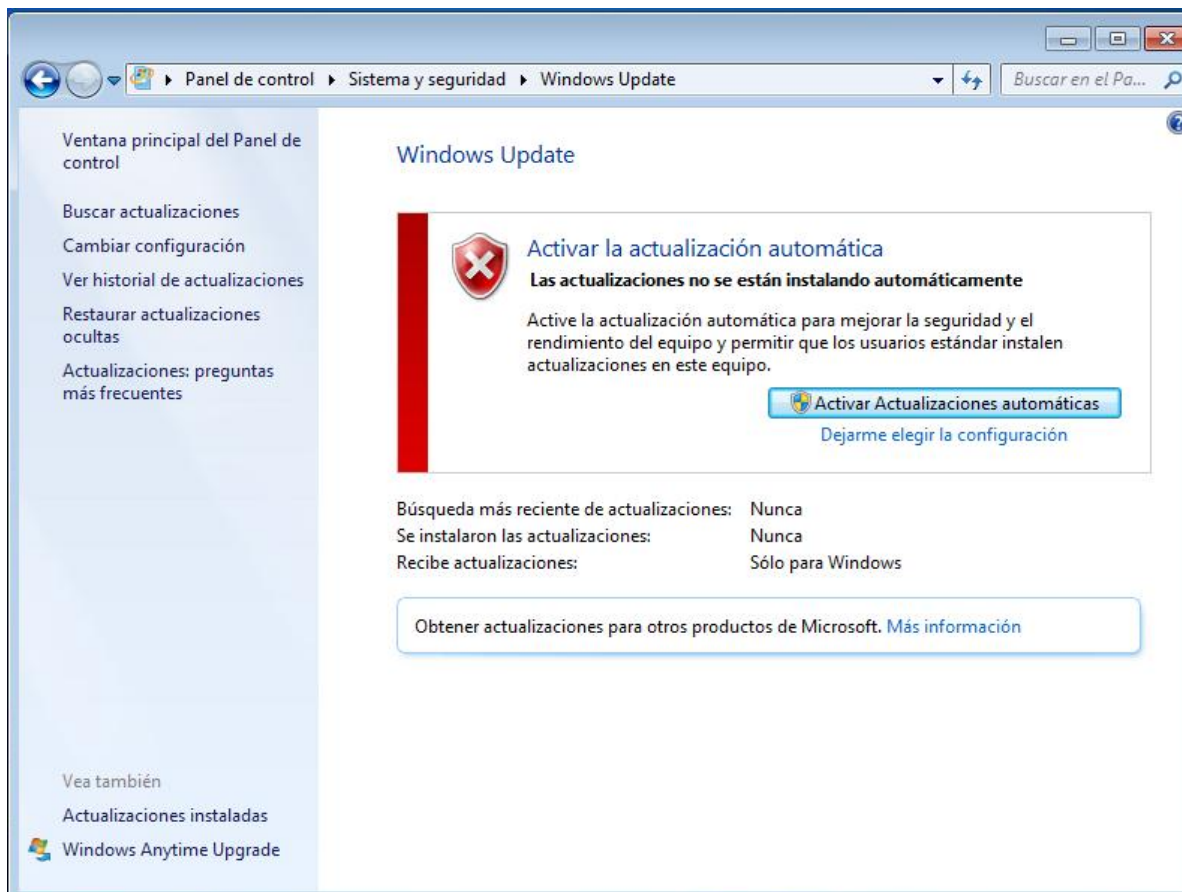
Exemplos actualizacións Sistema Operativo Windows.

Actualización Windows:





Activar Actualización automática Windows:



Exemplos actualizaci3n Sistema Operativo Ubuntu

Actualizaci3n Ubuntu:

Actualización de software

 Hay actualizaciones de software disponibles para este equipo. ¿Quiere instalarlas ahora?

▼ Detalles de las actualizaciones

| Instalar                                                                                                                                                                                          | Descarga       |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| <input checked="" type="checkbox"/>  Gestor de paquetes Synaptic                                                 | 1,4 MB         |
| <input checked="" type="checkbox"/>  SMPlayer                                                                    | 2,7 MB         |
| <input checked="" type="checkbox"/>  Minimal subset of the Python language (default python3 version)             | 24 kB          |
| <input checked="" type="checkbox"/>  <b>Base de Ubuntu</b>                                                       | <b>10,8 MB</b> |
| <input checked="" type="checkbox"/>  Access software for a blind person using a braille display                  | 1,1 MB         |
| <input checked="" type="checkbox"/>  Access software for a blind person using a braille display - xbrlapi        | 59 kB          |
| <input checked="" type="checkbox"/>  Braille display access via BRLTTY - Python3 bindings                        | 64 kB          |
| <input checked="" type="checkbox"/>  Braille display access via BRLTTY - shared library                          | 21 kB          |
| <input checked="" type="checkbox"/>  Converts MS Word files to text, PS, PDF and XML                             | 127 kB         |
| <input checked="" type="checkbox"/>  Core Perl modules                                                           | 2,6 MB         |
| <input checked="" type="checkbox"/>  Daemon to balance interrupts for SMP systems                                | 31 kB          |
| <input checked="" type="checkbox"/>  Default settings for the Ubuntu desktop                                     | 5 kB           |
| <input checked="" type="checkbox"/>  High level tools to configure network interfaces                            | 55 kB          |
| <input checked="" type="checkbox"/>  Interactive high-level object-oriented language (default python3 versi...  | 9 kB           |
| <input checked="" type="checkbox"/>  Interactive high-level object-oriented language (default python3 versi... | 7 kB           |
| <input checked="" type="checkbox"/>  IP lookup command line tools that use the GeoIP library (country data...  | 1,6 MB         |
| <input checked="" type="checkbox"/>  Larry Wall's Practical Extraction and Report Language                     | 238 kB         |
| <input checked="" type="checkbox"/>  Library to generate ODF documents                                         | 194 kB         |
| <input checked="" type="checkbox"/>  Minimal Perl system                                                       | 1,3 MB         |
| <input checked="" type="checkbox"/>  Shared Perl library                                                       | 3,3 MB         |

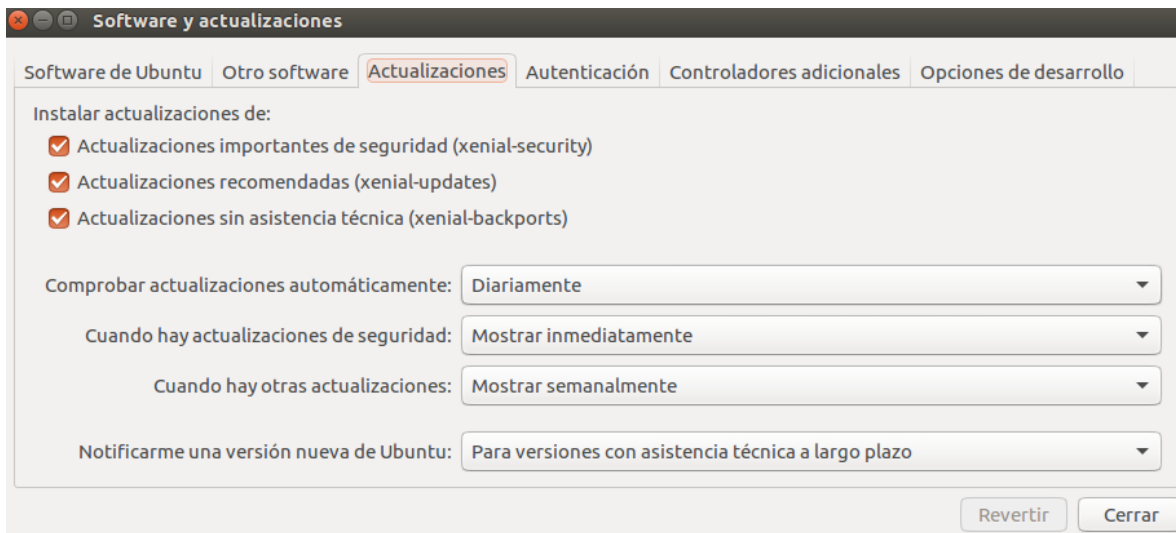
► Descripción técnica

 Se descargarán 14,8 MB.

Configuración... Recordármelo más tarde Instalar ahora

Imaxes derivadas por [Gabriel Ferreira](#), [Ana Veloso](#), [CC BY SA](#), da orixinal de [winlux](#) [CC BY SA](#)

Activar actualizaci3ns autom3ticas:

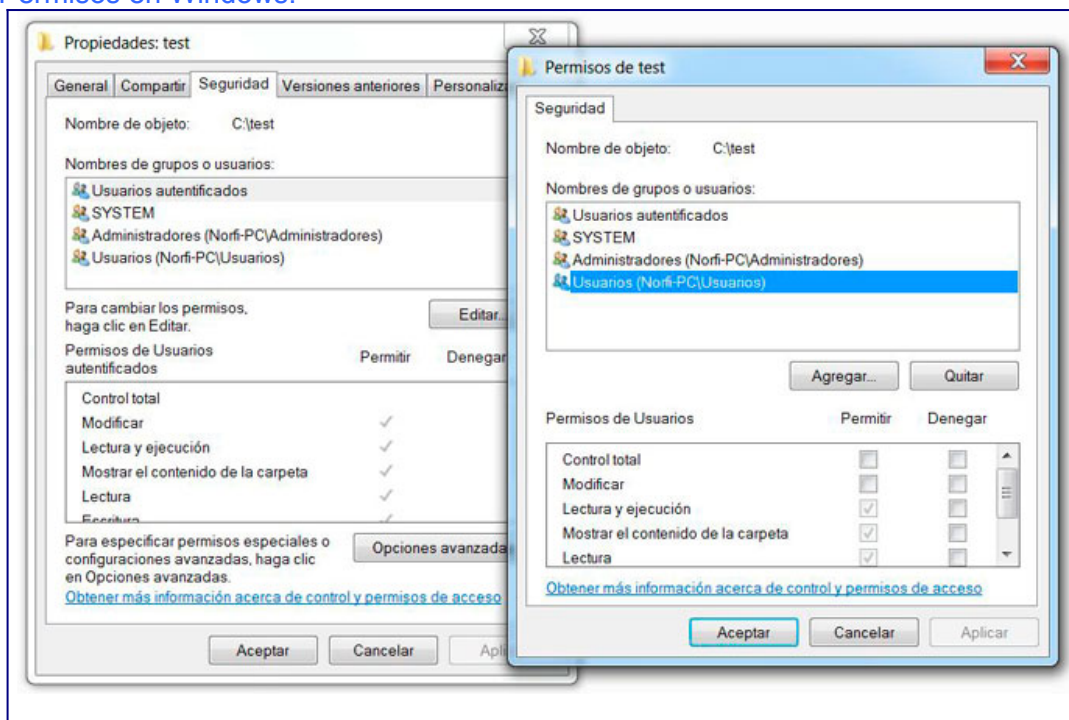


## Contas de usuarios

- As contas de usuarios son unha característica dos sistemas operativos que axuda a evitar cambios non autorizados no equipo informático.

Os usuarios e os permisos para os mesmos, defínense, créanse, elimínanse ou modifícanse, dende as ferramentas da interfaz que cada sistema operativo proporciona, ou dende a liña de comandos.

## Permisos en Windows:



Tamén podes atopar información sobre permisos en Windows 7 na ligazón [support.microsoft.com](http://support.microsoft.com)

**Permisos en Linux** (máis información sobre cómo facelo, pulsando na ligazón ou na imaxe):

|            |   |      |      |        |            |       |             |
|------------|---|------|------|--------|------------|-------|-------------|
| drwxr-xr-x | 3 | raul | raul | 4096   | 2005-02-16 | 14:47 | Desktop     |
| drwxr-xr-x | 5 | raul | raul | 4096   | 2005-02-16 | 14:47 | GNUstep     |
| -rw-r--r-- | 1 | raul | raul | 246417 | 2005-03-03 | 14:47 | foto1.png   |
| -rw-r--r-- | 1 | raul | raul | 232505 | 2005-03-03 | 16:26 | carta2.abw  |
| -rw-r--r-- | 1 | raul | raul | 239618 | 2005-03-03 | 18:15 | informe.abw |
| drwxr-xr-x | 2 | raul | raul | 4096   | 2005-02-16 | 14:47 | tmp         |

Tamén podes atopar información sobre asignación de permisos en Ubuntu en [ite.educacion.es](http://ite.educacion.es)

- Os roles aos que se asignan estas contas, poden ser
  - **Root ou Administrador:** con permisos de administración do sistema
  - **Usuario estándar:** con permisos unicamente para o seu entorno de traballo
  - **Usuarios especiais:** cos tipos de permisos que determine, en cada caso, o administrador

### Uso das contas de usuario

- A conta de **administrador**, en calquera dos sistemas operativos, permite facer ao seu posuidor, calquera tipo de cambios.
- É conveniente que **non** exista **máis dunha conta de administrador nun mesmo equipo**, en cambio, poden ser creadas varias contas de usuario con case as mesmas competencias que as de administrador, pero coa excepción de aqueles permisos que permitan realizar cambios que podan afectar á configuración de seguridade de outros usuarios, ademais de non poder instalar software.
- Por outra banda, **para realizar traballo cotián, é preferible utilizar unha conta estándar**, en lugar da de administrador, para evitar que, ante a entrada de calquera intruso, poda ser obtida esta.
- Ligazóns de interese:
  - [Windows 8.1: Administrar las cuentas de usuario](#)
  - [Cómo administrar las cuentas de usuario en Windows 10](#)
  - [Gestionar usuarios y grupos en Ubuntu](#)
  - [Usuarios y grupos de usuarios en Linux](#)

Se non podes acceder ao seguinte vídeo fai clic na ligazón [Crear cuentas usuario en Ubuntu 16.04](#)

### Devasas

- Unha das ferramentas das que dispoñen os sistemas operativos, son as **devasas** ou **firewalls**, que impiden a entrada de intrusos e programas maliciosos a



través da rede, de igual forma que controlan que non poda saír malware cara outros equipos.

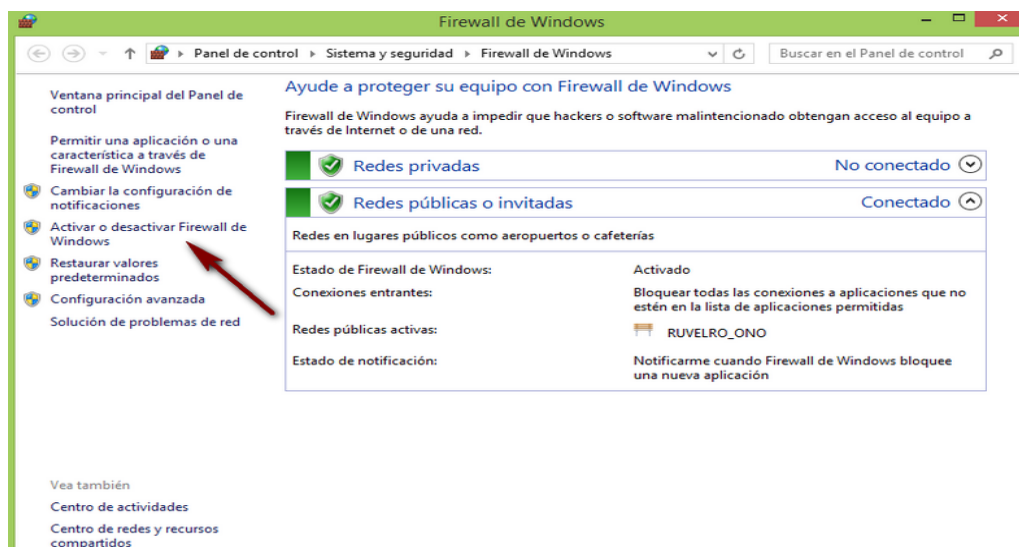
- É o propio usuario o que determina o grao de activación que prefire en cada momento, [permitindo ou denegando a conexión dende o exterior ao seu equipo](#), así como as [reglas que permitan o filtrado, por exemplo, por perfil, rol, por grupo de usuarios, etc.](#)

Para saber máis, podes facer clic nesta imaxe:

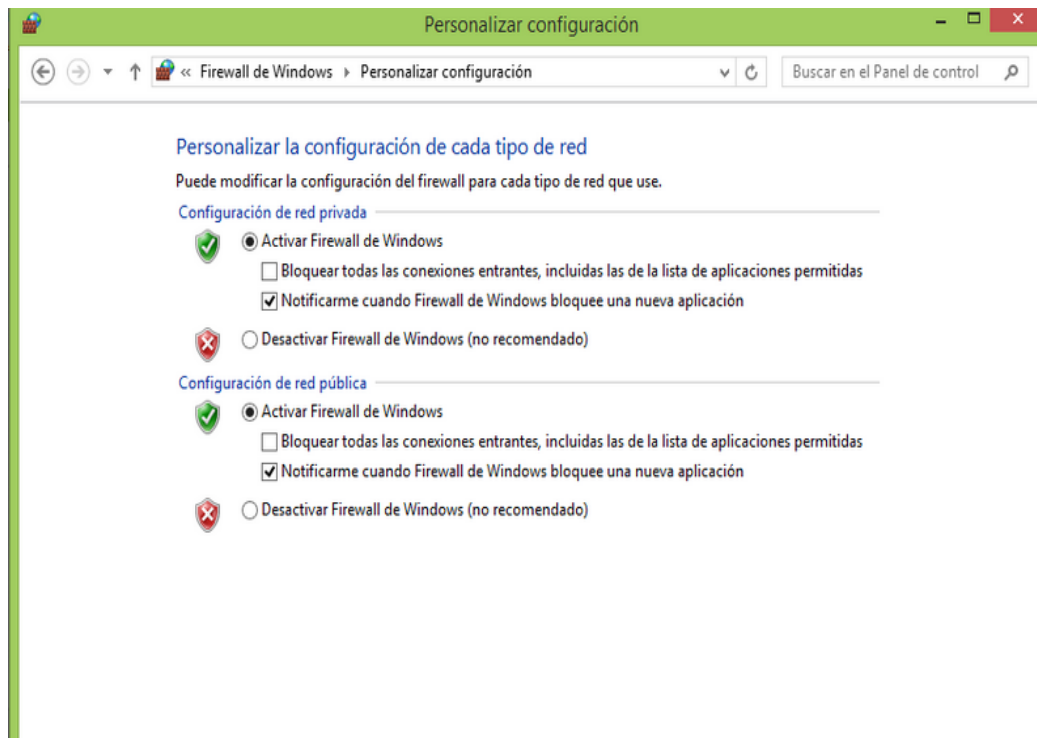


- Por suposto, aparte destas devasas, incluídas nos Sistemas Operativos, podemos optar por instalar e configurar aplicacións externas ao mesmo antivirus que inclúan esta funcionalidade, ou tamén facer uso dos firewalls que ten instalado o router da nosa casa, oficina...

De feito, Windows por exemplo, vén cun firewall moi sinxelo que se habilita por defecto coa instalación do sistema, de forma que os usuarios non teñan que preocuparse de buscar un, actívalo e configúralo. No entanto, o firewall de Windows é bastante pobre en funcións e en moitas ocasións pode xerar máis problemas que solucións aos seus usuarios, especialmente co uso de programas P2P que necesitan utilizar determinados portos e por defecto o Firewall de Windows tenos bloqueados impedindo o correcto funcionamento destes.







- Ligazóns interesantes:
  - [Cortafuegos](#): Nesta ligazón podemos atopar conceptos xerais, Firewall de Windows 7 e outras ferramentas de protección.
  - [Cómo configurar el Firewall de Windows 8.1 y Windows 10](#)
  - [Configurar el firewall gufw en linux](#)
- Por último indicaremos algúns dos mellores firewalls gratuítos que podedes instalar nos vosos equipos (aínda que se queres máis funcionalidades das que presenta por defecto, terás que pagar por elas): [ZoneAlarm](#), [Comodo Firewall](#), [AVG](#), [Private Firewall](#), [PCTools](#), [Endian Firewall](#), [IPCop](#), [pfSense](#).

## Seguridade no software

Entre as medidas de seguridade relativas ao software, podemos comentar:

- Eliminación de virus
- Restaurar o sistema
- Recuperar datos

L

## Eliminación de virus

- Unha vez que se **detecta** a entrada dun **virus** no sistema, débese proceder á súa eliminación, proceso que se realiza cun software específico, **antivirus**.

Fai clic na seguinte imaxe, se queres coñecer [Os 10 signos que indican que o teu ordenador está infectado por un virus](#):



- É conveniente utilizar este software para realizar [inspeccións periódicas](#) sobre o sistema. para detectar e eliminar toda presenza de virus.
- Podemos atopar moitas e moi boas ferramentas, tanto de carácter comercial como gratuito.
- Pero, a máxima que se debe ter sempre en conta e que, non hai antivirus válido se non se [instalan as actualizacións e se realizan inspeccións periódicas do sistema](#).
- Algúns dos antivirus gratuítos que mellores resultados están a ofrecer son: [Avast](#), [Avira](#), [AVG](#), [Panda](#), [Qihoo](#), [Comodo](#), [Ad-Aware](#), [virustotal](#), [Bitdefender](#), [clamav](#), [sophos](#), [Kaspersky](#). Varios destes antivirus ofrecen servizos a Windows, Mac e Linux.



- Pero como os nosos móbiles e tablets non se libran tampouco dos ataques malware, tamén é preciso facer uso de antivirus especializados, como por exemplo: [Eset Mobile Security](#), [NQ Mobile Security](#), [Avast! Mobile Security & Antivirus](#), [AVG Antivirus](#)...
- Segundo Computer Hoy, os mellores antivirus para android:



- Ademais podedes ler algún artigo onde fala das características dos mellores antivirus gratuítos:
  - [Los ocho mejores antivirus y herramientas de seguridad gratis para Windows](#)
  - [Los mejores antivirus gratis para PC 2016](#) (este artigo inclúe un vídeo con comparativas de antivirus para android).
  - [¿Cuáles son los mejores Antivirus para Android gratis? Móvil y Tablet](#)

## Antimalware

- A creación e distribución de virus estase vendo superado polo inxente incremento de adware, spyware e troianos, estamos notando nos últimos anos unha especialización do malware, con ataques dirixidos a obxectivos moi concretos.
- Os antivirus actuais detectan tanto os virus, como toda a tipoloxía de malware pero, [ter instalado un antivirus non é suficiente garantía de estar protexido](#), cada día aparecen novos virus, mutacións dos existentes, que se crean e reenvían aproveitando as vulnerabilidades do software para instalarse e executarse.
- O mesmo día no que se fai pública unha vulnerabilidade, xa se producen ataques que a explotan, ás veces, días antes de que as organizacións desenvolvedoras dos sistemas antivirus implanten as medidas específicas para deter ese novo malware. A estes ataques se lles denomina “[zero-day attack](#)”, capaces de chegar a infectar millóns de máquinas no período de tempo que transcorre entre o descubrimento da vulnerabilidade e o lanzamento do parche e do antivirus específico.

## Antiespías

Os [espías](#) son un tipo de [software maligno](#) xeneralmente [non detectado polos antivirus](#).

Poden realizar dous tipos de accións:

- Alterar o funcionamento normal do navegador de Internet facendo cousas como impedir o acceso a determinadas páxinas web, modificando a páxina de inicio, mostrando xanelas emerxentes, e redireccionándonos a enderezos con fins delitivos.
  - Recopilar información do usuario, programas instalados no ordenador, contrasinais (correo electrónico, contas bancarias...), páxinas máis visitadas, ..., para transmitila a tereceiras persoas ou empresas sen o consentimento nin coñecemento do propietario do ordenador

[Un antispyware](#) é un conxunto de [ferramentas que serven para previr e eliminar Spywares](#).

Recomendámosvos ler estes artigos:

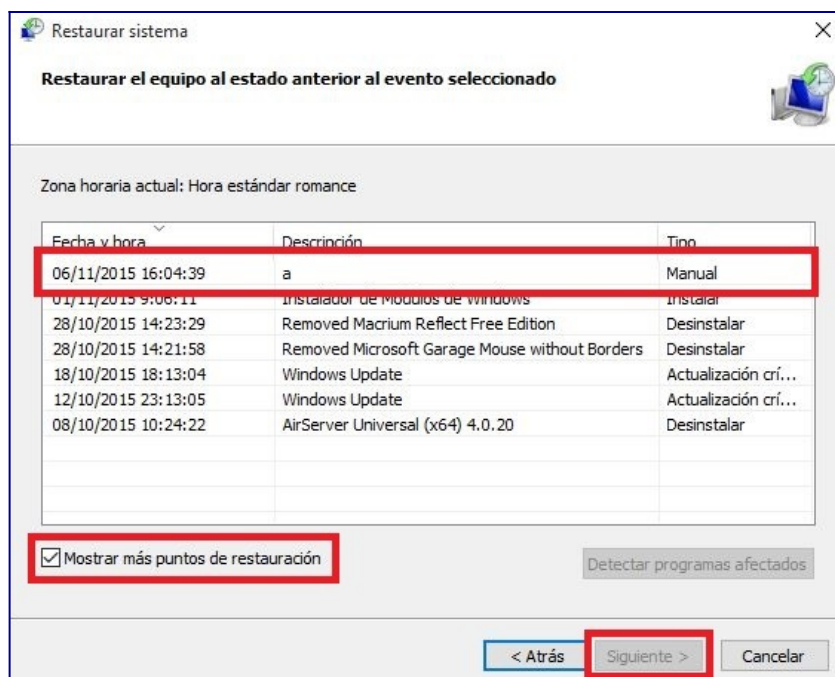
[Antiespías](#)

[DIFERENCIAS ENTRE ANTIVIRUS, FIREWALL, ANTIESPÍAS Y ANTIMALWARE](#)

Algunhas ferramentas antiespía: [CCleaner](#), [spybot](#), [malwarebytes](#), [spyware doctor](#), [adware](#), ...

## Restaurar o sistema

- Se se produce o fallo dalgún compoñente, e non é posible acadar a estabilidade do sistema para a normal utilización do mesmo, pode realizarse a [restauración](#) a un punto estable anterior.
  - Este proceso non elimina información, pero si aquelas aplicacións e actualizacións de software e configuracións realizadas no período de tempo transcorrido entre o momento actual e a data escollida para o punto de restauración.
    - Podemos atopar nos propios sistemas operativos ferramentas para a restauración do sistema a un punto determinado, por exemplo [Cómo restaurar el sistema en Windows 10](#)
- Se queres máis información sobre cómo configurar un punto de restauración en Windows 10, fai clic na seguinte imaxe:



- Tamén existen ferramentas externas como:
  - [TimeShift](#), [Cronopete](#), [Back In Time](#), [Systemback](#), ..., todas elas para linux
  - [wondershare](#), [EaseUS Mac](#), ..., para MAC

## Copias de seguridade

Este proceso debe ser realizado:

- cun software específico para restaurar información borrada, ou ben
- recuperar a mesma dende copias de seguridade feitas con anterioridade, ben en dvd, discos externos, memorias,...
- Dende o [Panel de Control de Windows](#), no apartado de Sistema e Seguridade, existe unha opción para crear copias de seguridade o restaurar os teus arquivos. Esta ferramenta permite gardar unha imaxe bastante completa de todo o contido actual do teu ordenador e exportala a un CD/DVD, ou a outro disco duro. Coa mesma ferramenta podes despois

- restaurar todos os arquivos noutro ordenador, outra instalación de Windows, ou nese mesmo PC en calquera momento do futuro.
- Nas [distribucións Linux baseadas en Ubuntu](#), existe dentro dos axustes de sistema, unha simple ferramenta chamada "Respaldo" que permite gardar os arquivos e as carpetas almacenadas no teu PC e gardalas noutro medio. Os respaldos poden programarse para que se realicen de forma automática segundo a cantidade de tempo que se escolla, permitindo tamén cifrar o contido do respaldo.
  - En [OS X](#) podes usar a utilidade [Time Machine](#) para realizar copias de seguridade do teu Mac nun disco duro externo.
  - Existen algunhas [ferramentas que permiten crear imaxes completas do disco](#), incluíndo sistema operativo, aplicacións e datos. Este tipo de solucións soen ser [proporcionadas por terceiros](#) e non polo mesmo fabricante do equipo nin tampouco veñen co sistema operativo. Algúns exemplos son:
    - [clonezilla](#), [Acronis True Image](#), [EaseUS Todo Backup Free 9.0](#), [AOMEI Backupper Standard 3.2](#), [Areca Backup 7.5](#), [CobianBackup](#), ...
    - Servicios na nube: [Drive de Google](#), [Dropbox](#), [OneDrive de Microsoft](#), [Box](#), ...
    - Podes visitar o artigo [Estas son las mejores aplicaciones para hacer backups](#), se queres coñecer ferramentas para [android](#).  
Se non podes acceder ao seguinte vídeo fai clic na ligazón [Copia de seguridad de todos los datos de Android](#)

## Recuperar datos

- Por moitas circunstancias borramos arquivos no noso ordenador e despois nos arrepentimos de telo feito ou simplemente os borramos por accidente.
- Cando borramos datos, non todo está perdido, xa que estes datos borrados, en moitos casos, se poden recuperar.
- Existen diferentes ferramentas para realizar a recuperación de información: [recuva](#), [Easeus Data Recovery](#), [DiskDigger](#), [Recuperación de archivos Word danados con damageddocx2txt](#), [Photorec](#), [GetDataBack](#) (estas últimas para fotos, ao igual que [recuva](#) que tamén é moi utilizada con este fin).

## Control de acceso á información

### Control de acceso á información

Como podemos ver en módulos anteriores, para velar polos principios da seguridade da información (confidencialidade, integridade, dispoñibilidade), se fai necesario establecer controis de acceso, implementados tanto sobre o sistema operativo, sobre aplicacións, bases de datos, programas específicos de control de acceso ou sobre dispositivos hardware.

Os principais métodos de control de acceso ao entorno físico, recordaremos que eran:

- Identificación, autenticación e roles
- Permisos de acceso
- Limitacións de horarios

Identificación e autenticación

Mediante os procedementos “clásicos”,



- Algo que temos: por exemplo tarxeta de acceso
- Algo que sabemos: contrasinais

Ou os de reforzo, biométricos:

- Algo que somos: biométricos

Se che interesa este tema, podes acceder a:

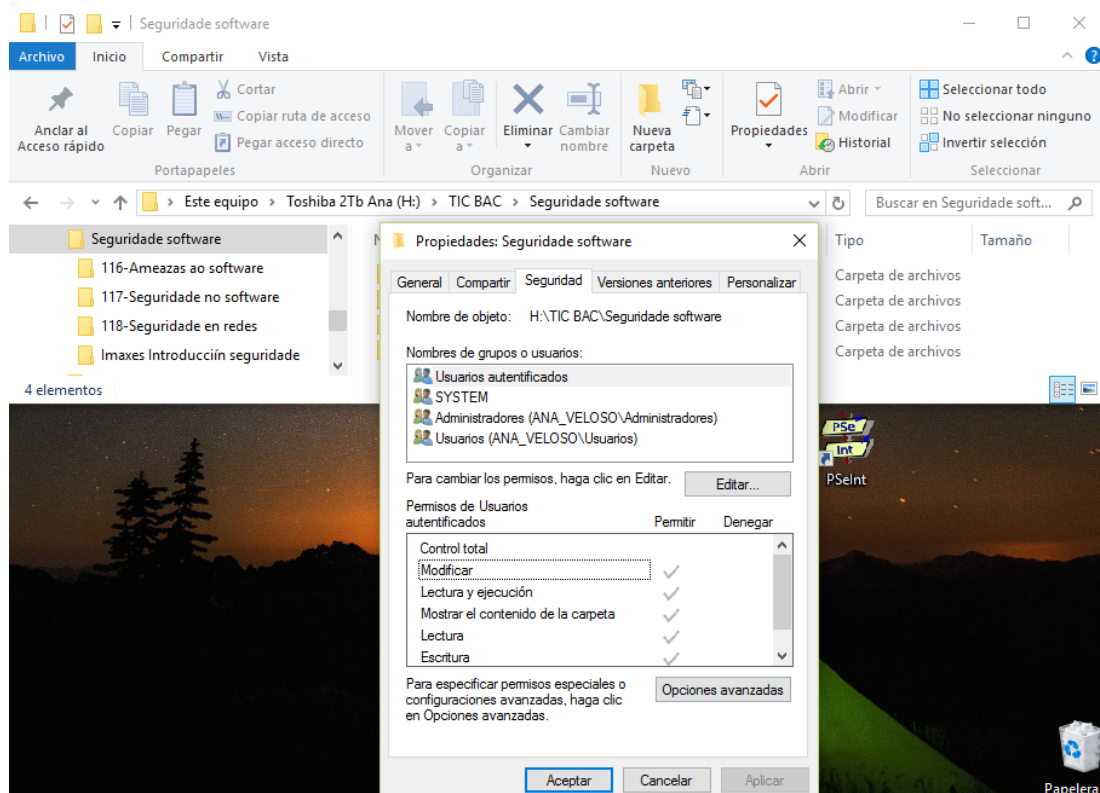
- [Productos:Control de Accesos biométrico](#)
- [Biometría informática](#)

En función do rol facilitado á persoa identificada, esta disporá de acceso a determinadas zonas, estancias ou períodos de tempo.

Todas estas limitacións, deben ser establecidas en función do sistema de control de acceso implementado na organización.

### Permisos de acceso

Aínda que os usuarios tiveran acceso ao mesmo software, é posible establecer permisos determinados e diferenciados para cada un deles, por exemplo lectura, inserción, modificación e borrado, execución, etc.



Ana Veloso, Gabriel Ferreiro. *Permisos por usuario.* [CC BY-SA 4.0](#)

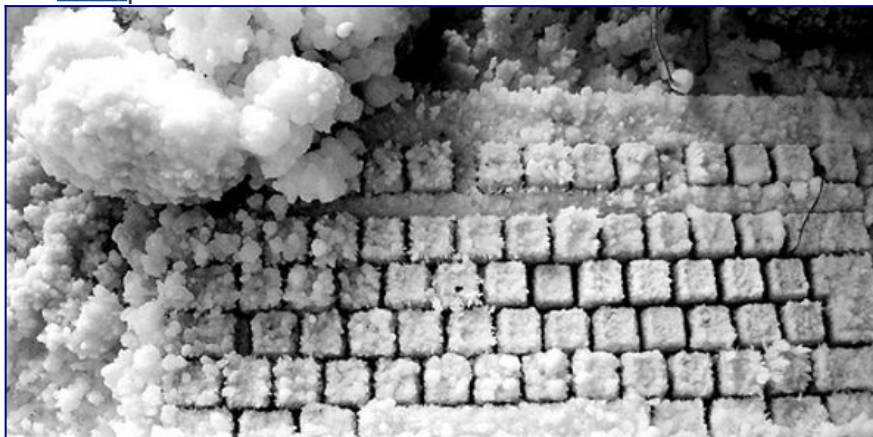
### Limitacións horarias

Consiste en incorporar limitacións ou permisos para acceder ou denegar o acceso aos sistemas ou software segundo franxas horarias ou períodos de tempo máis longos, por exemplo fora de horario laboral, en vacacións, etc.



## Conxelación do software

- Unha das ferramentas máis utilizadas para a protección dos sistemas informáticos, é o [software de “conxelación”](#).
- Estas utilidades son programas que permiten a un sistema informático a volta a un estado predeterminado no pasado. Ao usuario se lle permite navegar por internet, descargarse aplicacións, instalar aplicacións, programas, realizar cambios na configuración do sistema operativo, etc., coa particularidade de que, [unha vez que o sistema se reinicia, este volve a atoparse na situación previa á súa conxelación](#).
- Este proceso é especialmente útil nos centros académicos, permitindo conservar sempre a configuración que se determinou no seu momento como a óptima.
- O sistema informático pode ter vulnerabilidades e sufrir ataques de malware mentres se atopa en funcionamento pero, unha vez se reinicia, todo se volve atopar no estado óptimo. Si hai que ter en conta que [non é reversible](#) a situación de que o equipo sufra un ataque e sexa [roubada a información](#) do equipo e do usuario.
- Tamén é imprescindible coñecer que existe a posibilidade de que nos atopemos con [malware resistente a certos sistemas de conxelación](#), polo que tamén se fai inevitable realizar periodicamente inspeccións e actualizacións dos programas antivirus nos equipos.
- Exemplos de ferramentas de conxelación son:
  - [DeepFreeze](#) para Windows
  - [Ofris](#) para Linux. Fai clic na imaxe:



## Destrución de documentos

- No momento en que a [información](#) deixa de servir e estimamos que no futuro non será tida en conta, é necesario [destruír de forma segura](#) os soportes nos que se atopa, xa sexa formato papel ou electrónico.
- Moita da información que posúen as organizacións se atopa protexida por lei e, debido ao tratamento de información de carácter persoal, temos que ter moi en conta a non reutilización de determinados soportes. Por exemplo, [un disco duro, aínda que sexa formateado varias veces, é posible recuperar a súa información utilizando técnicas especiais](#), ao igual que un cd, dvd ou calquera outro soporte en formato electrónico.

Estes soportes deben ser destruídos de forma que se garanta a confidencialidade dos datos que contiñan. Existen empresas especializadas en recollida e reciclaxe deste tipo de material informático, así como documentación en papel, que entregan con posterioridade á súa destrución, un certificado que garante o proceso realizado.

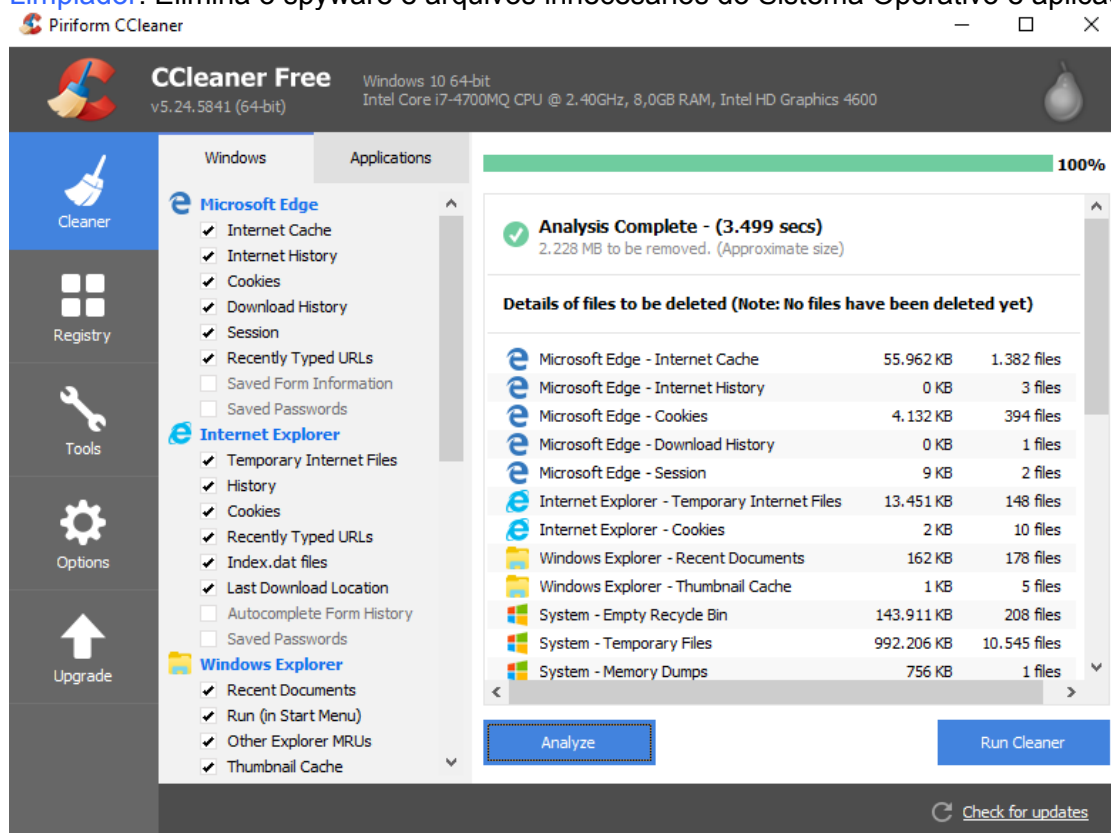
- Facilitamos varios artigos nos que se explica en que consiste un formateado a baixo nivel:
  - [Diferencias entre formateo rápido y formateo completo](#)
  - [Formatea un disco a bajo nivel con HDD Low Level Format](#)
  - [Como eliminar datos del disco duro definitivamente](#)

## Ferramenta CCleaner

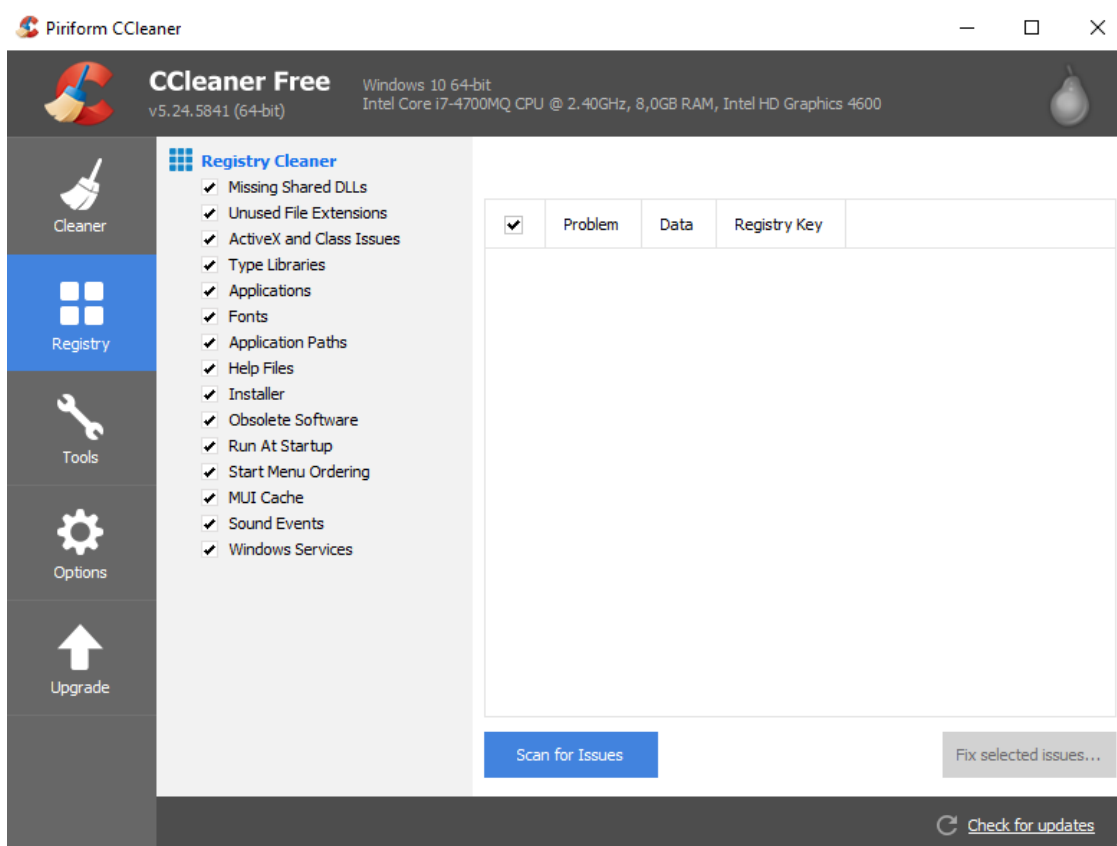
Existen algunhas ferramentas que se poden tamén utilizar para garantir a eliminación segura de arquivos, outras como [CCleaner](#) inclúen a posibilidade de borrar espazo libre para evitar a recuperación de calquera arquivo eliminado previamente, aparte de ser unha boa ferramenta antiespías.

### Funcións principais CCleaner

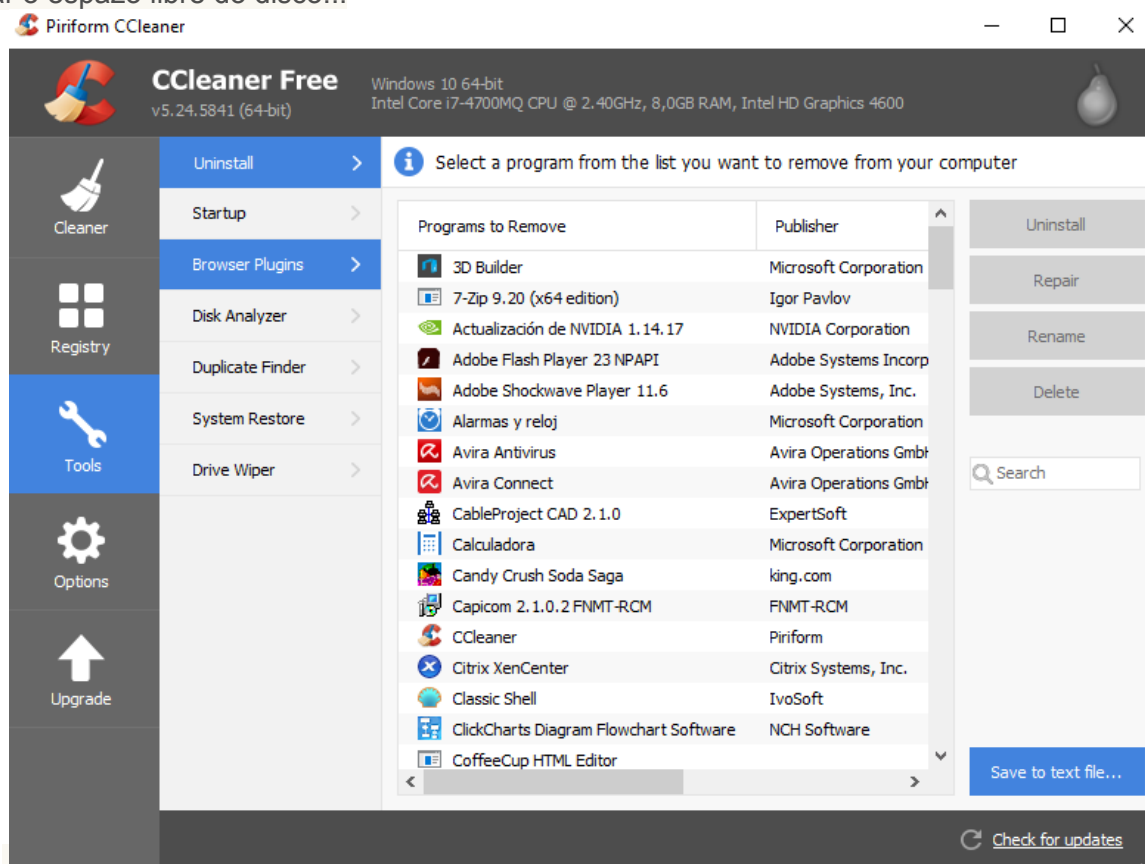
**Limpiador:** Elimina o spyware e arquivos innecesarios do Sistema Operativo e aplicacións.



**Rexistro:** Elimina entradas inválidas do rexistro provocadas pola desinstalación de software.



**Tools (Ferramentas):** Permite desinstalar programas, desactivar aplicaciones que se inician automáticamente al arrancar el equipo, restaurar el sistema, borrar de forma segura archivos, borrar el espacio libre del disco...



## Seguridade na Rede

Os nosos equipos non están aislados, Pc's, portátiles, tablets, móbiles,...todos están en contacto con outros equipos, tanto en redes locais como na gran rede, Internet.

### Ataques na rede

Entre os ataques que podemos sufrir na rede, podemos mencionar:

- **Ataque de suplantación.** O atacante faise pasar por unha terceira persoa ou empresa para dar informacións falsas. É habitual atopar este tipo de ataques en páxinas bancarias que son clonadas para que determinados usuarios que non toman as debidas precaucións, introduzan os seus datos crendo que son webs legais.
- **Ataque de intromisión.** Polo xeral son ataques internos ou de alguén que se consegue colar na rede e navega por ela explorando arquivos e documentos ata atopar información relevante que poda ser de utilidade e con fins delituosos.
- **Ataque de modificación.** Modifícanse arquivos ou documentos que se consideran válidos. Se o atacante obtén permisos de administrador, os danos poden ser enormes.
- **Ataque de interceptación.** A información que se quere controlar é desviada dende o seu destino ata o sitio web do atacante para ser estudada detidamente.
- **Ataque de espionaxe das liñas.** Polo xeral é utilizada a través de redes sen fíos, onde a comunicación é estudada observando as comunicacións.
- **Ataque de denegación de servizo.** Se trata de impedir o axeitado funcionamento dos sistemas a aqueles usuarios que están autorizados.

Vídeo

[Proteja su computadora del software malicioso.](#), [Federal Trade Commission](#), [Licenza de Youtube CC BY](#)

### Medidas para a seguridade na rede

Para establecer unha seguridade adecuada na nosa rede, debemos seguir unhas normas xerais, como ter ao día a configuración dos antivirus, tanto nos servidores como nos equipos persoais, configurando os firewall, utilizar VPN,

### Devasas e conexións seguras

Internet é, dende sempre, un medio rápido, fiable, pero non seguro, establecéndose as comunicacións sen cifrar, o que permite que calquera individuo poda interceptar as comunicacións.

### Conexión segura SSL/TTL

- O protocolo que se utiliza habitualmente para o cifrado en internet, se denomina **ssl**, protocolo de capa de conexión seguro.
- O protocolo **https** utiliza o cifrado baseado en **ssl/ttl**. Unha boa forma para saber se os datos que introducimos nunha web viaxan de forma segura, é observar na barra de direccións do noso navegador se aparece **https://**, o que indicaría que é unha **web segura**, cifrada a comunicación con ssl.

Se unicamente aparece **http://**, a **información non vai cifrada (encriptada)**.

Se non podes acceder ao seguinte vídeo fai clic na ligazón [HTTPS and SSL tutorial](#)

## Devasa

- Como xa vimos, unha **devasa** é un dispositivo ou conxunto de dispositivos, que está configurado para impedir o acceso non autorizado a unha determinada zona da rede ou a un dispositivo pero que, ao mesmo tempo, permite o acceso ás comunicacións autorizadas.
- A implementación das devasas pode ser:
  - vía **hardware**: este tipo de sistema é colocado sobre os dispositivos usados para saír a Internet, é dicir nos “routers”. Normalmente a instalación xa se encontra realizada cando compramos o router, aínda que podemos configurala segundo as nosas necesidades.



- vía **software**: tal e como vimos no punto "Devasas" dentro de "Recursos de Seguridade no Sistema Operativo"

Pódense aplicar dous tipos de políticas:

- **Restritivas**. Impiden todo o tráfico salvo o autorizado expresamente na configuración da devasa.
- **Permisivas**. Permite o paso de toda comunicación, salvo a prohibida expresamente.

## Escanear os portos

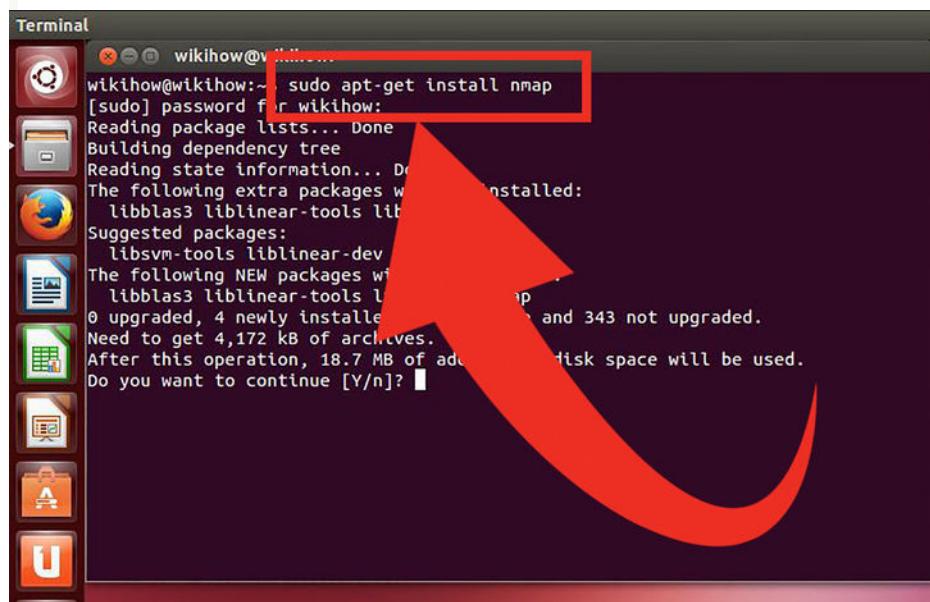
### Escaneo de portos

- Outra das ferramentas das que dispoñemos para detectar posibles vulnerabilidades no sistema é utilizar certas **ferramentas para escanear qué portos se manteñen abertos** no sistema.
- Recordemos que o **número de porto** se utiliza para **identificar ás aplicacións emisoras e receptoras**. Cada lado da conexión TCP ten asociado un número de porto asignado pola aplicación emisora ou receptora. Por exemplo, os servizos de internet http, ftp, telnet, teñen asignados portos específicos, 80, 21, 23... se non se están utilizando estes servizos ou se se pensa que non se utilizarán durante determinado tempo, o máis seguro é pechar os portos que correspondan.
- Podemos executar algúns programas que realizan un escaneado de portos no equipo para mostrar ao usuario cales son os portos que se manteñen abertos, pechados ou bloqueados pola devasa.

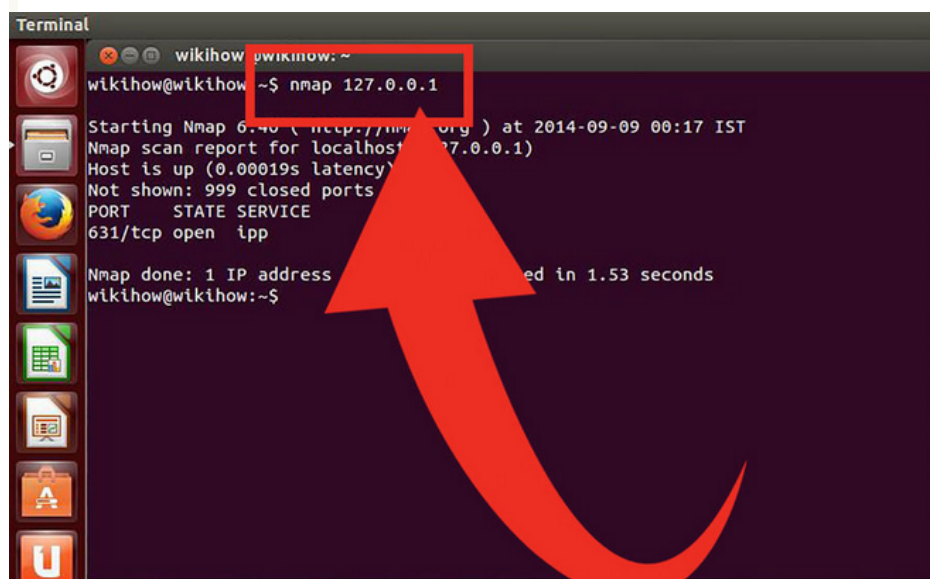
- Existen diferentes ferramentas para o chequeo de portos abertos, tanto nunha ip dun equipo local como nun equipo remoto. A ferramenta clásica para esta labor é [NMAP](#). Podemos atopar información sobre o seu uso e forma de traballar en moitas páxinas, por exemplo en [openwebinars](#), en [redeszone](#), ou en [adslzone](#).

Exemplo uso de NMAP

Exemplo de instalación e chequeo dos portos abertos do propio equipo:

A terminal window titled 'Terminal' with the prompt 'wikihow@wikihow:~'. The command 'sudo apt-get install nmap' is entered and highlighted with a red box. The output shows the installation process, including reading package lists, building a dependency tree, and installing additional packages like libblas3 and liblinear-tools. A large red arrow points from the command box down to the next terminal screenshot.

```
Terminal
wikihow@wikihow:~$ sudo apt-get install nmap
[sudo] password for wikihow:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  libblas3 liblinear-tools libsvm-tools liblinear-dev
Suggested packages:
  libsvm-tools liblinear-dev
The following NEW packages will be installed:
  libblas3 liblinear-tools libsvm-tools liblinear-dev
0 upgraded, 4 newly installed, 0 to remove and 343 not upgraded.
Need to get 4,172 kB of archives.
After this operation, 18.7 MB of additional disk space will be used.
Do you want to continue [Y/n]?
```

A terminal window titled 'Terminal' with the prompt 'wikihow@wikihow:~'. The command 'nmap 127.0.0.1' is entered and highlighted with a red box. The output shows the Nmap scan report for localhost, indicating that the host is up and that port 631/tcp is open. A large red arrow points from the command box down to the next terminal screenshot.

```
Terminal
wikihow@wikihow:~$ nmap 127.0.0.1
Starting Nmap 6.40 ( http://nmap.org ) at 2014-09-09 00:17 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00019s latency)
Not shown: 999 closed ports
PORT      STATE SERVICE
631/tcp   open ipp
Nmap done: 1 IP address scanned in 1.53 seconds
wikihow@wikihow:~$
```

Existen tamén algunhas páxinas web dende as que podemos realizar un chequeo de portos online, como [www.internautas.org](#), [incloak.es](#), [puertosabiertos.com](#),

Exemplo escaneo portos dende internautas.org



Asociación de Internautas



SCAN ON LINE DE PUERTOS



IP analizada: 83.165.12.108

Resultado del Escaner a los puertos habituales (espera que se cargue completamente la página)

| Puerto | Desc.  | Estado  | Observaciones           |
|--------|--------|---------|-------------------------|
| 20     | FTP    | cerrado | Utilizado por FTP       |
| 21     | FTP    | cerrado | Utilizado por FTP       |
| 22     | SSH    | cerrado | Secure Shell.           |
| 23     | TELNET | cerrado | Acceso remoto           |
| 25     | SMTP   | cerrado | Servidor de correo SMTP |

Ana Veloso, Gabriel Ferreiro. *Exemplo escaneo portos dende internautas.org.* [CC BY-SA 4.0](#)

Exemplo escaneo portos dende puertosabiertos.com

www.puertosabiertos.com/es/escaner-de-puertos.htm

Buscar

**Puertos Abiertos.com**

**Inicio**  
**Escanear puertos on-line**  
**Conoce tu IP**  
**Información de Puertos**  
**Listado de Puertos**  
**Geolocalizar IP**  
**Archivos peligrosos e-mail**  
**Generar QR Code**  
**QR Contacto**  
**QR Correo electrónico**  
**QR Dirección Web**  
**QR Localización**  
**QR MMS**  
**QR SMS**  
**QR Tarjeta de Visita**  
**QR Teléfono**  
**QR Texto**

**Seleccione un conjunto de puertos**

Seleccione ->  y pulse ->

**Escriba un puerto personalizado**

**Susceptibles**

| Puerto | Nombre | Estado    | Información                                                                                                                                                             |
|--------|--------|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 21     | FTP    | ● Cerrado | Servicio para compartir archivos FTP.                                                                                                                                   |
| 23     | Telnet | ● Cerrado | TELEcommunication NETWORK permite controlar un equipo remotamente. Puerto potencialmente peligroso.                                                                     |
| 25     | SMTP   | ● Cerrado | TELEcommunication NETWORK, usado para envío de correo electrónico. Un puerto muy escaneado para aprovechar vulnerabilidades para el envío de SPAM. Asegúrate de validar |

Tamén existen ferramentas que é preciso descargar para ser executadas e que permiten chequeo de ip's e de portos abertos en redes locais, como [Angry IP Scanner](#), [PortScan](#), [NetworkActiv Port Scanner](#), ...

Exemplo escaneo con Angry IP

**IP Range - Angry IP Scanner**

File Go to Commands Favorites Tools Help

IP Range: 66.249.93.32 to 66.249.93.200 IP Range

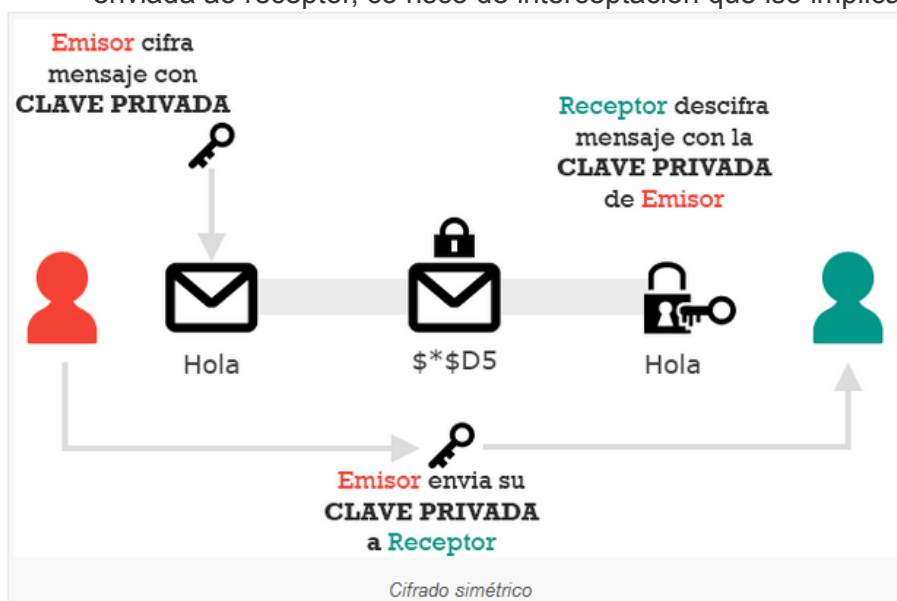
Hostname: ug-in-f99.google.com  Netmask

| IP           | Ping    | Hostname             | Ports [2+] | Web detect |
|--------------|---------|----------------------|------------|------------|
| 66.249.93.82 | 123 ms  | ug-in-f82.google.com | 80,443     | gws        |
| 66.249.93.83 | 133 ms  | ug-in-f83.google.com | 80,443     | gws        |
| 66.249.93.84 | 123 ms  | ug-in-f84.google.com | 80,443     | gws        |
| 66.249.93.85 | 117 ms  | ug-in-f85.google.com | 80,443     | GFE/1.3    |
| 66.249.93.86 | [n/a]   | [n/s]                | [n/s]      | [n/s]      |
| 66.249.93.87 | [n/a]   | [n/s]                | [n/s]      | [n/s]      |
| 66.249.93.88 | 76 ms   | ug-in-f88.google.com | 80,443     | gws        |
| 66.249.93.89 | [n/a]   | [n/s]                | [n/s]      | [n/s]      |
| 66.249.93.90 | [n/a]   | [n/s]                | [n/s]      | [n/s]      |
| 66.249.93.91 | 66 ms   | ug-in-f91.google.com | 80,443     | gws        |
| 66.249.93.92 | [n/a]   | [n/s]                | [n/s]      | [n/s]      |
| 66.249.93.93 | [n/a]   | [n/s]                | [n/s]      | [n/s]      |
| 66.249.93.94 | [n/a]   | [n/s]                | [n/s]      | [n/s]      |
| 66.249.93.95 | [n/a]   | [n/s]                | [n/s]      | [n/s]      |
| 66.249.93.96 | 2083 ms | ug-in-f96.google.com | [n/a]      | [n/a]      |
| 66.249.93.97 | 2053 ms | ug-in-f97.google.com | [n/a]      | [n/a]      |

Ready Display: All Threads: 0

## Encriptación de datos, criptografía

- A **criptografía** é a ciencia que se encarga do cifrado e descifrado de información para ser transmitida de forma segura, garantindo que unicamente sexa entendido por emisor e receptor.
- Para levar a cabo esta misión, a criptografía pode utilizar diferentes tipos de cifrado e descifrado.
  - **Criptografía simétrica**. Utiliza a mesma clave para cifrar e descifrar, polo que debe ser coñecida previamente tanto por emisor como por receptor, ou ben debe ser tamén enviada ao receptor, co risco de interceptación que iso implica.



- **Criptografía asimétrica**. Neste caso utilízase unha clave para cifrar e outra distinta para descifrar, necesítanse dúas claves:
  - unha **pública e compartida**: para **cifrar**
  - unha **privada e secreta** que só coñece o receptor: para **descifrar**



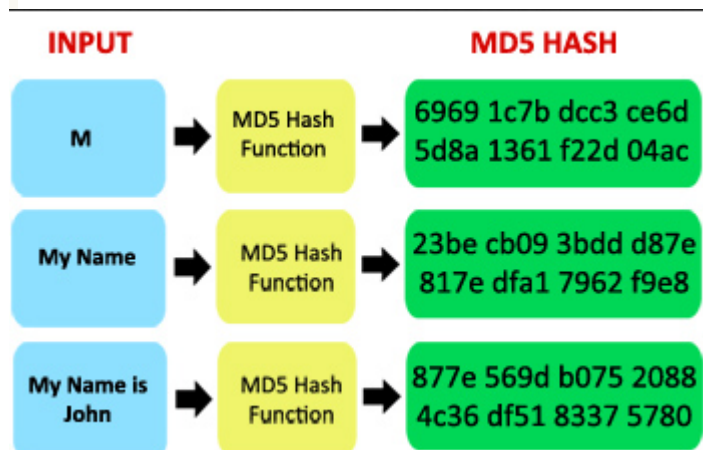
- Ligazón interesante: [Tipos de criptografía: simétrica, asimétrica e híbrida](#)

## Verificación no envío

### Funcións Hash

Os **hash** ou **funcións de resumo**, son algoritmos que conseguen crear a partir dunha entrada (que pode ser por exemplo un texto, un contrasinal ou un arquivo), unha saída alfanumérica de

lonxitude normalmente fixa e que vai representar un resumo de toda a información da citada entrada, polo tanto, a partir dos datos da entrada xera unha cadea que só pode volverse a crear con eses mesmos datos.



Imaxe derivada por [Gabriel Ferreiro](#), [Ana Veloso](#), [CC BY SA](#), da orixinal de [gohacking](#) [CC BY SA](#)

Estas funcións teñen a misión de asegurar por exemplo, que o arquivo que se envía, non foi modificado durante a transmisión ou firmar dixitalmente un documento.

Se a cadea que xera o arquivo recibido é diferente da orixinal, significará que o documento recibido é diferente ao enviado.

#### Exemplo de HASH MD5

- MD5 é un algoritmo moi utilizado actualmente para comprobar que un arquivo se descargou correctamente, é dicir, que se corresponde co que se desexaba descargar, protexéndonos, por exemplo, da incorporación de malware na descarga.
- Para realizar a comprobación, necesitamos coñecer a suma MD5 do arquivo orixinal e comprobar que coincide coa que nós obtemos ao facer o cálculo.
- Podemos ver algún exemplo e explicación interesante en:
  - [¿Qué son y para qué sirven los hash?: funciones de resumen y firmas digitales](#)
  - [Cómo verificar que tus descargas no se han dañado por el camino](#)
- Tamén podedes practicar, xerando código MD5, coas aplicacións on line [MD5online](#), [Generador MD5 Hash](#), [MD5 Hash Generator](#), [function md5](#), ...

www.md5.cz

function md5()

Online generator [md5 hash](#) of a string

md5 (  )

hash darling, hash!

md5 checksum:

--

Implementations MD5:

[php manual function md5\(\)](#) | [md5 in JavaScript](#) | [md5 in MySQL](#) | [md5 in MariaDB](#)

[MD5 on Wikipedia.org](#)

www.md5.cz

function md5()

Online generator [md5 hash](#) of a string

md5 (  )

hash darling, hash!

md5 checksum:

4d186321c1a7f0f354b297e8914ab240

Implementations MD5:

[php manual function md5\(\)](#) | [md5 in JavaScript](#) | [md5 in MySQL](#) | [md5 in MariaDB](#)

[MD5 on Wikipedia.org](#)

### Firma dixital

A [firma dixital](#) serve para [vincular un documento e comunicación](#), de forma unívoca, [a unha persoa física](#). Esta firma dixital ten unha [utilidade similar á firma manuscrita](#) e, moitas veces, é incluso máis fiable en relación á posibilidade de falsificación.

Como características da firma dixital, poderíase comentar:

- Cada firma é [única para cada un dos usuarios](#).
- É [infalsificable](#), polo menos, ata o momento actual non foi posible falsificar unha firma dixital e, o método polo que se tratan os datos non fai previsible a súa falsificación en moito tempo.
- [Doado de autenticar](#). Unha terceira persoa que poda recibir un documento firmado pode identificar de xeito sinxelo e comprobar a veracidade da firma recibida.
- [Imposible de rexeitar](#). O autor dun documento firmado dixitalmente non pode negar a autenticidade do documento nin da firma.
- [Doado de xerar](#). As firmas dixitais son xeradas mediante un proceso doado.

Para firmar un documento, faise necesario posuír unha firma dixital. O actual [dni electrónico](#), [inclúe unha firma dixital](#) que pode ser usado mediante un lector de tarxetas.

## Certificado dixital

O **certificado dixital** é un **documento no que unha autoridade de certificación**, unha empresa ou organismo de confianza que se encarga de emitir e revocar os certificados dixitais e certificados de firmas electrónicas, **garante que unha clave pública e unha determinada persoa están realmente asociados**, evitando posibles suplantacións de identidade.

Cada certificado contén:

- **Firma dixital** da autoridade de certificación, para comprobar que realmente a autoridade garante que a información contida é certa, e a vinculación entre clave e persoa, tamén.
- **Nome e dirección da persoa** que solicita o certificado dixital.
- **Nome e dirección da autoridade certificadora**.
- **Clave pública do propietario** do certificado.
- **Método de verificación da firma dixital** incluída no certificado.
- **Número de serie**, para poder identificar o certificado.
- **Data de validez do certificado**, tanto na que é emitido como na que expira.

A **autoridade de certificación** á que podemos solicitar un certificado dixital, é a **FNMT**, **Fábrica Nacional de Moeda e Timbre**.

Se non podes acceder ao seguinte vídeo fai clic na ligazón [Certificado digital: cómo solicitar tu certificado digital](#)

## Listas de control de acceso

- As **listas de control de acceso** son un elemento máis de seguridade nas redes, pois son **utilizadas para permitir o acceso dos usuarios a determinados sistemas, aplicacións, bases de datos, etc.**, en función de seu rol ou privilexios de acceso.
- Controlan o tráfico en switches e routers, encargándose de filtrar o tráfico que pasa por estes dispositivos, permitindo ou denegando o acceso, ou restrinxíndoo por horas e datas.
- Os routers incorporan o software necesario para manexar as listas de acceso por control de MAC ou IP.

### ¿Qué es una lista de control de acceso?

► Según Cisco CCNA, Una ACL es una serie de comandos del IOS que controlan si un router reenvía o descarta paquetes según la información que se encuentra en el encabezado del paquete.

Qué es una ACL?

- Permitir correo electrónico entrante  
Denegar Telnet entrante
- Denegar video al S1  
Denegar acceso del S1 al S2
- Denegar acceso a HR
- Denegar actualizaciones  
Denegar FTP  
Denegar la web

## Política de contrasinais



Os contrasinais son métodos básicos en todos os aspectos da seguridade, polo que se deben establecer contrasinais o suficientemente robustas para cada nivel de acceso, establecendo períodos de tempo para a súa validez.

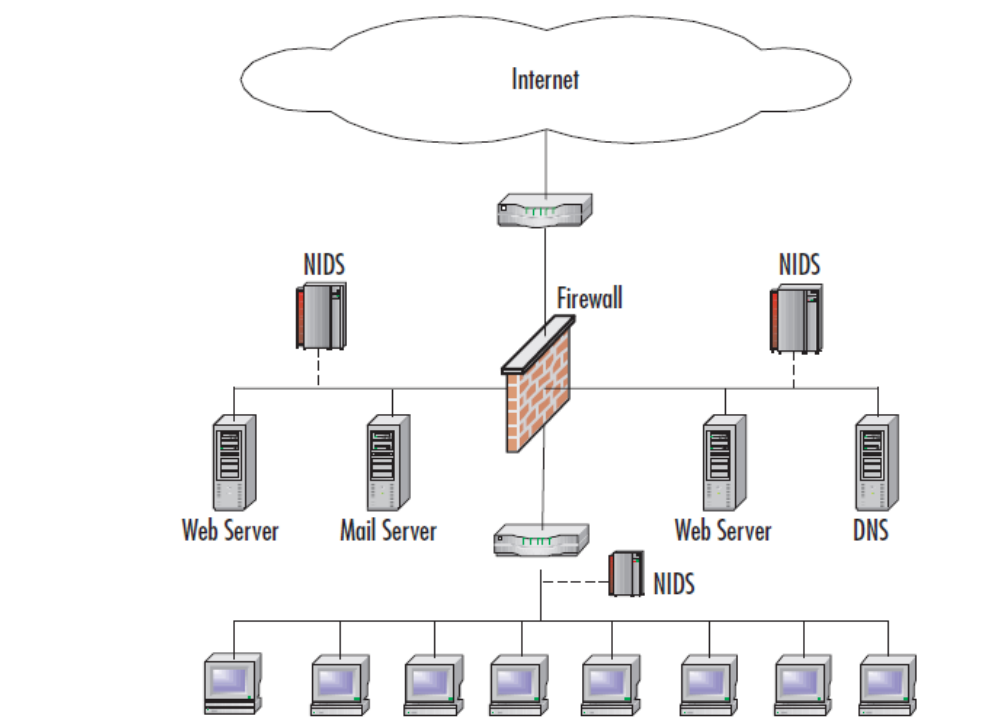
Como características básicas da política de contrasinais, pódense ter en conta:

- Os [contrasinais](#) deben ser [totalmente secretos](#), non deben ser coñecidos por ningunha outra persoa da organización.
- Para a súa elaboración, non deben ser utilizados o nome, dni, data de nacemento, secuencias, ...
- Non utilizaremos palabras que aparezan nos dicionarios, nin combinacións destas, xa que un dos ataques máis habituais é utilizar os dicionarios para probar todas as posibilidades posibles.
- [Non deben ser apuntados](#) os contrasinais que se escollan, deben ser recordados.
- Deben ser de longa lonxitude, cantos máis caracteres teñan, mellor.
- [Utilizar sempre maiúsculas, minúsculas, números e signos de puntuación](#).
- Evitaremos utilizar contrasinais que sexan doadas de descubrir por factores sociais, de actualidade ou comodidade.
- Podemos considerar contrasinais seguras se teñen [máis de 8 caracteres](#), combinando todos os existentes no alfabeto, por exemplo 7Bp\_7y\*X, xa que o tempo necesario para rompela utilizando a técnica de forza bruta, é tan longo que non compense o tempo dedicado para descifrala.
- Unha [recomendación](#) moi sinxela para elaborar un contrasinal seguro: Coller a primeira letra de cada unha das palabras dunha frase.  
Por exemplo: [AmicXet17a](#). (A miña irmá chámase Xiana e ten 17 anos.)

Unha ligazón interesante con consellos sobre [¿Cómo crear una contraseña segura?](#)

## NIDS

- Un [NIDS](#) é un sistema de detección de intrusos nunha rede.
- Encárganse de [atopar patróns de comportamento sospeitosos](#), intentos de acceso aos equipos ou ataques de denegación de servizo.
- [Analizan o tráfico de rede](#), tanto entrante como saínte e tamén o local da propia rede, para garantir a máxima vixilancia.
- Necesitan [ser actualizados con moita frecuencia](#).
- [Traballan en conxunción co firewall](#), e contan con información de tipos de ataques para poder utilizalos como patróns.



### Navegar con seguridad

Son moitos os consellos que podemos e debemos seguir á hora de navegar por Internet.

Os ordenadores, dende o momento no que se conectan, están a almacenar información continuamente, o solicitemos nós ou non. Almacenan as páxinas web que visitamos, os arquivos que descargamos, as buscas que facemos, etc.

Temos que ter en conta que é conveniente que teñamos nós, sempre, o control sobre:

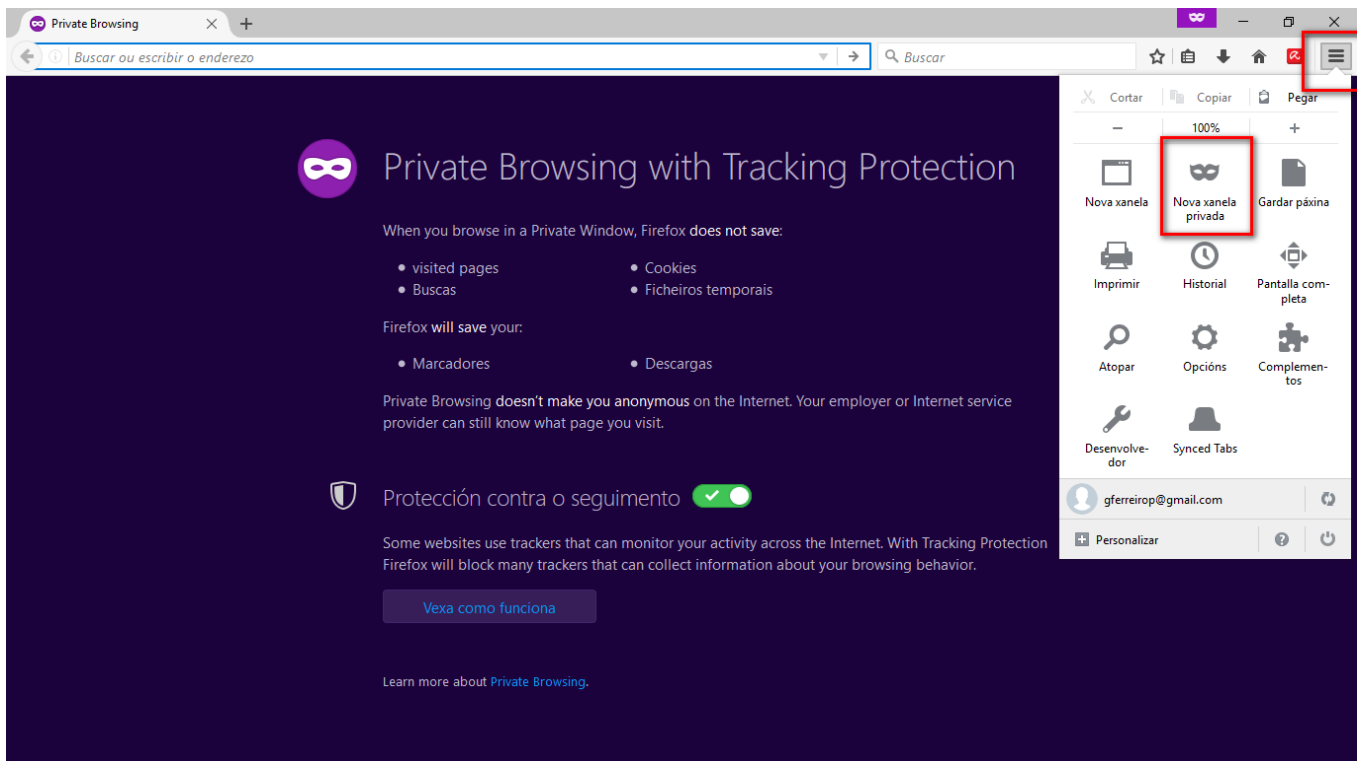
- **Configurar axeitadamente o Navegador.** O navegador permite configurar diferentes niveis de seguridade, establecendo filtros que frean a suplantación de identidade, control parental, ...
- **Historial do navegador.** É conveniente borrar periodicamente o contido do mesmo, ninguén que acceda ao noso equipo ten que saber cales son as páxinas que visitamos.
- **As cookies gardadas.** Son datos que os sitios web e os navegadores utilizan para gardar certa información sobre a nosa navegación, para utilizalos posteriormente de formas diversas, sendo o principal e lícito, o de recordar preferencias, configuracións, manter listas da compra, produtos escollidos en páxinas de comercio electrónico, etc.

Por outra banda, moitas veces se utilizan estas cookies para realizar seguimentos que realiza o usuario dentro dunha páxina ou en toda a rede, xeralmente para utilización comercial, algo que non é o seu propósito.

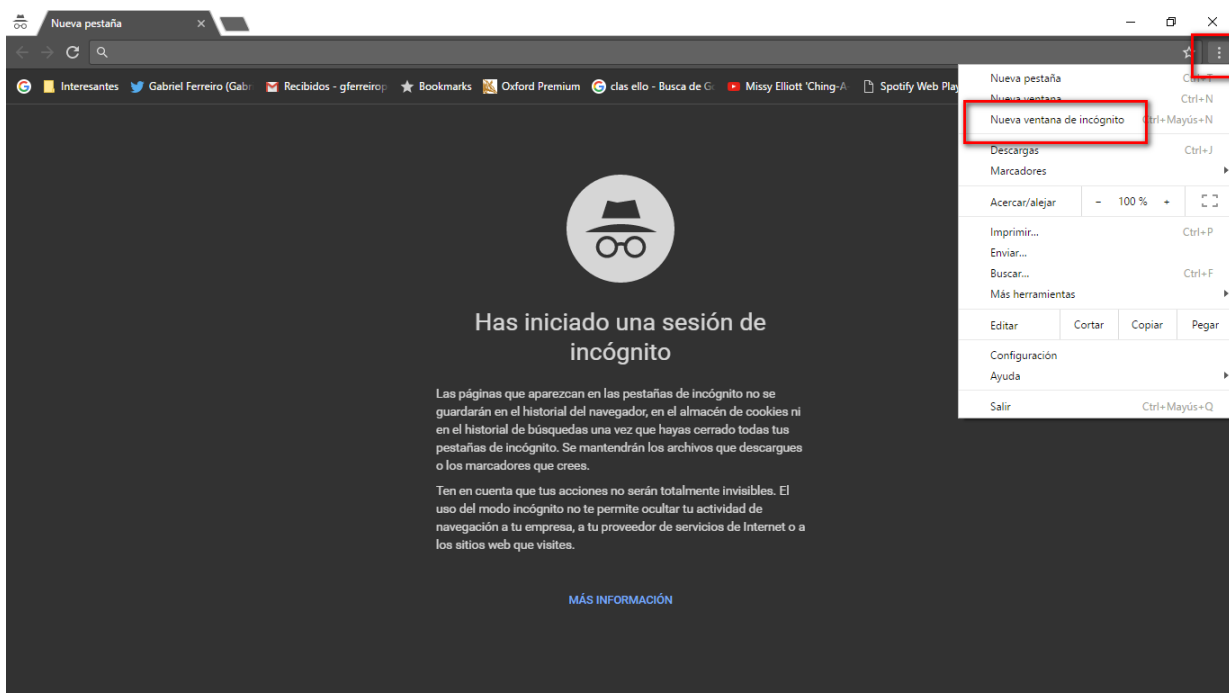
- **Os arquivos descargados, imaxes e webs.** Esta información gárdase en arquivos temporais que é imprescindible borrar periodicamente.
- **Ás veces, se navegamos en equipos que non son da nosa propiedade, é conveniente utilizar a navegación privada** pola rede, algo que, practicamente todos os navegadores

facilitan, co fin de que o navegador non almacene información como cookies, usuarios, contrasinais, historial, ...,

## Navegación privada en Mozilla Firefox



## Navegación privada en Google Chrome



- Moitos programas e aplicacións que descargamos de internet que, aínda que poden ou non ter utilidade, teñen como fin o facilitar información a terceiros sobre os nosos intereses e preferencias de navegación. Debemos [SEMPRE descargar aplicacións de sitios web oficiais](#).
- Debemos asegurarnos de que o navegador non acepte a instalación de software descargado de internet en forma automática.
- [Protexer os datos pessoais](#). Nunca proporcionar nome, apelidos, enderezo ou número de tarxeta de crédito naquelas páxinas que non sexan de confianza e que ademais non utilicen o protocolo HTTPS. Nunca accederemos a estes sitios facendo clic en ligazóns que recibimos, por exemplo, por correo electrónico.

Ligazóns interesantes

[10 consejos para navegar seguro por Internet](#)

[Algunos consejos para navegar más seguros en la Web](#)

## Correo electrónico

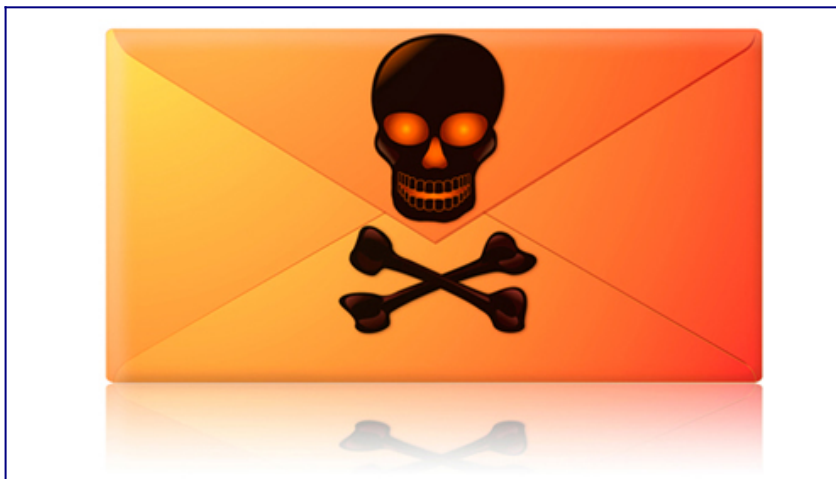
Como apartado especial dentro da navegación, imos estudar o correo electrónico.

Para a correcta utilización do correo electrónico faise necesario manter unhas mínimas prácticas e medidas de seguridade para evitar, tanto a entrada de código malicioso, como a posta en perigo da privacidade das persoas. Entre as prácticas aconselladas, pódense comentar as relacionadas con:

- Archivos achegados
- Copia oculta
- Reenvío
- Cadeas
- Enlaces
- Spam
- Denuncia
- Decálogo

## Archivos achegados

- Aínda que a persoa que remite un correo electrónico con arquivos achegados sexa de total confianza, calquera tipo de arquivo, non só executables, tamén fotografías, vídeos, documentos de texto, etc., pode conter código malicioso, malware, oculto. Incluso moitas veces, nen sequera esa persoa nos está a enviar a mensaxe, senón que algún virus está a enviar mensaxes a todos os contactos que atopa no seu correo.
- Faise imprescindible, como boa práctica, [configurar axeitadamente o servizo de correo electrónico para que o sistema antivirus realice a comprobación das mensaxes e arquivos adxuntos](#) e, se se decide descargar, pasarlle un antivirus antes de abri-lo.



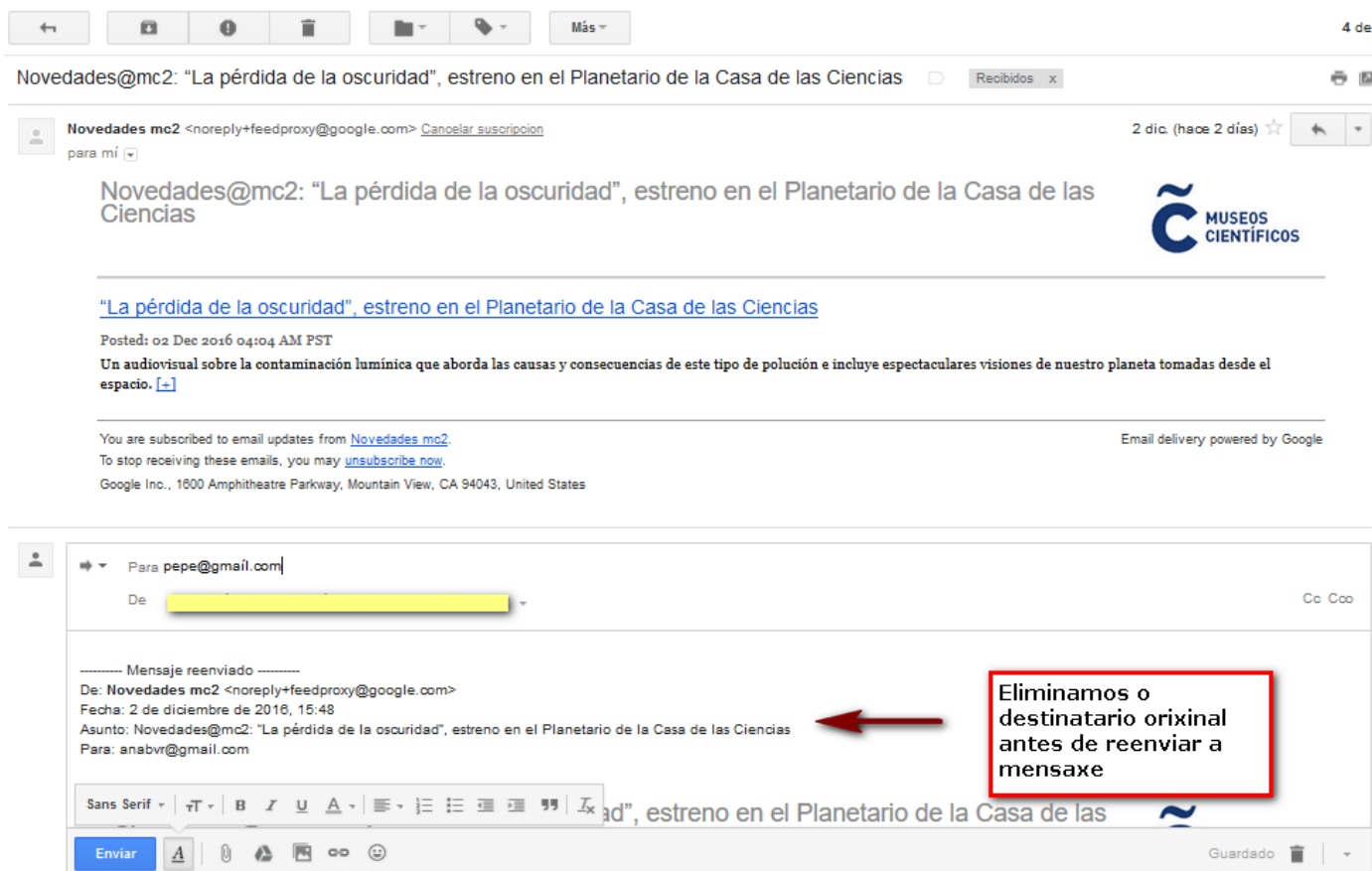
## Copia oculta

Unha das boas prácticas de utilización do correo electrónico indica que, [se realizamos o envío dunha mensaxe a varias persoas, os enderezos dos destinatarios deben ser incorporados como copia oculta](#) na mesma. Deste xeito, cada unha das persoas que reciben a mensaxe unicamente teñen visible o seu enderezo, non podendo visualizar os enderezos do resto, co que a privacidade das comunicacións se cumpre.



## Reenvío

Se estimamos necesario realizar o [reenvío](#) dunha mensaxe, faise [aconsellable borrar os enderezos dos destinatarios orixinais](#) da mesma, polo mesmo motivo que o comentado na boa práctica anterior.



## Cadeas Hoax

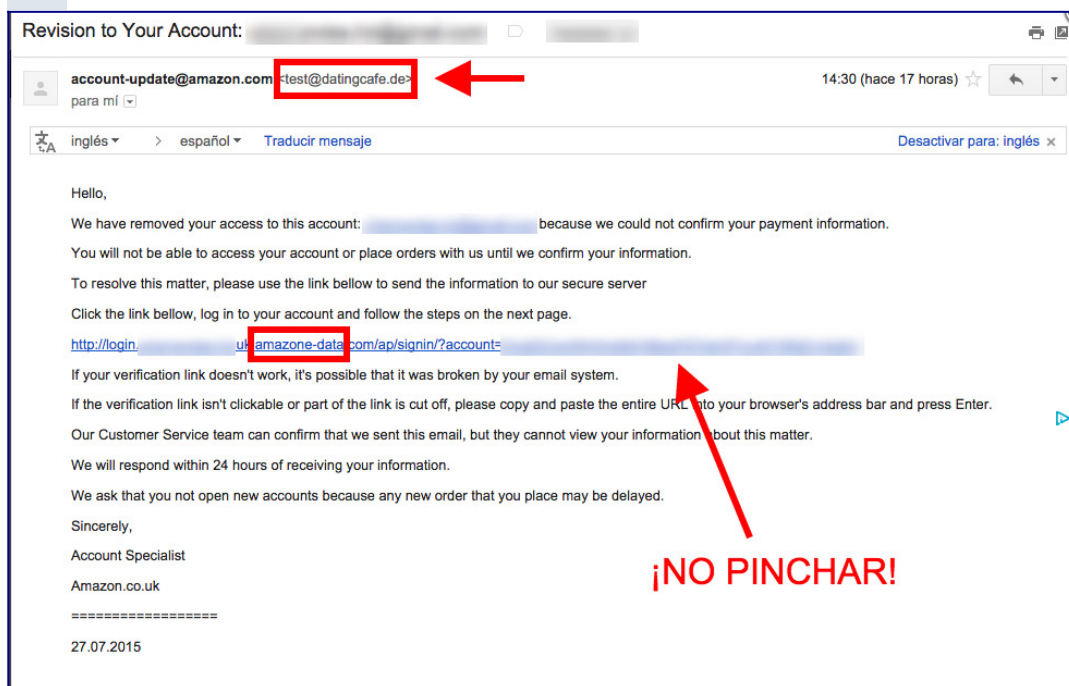
- O **obxectivo** que se persigue co envío e reenvío de **correos cadea** é unicamente **recompilar enderezos de persoas** para posteriormente, ser utilizados como caixas de entrada válidas aos que **enviar o spam**.
- Faise **imprescindible**, se recibimos un correo deste tipo, **cortar a cadea non reenviando o mesmo**.
- Podes atopar máis información nas seguintes ligazóns:
  - [Rompe las cadenas Hoax, tus amigos te lo agradecerán](#)
  - [Cadena de correo electrónico](#)

## Ligazóns

- Recordemos que a técnica de **phishing** consiste en enviar correos electrónicos con aparencia de correos de organismos oficiais, bancos, etc., que conteñen ligazóns a páxinas web falsas, aínda que moi semellantes, ou mesmo idénticas, as orixinais.
- A pretensión é enganar ao usuario facéndolle crer que está a entrar en, por exemplo, o sitio web da banca electrónica do seu banco, onde incorporará as claves ou coordenadas da súa tarxeta bancaria, número de conta ou de tarxeta de crédito, etc., co fin de copiarlla e utilizala posteriormente de forma fraudulenta, causándolle dano.
- Non** se debe pinchar ou **facér click** co rato **nunha ligazón deste tipo recibido por correo electrónico**, debese **acceder directamente á páxina de confianza escribindo o enderezo**.



## Exemplo Phising Amazon (fai clic na imaxe):



## Spam

- Se recibimos na nosa conta de correo **spam** ou correo indiscriminado, debemos **comunicalo ao noso servizo de correo electrónico**.
- Unha das medidas das que dispoñemos é **marcalo como spam**, o servizo de correo utiliza algoritmos para mellorar a experiencia dos usuarios e, o máis probable é que ese enderezo de correo non volva a importunarnos na bandexa de entrada, pasará automaticamente á carpeta de spam.
- Ligazóns moi interesantes:
  - [Cómo detener la llegada de mensajes maliciosos o spam a nuestro correo electrónico](#)
  - [Consejos de seguridad: cómo evitar estafas de phishing](#)
  - [Correo no deseado \(spam\)](#)
- [Cómo borrar automáticamente los correos recibidos en Gmail de una dirección concreta:](#)

## Denuncia

- Se estimamos realizar **denuncia** ante as forzas e **corpos de seguridade do estado** por un intento de dano ou fraude ou calquera outra situación grave ou desagradable, debemos **manter o correo orixinal** presentar o **encabezado da mensaxe**, no que se detalla a relación de ip da que parte e polas que vai pasando.
- Ligazóns interesantes:
  - [La Policía Nacional crea una dirección de correo electrónico donde denunciar el phishing](#)
  - [50 millones estafados con el timo de moda: hackear el mail a ejecutivos](#)
  - [La Policía alerta de una oleada de correos 'phishing' con facturas falsas de Endesa](#)
  - [Avisos de seguridad \(Oficina de Seguridad del Internauta\)](#)

## Decálogo antispam

### DECÁLOGO ANTISPAM DA AXENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Tal e como se pode ler no seu sitio web, o día de internet de 2005, a Axencia Española de Protección de Datos publicou un decálogo bastante útil para todos os internautas que se quixeran protexer contra o spam, que, por aquel momento representaba o 70% do correo electrónico.

Varios anos despois, aínda seguen a estar de actualidade e ser útiles:

Ser coidadoso ao facilitar a dirección de correo. Facilitar unicamente a dirección de correo a aquelas persoas e organizacións nas que confía e que queira comunicar.

Utilizar dous ou máis direccións de correo electrónico. Utilice unha dirección para aqueles casos nos que non se confíe ou coñeza o suficiente ao destinatario, e outra dirección persoal que sexa coñecida unicamente polos seus amigos ou polos seus contactos profesionais.

Elixir unha dirección de correo pouco identificable. Para crear unha dirección de correo electrónico e reducir o envío de spam, sería conveniente non introducir campos que sexan potencialmente identificables polo spammer.

Non publicar a dirección de correo. Non se debe anunciar a dirección de correo en buscadores, directorios de contactos, foros ou páxinas web. Cando envíe correos nos que aparezan moitas direccións, envíeas usando con copia oculta. Se é necesario facilitar a dirección de correo nalgunha web, escriba [at](#) ou [arroba](#) en lugar de @. Así mesmo, se reenvía un correo, elimine as direccións dos anteriores destinatarios.

Ler detidamente as Políticas de Privacidade e as Condicións de Cancelación. Se se vai a subscribir a un servizo en liña ou a contratar un produto, revise a política de privacidade. Non dubide en exercer os dereitos de acceso e cancelación sobre os seus datos ante estas empresas.

Sensibilizar aos nenos sobre a utilización do correo e a mensaxería instantánea. Os nenos son obxectivos ideais para promocionar información sobre a composición e as prácticas de consumo do fogar. Ademais, os correos que poden ter contidos non aptos para os nenos.

Non é conveniente contestar ao spam. É conveniente desactivar a opción que envía un acuse de recibo ao remitente das mensaxes lidas do sistema de correo electrónico. Se un spammer recibe dito acuse saberá que a dirección está activa, e o máis probable é que lle envíe máis spam.

Non pique sobre os anuncios dos correos lixo. Entrando nas páxinas web dos spammers podemos demostrar que a nosa conta de correo está activa, co que pode converterse nun obxectivo para novos envíos.

Utilice filtros de correo. Os programas de xestión de correo electrónico e moitas páxinas web ofrecen a posibilidade de activar filtros que separan o correo desexado do spam.

Manteña ao día o seu sistema. Utilice programas antivirus e actualizacións e parches que corríxen os problemas detectados nos programas do seu equipo. Ademais, é moi recomendable a instalación de devasa para monitorizar o que ocorre no computador.

### Medidas en función do medio de comunicación na rede

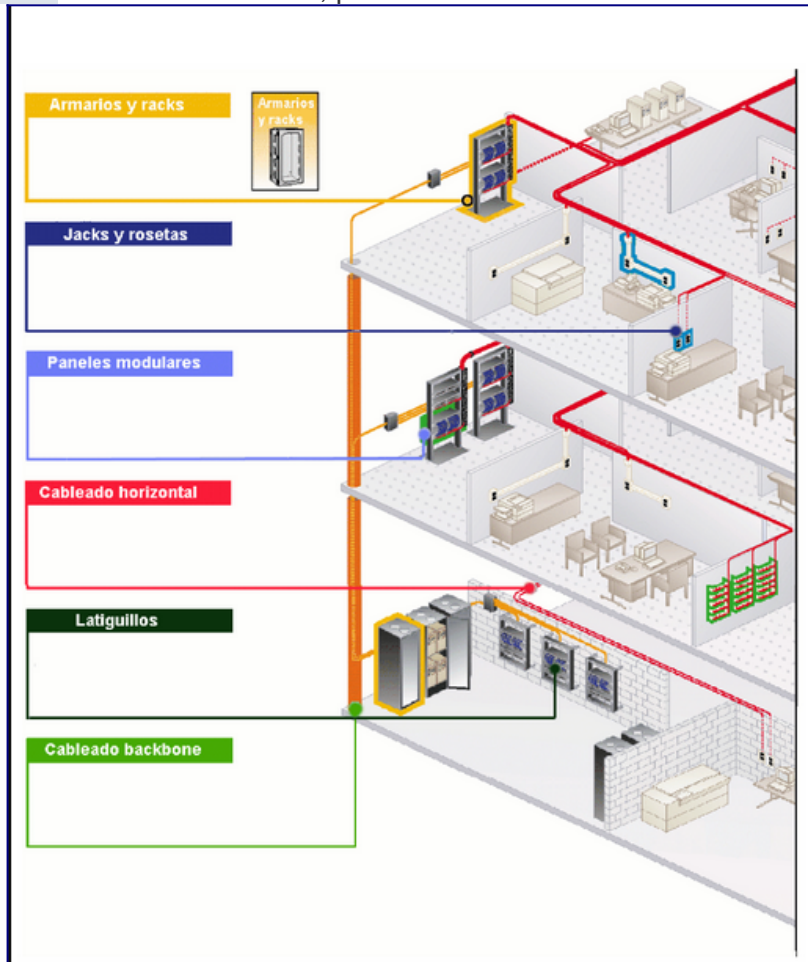
O máis habitual é que na nosa rede local, sexa na casa ou na empresa, contemos con equipamento que se conecta á rede:

- ben a través de cable
- ben a través de tecnoloxía sen fíos.

## Redes cableadas

- Os equipos e periféricos conéctanse a través de cables e a súa limitación é física, xa que o alcance dos cables é limitado, xeralmente dentro dun mesmo edificio.
- Este tipo de redes son as máis utilizadas en empresas e edificios para conectar os equipos entre eles e cos servidores.

Se fas clic na imaxe, podes obter información sobre cableado estruturado:



Tamén podes obter información sobre cableado estruturado en [Técnicas Profesionales](#).

- Para que se leve a cabo un ataque dunha rede [LAN](#) (Rede de área Local), o atacante debe estar fisicamente conectado a ela, atoparse dentro da organización. Moitas veces, os ataques son cometidos por persoas da propia organización, empregados.
- O cable non pode atoparse fisicamente visible, tarde ou cedo o atacante acaba por realizar o cometido, faise necesario establecer certas normas de seguridade, utilizar canaletas de protección, falso chan ou falso teito e unha instalación na zona de seguridade do edificio.
- O [ataque máis habitual](#) é o que se realiza mediante software, empregando [sniffers](#), un programa que rexistra todo o tráfico da rede en busca de contrasinais e datos relevantes que poda transmitir.
- Se queremos protexernos dos sniffers, debemos utilizar as conexións privadas para cada dispositivo, por exemplo, con unha [VPN](#).
- Tamén se pode realizar filtrado por [MAC](#) e por [IP](#), así como abrir e pechar [portos](#) do router, accedendo ao mesmo mediante un navegador. É dicir, podemos establecer que equipos con que MAC's ou con que IP's se poden conectar á rede, de xeito que calquera outro

equipo que o intente, non poda facelo sen pedir ao administrador da rede que inclúa o seu enderezo no grupo de enderezos aos que se lles permite o acceso á rede.

## Redes sen fíos

- Todas as redes sen fíos perden a seguridade que ofrecen as LAN cableadas, dado que é posible acceder a elas sen necesidade de acceso ao entorno físico.
- Calquera equipo que se conecte á rede sen fíos terá acceso ao resto da rede. É imprescindible protexer os equipos para que, se se da a intrusión, se manteña a máxima seguridade posible, pero tamén debemos evitar que sistemas non autorizados rompan a seguridade sen fíos e se podan conectar.
- Podemos establecer unha serie de consellos básicos de seguridade para a nosa rede:
  - **Non** deixes a rede sen fíos **aberta**, sen protección (sen contrasinal), posto que calquera podería acceder aos nosos datos privados e ademais reduciríase o ancho de banda, posto que teríamos que repartilo entre os equipos que se conecten.
  - **Cambia a configuración por defecto do router**. Aínda que agora a maioría dos routers levan activada unha encriptación básica, cun contrasinal que vén de fábrica e que está indicada no manual ou nunha pegatina pegada ao propio router, este contrasinal é facilmente descifrado. Para acceder á configuración do router e cambiala, debemos escribir a súa dirección no navegador, (debería vir indicado no manual do router, por exemplo 192.168.0.1). Dende aquí poderás cambiar calquera aspecto que estimes, empezando polo nome da propia rede (SSID) e o contrasinal necesario para unirse á rede e que debe ser diferente do contrasinal para acceder á configuración do router.
  - Debemos **utilizar** algún tipo de **encriptación** na nosa rede, onde a información debe viaxar encriptada cun algoritmo de complexa desencriptación, cunha lonxitude de contrasinal de encriptación o máis longa posible, se pode ser 512 bits, non utilizemos 128.

Os routers sen fíos poden utilizar diferentes tipos de encriptación, por exemplo:

- **WEP**. É o tipo de encriptación que incorporan por defecto, algoritmo non moi fiable, de fácil desencriptado.
- **WPA**. É un protocolo máis robusto que o anterior. Non é indescifrado, o desencriptado pódese realizar utilizando dicionarios e forza bruta, pero se mantemos unha boa política de contrasinais, é moi fiable.
- **WPA2**. O algoritmo máis completo, é un algoritmo complexo e de difícil desencriptación.

Usuario e contrasinal de acceso ao router para configurar a rede



THOMSON  
images & beyond

Administration

Gateway

VoIP

Status -

Network -

Advanced -

Firewall -

Parental Control -

Wireless

Software

Connection

**Password**

Diagnostics

Event Log

Initial Scan

Switch Mode

Backup/Restore

### Status

**Password :** This page allows configuration of administration access privileges and the ability to restore factory defaults to the system.

---

User Name

Password

••••••

Re-Enter Password

••••••

Restore Factory Defaults

☐ Yes
 ☒ No

### Exemplo encriptación WPA2 para a rede



THOMSON  
images & beyond

Administration

Gateway

VoIP

Status -

Network -

Advanced -

Firewall -

Parental Control -

Wireless

Radio

**Primary Network**

Guest Network

Access Control

Advanced

Bridging

WMM

### Wireless

**802.11 Primary Network :** This page allows configuration of the Primary Wireless Network and its security settings.

---

Primary Network

(00:24:d1:8d:b0:15)

Primary Network

Network Name (SSID)

Closed Network

WPA

WPA-PSK

WPA2

WPA2-PSK

WPA/WPA2 Encryption

WPA Pre-Shared Key

••••••••••

☐ Show Key

RADIUS Server

RADIUS Port

RADIUS Key

**Identificador, nome da rede**

**Automatic Security Configuration**

**Encriptación WPA2**

Group Key Rotation Interval

WPA/WPA2 Re-auth Interval

Podemos proporcionar aínda máis seguridade adicional á nosa rede sen fíos, para o cal:

- Creamos unha **lista coas direccións MAC que desexemos se conecten á rede**. Cada dispositivo con tarxeta de rede sen fíos, xa sexa móbil, tablet u ordenador, ten unha dirección única que o identifica, a dirección MAC. Con esa información, podemos crear unha lista de dispositivos autorizados na nosa rede, para que ningún outro dispositivo se poda conectar sen que lle deamos de alta a súa dirección na lista. De todos os

xeitos, esta medida tampouco é infalible, xa que un usuario avanzado con malas intencións pode simular que a MAC do seu ordenador é unha das MAC autorizadas.

- **Comprobar que dispositivos están conectados á nosa rede.** Desta forma, podemos saber se temos un intruso, e actuar en consecuencia, cambiando inmediatamente o contrasinal e o SSID da nosa rede.
- **Actualizar o firmware.** Recordemos que o firmware é o software que controla os dispositivos. Habitualmente, os fabricantes proporcionan actualizacións para subsanar erros de seguridade detectados, para mellorar o rendimento, ...

MAC's admitidas e equipos conectados neste momento

## Wireless

**802.11 Access Control** : This page allows the configuration of the Access Control to the AP as well as status on the connected clients.

Administration Web Page Access  (Allow or Deny Access to Administration Web Page from PC connected over Wifi.)

Wireless Interface

MAC Restrict Mode

|               |                      |                      |
|---------------|----------------------|----------------------|
| MAC Addresses | BC:85:56:B1:59:23    | <input type="text"/> |
|               | C0:C9:76:87:96:D0    | <input type="text"/> |
|               | 98:FE:94:A1:88:A7    | <input type="text"/> |
|               | 14:DA:E9:35:35:B0    | <input type="text"/> |
|               | C0:C9:76:25:FA:28    | <input type="text"/> |
|               | <input type="text"/> | <input type="text"/> |
|               | <input type="text"/> | <input type="text"/> |
|               | <input type="text"/> | <input type="text"/> |

MAC's que teñen permiso para conectarse á rede

Equipos conectados neste momento

| Connected Clients | MAC Address       | Age(s) | RSSI(dBm) | Type | IP Addr      | Host Name                |
|-------------------|-------------------|--------|-----------|------|--------------|--------------------------|
|                   | BC:85:56:B1:59:23 | 0      | -79       | 11g  | 192.168.0.13 | Ana_Veloso               |
|                   | C0:C9:76:87:96:D0 | 9      | -66       | 11g  | 192.168.0.15 | android-54f7614e6c24fb85 |
|                   | 98:FE:94:A1:88:A7 | 9      | -57       | 11g  | ERROR        | ERROR                    |
|                   | 14:DA:E9:35:35:B0 | 9      | -68       | 11g  | 192.168.0.11 | android-560dfbd31460ff42 |

- **Ocultamos a nosa rede**, indicando que o **SSID non sexa visible**. Aínda que existen ferramentas que poden revelar este nome con facilidade, sempre complica as cousas un pouco. Ademais, para moitos, se non se ve, non existe, polo que a rede pasará desapercibida para moitos posibles agresores.



Ocultar SSID

Administration

Gateway VoIP Status - Network - Advanced - Firewall - Parental Control - Wireless ↻

**Wireless**

802.11 Primary Network : This page allows configuration of the Primary Wireless Network and its security settings.

Primary Network Figueira (00:24:d1:8d:b0:15)

Primary Network  Automatic Security Configuration

Network Name (SSID)

Closed Network

WPA

WPA-PSK

WPA2

WPA2-PSK

Marcamos closed para hacer oculto o SSID

- Limitar o número de conexións á rede, para que non haxa máis das que necesites, de xeito que cando chegue ao máximo establecido, non admitirá novas conexións. Se nalgún momento necesitamos aumentar o número de dispositivos que se poden conectar simultaneamente, podemos ampliála temporalmente.
- Configurar o router para que só se poda acceder e configurar dende unha conexión LAN, e non a través da rede WiFi.
- Tamén é unha boa opción desactivar o DHCP e asociar direccións MAC a IPs de maneira estática no router.

Activación/desactivación DHCP

THOMSON  
images & beyond

Administration

Gateway VoIP Status - Network - Advanced - Firewall - Parental Control - Wireless ↻

**Network**

LAN : This page allows configuration and status of the optional internal DHCP server for the LAN.

Network Configuration

IP Address

Subnet Mask

MAC Address

DHCP Server ☒ Yes ☐ No

Lease Pool Start

Lease Pool End

Lease Time

Apply

Activar/Desactivar DHCP para asignar/ou non IP de forma automática ás máquinas da rede

Rango de IP's que proporciona o router

Por último, citaremos algún manual de router que atopamos ben documentado, aínda que como sabedes, cada modelo ten as súas particularidades.

O importante é saber o que temos que configurar, para despois buscar como facelo no router co que esteamos a traballar.

[MANUAL DE PROCEDIMIENTO: CONFIGURACION DE CONEXION. WIFI SEGURA EN EL HOGAR](#)

[Cómo configurar correctamente la seguridad en nuestro router](#)

[TP-LINK TL-WR1043ND ULTIMATE: Manual de configuración](#)

### Vídeos interesantes

Se non podes visualizar o seguinte vídeo, fai clic na ligazón [Chema Alonso: 'Internet no se creó como una herramienta híper segura'](#)

Chema Alonso: 'Internet no se creó como una herramienta híper segura' | [TecnoXplora Licenza de Youtube CC BY](#)

[Cómo usar las redes públicas wifi](#) | [Federal Trade Commission Licenza de Youtube CC BY](#)

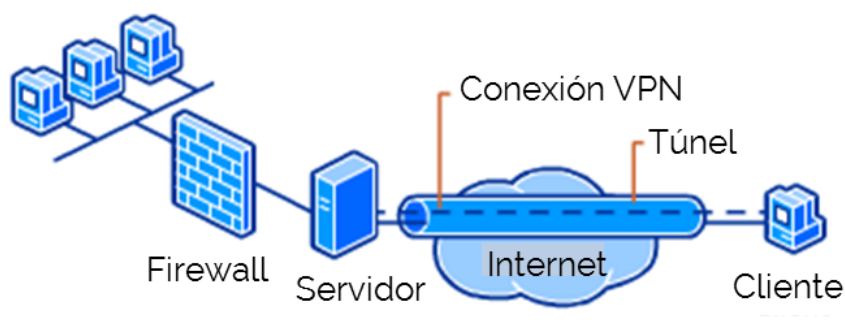
### Redes privadas virtuais

As redes privadas virtuais, ou [VPN](#), son conexións privadas entre dous ordenadores, que se establece a través dun modo público como internet.

Toda a información que se transmite a través dunha VPN viaxa cifrada e unicamente pode ser descifrado polo receptor, deste xeito, non quedan expostos a terceiros en internet.

Para que todo o tráfico VPN se poda considerar seguro, é necesario que se garantan catro principios básicos:

- Autentificación e autorización
- Non repudio
- Integridade
- Confidencialidade



Se vos interesa profundar neste tema podedes consultar os seguintes artigos:

[Qué es una conexión VPN, para qué sirve y qué ventajas tiene?](#)

[Cómo conectarte, crear y configurar tu propia red VPN](#)

Se non podes acceder ao seguinte vídeo fai clic na ligazón [How VPN Works](#)

[How VPN Works](#), [CyberGhost VPN](#), [Licenza de Youtube CC BY](#)

Algúns servizos de VPN dispoñibles actualmente que ofrecen solucións gratúitas para os usuarios que desexan cifrar o seu tráfico, protexer a súa identidade, ou saltar bloqueos rexionais de sitios web, son:

- [TunnelBear](#): [TunnelBear. Manual de uso e rendemento](#)
- [Hotspot Shield](#): [Revisión de Hotspot Shield](#), [Hotspot Shield](#), [Proxy seguro gratuito para tus conexiones WIFI](#)
- [FrootVPN](#): [FrootVPN, el servidor VPN gratuito que lucha contra el espionaje en la red](#)

### Ligazóns

Outras ligazóns nas que podedes atopar información de utilidade son as seguintes:

<http://www.softzone.es/herramientas-del-sistema/>  
<https://www.infospysware.com/>  
<https://www.consumidor.ftc.gov/temas/Privacidad%2C-identidad-y-seguridad-en-l%C3%ADnea>  
<https://www.consumidor.ftc.gov/recursos>  
<http://handbook.parentnets.com/gl/>  
<http://busport.blogspot.com.es/2012/07/como-crear-una-contrasena-segura.html>  
<http://es.wikihow.com/navegar-seguro-en-Internet>