

## **Introducción**

Esta página pretende dar unos consejos básicos para trabajar de forma más segura dentro de una red como la de UGR. Los consejos son generales y se pueden seguir independientemente del sistema operativo que utilicemos. Concretamos estos consejos para el sistema operativo *Windows 7*, pero todo lo que decimos (excepto algunas cosas puntuales) son igualmente válidas para las versiones anteriores de Windows.

## **Software Maligno**

El software maligno habitual con el que nuestro equipo puede ser infectado:

- Virus
- Gusanos
- Troyanos
- Puertas Traseras
- Nukers
- Keyloggers

## **Incidentes habituales**

Las cuestiones habituales por las que su equipo puede tener una incidencia de seguridad son:

- Virus/gusanos
- Almacenes de warez (software ilegal, música, películas,...)
- Servidores de IRC.
- Ataques a otras máquinas
- Control total de la maquina pirateada

La evolución natural de un fallo de seguridad es:

1. Descubrimiento del fallo en la seguridad de su equipo
2. Comunicación al responsable del mismo
3. Publicación del fallo
4. Parche disponible
5. Instalación del parche por parte de los usuarios
6. Aprovechamiento del error por parte de los piratas

## **Soluciones Generales**

Estos consejos son válidos para cualquier sistema operativo y versión.

1. Mantener el sistema actualizado
2. Reducir los servicios ofrecidos a los necesarios, como compartir archivos, servidor web, servidor ftp,...
3. Utilizar un antivirus
4. Utilizar un cortafuegos
5. Evitar ejecutar programas de dudosa procedencia (adjuntos de correo, descargas de internet,...)

## Consejos para Windows 7

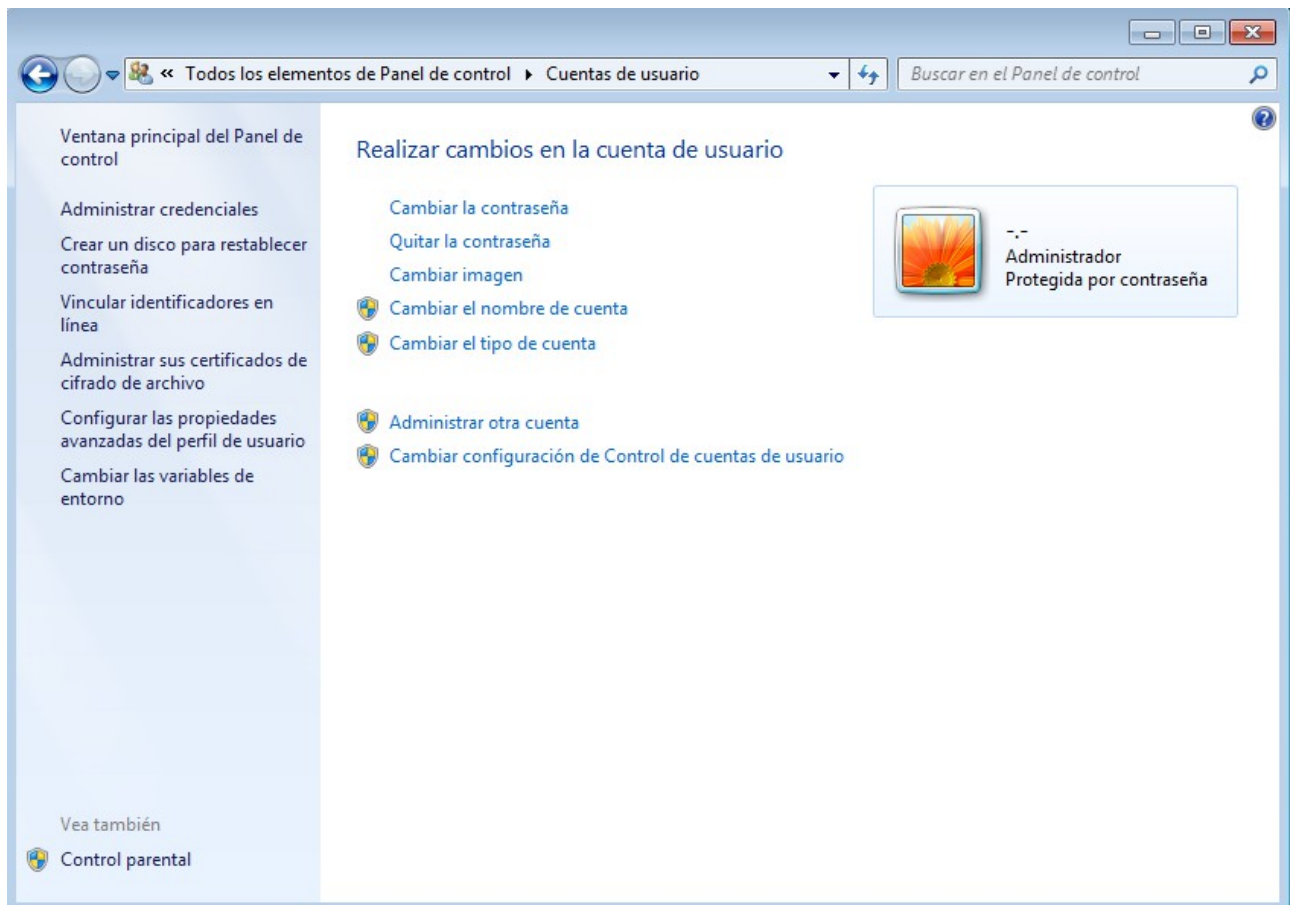
Este apartado trata de explicar más detalladamente las ideas expuestas anteriormente, concretamente para Windows 7 pero son consejos igualmente válidos para Windows anteriores.

### Usuarios y Contraseñas

Es importante crear usuario y asignarles contraseñas.

Al encender el equipo por primera vez, Windows nos indicará que hay que elegir un usuario y una contraseña, si no fuese así deberemos hacerlo manualmente. Para hacerlo:


Inicio --> Panel de Control --> Cuentas de usuario




Seleccionamos Administrar otra cuenta y después Crear una nueva cuenta

Windows Control Panel window: "Cuentas de usuario" > "Administrar cuentas". Search bar: "Buscar en el Panel de control".

### Elegir la cuenta que desee cambiar




Administrador  
Protegida por contraseña



Invitado  
La cuenta de invitado está desactivada

[Crear una nueva cuenta](#)  
[¿Qué es una cuenta de usuario?](#)

**Acciones adicionales que se pueden realizar**

-  [Configurar Control parental](#)
- [Ir a la página principal de Cuentas de usuario](#)

Windows Control Panel window: "Administrar cuentas" > "Crear nueva cuenta". Search bar: "Buscar en el Panel de control".

### Dar un nombre a la cuenta y elija un tipo de cuenta

Este nombre aparecerá en la pantalla de inicio de sesión y en el menú Inicio.

- Usuario estándar**  
Los usuarios de cuentas estándar pueden usar la mayoría de software y cambiar la configuración del sistema que no afectan a otros usuarios ni a la seguridad del equipo.
- Administrador**  
Los administradores tienen acceso completo al equipo y pueden hacer los cambios que deseen. Según la configuración de las notificaciones, es posible que se pida a los administradores que proporcionen su contraseña o una confirmación antes de realizar cambios que puedan afectar a otros usuarios.

Se recomienda proteger todas las cuentas con una contraseña segura.

[¿Por qué se recomienda usar una cuenta estándar?](#)

Windows Control Panel window: **Cuentas de usuario > Administrar cuentas**. Search bar: *Buscar en el Panel de control*.

### Elegir la cuenta que desee cambiar



Administrador  
Protegida por contraseña



Usuario  
Administrador



Invitado  
La cuenta de invitado está desactivada

[Crear una nueva cuenta](#)  
[¿Qué es una cuenta de usuario?](#)


**Acciones adicionales que se pueden realizar**

-  [Configurar Control parental](#)
- [Ir a la página principal de Cuentas de usuario](#)

Windows Control Panel window: **Administrar cuentas > Cambiar una cuenta**. Search bar: *Buscar en el Panel de control*.


### Realizar cambios en la cuenta de Usuario

- [Cambiar el nombre de cuenta](#)
- [Crear una contraseña](#)
- [Cambiar la imagen](#)
- [Configurar Control parental](#)
- [Cambiar el tipo de cuenta](#)
- [Eliminar la cuenta](#)
- [Administrar otra cuenta](#)



Usuario  
Administrador

Crear una contraseña para la cuenta de Usuario

 Usuario  
Administrador

Está creando una contraseña para Usuario.

**Si hace esto, Usuario perderá todos los archivos EFS cifrados, certificados personales y contraseñas almacenadas para los sitios web o los recursos de red.**

Para evitar pérdida de datos en el futuro, solicite a Usuario que cree un disquete para restablecer contraseñas.

Si la contraseña contiene mayúsculas, no se olvide de escribirlas de la misma forma.  
[Cómo crear una contraseña segura](#)

El indicio de contraseña será visible para todos los usuarios que utilicen este equipo.  
[¿Qué es un indicio de contraseña?](#)

### Constraseñas que deben evitarse

- Nombres y apellidos propios o de familiares y amigos
- Nombre del sistema operativo, cuenta, nombre de usuario o máquina que se esté usando.
- Números de teléfono, fechas de nacimiento, DNI, matriculas,...
- Lugares geográficos
- Nombres de famosos, marcas, personajes de ficción, ...
- Cualquier palabra de un diccionario español o extranjero
- Añadir un dígito o un carácter especial a una palabra de las categorías anteriores NO SIRVE DE NADA. Por ejemplo, NO SON BUENAS CONTRASEÑAS: manolo1, 2hermanas, ...

### Sugerencias para elegir una contraseña

- Difícil de adivinar y fácil de recordar
- Acrónimo separado por caracteres especiales (/,#,!,-,...)
- Siglas de frase no muy conocida (o propia) e intercalar caracteres especiales

### Protección de la clave

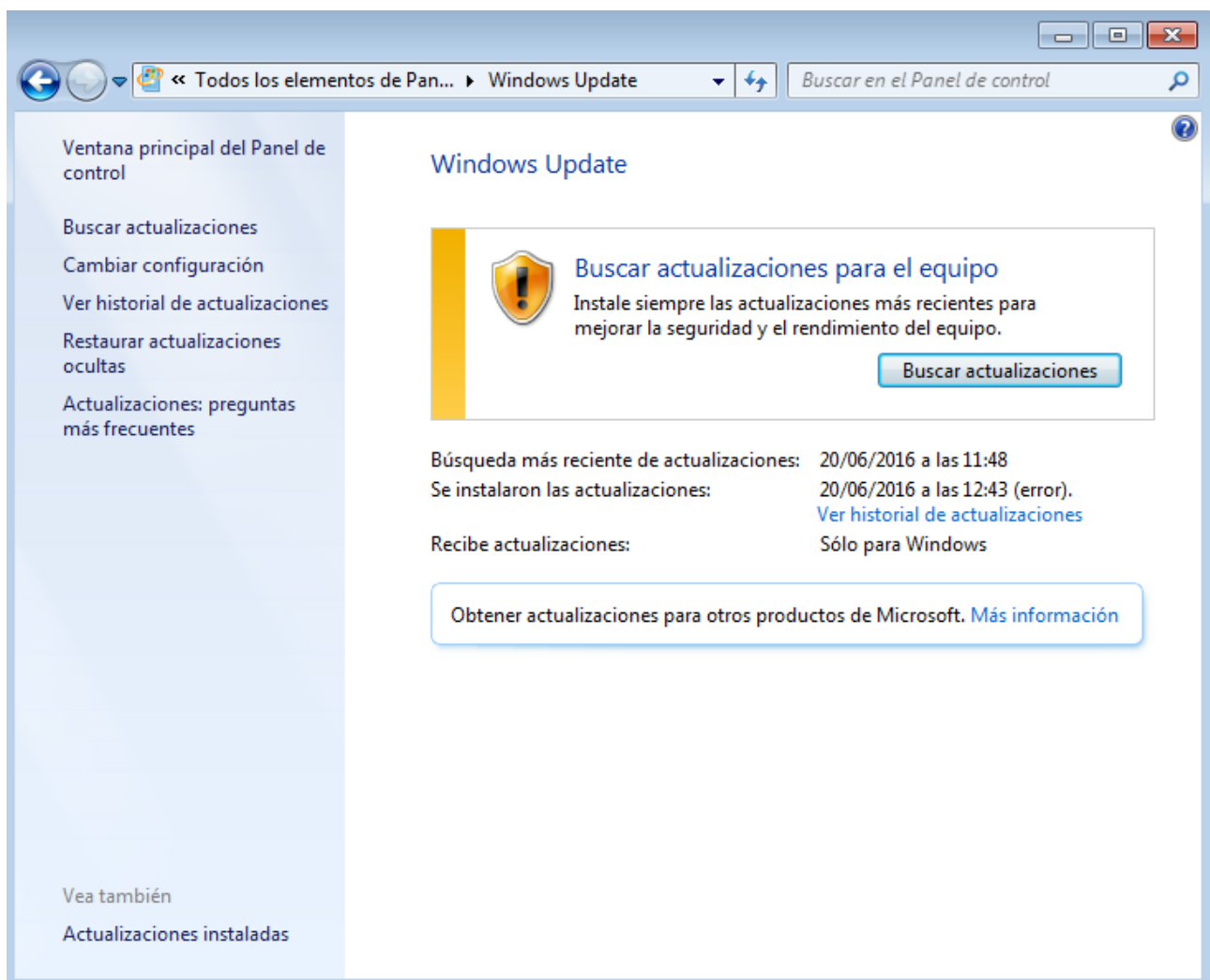
- No permitas que nadie use tu clave
- No anotes tu clave
- No la teclees cuando alguien te mira
- Si la has compartido, cámbiala inmediatamente.
- **RECUERDE:** UGR nunca le pedirá su usuario y clave a través de e-mail, teléfono, fax, sms, ....

## Consejos básicos

- No tener la misma clave en diferentes ordenadores
- Longitud de al menos 8 caracteres
- Usar al menos dos caracteres no alfabéticos y evitar situarlos al principio o al final
- No usar secuencias de teclado, "qwerty"
- Alternar mayúsculas y minúsculas
- Cambiarlo al menos cada 3 meses
- Si la has compartido, cámbiala de inmediato

## **Windows Update y Actualizaciones Automáticas**

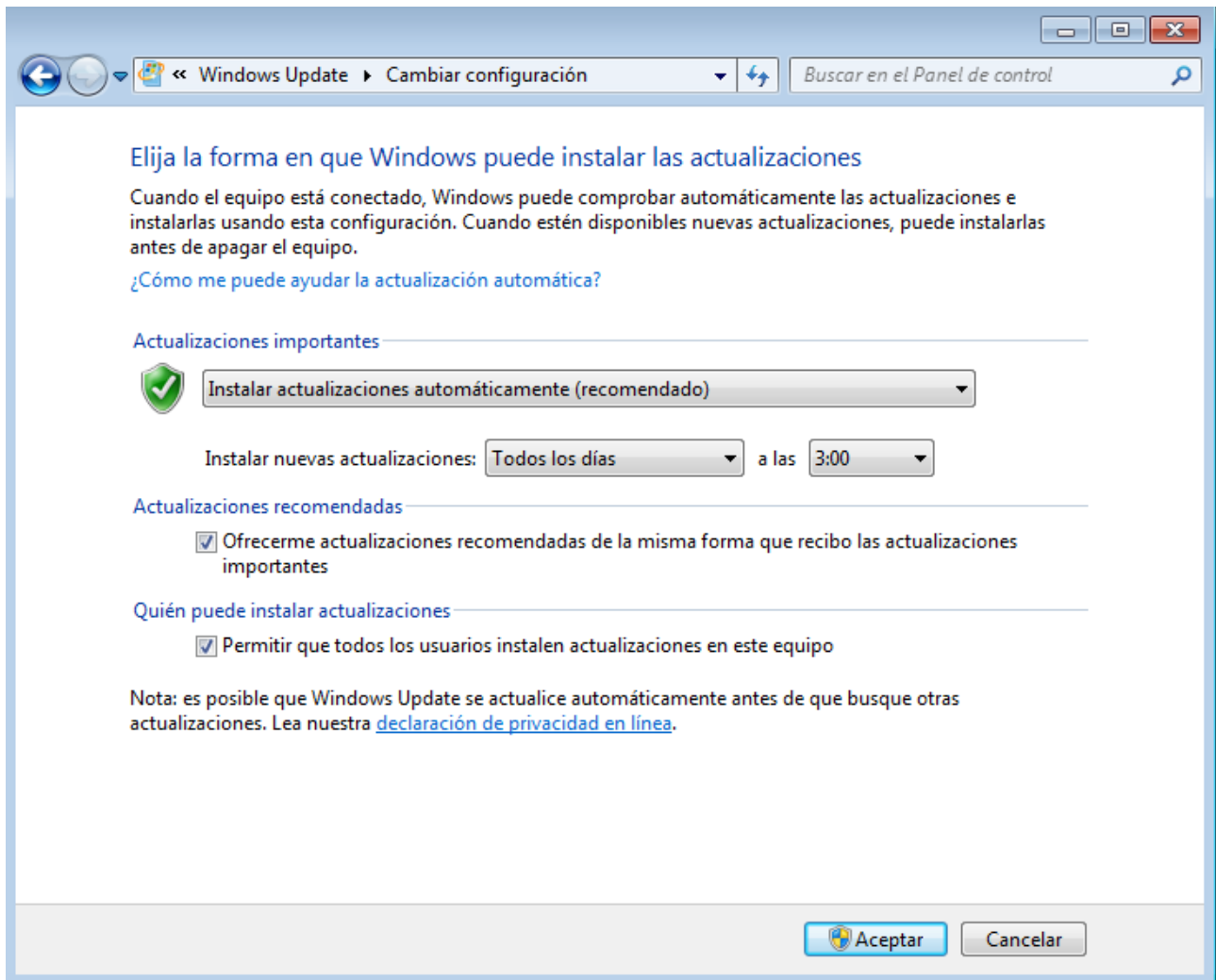
Proceso a seguir para instalar los Service Pack por primera vez tras la instalación del sistema operativo Windows. Para ello hay que acceder a la página de Windows Update, se puede llegar desde Panel de control-->Windows Update.



Una vez encontrados los Service Pack disponibles para nuestro Windows 7 así como los parches de seguridad, los instalaremos todos para tener el sistema operativo del ordenador al día.

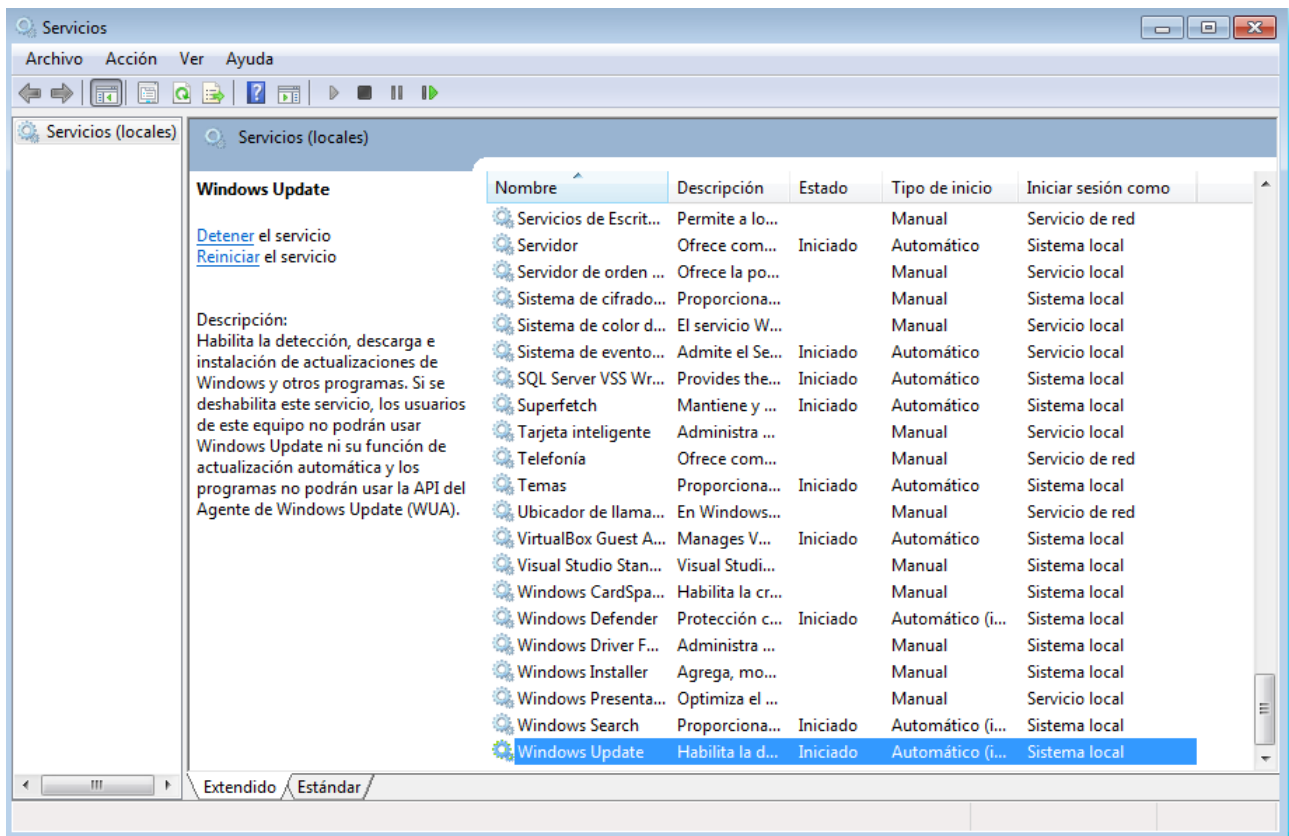
Una vez actualizado por primera vez el sistema operativo podemos configurar las *Actualizaciones*

automáticas. Para hacerlo entramos en la pestaña cambiar configuración



Elegimos la opción más adecuada a nuestras necesidades.

Para asegurarnos que está activado, comprobamos los servicios: Inicio --> Panel del control --> Herramientas Administrativas --> Servicios



Con este servicio activo se mantendrá nuestro Windows 7 actualizado.

## Servicios Peligrosos

A continuación se muestran los servicios que pueden constituir un riesgo para la seguridad de nuestro equipos y porqué.

- Pueden ser la vía de acceso para que los intrusos pueda:
  - Crear, borrar, modificar o extraer archivos del equipo.
  - Lanzar programas, por ejemplo un servidor web, un almacén de warez,...
  - Atacar otros equipos cercanos
- En la versión profesional están casi todos los servicios deshabilitados
- Los servicios que se deben deshabilitar si no se utilizan son:
  - Telnet: permite que un usuario remoto inicie una sesión en el equipo y ejecute programas
  - Asistencia remota y escritorio remoto: Inicio --> Panel de control --> Sistema --> Acceso remoto
  - Compartir archivos
  - Servidor web
  - Servidor ftp

## Utilizar un antivirus

Es importante utilizar un antivirus y tenerlo actualizado.

La UGR tiene licencia para [PANDA](#).



## Cortafuegos (Firewall)

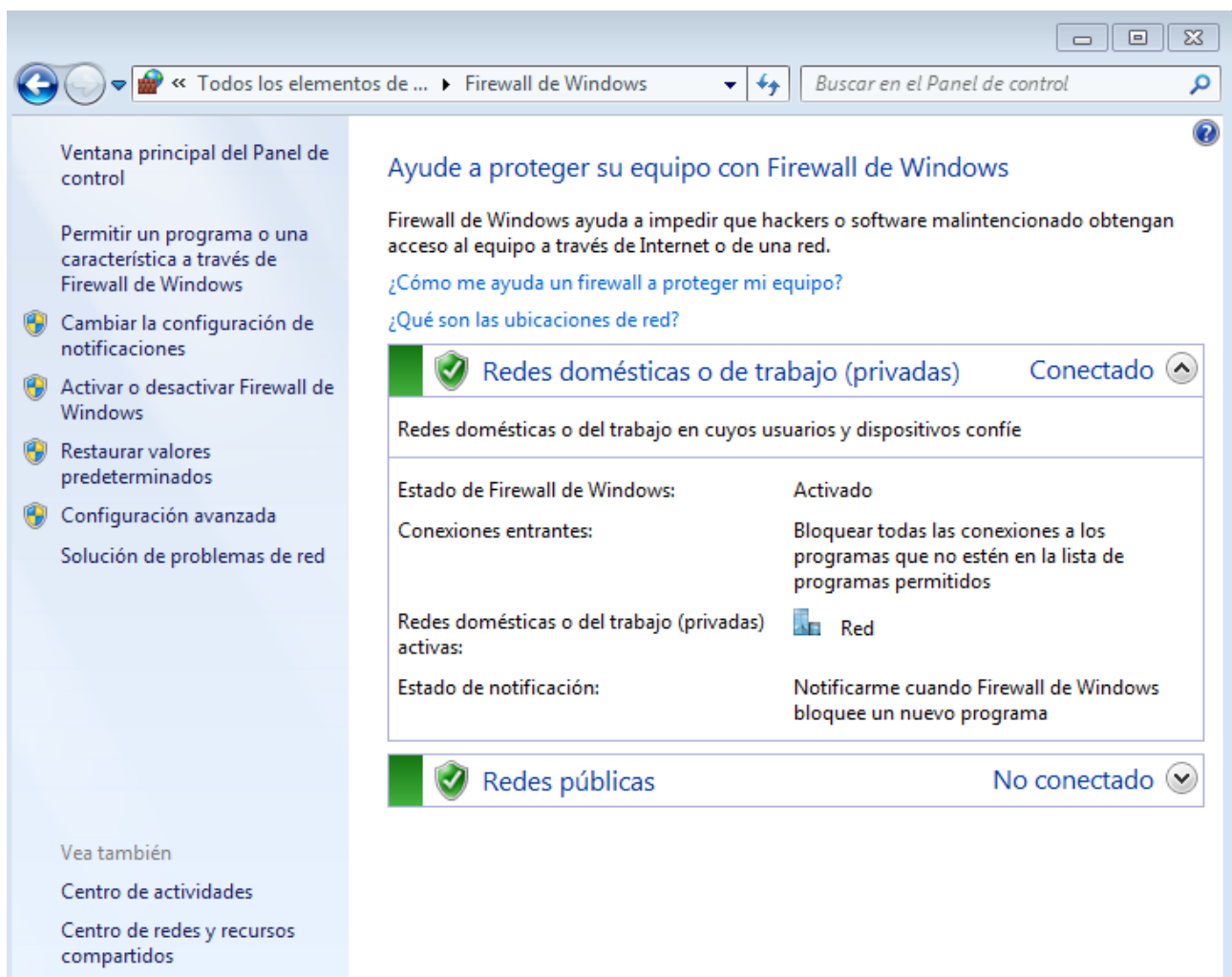
El cortafuegos aísla el ordenador de la conexión a la red filtrando información. Una configuración general debe llevar conexiones prohibidas, conexiones permitidas y conexiones permitidas con condiciones.

**IMPORTANTE:** SI ALGO DEJA DE FUNCIONAR, ANTES DE NADA, DESACTIVAR EL CORTAFUEGOS Y PROBAR SI FUNCIONA.

Hay muchas opciones a la hora de elegir un cortafuegos, algunos ejemplos son:

### De Windows 7

Inicio → Panel de control → Firewall de Windows



### Panda

- Versión primitiva -- no funciona bien sobretodo si se comparten recursos
- Si queremos instalar cualquier otro cortafuegos y tenemos o hemos tenido el PANDA activo, es importante desinstalar PANDA y luego volverlo a instalar sin la protección de firewall.

### **Configuración Cortafuegos de PANDA**

Inicio ▾



<b>Monitor de procesos</b>  <b>ACTIVADO</b> 45 procesos	<b>Navegación segura</b>  <b>ON</b>	<b>Firewall personal</b>  <b>ACTIVADO</b> Trabajo		
<b>Soporte</b> 	<b>Control de aplicaciones</b>  <b>OFF</b>	<b>Protección USB</b>  <b>ON</b>	<b>Kit de rescate</b> 	<b>Teclado virtual</b> 
<b>Protección de datos</b> 	<b>Optimizar PC</b> 	 <b>¿Quieres mejorar tu protección?</b>		



Configuración



General

Antivirus

Protección USB

Firewall

Monitor de procesos

Protección Wi-Fi

Navegación segura

Control de aplicaciones

Protección Firewall

ON

### Control de programas

Reglas de usuario:

- System (Allow incoming)
- inf\_evento\_inicio.exe (Allow outgoing)
- PSUAService.exe (Allow outgoing)
- svchost.exe (Allow incoming)
- AgentSvc.exe (Allow outgoing)
- PSANHost.exe (Allow outgoing)
- svchost.exe (Allow outgoing)

↑ ↓  
Añadir...  
Editar...  
Eliminar  
Restaurar

Importar... Exportar...

Activar reglas recomendadas por nuestros laboratorios.  
*Tienen menos prioridad que las reglas de usuario*

- Internet Information Server (Remote Administration)
- Remote Desktop
- Block Distributed Transaction Coordinator network connections on public networks

Visualizar...

Configuración



General

Antivirus

Protección USB

Firewall

Monitor de procesos

Protección Wi-Fi

Navegación segura

Control de aplicaciones

Activar reglas recomendadas por nuestros laboratorios.  
*Tienen menos prioridad que las reglas de usuario*

- Internet Information Server (Remote Administration)
- Remote Desktop
- Block Distributed Transaction Coordinator network connections on public networks
- Deny NetBIOS (UDP) over public networks (NT platform). Incoming connections
- Deny NETBIOS over public networks
- Deny INCOMING ICMP communications over public networks

Visualizar...

### Prevención de intrusiones

- Ip explicit path
- Land attack
- SYN flood
- TCP port scan
- TCP flag check