



INSTITUTO NACIONAL DE CIBERSEGURIDAD

# Taller formativo “Seguridad en dispositivos Windows y macOS”

---



GOBIERNO  
DE ESPAÑA

VICEPRESIDENCIA  
PRIMERA DEL GOBIERNO  
  
MINISTERIO  
DE ASUNTOS ECONÓMICOS  
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO  
DE DIGITALIZACIÓN E  
INTELIGENCIA ARTIFICIAL



TU AYUDA EN  
CIBERSEGURIDAD  




Oficina  
de Seguridad  
del Internauta



- ❖ Roles y usuarios: aspectos de seguridad y privilegios.
- ❖ Actualizaciones automáticas: sistema operativo y aplicaciones.
- ❖ Antivirus y herramientas de protección básicas.
- ❖ Características y gestión de las contraseñas.
- ❖ Copias de seguridad.
- ❖ Redes inalámbricas en el ordenador
- ❖ Seguridad básica en las redes.
- ❖ Cuestionario de evaluación.

# INTRODUCCIÓN

Nuestros dispositivos son una parte fundamental hoy en día.

Por ello es tan importante que **conozcamos algunas de sus funciones de seguridad básicas, así como las tareas de mantenimiento o configuraciones de seguridad que podemos llevar a cabo junto a los procesos automáticos que la mejoran.**



# 1. ROLES Y USUARIOS: ASPECTOS DE SEGURIDAD Y PRIVILEGIOS

Si no gestionamos adecuadamente los roles y cuentas, corremos el **riesgo** de:



Manipulación de información



Modificación de configuración



Acceso a nuestras cuentas

Por seguridad, lo ideal es mantener **un único usuario administrador por dispositivo** y **mantener al mínimo los privilegios del resto de cuentas** de usuario para evitar riesgos.



# 1.1 ROLES Y USUARIOS WINDOWS

Existen diferentes **tipos de cuentas**:



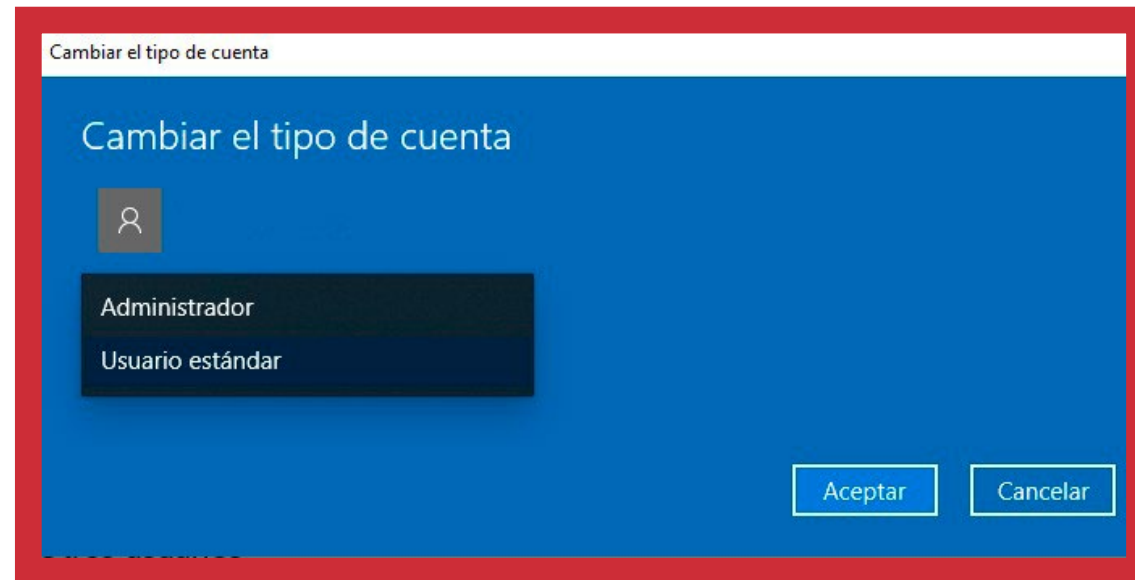
Usuario Administrador



Usuario “Tu familia”



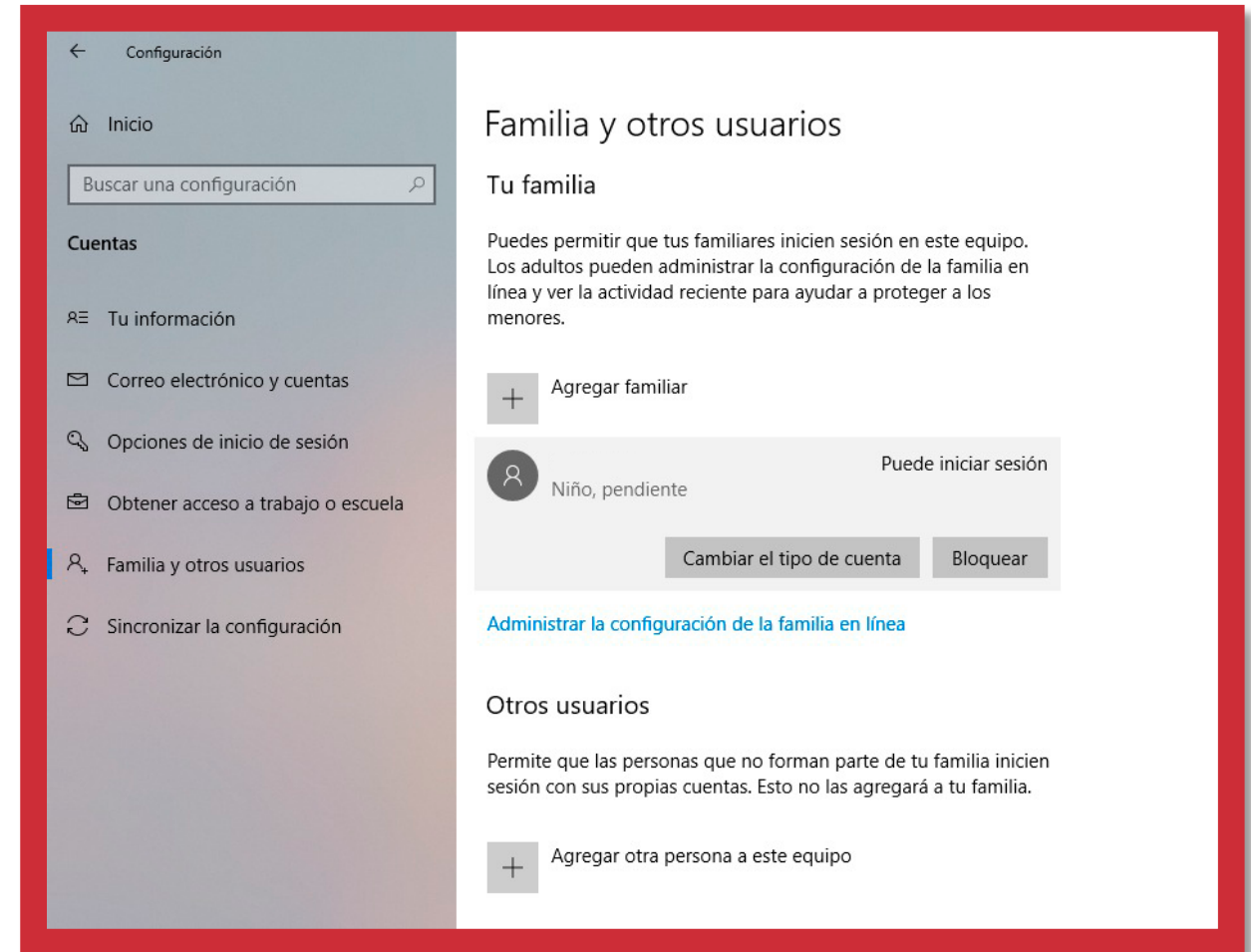
Otros usuarios



## 1.1 ROLES Y USUARIOS WINDOWS

Para **crear cuentas**:

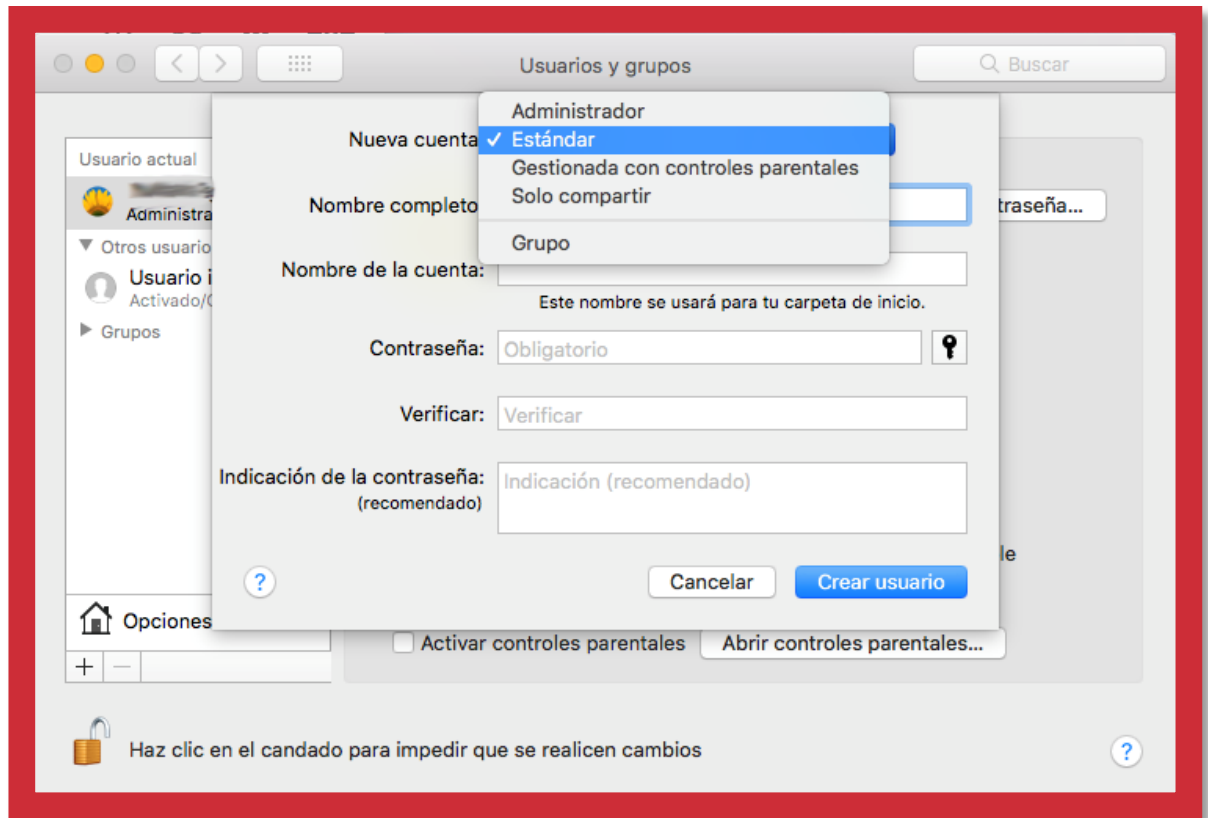
- ❖ Iremos a la **imagen de Windows** en la parte inferior izquierda.
- ❖ Clic en **Configuración > Cuentas > Familia y otros usuarios** u **Otros usuarios**.



## 1.2 ROLES Y USUARIOS MACOS

Debemos tener en cuenta que esta configuración solo la puede realizar un **administrador del sistema**:

- ❖ Logo Apple y clic en **Preferencias del sistema > Usuarios y Grupos**.
- ❖ Luego, clic sobre el **candado** para que se desbloquee.
- ❖ Ingresaremos con el **nombre del administrador y contraseña de acceso**.
- ❖ Seleccionaremos en el menú **Nueva carpeta** y elegiremos el **tipo de usuario** que queremos crear.



## 1.2 ROLES Y USUARIOS MACOS

Ahora podremos **configurar el perfil**:



Asignar clave



Asignar privilegios



Otras funciones



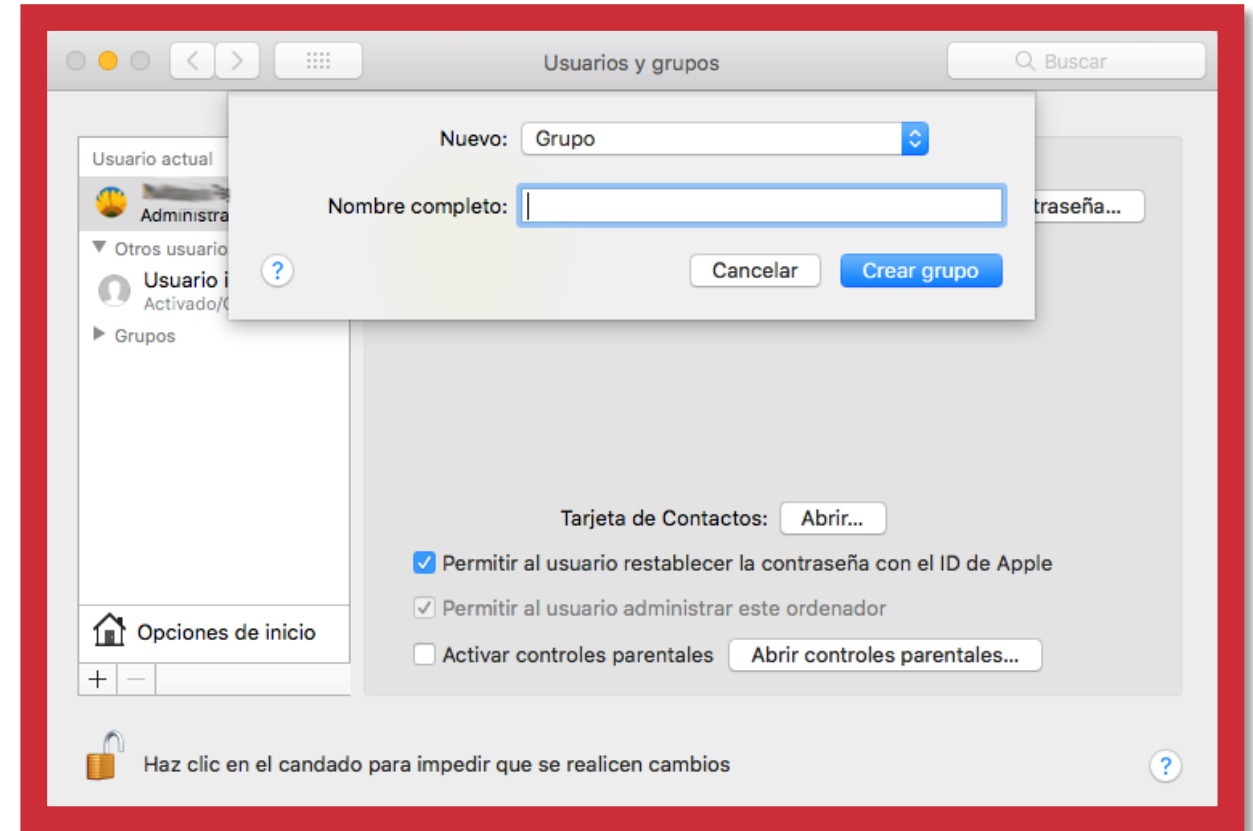
## 1.2 ROLES Y USUARIOS MACOS

### Otros perfiles y usuarios:

**Crear Grupo:** permite que varios usuarios puedan tener acceso al dispositivo o a un archivo específico, sin el nivel administrativo.

- ❖ **Usuarios y grupos > clic en candado > Ingresamos con nuestros datos.**
- **Añadir > Nueva cuenta > Nuevo grupo > Crear grupo.**

Luego, elegiremos los usuarios y podremos utilizar **Preferencias** para dar **permisos de compartir pantalla/archivos**.



**Usuarios ocasionales:** No requieren contraseñas, ni tienen privilegios de ningún tipo. Son temporales.



## 1.3 ROLES Y USUARIOS: ACTIVIDAD

### Actividad 1



Configurar los usuarios en el dispositivo, ayudará a evitar que se le realicen modificaciones al sistema sin nuestra autorización, con lo cual la seguridad sobre el dispositivo mejorará, así que vamos a crear nuestro propio usuario y asegurémoslo con una contraseña robusta.

## 2. ACTUALIZACIONES AUTOMÁTICAS: SISTEMA OPERATIVO Y APLICACIONES

Las actualizaciones son modificaciones realizadas sobre el sistema operativo o el *software* instalado en nuestros dispositivos. Su función es:

- ❖ Mejorar aspectos de funcionalidad.
- ❖ Mejorar la seguridad.
- ❖ Corregir vulnerabilidades o errores.



## 2.1 ACTUALIZACIONES AUTOMÁTICAS WINDOWS

### Actualizar el sistema operativo:

- ❖ Iremos a **Configuración > Actualización y Seguridad > Buscar actualizaciones**.

### Actualizar las apps y software:

- ❖ Utiliza **software original**.
- ❖ Descarga de la **página oficial**.
- ❖ Habilita **actualizaciones automáticas**.



## 2.2 ACTUALIZACIONES AUTOMÁTICAS MACOS

### Actualizar el sistema operativo:

- ❖ Iremos al logo de Apple > Preferencias del sistema > Actualizaciones del software.

### Actualizar las apps y software:

- ❖ Descarga de la página oficial > Actualizaciones > Mantener el Mac actualizado.



## 2.3 ACTUALIZACIONES AUTOMÁTICAS: ACTIVIDAD



GOBIERNO  
DE ESPAÑA

VICEPRESIDENCIA  
PRIMERA DEL GOBIERNO

MINISTERIO  
DE ASUNTOS ECONÓMICOS  
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO  
DE DIGITALIZACIÓN E  
INTELIGENCIA ARTIFICIAL



INSTITUTO NACIONAL DE CIBERSEGURIDAD

### Actividad 2



Un dispositivo actualizado es un dispositivo preparado para defenderse de todo tipo de virus y ataques al sistema. Tomemos unos minutos, accedamos a la configuración de nuestro dispositivo y asegurémonos de que está actualizado a la última versión, así como el software que tengamos instalado.

### 3. ANTIVIRUS Y HERRAMIENTAS DE PROTECCIÓN BÁSICAS

Su objetivo es **evitar** que los ataques a nuestro sistema logren causar daño o robar información.



Antivirus



Firewall



## 3.1 ANTIVIRUS Y HERRAMIENTAS DE PROTECCIÓN BÁSICAS WINDOWS

Microsoft incorpora un **antivirus (Windows Defender)** y un **Firewall** integrados.



Pueden configurarse desde el **Centro de Seguridad**:

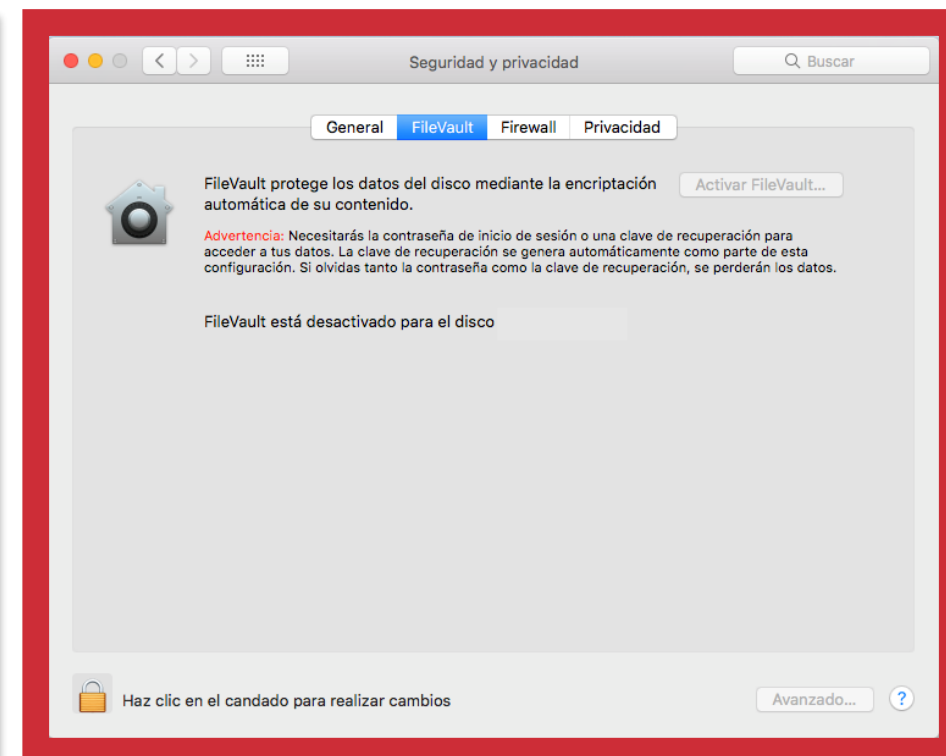
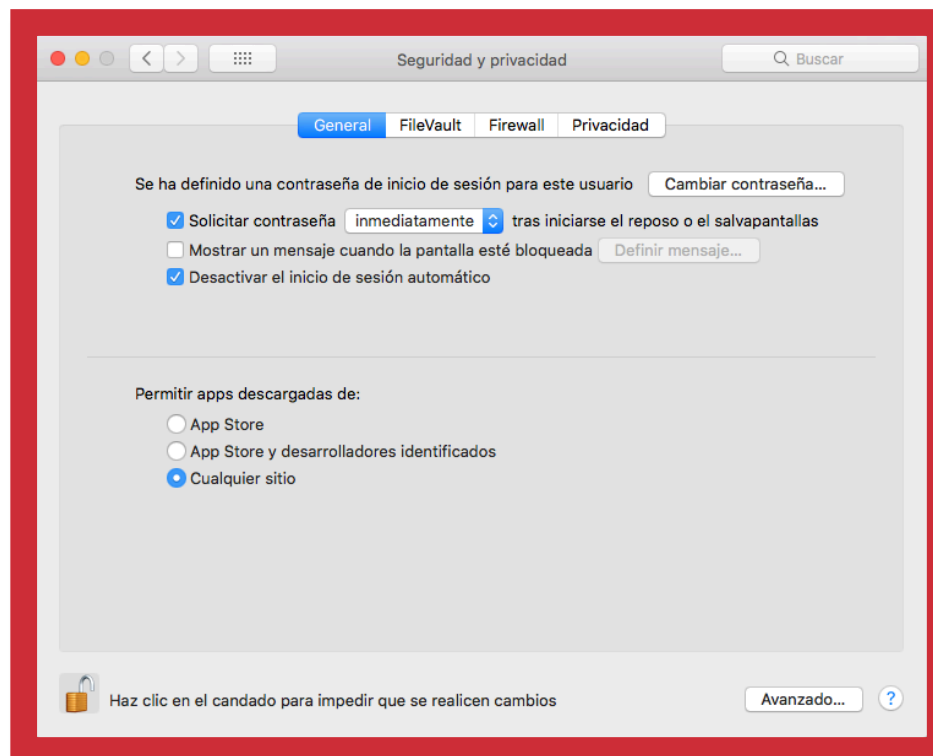
❖ Clic en el icono de **Windows Configuración** > **Actualización y Seguridad**.



## 3.2 ANTIVIRUS Y HERRAMIENTAS DE PROTECCIÓN BÁSICAS MAC

### Medidas de protección en Mac:

- ❖ Chip M1.
- ❖ Protección de la aplicación.
- ❖ App Review y Gatekeeper.
- ❖ Control sobre aplicaciones.
- ❖ FileVault2.



## 3.3 ANTIVIRUS Y HERRAMIENTAS DE PROTECCIÓN BÁSICAS: ACTIVIDAD

### Actividad 3



Las herramientas de protección de nuestro sistema nos protegen de una gran variedad de riesgos. Quizás sea el momento de asegurarnos que nuestras defensas están activadas. Vamos a entrar al sistema y comprobar que las herramientas mencionadas anteriormente están activadas y funcionando.

## 4. CARACTERÍSTICAS Y GESTIÓN DE LAS CONTRASEÑAS

Las pautas para crear una **contraseña robusta** son:

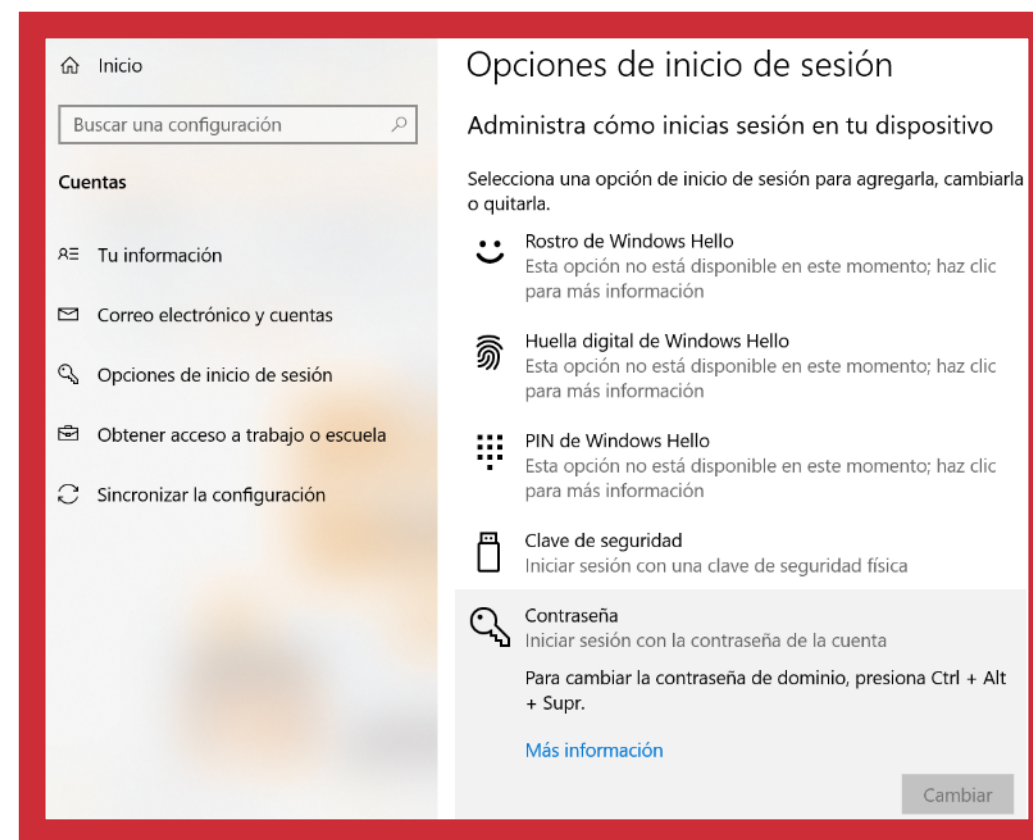
- ❖ Utilizar entre **8 y 10 caracteres mínimo**.
- ❖ Combinar **letras mayúsculas, minúsculas, números y caracteres especiales**.
- ❖ Evitar palabras comunes e **información personal**.
- ❖ **No repetir contraseñas y actualizarlas** cada cierto tiempo.
- ❖ Utilizar un **gestor de contraseñas**.
- ❖ Utilizar **doble factor de autenticación**.



## 4.1 CARACTERÍSTICAS Y GESTIÓN DE LAS CONTRASEÑAS WINDOWS

Para **agregar/modificar** una contraseña de inicio de sesión:

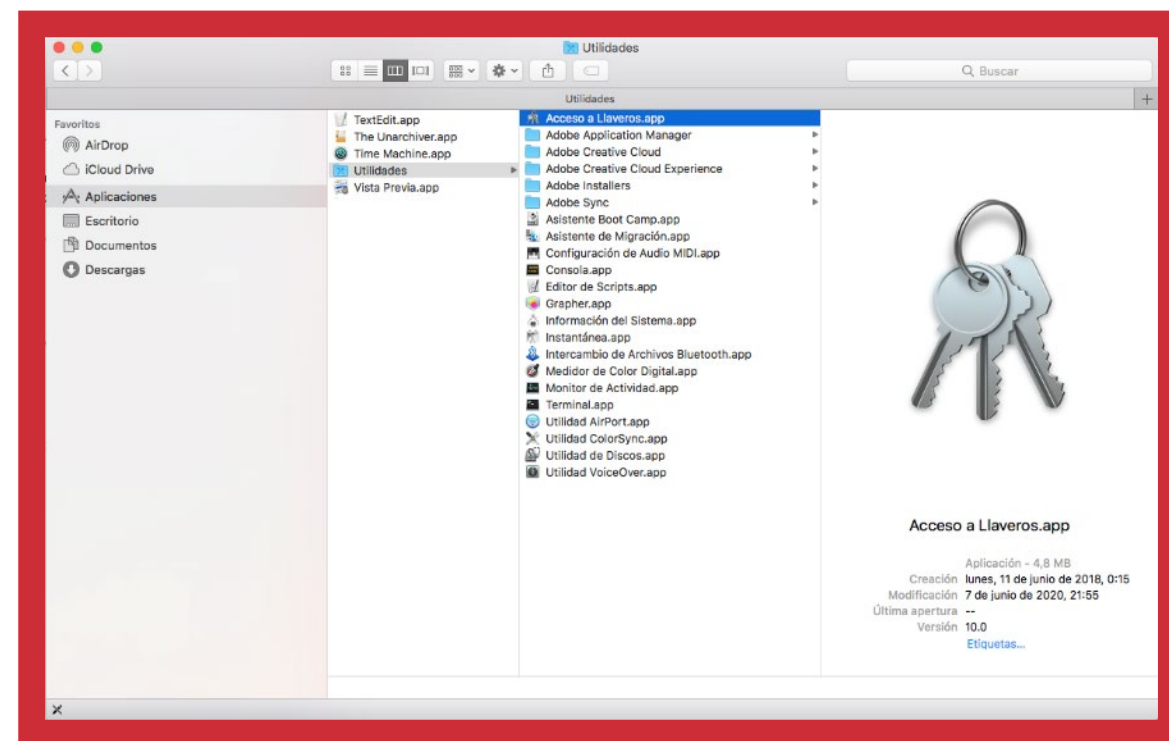
- ❖ Volveremos a **Configuración > Cuentas > Opciones de inicio de sesión**.
- ❖ Seleccionaremos **Contraseña**.



## 4.2 CARACTERÍSTICAS Y GESTIÓN DE LAS CONTRASEÑAS MACOS

Podemos **cambiar una contraseña de usuario ya creada:**

- ❖ Volveremos al menú **Preferencias del sistema > Usuarios y grupos > Cambiar contraseña.**
- ❖ Desde **Aplicaciones > Utilidades** podremos ir a la app **Acceso a llaveros** (Obtener información, mostrar contraseña, control de acceso...).



## 4.3 CARACTERÍSTICAS Y GESTIÓN DE LAS CONTRASEÑAS: ACTIVIDAD

### Actividad 4



¿Tenemos una contraseña robusta? Si no estamos seguros no pasa nada, más vale tarde que nunca. En el siguiente [enlace](#) encontraremos un recurso con el que poner a prueba nuestros conocimientos.



## 5. COPIAS DE SEGURIDAD

La **copia de seguridad** evitara que perdamos la información que hemos almacenado en nuestro dispositivo, por daño, robo del dispositivo o simplemente pérdida de la información.



## 5.1 COPIAS DE SEGURIDAD WINDOWS

Podemos **crear una copia de seguridad** de nuestro sistema fácilmente, solo necesitaremos disponer de un **dispositivo externo de almacenamiento** conectado a nuestro equipo:

- ❖ Iremos al menú **Configuración > Actualización y Seguridad > Copia de seguridad > Agregar una unidad.**
- ❖ Desde **Más opciones**, podremos:

**Hacer una copia**



**Programar**



**Deseleccionar**

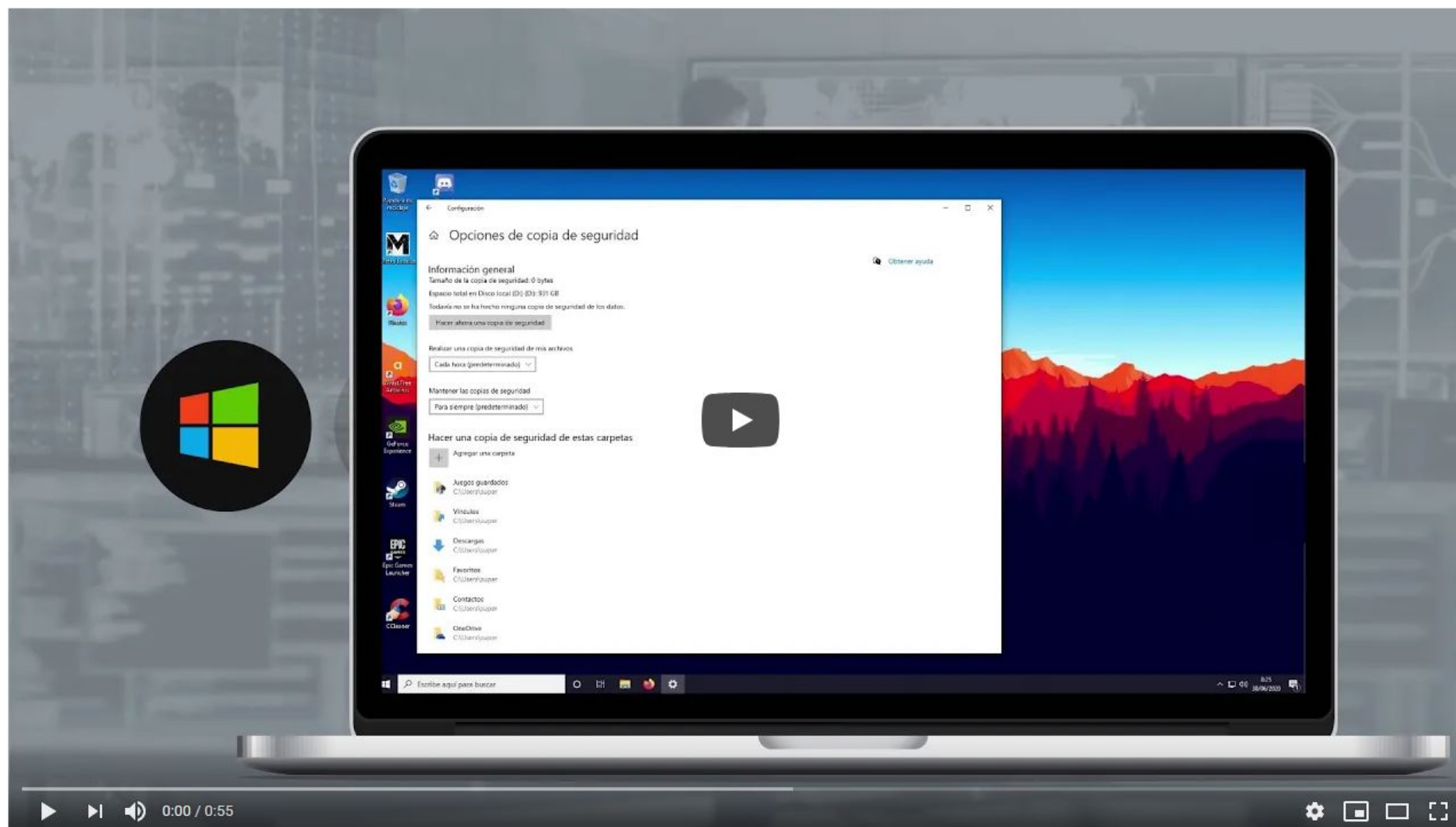


## 5.2 COPIAS DE SEGURIDAD MAC

**Time Machine:** Permite realizar copias de seguridad de todos nuestros archivos de forma automática.



## 5.3 COPIAS DE SEGURIDAD



## 5.4 COPIAS DE SEGURIDAD: ACTIVIDAD

### Actividad 5



Tener una copia de seguridad de archivos y aplicaciones instaladas en el ordenador nos protegerá en caso de pérdida, ya sea por un fallo en el sistema, un descuido por nuestra parte o por un ciberataque. Así que, dediquemos unos minutos a configurar nuestro sistema para que lo realice de manera automática.

## 6. REDES INALÁMBRICAS EN EL ORDENADOR

Entre las funciones de los ordenadores, se encuentran las **redes inalámbricas**:



BLUETOOTH



WIFI



## 6.1 REDES INALÁMBRICAS EN EL ORDENADOR: WIFI

En Windows: viene integrado o puede agregarse mediante un puerto USB.

- ❖ Para activarlo, iremos al menú **Configuración > Redes e Internet > Wifi**.

En macOS: podemos activarlo desde el icono en la barra superior izquierda. Para compartir datos de Internet:

- ❖ Iremos al **icono Wifi** para activarlo y seleccionar la red.
- ❖ Si está oculta, clic en **Acceder a otra red** para ingresar la red.
- ❖ Finalmente, seleccionaremos **Recordar esta red**.



## 6.1 REDES INALÁMBRICAS EN EL ORDENADOR: WIFI

El mayor **riesgo** de las conexiones Wifi son aquellos relacionados con las **redes públicas**:



Nuestro consejo es que **no os conectéis a redes públicas, a no ser que sea imprescindible y, a poder ser, siempre con una VPN.**



## 6.2 REDES INALÁMBRICAS EN EL ORDENADOR: BLUETOOTH

En Windows: viene integrado o puede agregarse mediante un puerto USB.

Para activarlo, iremos al menú **Configuración > Dispositivo**.

En macOS: ofrece muchas ventajas:

- ❖ Recibir o compartir conexión a Internet.
- ❖ Explorar carpetas públicas.
- ❖ Enviar y recibir archivos.

Para utilizarlo, iremos al menú **Preferencias del sistema > Bluetooth**.



Una vez hayamos terminado de utilizarlo, **desactiva el Bluetooth**.



## 7. SEGURIDAD BÁSICA EN LAS REDES

La **seguridad de las redes inalámbricas** de nuestros dispositivos es fundamental. A continuación, vamos a ver algunas **medidas de seguridad** a implementar en nuestro router:

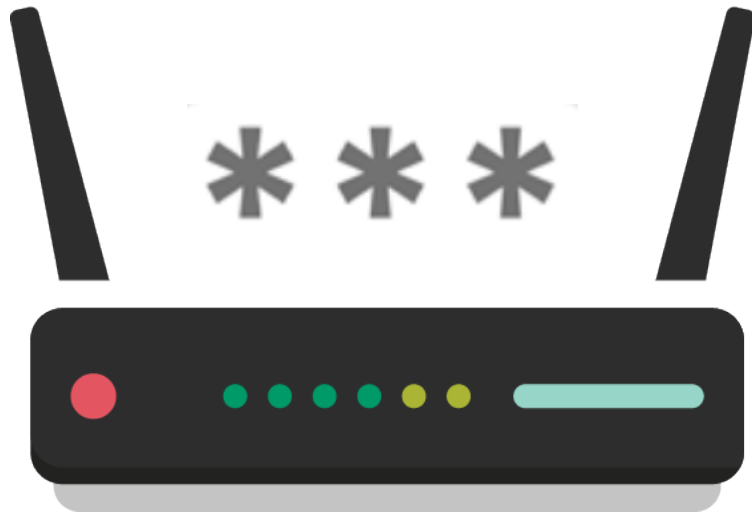


**Modificar el SSID**

**Desactivar WPS**



## 7. SEGURIDAD BÁSICA EN LAS REDES



**Contraseñas de acceso y administración**

**Deshabilitar conexión remota**



## 7. SEGURIDAD BÁSICA EN LAS REDES



**Cifrado**

**Limitar conexiones, ancho de banda y tiempo de conexión**



## 7. SEGURIDAD BÁSICA EN LAS REDES

Otra buena práctica que podemos seguir es revisar eventualmente los dispositivos que están conectados a nuestra red y realizar un **filtrado por dirección MAC**. Conociéndola, podemos crear una **lista blanca** de direcciones permitidas.

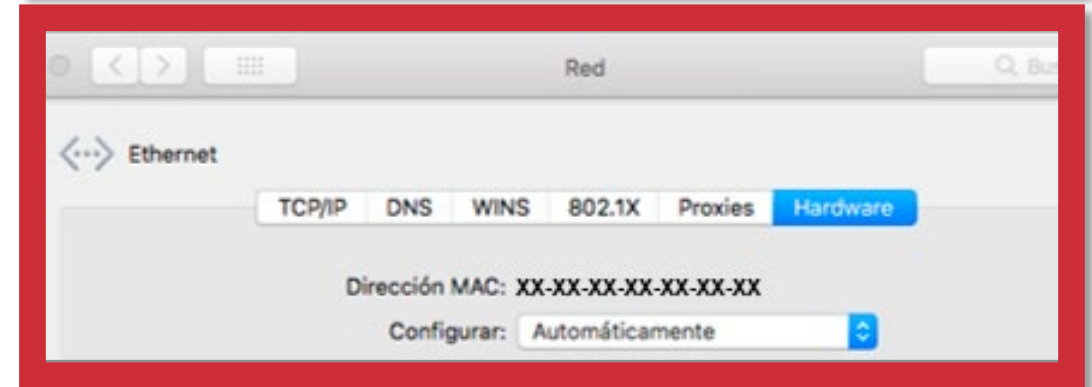
Para conocer nuestra dirección en **Windows**:

- **MS-DOS > ipconfig/all.**

```
Adaptador de LAN inalámbrica Wi-Fi:  
  
Sufijo DNS específico para la conexión. . . :  
Descripción . . . . . :  
Dirección física. . . . . : XX-XX-XX-XX-XX-XX  
DHCP habilitado . . . . . :
```

Para conocer nuestra dirección en **Mac**:

- **Preferencias del sistema > Redes > Avanzado > Ethernet/AirPort.**



Recuerda **visualizar todos los dispositivos conectados a la red cada cierto tiempo e identificar aquellos de confianza.**



## 7. SEGURIDAD BÁSICA EN LAS REDES

Crear una **red de invitados** no está disponible para todos los routers, pero permitirá **compartir nuestra conexión en una red distinta a la principal**.



- Ve a los **Ajustes** del router mediante nuestra **dirección IP (192.168.1.1)**.
- Iremos a la **Configuración de las redes inalámbricas > Red para invitado**.
  - Nombre y contraseña.
  - Método de autenticación (WPA2).
  - Tipo de red (2,4 GHz).



# EN INCIBE TE AYUDAMOS



INSTITUTO NACIONAL DE CIBERSEGURIDAD

[www.incibe.es](http://www.incibe.es)



TU AYUDA EN  
CIBERSEGURIDAD



[www.osi.es](http://www.osi.es)



[www.is4k.es](http://www.is4k.es)



[www.incibe.es](http://www.incibe.es)



Programas de  
formación



**Recursos:** servicios,  
herramientas, guías,  
juegos, etc.

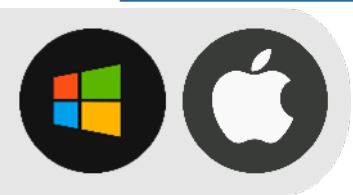


## 8. CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:

1. Lo más recomendable a la hora de crear cuentas en un sistema es:

- A. Crear 1 cuenta administrador.
- B. Crear 2 cuentas de administrador.
- C. Crear 1 cuenta de administrador por cada usuario.



## 8. CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:

2. ¿Para qué sirve tener un sistema actualizado?

- A. Para disponer de la última versión de nuestros programas favoritos.
- B. Para solucionar posibles vulnerabilidades.
- C. Para mejorar el rendimiento del sistema.



## 8. CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:

3. La herramienta que analiza y verifica las conexiones entrantes y salientes se conoce como:

- A. *Firewall.*
- B. *Antivirus.*
- C. *Router.*

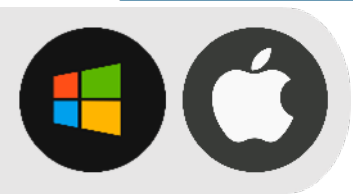


## 8. CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:

4. ¿Cuál de las siguientes opciones es una contraseña robusta?

- A. 1234567890
- B. 20101990
- C. M1contr4s3na.



## 8. CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:

5. ¿Es correcto utilizar la misma contraseña para más de 1 cuenta?

- A. Si, así evitamos olvidarlas.
- B. No, nunca.
- C. No, excepto si son cuentas secundarias.



## 8. CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:

### 6. Las copias de seguridad nos ayudan a:

- A. Proteger nuestra información en caso de pérdida, daño o robo.
- B. Organizar nuestra información en la nube.
- C. Mejorar la seguridad de nuestras cuentas.



## 8. CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:

7. La regla del 3-2-1 hace referencia a:

- A. 3 copias de seguridad en 2 soportes diferentes y 1 en la nube.
- B. 3 copias de seguridad en 2 carpetas diferentes y 1 cifrada.
- C. 3 copias de seguridad en 2 soportes diferentes y 1 en un lugar físico distinto.



## 8. CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:

8. Cuando vinculamos dos dispositivos entre sí habilitando una conexión inalámbrica, hablamos de:

- A. Wifi.
- B. Bluetooth.
- C. VLAN.



## 8. CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:

**9. Estás en un centro comercial con la red wifi gratuita, ¿cuál de las opciones es la más segura?**

- A. Conectarse, así se ahorran datos móviles.
- B. Revisar las redes wifi disponibles y conectarse solo a la que tenga mejor señal.
- C. Desactivar la opción que permite al dispositivo conectarse automáticamente.

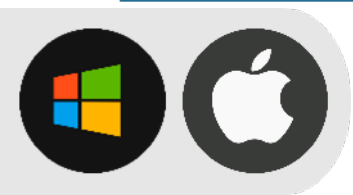


## 8. CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:

**10. ¿Qué harías si encontrases varios dispositivos desconocidos conectados a tu red wifi?**

- A. Cambiar la contraseña de acceso al *router*, así como de conexión a la red wifi.
- B. Bloquearlos y hacer un filtro de direcciones MAC.
- C. Ambas opciones son correctas.





INSTITUTO NACIONAL DE CIBERSEGURIDAD

# Gracias por vuestra atención

---



GOBIERNO  
DE ESPAÑA

VICEPRESIDENCIA  
PRIMERA DEL GOBIERNO  
  
MINISTERIO  
DE ASUNTOS ECONÓMICOS  
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO  
DE DIGITALIZACIÓN E  
INTELIGENCIA ARTIFICIAL



TU AYUDA EN  
CIBERSEGURIDAD  




Oficina  
de Seguridad  
del Internauta

**LICENCIA DE CONTENIDOS**

La presente publicación pertenece a Instituto Nacional de Ciberseguridad (INCIBE) y está bajo licencia Reconocimiento-No Comercial-CompartirIgual 4.0 Internacional de Creative Commons. Por esta razón está permitido copiar, distribuir y comunicar públicamente esta obra bajo las condiciones siguientes:

- **Reconocimiento.** El contenido de esta publicación se puede reproducir total o parcialmente por terceros, citando su procedencia y haciendo referencia expresa a INCIBE y su sitio web: <https://www.incibe.es>. Dicho reconocimiento no podrá en ningún caso sugerir que INCIBE presta apoyo a dicho tercero o apoya el uso que hace de su obra.
- **Uso No Comercial.** El material original y los trabajos derivados pueden ser distribuidos, copiados y exhibidos mientras su uso no tenga fines comerciales.
- **Compartir Igual.** Si altera o transforma esta obra, o genera una obra derivada, sólo puede distribuirla bajo esta misma licencia.

Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra.

Alguna de estas condiciones puede no aplicarse si se obtiene el permiso de INCIBE como titular de los derechos de autor.

Texto completo de la licencia: [https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es\\_ES](https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es_ES)

