



Govern d'Andorra

# Assegurat de Routers Domèstics

## Conscienciació en ciberseguretat

Juliol de 2022





# ÍNDEX

- 1. Aspectes a tenir en compte**
- 2. El nostre router**
- 3. Assegurant el nostre router**
- 4. Canviant la contrasenya**
- 5. Quins riscos suposa deixar com està el nostre router**
- 6. Canviar la contrasenya d'accés Wi-Fi**
- 7. Més seguretat**
- 8. Altres mesures de seguretat**
- 9. Control Parental**

# 1. Aspectes a tenir en compte

El router de la nostra casa o negoci és la **porta de sortida a tot internet**, però també hem de ser conscients que és una **porta d'entrada** que hem d'assegurar.

✓ Per a això, aprendrem algunes qüestions bàsiques sobre com fer-ho més segur.



Què podem fer per a assegurar la nostra connexió?

- Canvi de contrasenyes per defecte
- Canvi de clau wifi
- Emprar protocols segurs
- Desactivar accés remot
- Desactivar WPS i altres mètodes "ràpids"
- Restringir ports d'entrada
- Servidor UPnP
- Crear una Xarxa Per a Convidats
- Possibilitats de control parental



# ÍNDEX

1. Aspectes a tenir en compte
2. El nostre router
3. Assegurant el nostre router
4. Canviant la contrasenya
5. Quins riscos suposa deixar com està el nostre router
6. Canviar la contrasenya d'accés Wi-Fi
7. Més seguretat
8. Altres mesures de seguretat
9. Control Parental

## 2. El nostre router

Normalment, el nostre router és subministrat per l'empresa que ens presta serveis i sigui com sigui el mètode de connexió externa, satèl·lit, fibra òptica, xarxa de coure, etc., ho tindrem a casa i estarà accessible per a nosaltres.

Ara aprendrem algunes qüestions per a fer-ho més segur.



En la part baixa trobem usualment un adhesiu amb les **contrasenyes per defecte** per la nostra xarxa wifi així com el nom **d'usuari i contrasenya** per a accedir al **panell de control**.



# ÍNDEX

1. Aspectes a tenir en compte
2. El nostre router
3. Assegurant el nostre router
4. Canviant la contrasenya
5. Quins riscos suposa deixar com està el nostre router
6. Canviar la contrasenya d'accés Wi-Fi
7. Més seguretat
8. Altres mesures de seguretat
9. Control Parental



### 3. Assegurant el nostre router



Normalment, l'accés sol ser escrivint en el nostre navegador:

**192.168.1.1**

Això ens dona accés a un panell **d'administració** molt similar en tots els fabricants.

Les **credencials** habituals solen ser:

Usuari: **admin** contrasenya: **admin**

Usuari: **admin** contrasenya: **123456**



Una vegada accedim al nostre panell podem **canviar les configuracions** del nostre equip

Com podem imaginar, en ser tan conegudes un tercer amb accés **podria tenir control de la nostra xarxa domestica** i les dades que circulin en aquesta.



# ÍNDEX

- 1. Aspectes a tenir en compte**
- 2. El nostre router**
- 3. Assegurant el nostre router**
- 4. Canviant la contrasenya**
- 5. Quins riscos suposa deixar com està el nostre router**
- 6. Canviar la contrasenya d'accés Wi-Fi**
- 7. Més seguretat**
- 8. Altres mesures de seguretat**
- 9. Control Parental**



## 4. Canviant la contrasenya



- ✓ Una **contrasenya adequada** hauria de contenir **majúscules, minúscules, números i símbols intercalats** i sumar més de **8 caràcters (recomanable més de 12)**.
- ✓ Una contrasenya de 8 caràcters, amb les recomanacions anteriors, pot ser vulnerada en minuts o poques hores. Per contra, una de **12 caràcters**, pot trigar anys a vulnerar-se.



# ÍNDEX

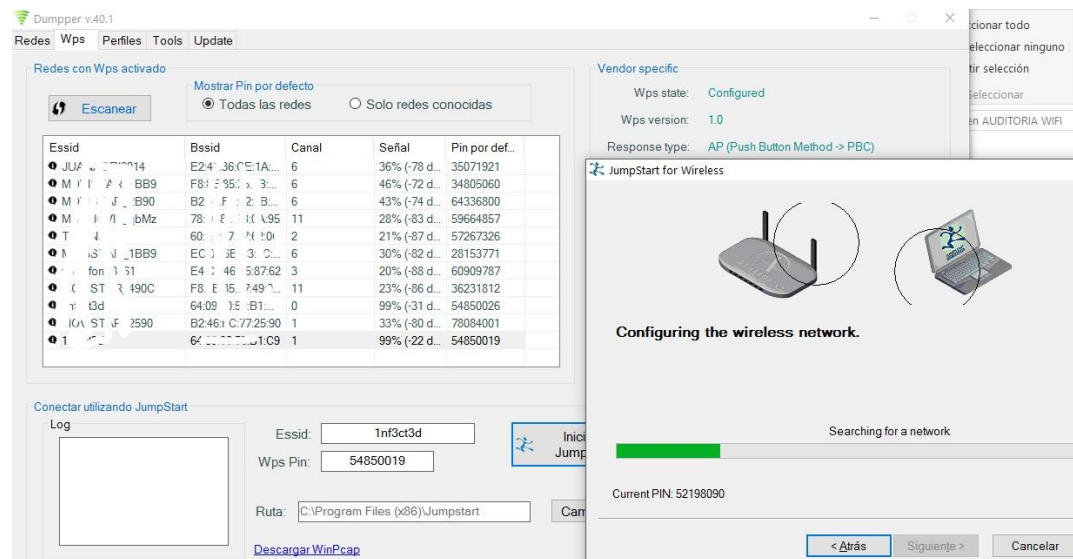
1. Aspectes a tenir en compte
2. El nostre router
3. Assegurant el nostre router
4. Canviant la contrasenya
5. Quins riscos suposa deixar com està el nostre router
6. Canviar la contrasenya d'accés Wi-Fi
7. Més seguretat
8. Altres mesures de seguretat
9. Control Parental



# 5. Quins riscos suposa deixar com està el nostre router



- ✓ Poden espionar les nostres comunicacions
- ✓ També, podrien usar la xarxa per a enviament de spam, realitzar atacs Dos (denegació de servei), descàrrega de contingut il·legal, etc.
- ✓ Infecció dels nostres dispositius connectats amb malware.
- ✓ Reduir l'amplada de banda.



En l'actualitat existeixen múltiples mecanismes per a accedir a routers amb la configuració del fabricant, molts d'ells senzills i automatitzats que pot utilitzar algú sense grans coneixements.



# ÍNDEX

- 1. Aspectes a tenir en compte**
- 2. El nostre router**
- 3. Assegurant el nostre router**
- 4. Canviant la contrasenya**
- 5. Quins riscos suposa deixar com està el nostre router**
- 6. Canviar la contrasenya d'accés Wi-Fi**
- 7. Més seguretat**
- 8. Altres mesures de seguretat**
- 9. Control Parental**

## 6. Canviar la contrasenya d'accés Wi-Fi



Des del panell de control del nostre router també podem canviar la contrasenya i el nom per defecte de la nostra WI-FI.

- ✓ En **canviar el nom** no revelem dades del fabricant ni de l'operador (li posem difícil als atacants).
- ✓ Ara **no podran endevinar la contrasenya** que teníem preconfigurada.
- ✓ També podem canviar el **canal** per si hi ha moltes altres antenes Wi-fi en el veïnat (per a evitar baixada de qualitat per interferències)
- ✓ Crearem **una Wi-fi per a convidats** (aïllada) perquè les nostres visites no tinguin accés als nostres serveis privats



# ÍNDEX

- 1. Aspectes a tenir en compte**
- 2. El nostre router**
- 3. Assegurant el nostre router**
- 4. Canviant la contrasenya**
- 5. Quins riscos suposa deixar com està el nostre router**
- 6. Canviar la contrasenya d'accés Wi-Fi**
- 7. Més seguretat**
- 8. Altres mesures de seguretat**
- 9. Control Parental**



Usarem el protocol de seguretat wifi més avançat.



- En el mateix panell de la Wi-fi triarem, si podem, **WPA2/AES** com a mínim i deshabilitem o no seleccionem les altres opcions.
- Desactivem WPS** (molt vulnerable)
- Desactivem l'accés remot.** Hem de consultar amb el nostre operador, però aquest accés també és conegut per molts possibles assaltants de la nostra xarxa.

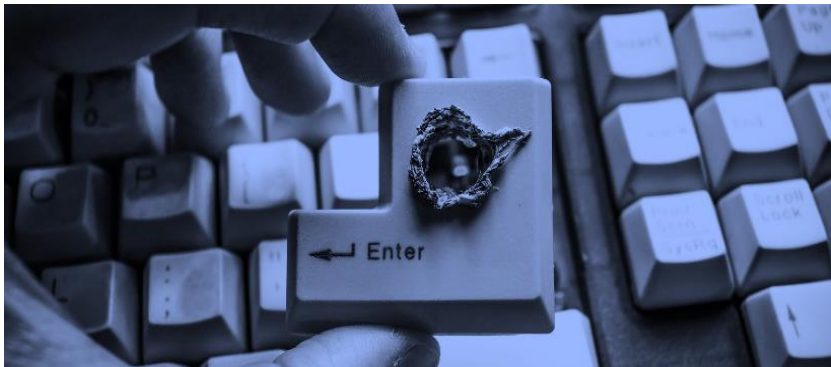


# ÍNDEX

- 1. Aspectes a tenir en compte**
- 2. El nostre router**
- 3. Assegurant el nostre router**
- 4. Canviant la contrasenya**
- 5. Quins riscos suposa deixar com està el nostre router**
- 6. Canviar la contrasenya d'accés Wi-Fi**
- 7. Més seguretat**
- 8. Altres mesures de seguretat**
- 9. Control Parental**



Molts routers tenen la possibilitat de tancar ports i restringir direccions mitjançant una capa de Tallafocs (Firewall).



### Tanquem ports que no necessitem

En les configuracions avançades del nostre router trobem la gestió de ports. Els nostres equips, reconeixen 65.536 ports. Molts d'ells no són necessaris i fins i tot alguns poden resultar perillosos. Els més usats són el **80** (http), el **443** (https) per a navegar, igual que el **8080** o el **8443**, vinculats a la navegació també, o el **25** per a clients de correu electrònic.

Vigila els que estan actius i tanca els que no empris. Per exemple el **3389** és fet servir per a escriptori remot i molts atacs de programari maliciós també ho utilitzen.

Recorda que després de cada canvi probablement has de reiniciar el teu router



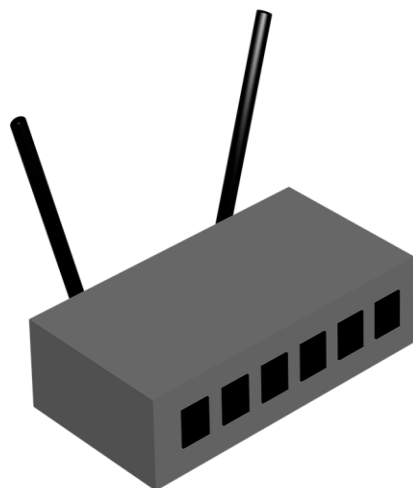


# ÍNDEX

- 1. Aspectes a tenir en compte**
- 2. El nostre router**
- 3. Assegurant el nostre router**
- 4. Canviant la contrasenya**
- 5. Quins riscos suposa deixar com està el nostre router**
- 6. Canviar la contrasenya d'accés Wi-Fi**
- 7. Més seguretat**
- 8. Altres mesures de seguretat**
- 9. Control Parental**

Si bé és cert que establir un control parental des del router és una mesura avançada, podem fer alguns canvis senzills per a millorar-lo.

**Canviar les DNS per defecte** per una que compleixi amb criteris de filtratge de continguts agrega una capa extra de seguretat



Per a canviar les DNS, acudim a la configuració avançada del nostre dispositiu

Algunes de les direccions amb filtratge més conegudes, són:

•**Norton ConnectSafe seguretat i contingut per a adults:**

199.85.126.20 i 199.85.127.20.

**Norton ConnectSafe seguretat, contingut per a adults:**

199.85.126.30 i 199.85.127.30.

**OpenDNS Family Shield:**

208.67.222.123 i 208.67.220.123

**DNS Family:**

77.88.8.7 i 77.88.8.3

**Cloudflare DNS, blocking malware and adult content:**

1.1.1.3 i 1.0.0.3



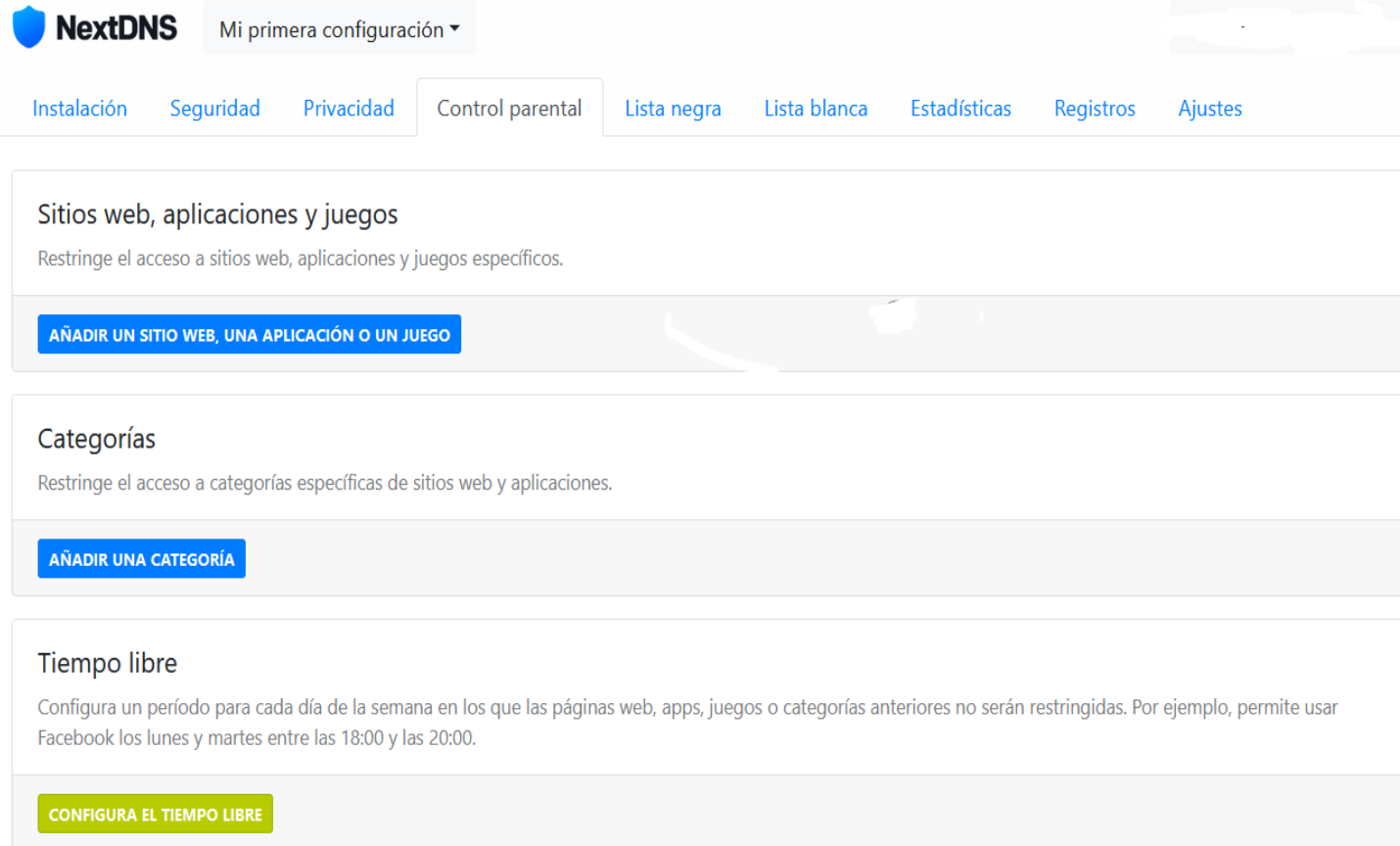
També existeixen unes DNS configurables per nosaltres mateixos que ens donen control i visibilitat de tota la navegació i els filtres a usar.

És senzilla d'utilitzar i en el nostre router tan sols cal afegir les DNS que ens crea per a nosaltres.

També ens aporta una guia senzilla per a la seva instal·lació i ús.



<https://nextdns.io/>



The screenshot shows the NextDNS control panel interface. At the top, there is a navigation menu with tabs for 'Instalación', 'Seguridad', 'Privacidad', 'Control parental', 'Lista negra', 'Lista blanca', 'Estadísticas', 'Registros', and 'Ajustes'. The 'Control parental' tab is currently selected. Below the navigation, there are three main sections: 'Sitios web, aplicaciones y juegos' with a sub-description 'Restringe el acceso a sitios web, aplicaciones y juegos específicos.' and a blue button 'AÑADIR UN SITIO WEB, UNA APLICACIÓN O UN JUEGO'; 'Categorías' with a sub-description 'Restringe el acceso a categorías específicas de sitios web y aplicaciones.' and a blue button 'AÑADIR UNA CATEGORÍA'; and 'Tiempo libre' with a sub-description 'Configura un período para cada día de la semana en los que las páginas web, apps, juegos o categorías anteriores no serán restringidas. Por ejemplo, permite usar Facebook los lunes y martes entre las 18:00 y las 20:00.' and a green button 'CONFIGURA EL TIEMPO LIBRE'.



Mantinguis alerta mentre navegues

Navega segur!



Govern d'Andorra



ANDORRA  
DIGITAL

---

Entitats col·laboradores

---

