

# Guía completa para asegurar ruteadores 2wire de Infinitem

## 1. Cambiar rango default de direcciones IP

Seleccionamos **Red Domestica**, **Configuración avanzada**, en **Red privada** seleccionamos **Configurar manualmente**. Ponemos una dirección del ruteador inventada y una máscara y rango de subred correspondiente.



The screenshot shows the Prodigy Infinitem router configuration interface. At the top, there are navigation tabs: 'Resumen', 'Configuración inalámbrica', and 'Configuración avanzada' (which is selected). Below the tabs, the main heading is 'Modificar la configuración avanzada'. A warning box labeled 'ADVERTENCIA' states: 'La modificación de la configuración de esta página puede afectar la capacidad de las banda ancha. Las modificaciones también pueden afectar las aplicaciones y los serv'. The main configuration area is titled 'Configuración' and contains a section for 'Red privada'. It includes a warning: 'Si modifica el intervalo de dirección IP, deberá renovar la concesión DHCP de todos los dispositivos de la red.' There are three radio button options for IP configuration: '192.168.1.0 / 255.255.255.0 (predeterminado)', '172.16.0.0 / 255.255.0.0', and '10.0.0.0 / 255.255.0.0'. The 'Configurar manualmente' option is selected. Below this, there are input fields for 'Dirección del ruteador:' (1.2.3.4), 'Máscara de subred:' (255.255.0.0), a checked checkbox for 'Habilitar DHCP', and two more input fields for 'Primera dirección DHCP:' (1.2.3.0) and 'Última dirección DHCP:' (1.2.3.50).

*La mayoría de los ataques CSRF son dirigidos a dominios y direcciones IPs default. No debemos usar ninguno de los rangos que vienen por default.*

## 2. Usar servidores DNS de OpenDNS

Seleccionamos *Enlace de banda ancha, Configuración avanzada*, en **DNS de banda ancha** seleccionamos *Configurar manualmente la información de DNS*. Ponemos los servidores de OpenDNS: 208.67.222.222 y 208.67.220.220



DNS de banda ancha

Obtener información de DNS automáticamente.

Configurar manualmente la información de DNS:

Servidor principal:

Servidor secundario:

Nombre de dominio:

*La mayoría de los ataques CSRF son dirigidos a dominios y direcciones IPs default. También debemos especificar en nuestra computadora los servidores de OpenDNS para deshabilitar los dominios que apuntan al ruteador por default, como: home y gateway.2wire.net.*

## 3. Deshabilitar la difusión del SSID

Seleccionamos *Red Domestica, Configuración inalámbrica*, en **Identificar la red** deshabilitamos **Difusión SSID**.

*Evitamos mostrar el nombre de nuestra red. Un atacante avanzado podría conocer fácilmente el nombre de nuestra red a pesar de esto.*

## 4. Cambiar el SSID default del ruteador

Seleccionamos *Red Domestica, Configuración inalámbrica*, en **Identificar la red** cambiamos el **Nombre de red**. Ponemos un nombre inventado.

*Existen ataques para la red inalámbrica que se aprovechan del SSID por default del ruteador.*

## 5. Cambiar autenticación a WPA

Seleccionamos *Red Domestica, Configuración inalámbrica*, en **Seguridad Inalámbrica** cambiamos autenticación a **WPA-PSK**.

*WEP es vulnerado fácilmente por cualquier persona desde hace mucho tiempo.*

## 6. Cambiar la clave default de wireless

Seleccionamos *Red Domestica, Configuración inalámbrica*, en **Seguridad Inalámbrica** seleccionamos *Utilizar clave de encriptación personalizada* y ponemos una clave segura, es posible generar claves seguras en <http://www.kurtm.net/wpa-pskgen/>

## Configuración

### Identificar la red

Nombre de red:

Canal inalámbrico:

**Habilitar** Difusión SSID

Permite que el nombre de la red inalámbrica se difunda públicamente a cualquier usuario inalámbrico dentro del alcance inalámbrico de la red. Si se deshabilita la difusión SSID, el nombre de la red pasa a ser privado y ofrece una mayor seguridad, ya que exige al usuario inalámbrico ingresar el nombre de la red manualmente al crear un perfil de red inalámbrica en la computadora.

---

### Seguridad inalámbrica

**Habilitar** Seguridad de red inalámbrica

Autenticación:

Utilizar clave de encriptación predeterminada

Utilizar clave de encriptación personalizada

Clave:

---

### Configuración adicional (se recomienda utilizar los valores predeterminados)

Modo inalámbrico:

Período de DTIM (segundos):

Velocidad de conexión máxima:

Potencia de Transmisión:

#### 7. Disminuir la potencia de Transmisión

Seleccionamos *Red Domestica, Configuración inalámbrica*, en **Configuración adicional** seleccionamos *Potencia de Transmisión* y ponemos lo mínimo que necesitemos.

*De esta forma disminuimos el rango de alcance de nuestra red inalámbrica.*

### Configuración

**Seguridad** ?

Marque las funciones siguientes para habilitarlas:

- Modo sombra
  - Bloquear ping
- Control de sesión UDP estricta

---

**Control de entrada y de salida** ?

Si marca la casilla de verificación, el tipo de tráfico asociado accederá a través del cortafuegos.

Saliente	Entrante
<input checked="" type="checkbox"/> HTTP	<input type="checkbox"/> Administración remota
<input checked="" type="checkbox"/> HTTPS	<input type="checkbox"/> NetBIOS
<input checked="" type="checkbox"/> FTP	
<input checked="" type="checkbox"/> Telnet	
<input checked="" type="checkbox"/> SMTP	
<input checked="" type="checkbox"/> DNS	
<input type="checkbox"/> NetBIOS	

### Instrucciones

Es posible que la limitación del tráfico de datos deshabilite la compatibilidad para aplicaciones hospedadas que requieren comunicaciones entrantes como, por ejemplo, servidores web, juegos o programas de chat por Internet. El tráfico de datos seguirá accediendo y analizándose a través del cortafuegos con el fin de impedir ataques por parte de piratas informáticos.

### Detección de ataques

Compruebe si se detectaron los tipos de ataques que aparecen a continuación:

- Detección de exceso de sesiones
- Exploración de puerto TCP/UDP
- La dirección IP de origen/destino no es válida
- Desborde de paquetes (SYN/UDP /ICMP/Otros)
- Los ataques de marca TCP no son válidos (NULL/XMAS/Otros)
- Detección de ICMP no válido
- Varios

## 8. Bloquear ping / deshabilitar puerto 50001 de Administración remota

Seleccionamos **Bloqueo de intrusos**, **Configuración avanzada**, en **Seguridad** habilitamos **modo sombra** y **Bloquear ping**. En **Control de entrada y de salida** deshabilitamos **Administración remota**. **Bloqueamos ping** para evitar ser víctima de escaneos y ataques aleatorios, **deshabilitamos la administración remota** para evitar alguna vulnerabilidad y también evitar ser identificados por ese puerto abierto.

Usar la última versión de **Firefox** con los plugins de **No-Script** y **RequestPolicy**.

*Estos plugins bloquean los ataques de CSRF y clickjacking que podría afectar routers.*

Utilizar los **DNS de OpenDNS** en el sistema operativo.

<https://www.opendns.com/smb/start/computer/>

*Para evitar ataques CSRF/XSS que estén dirigidos a los dominios default como home y gateway.2wire.net*

**Debemos tomar en cuenta que nunca tendremos un router completamente seguro. Probablemente existen muchas vulnerabilidades desconocidas.**

Cualquier duda comentario o sugerencia a [hkm@hakim.ws](mailto:hkm@hakim.ws)