

# Consideraciones de seguridad al ejecutar un nodo de Bitcoin



[Yohan Graterol](#)

23 PlatziRank

Nov. 16, 2017

Ejecutar un nodo de Bitcoin tiene diferentes ventajas, como la posibilidad de poder usar ese nodo para implementar Bitcoin -o cualquier blockchain- en un comercio electrónico, o para cualquier otra actividad económica. Sin embargo la seguridad es una parte fundamental a la hora de crear un nuevo nodo de Bitcoin y en este material te explicaré algunos tips para tener en cuenta a la hora de ejecutar un nodo.

## Asegurar puerto SSH

La mayoría de los proveedores de computación en la nube ofrecen configuración de sus máquinas virtuales con SSH, por lo general esto es seguro ya que usan llaves RSA para autenticar los usuarios. Aún así, es posible hacer algunas configuraciones adicionales para lograr una mayor seguridad.

### Implementar fail2ban

[fail2ban](#) es un software que permite bloquear IPs que tengan múltiples intentos de login a un puerto, en este caso SSH, si una persona intenta múltiples veces conectarse a SSH aplicando fuerza bruta para tratar de adivinar la contraseña de un usuario, fail2ban lo bloqueará y evitará que continúe haciendo ese ataque.

### Evitar root

Al instalar un cliente de Bitcoin es importante evitar al máximo hacer instalación con el usuario `root`, lo mejor es crear un nuevo usuario -si lo instalas en Linux- y en el home de dicho usuario instalar tu nodo de Bitcoin y que quede separado de otros nodos, si instalas varios clientes de blockchain en un mismo servidor.

También es importante evitar el login a través de SSH con el usuario `root`, es importante deshabilitarlo de la configuración de SSH.

## Bloquea y crea backups de tu wallet

Es importante crear una contraseña para bloquear tu wallet y es importante que el archivo de tu wallet tenga respaldo a diario, sobre todo si haces muchos movimientos al día. Si el uso de tu wallet es semanal, podrías hacer un respaldo semanal.

Jamás olvides este consejo.

## Asegura tu red

Muchas veces abrimos puertos en un firewall y se nos olvida. Es importante abrir los puertos necesarios y especificar quiénes se pueden conectar a dicho puerto. Bitcoin utiliza dos puertos: el puerto 8333, para comunicarse entre nodos en el protocolo Bitcoin y el puerto 8332, para comunicaciones sobre RPC-JSON.

Mi recomendación es que abran 8333 al público y dejen el puerto 8332 configurado para ciertas IPs, incluso si es necesario solo permitir conexiones a `localhost`, si es importante que reciba conexiones desde otros servidores entonces la solución más eficiente es configurar el firewall para que reciba conexiones entrantes a ese puerto solo desde esa IP.

Otra recomendación es cambiar el número del puerto RPC en la configuración de Bitcoin que por lo general se encuentra en alguna de las siguientes rutas:

### Windows

%APPDATA%\Bitcoin\

Ej: C:\Users\username\AppData\Roaming\Bitcoin\bitcoin.conf

### Linux

\$HOME/.bitcoin/

Ej: /home/username/.bitcoin/bitcoin.conf

### Mac OSX

\$HOME/Library/Application Support/Bitcoin/

Ej: /Users/username/Library/Application Support/Bitcoin/bitcoin.conf

En ese archivo pueden cambiar el puerto a través de la configuración llamada:

`rpcport`

Si combinan esa configuración con `rpallowip` para indicar explícitamente quienes se pueden conectar, podrán tener un Nodo de Bitcoin mucho más seguro.