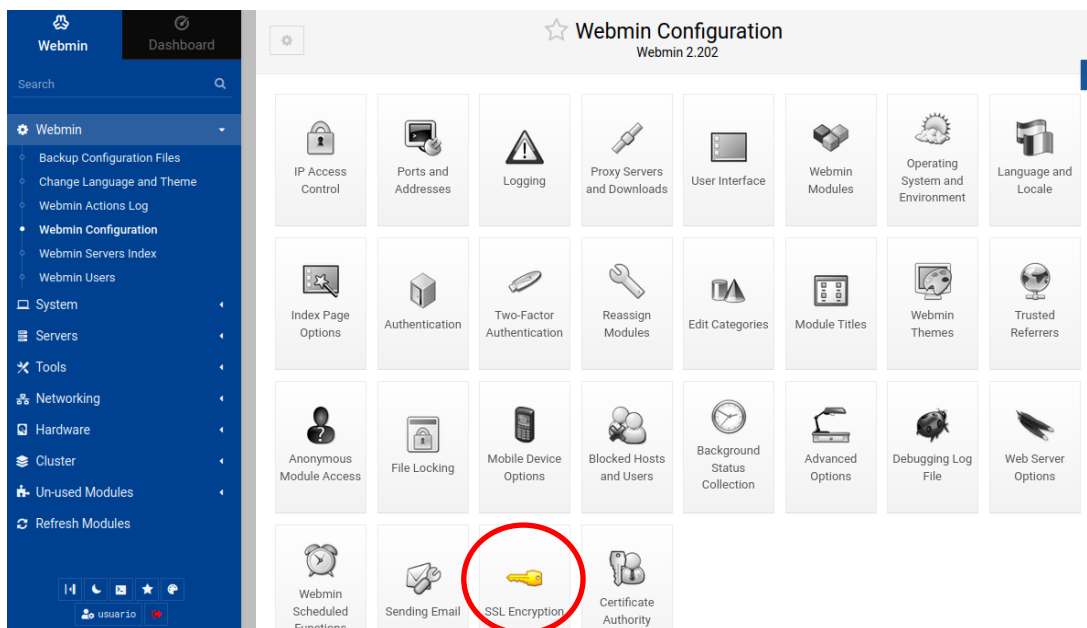


Partiendo de nuestra configuración en el ejercicio anterior para HTTP en Linux, haremos los pasos necesarios para que el paso sea seguro, como hicimos en el caso de Windows.

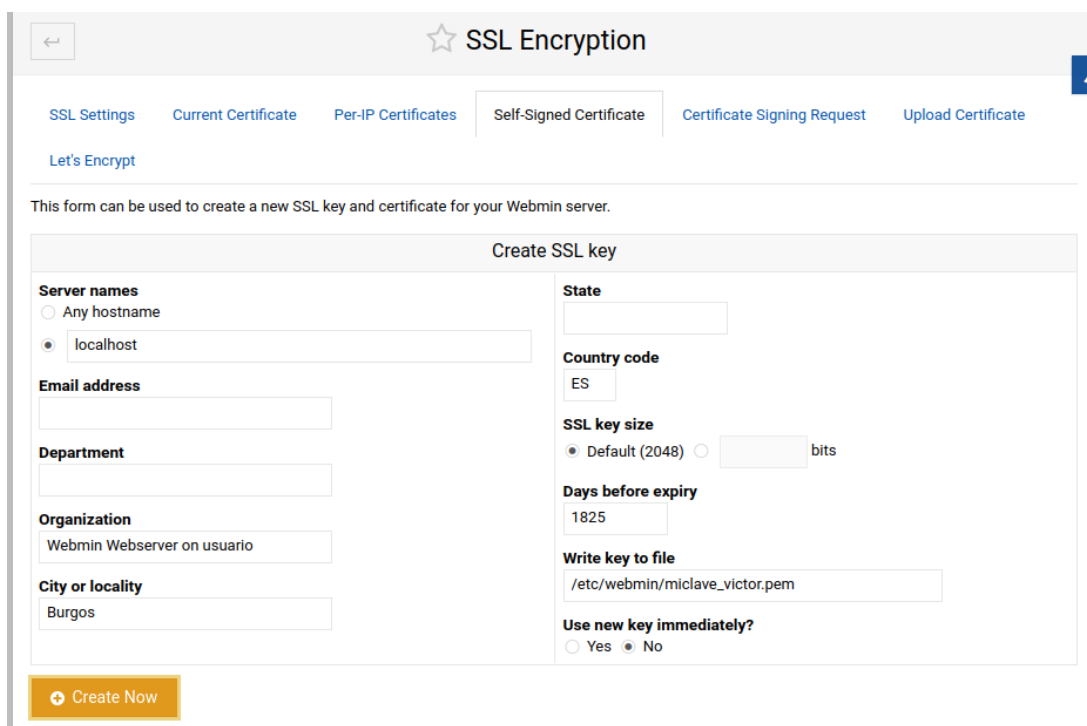
Recordad que para nosotros en Linux la herramienta de configuración es Webmin.

## BLOQUE 1: Creación del certificado

En la propia configuración de Webmin seleccionamos Ecriptación SSL:



Después la opción Certificado autofirmado y configuramos la clave SSL.



SSL Settings   Current Certificate   Per-IP Certificates   **Self-Signed Certificate**   Certificate Signing Request   Upload Certificate

Let's Encrypt

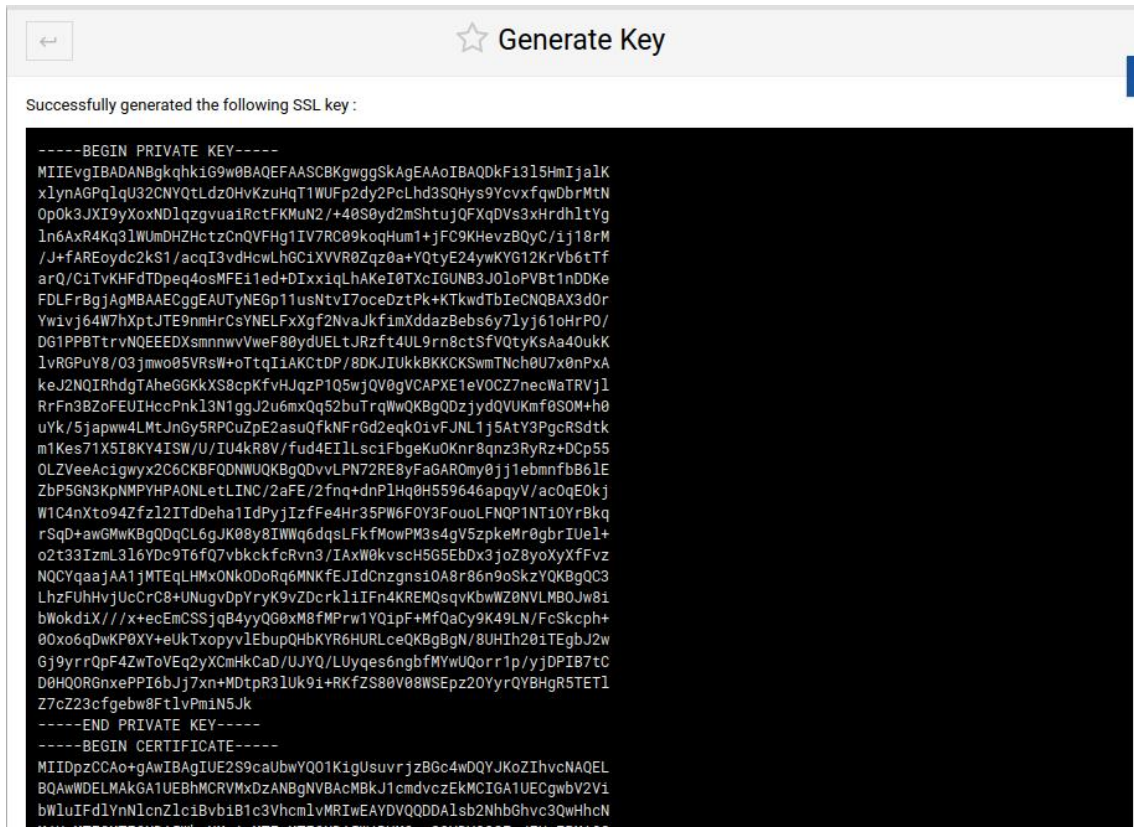
This form can be used to create a new SSL key and certificate for your Webmin server.

**Create SSL key**

<b>Server names</b> <input type="radio"/> Any hostname <input checked="" type="radio"/> localhost	<b>State</b> <input type="text"/>
<b>Email address</b> <input type="text"/>	<b>Country code</b> ES
<b>Department</b> <input type="text"/>	<b>SSL key size</b> <input checked="" type="radio"/> Default (2048) <input type="radio"/> <input type="text"/> bits
<b>Organization</b> Webmin Webserver on usuario	<b>Days before expiry</b> 1825
<b>City or locality</b> Burgos	<b>Write key to file</b> <input type="text" value="/etc/webmin/miclave_victor.pem"/>
<b>Use new key immediately?</b> <input type="radio"/> Yes <input checked="" type="radio"/> No	

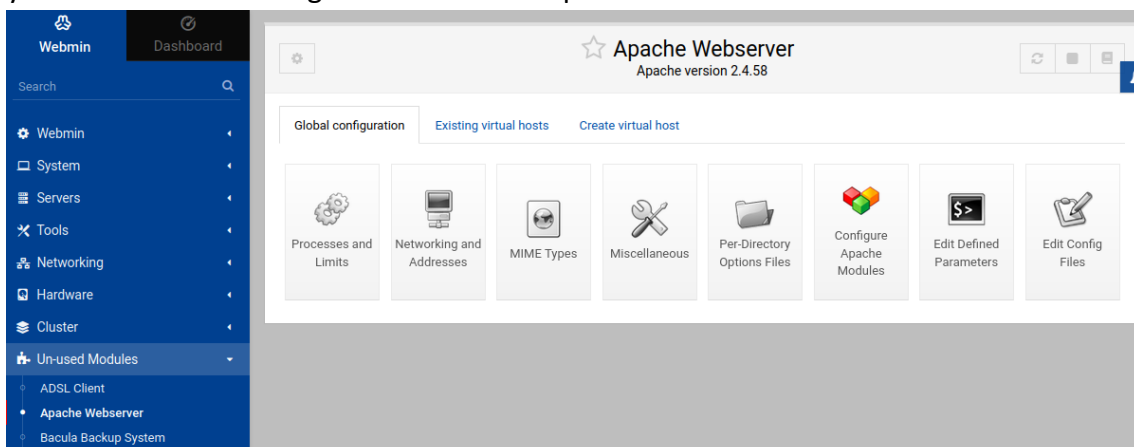
**Create Now**

Al crear el certificado, lo veremos:



## BLOQUE 2: Activación del módulo de criptografía

A través de Webmin, accedemos a la “Configuración Global” del Servidor Web Apache y seleccionamos “Configurar módulos de Apache”.



Marcamos la casilla “ssl” y habilitamos los módulos seleccionados.

<input type="checkbox"/> ext_filter	Disabled	<input type="checkbox"/> socache_redis	Disabled
<input type="checkbox"/> file_cache	Disabled	<input type="checkbox"/> socache_shmcb	Disabled
<input checked="" type="checkbox"/> filter	Enabled	<input type="checkbox"/> spelling	Disabled
<input type="checkbox"/> headers	Disabled	<input checked="" type="checkbox"/> ssl	Disabled
<input type="checkbox"/> heartbeat	Disabled	<input checked="" type="checkbox"/> status	Enabled
<input type="checkbox"/> heartmonitor	Disabled	<input type="checkbox"/> substitute	Disabled
<input type="checkbox"/> http2	Disabled	<input type="checkbox"/> suexec	Disabled
<input type="checkbox"/> ident	Disabled	<input type="checkbox"/> unique_id	Disabled
<input type="checkbox"/> imagemap	Disabled	<input type="checkbox"/> userdir	Disabled
<input type="checkbox"/> include	Disabled	<input type="checkbox"/> usertrack	Disabled
<input type="checkbox"/> info	Disabled	<input type="checkbox"/> vhost_alias	Disabled
<input type="checkbox"/> lbmethod_bybusyness	Disabled	<input type="checkbox"/> xml2enc	Disabled
<input type="checkbox"/> lbmethod_byrequests	Disabled		

☒ Enable Selected Modules

### BLOQUE 3: Creación de un servidor virtual cifrado con HTTPS

- 1.) Para dar contenido al servidor, crea el archivo “/var/nombre-seguro/index.html” de forma que, al visualizarlo desde el navegador, se lea el mensaje: *Portal web seguro de Nombre*

```
usuario@usuario:~$ tree /var/victor-seguro/
/var/victor-seguro/
└── index.html
```

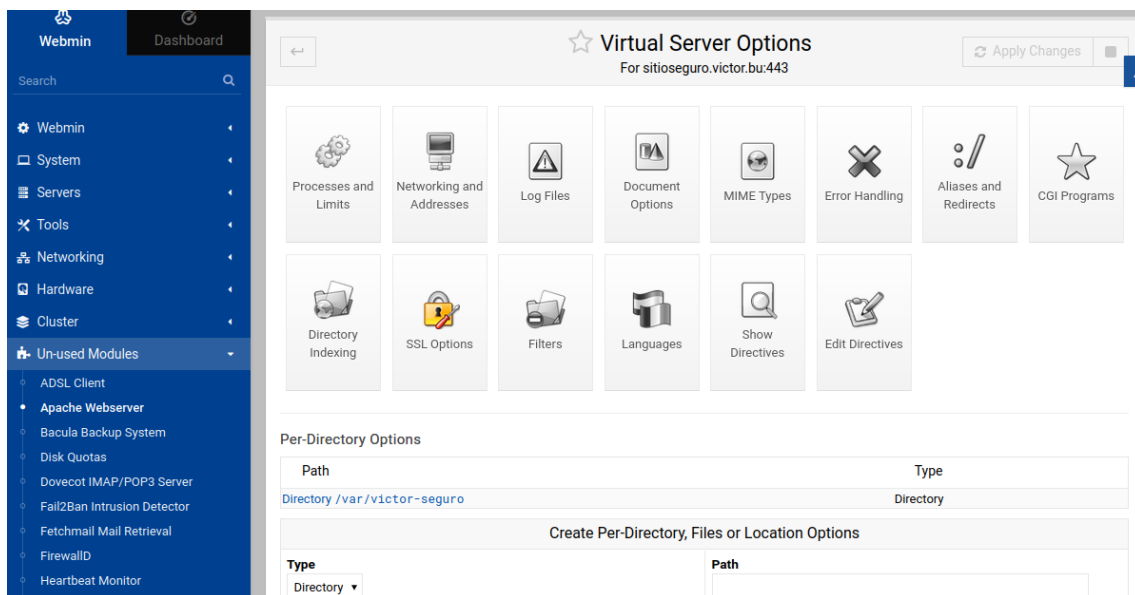
- 2.) Para acceder a este servidor se usará el nombre seguro.nombre.bu. Importante darnos cuenta de que tenemos que poner el puerto seguro 443.
- 3.) . Abre Webmin y accede al enlace *Servidor Web Apache* de la sección *Servidores* del menú principal. Y haz clic en la pestaña *Create virtual host* para crear un servidor.

The screenshot shows the Apache Webserver Webmin interface. The top bar indicates 'Apache Webserver' and 'Apache version 2.4.58'. The navigation tabs include 'Global configuration', 'Existing virtual hosts', and 'Create virtual host'. The 'Create a New Virtual Server' form is displayed with the following fields:

- Handle connections to address:**
  - ☐ Those not handled by another server
  - ☐ Any address
  - ☒ Specific address ..
- Port:**
  - ☐ Default
  - ☐ Any
  - ☒ 443
- Add virtual server to file:**
  - ☐ Standard httpd.conf file
  - ☒ New file under virtual servers directory /etc/apache2/sites-available
  - ☐ Selected file..
- Copy directives from:**
  - ☐ Nowhere
- Document Root:**
  - 
  - ☒ Allow access to this directory
- Server Name:**
  - ☐ Automatic
  - ☒ miUbuntuServer.victor.bu

A green 'Create Now' button is located at the bottom left of the form.

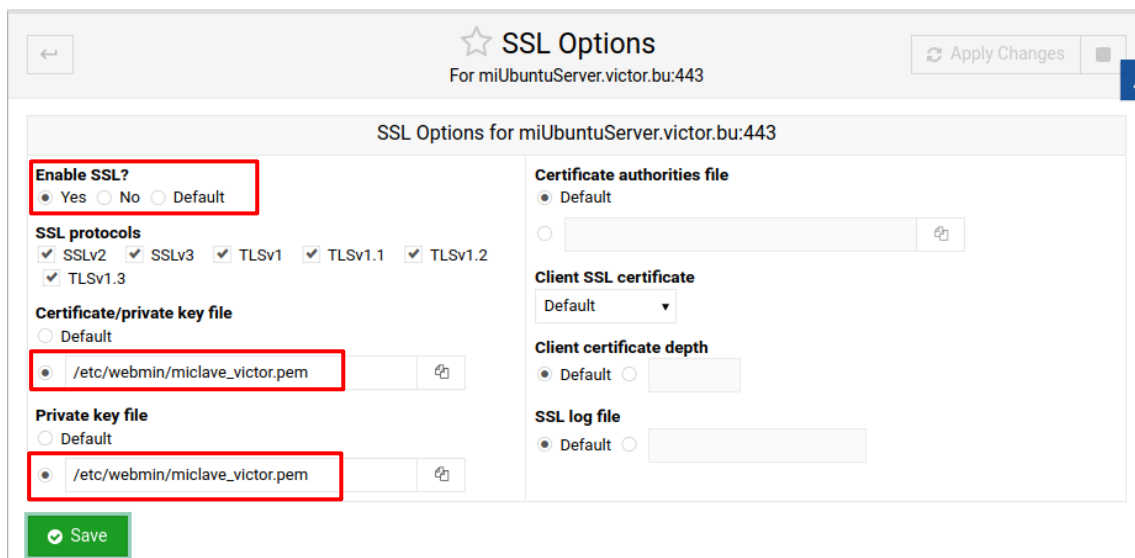
4.) Una vez creado lo seleccionamos clicando sobre él, y seleccionamos “Opciones SSL



5.) Aplicamos los cambios en la flecha de arriba a la derecha.



6.) Marcamos la opción sí en las opciones SSL y añadimos el certificado creado.



7.) Aplicamos los cambios en la flecha de arriba a la derecha.



8.) Y antes de probarlo crea un registro de alias de este nombre en el servidor DNS.

☆ **Name Alias Records**  
In victor.bu

**Add Name Alias Record**

**Name**  
sitioseguero

**Real Name**  
miUbuntuServer (Absolute names must end with a .)

**Time-To-Live**  
☒ Default  
☐ seconds

**Create**

☆ **Name Alias Records**  
In victor.bu

**Add Name Alias Record**

**Name**

**Real Name**  
(Absolute names must end with a .)

**Time-To-Live**  
☒ Default  
☐ seconds

**Create**

Show records matching:  **Search**

☒ Select all ☐ Invert selection

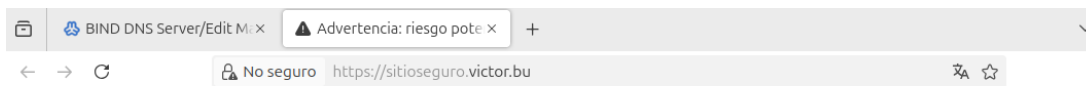
Name	TTL	Real Name
<input type="checkbox"/> www.victor.bu.	3600	miUbuntuServer
<input type="checkbox"/> blog.victor.bu.	3600	miUbuntuServer
<input type="checkbox"/> sitioseguero.victor.bu.	3600	miUbuntuServer

☒ Select all ☐ Invert selection

**Delete Selected**

9.) Guardamos e **Importante Aplicamos los cambios**, en la parte superior derecha (recordad los problemas que nos da no hacerlo, es posible que en este punto tengamos que reiniciar el servidor).

Una vez hecho nos conectamos a nuestra página y ya tenemos una repuesta conocida



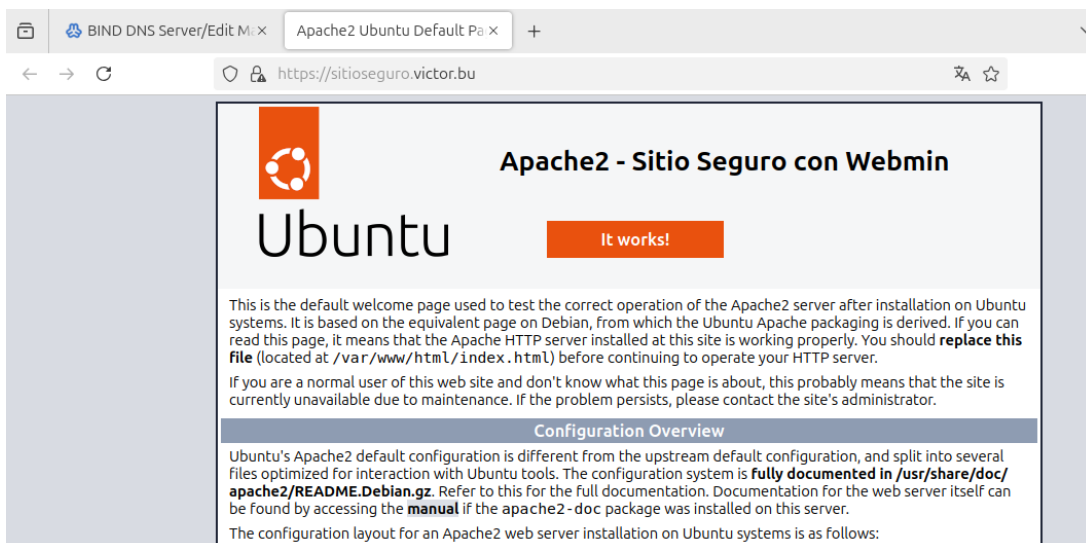
## Advertencia: riesgo potencial de seguridad a continuación

Firefox ha detectado una posible amenaza de seguridad y no ha cargado **sitioseguero.victor.bu**. Si visita este sitio, los atacantes podrían intentar robar información como sus contraseñas, correos electrónicos o detalles de su tarjeta de crédito.

[Más información...](#)

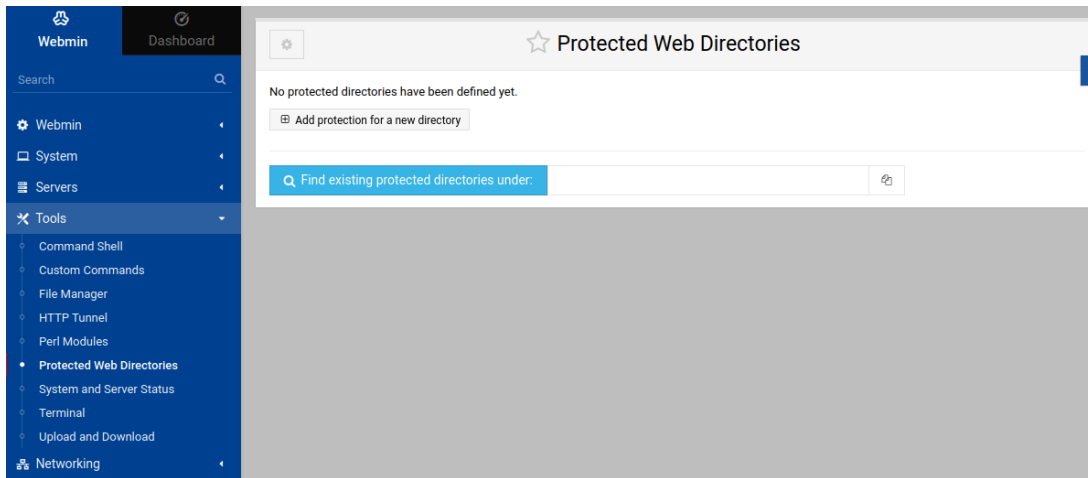
Retroceder (recomendado)

Avanzado...

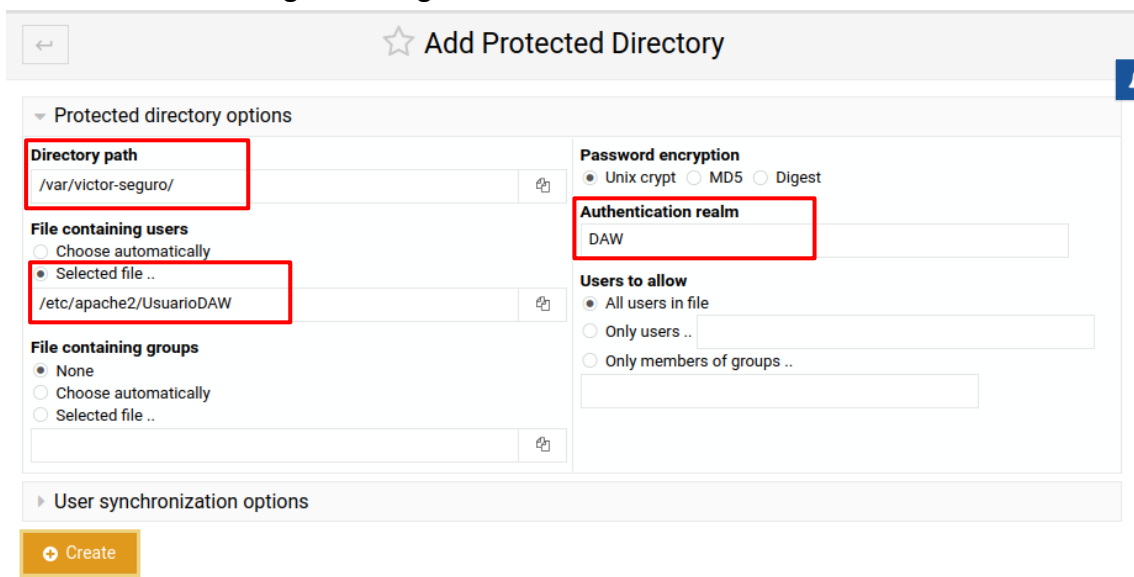


## BLOQUE 4: Configurar el servidor con autenticación básica

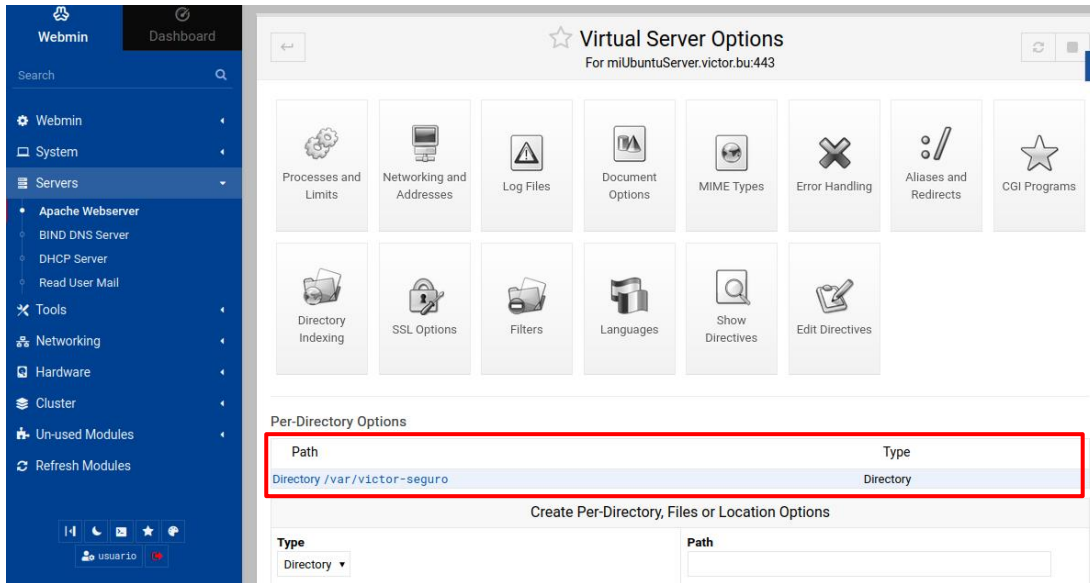
1. Abre Webmin y accede al enlace Directorios Web Protegidos de la sección Herramientas del menú principal.



2. Haz clic sobre el enlace Agregar protección para un nuevo directorio y rellenamos según la imagen.



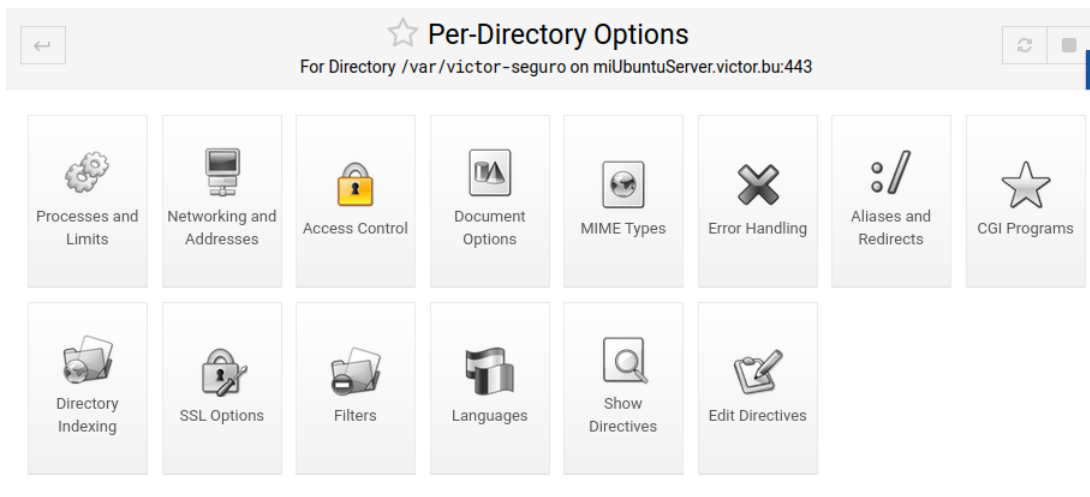
3. Desde el servidor de apache, haz clic sobre el directorio seguro



The screenshot shows the Webmin interface for configuring Virtual Server Options. The left sidebar contains a navigation menu with categories like Webmin, System, Servers, Tools, Networking, Hardware, Cluster, Un-used Modules, and Refresh Modules. The main content area is titled 'Virtual Server Options' and lists various configuration categories as icons. Below these, the 'Per-Directory Options' section is highlighted with a red box. It contains a table with two columns: 'Path' and 'Type'. The table has one entry: 'Directory /var/victor-seguro' with the type 'Directory'. Below the table, there is a section titled 'Create Per-Directory, Files or Location Options' with input fields for 'Type' (set to 'Directory') and 'Path'.

Path	Type
Directory /var/victor-seguro	Directory

4. Dentro, haz clic sobre el botón de “Access Control”



The screenshot shows the 'Per-Directory Options' page for the directory /var/victor-seguro. The page title is 'Per-Directory Options' and the subtitle is 'For Directory /var/victor-seguro on miUbuntuServer.victor.bu:443'. The main content area displays a grid of configuration categories as icons. The 'Access Control' icon, which features a yellow padlock, is highlighted. Other categories include Processes and Limits, Networking and Addresses, Document Options, MIME Types, Error Handling, Aliases and Redirects, CGI Programs, Directory Indexing, SSL Options, Filters, Languages, Show Directives, and Edit Directives.



5. Configura el control de acceso al directorio como aparece en la imagen y aplica los cambios después de guardar.

**Access Control**  
For Directory /var/victor-seguro on miUbuntuServer.victor.bu:443

Access Control for Directory /var/victor-seguro

**Authentication realm name**  
☐ Default ☒ DAW

**Authentication type**

**Pass basic login failures to next module?**  
☐ Yes ☐ No ☒ Default

**Basic login user file types**

**Restrict access by login**  
☐ Default  
☐ Only these users:   
☐ Only these groups:   
☒ All valid users

**User text file**  
☐ Default  
☒ /etc/apache2/UsuarioDAW

**Clients must satisfy**  
☒ Default  
☐ All access controls  
☐ Any access control

**Restrict access**  
 Access checking order: ☐ Deny then allow ☐ Allow then deny ☐ Mutual failure ☒ Default

Action	Condition
<input type="text" value="All requests"/>	<input type="text"/>

6. Volvemos al apartado anterior de “Protección de directorios web” y clicamos en nuestro directorio protegido el botón de crear nuevo usuario.

**Protected Web Directories**

☒ Select all ☐ Invert selection

Protected directory	Associated users and groups
<input type="checkbox"/> /var/victor-seguro/	No users have been defined yet. <input type="button" value="Add a new user"/>

☒ Select all ☐ Invert selection

7. Creamos un nuevo usuario.

**Create User**

Web authentication user details

**Username**

**Password**

**Enabled?**  
☒ Yes ☐ No

8. Una vez creado el usuario comprobaremos que aparece en la lista

```
usuario@usuario:~$ cat /etc/apache2/UsuarioDAW
Victor:$y$j9T$FJBT.keuaAQUGCZwpy0ov.$S5YbEQxZb2YWjvNHfLJXDwdP9L5GNoLeuBWxzY4tpU9
```

9. A partir de ahí el funcionamiento al conectarnos a nuestra página web debería ser como en el caso de Windows.

