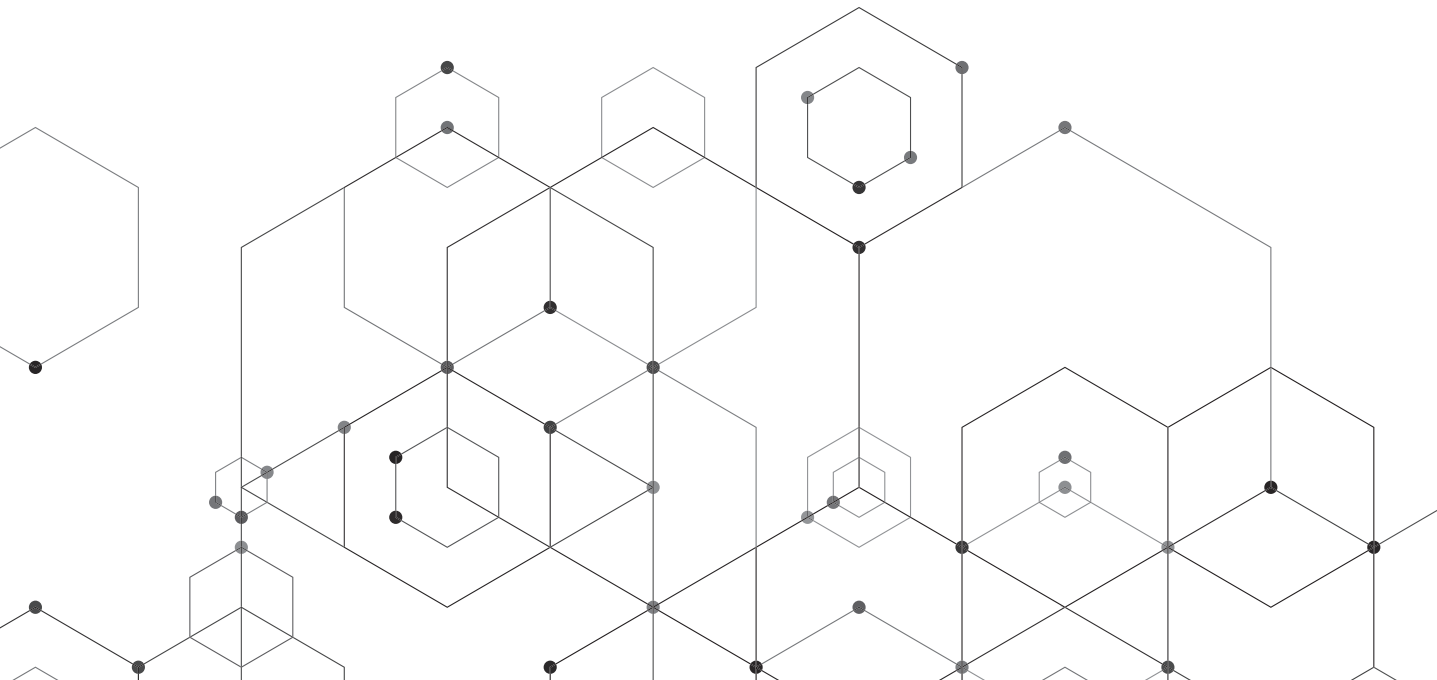
Moodle 3.x. Sistema de gestión de aprendizaje

Guía ilustrada para docentes y administradores



Moodle 3.x. Sistema de gestión de aprendizaje. Guía ilustrada para docentes y administradores
Coordinadores: Miguel Omar Muñoz Domínguez · Glenda Mirtala Flores Aguilera.

México, Editorial Didáctica: 2021
238 p. : gráf. ; 19 × 21.5 cm
ISBN 978-607-99443-3-9

Primera edición: 2021
Impreso en México

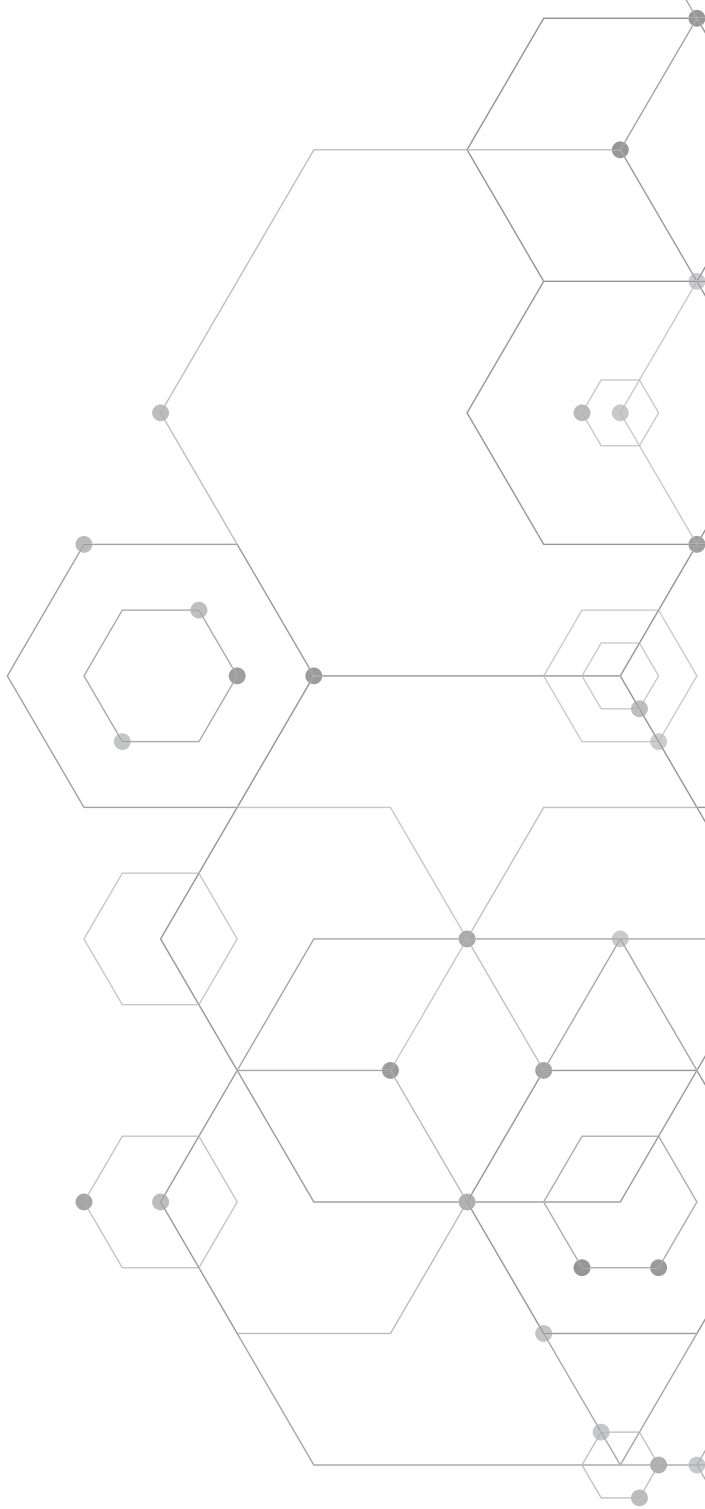
Dirección editorial
Carlos Iván Díaz Barriga de los Cobos

Control de calidad
Simitrio Quezada

Producción editorial
Dalia de la Torre Jiménez

www.editorialdidactica.mx
direccion@editorialdidactica.mx
492 189 0984

Esta obra fue doblemente arbitrada por académicos.



CONTENIDOS

PARTE UNO

CAPÍTULO III
Seguridad en Moodle

Raúl Armando Valadez Estrada
Susana Cordero Dávila

Es fundamental conocer los aspectos necesarios de seguridad mínimos para salvaguardar la privacidad de los estudiantes y el correcto funcionamiento de la plataforma LMS y el servidor mismo. Se categorizan en 3 apartados los aspectos básicos de seguridad:

- Protección exterior del servidor.
- Protección al interior del servidor.
- Seguridad dentro del LMS Moodle.

Protección exterior del servidor

Al ofertar algún servicio en la Internet, en este caso LMS Moodle, es necesario estar protegido contra posibles ataques al servidor que hospeda el Moodle. Si sólo se desea que se acceda al LMS desde Internet, es necesario saber qué puertos usa el LMS. Principalmente son dos: el puerto 80, del servidor Web, puerto en el que se conecta mediante el protocolo de comunicaciones HTTP (HyperText Transfer Protocol o Protocolo de Transferencia de HiperTexto) y el puerto 443 donde se conecta el HTTPS (el protocolo HTTP Seguro, en el cual se encriptan todos los datos que se envían y reciben al Moodle).

Sin embargo para emplear el HTTPS es necesario adquirir un certificado SSL de conexión segura; de modo gratuito o mediante alguna compañía que oferta certificados verificados por ellos mismos o terceros. Los certificados gratuitos como los de https://www.sslforfree.com/ son bastante seguros. No se recomienda usar HTTPS (puerto 443) con un dominio generado por nosotros mismos, pues eso sólo confundirá a los usuarios que se conecten, pues les dará advertencia que se está empleando un certificado no verificado y les pedirá cancelar o continuar con la conexión y se acostumbrarán a aceptar certificados no verificados.

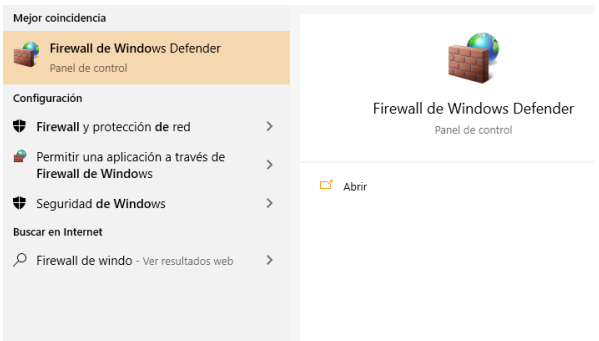
Si no se tiene certificado, los usuarios se conectarán en el puerto 80. Una vez que se instale algún certificado SSL se accederá por (HTTPS) y a partir de ese momento se podrá cerrar el puerto 80 o redireccionar todas las conexiones entrantes en el HTTP hacia el HTTPS.

Si se desea también que se reciba correo electrónico a la plataforma (no muy recomendado), sólo enviar, puede abrirse el puerto 25 de SMTP (Send Mail Transfer Protocol o Protocolo de Transferencia de Envío de Correo). Requerirá una configuración más complicada en el servicio de envío y recepción de correo electrónico (SMTP), para evitar que lo usen como SPAM Relay (envío de publicidad basura y Malware).

De no estar correctamente configurado, el servidor pasará a listas negras de servidores SPAM, por lo que no se recomienda en un principio habilitar el servicio de correo y abrir en el cortafuegos el puerto 25 (ya que el correo podrá enviarse a un servidor de terceros como Gmail para que se entregue mediante ellos y minimizar los riesgos en nuestro servidor).

Configuración del Firewall de Windows

Para agregar las reglas de acceso al puerto 80 y 443 que requiere el LMS Moodle, es necesario buscar en el botón de inicio el Firewall de Windows Defender (figura 3.1).
Enseguida es necesario ingresar a la configuración avanzada del mismo:



Una vez que se elige la configuración avanzada se abrirá una nueva ventana. En ella se elige Reglas de entrada (figura 3.2).

Figura 3.1 (2) Localizando el Firewall de Windows Defender.
Fuente: Elaboración propia.

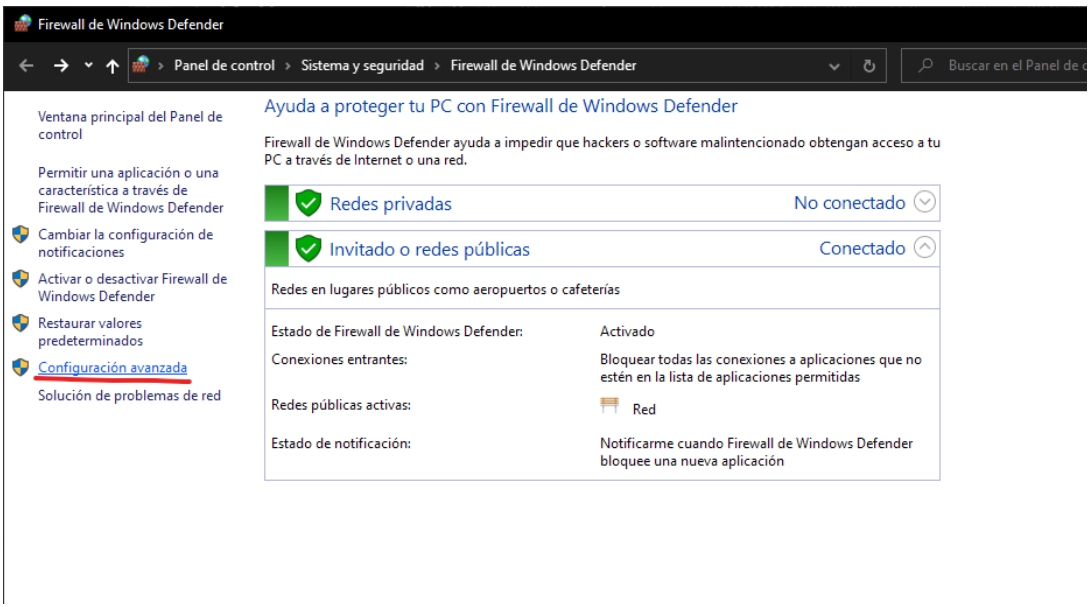


Figura 3.2 (2) Accediendo a la configuración avanzada del Firewall de Windows Defender.
Fuente: Elaboración Propia.

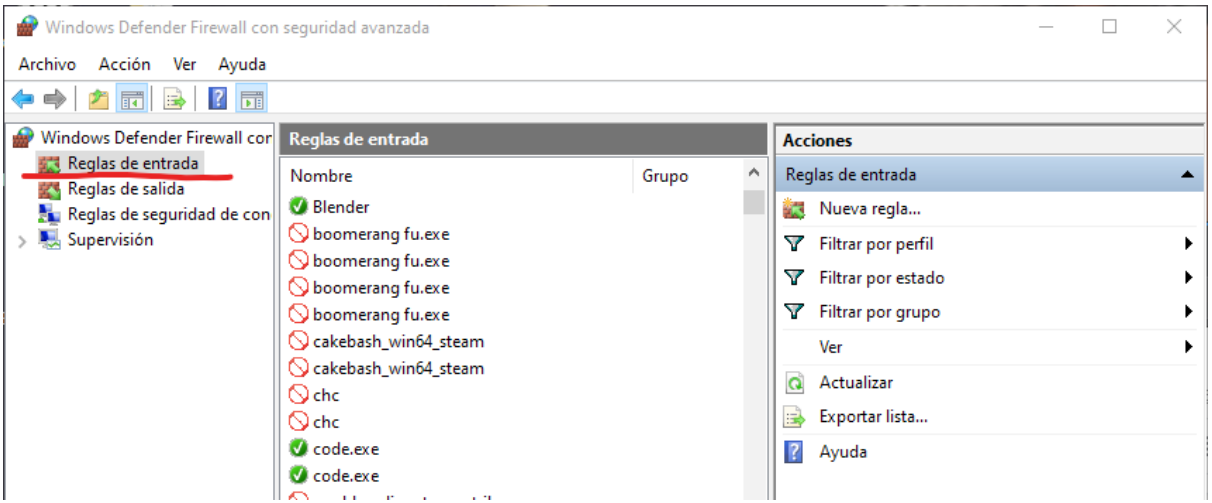


Figura 3.3 (2) Reglas de entrada del Firewall de Windows Defender.

A la derecha, en el apartado *Acciones*, está la opción Nueva regla (figura 3.4).

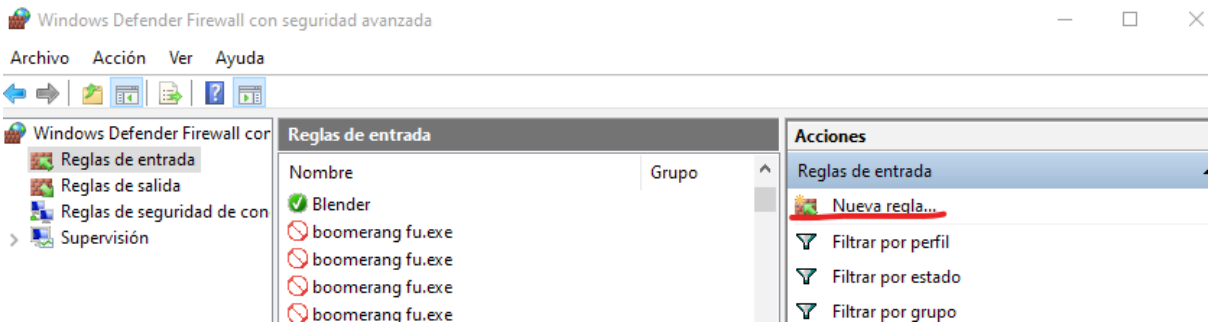


Figura 3.4(2) Adición de nueva regla del firewall.

Se abre una ventana donde se pide ingresar el tipo de nueva regla. Deberá elegirse la opción de puerto y se pulsa Siguiente (figura 3.5).

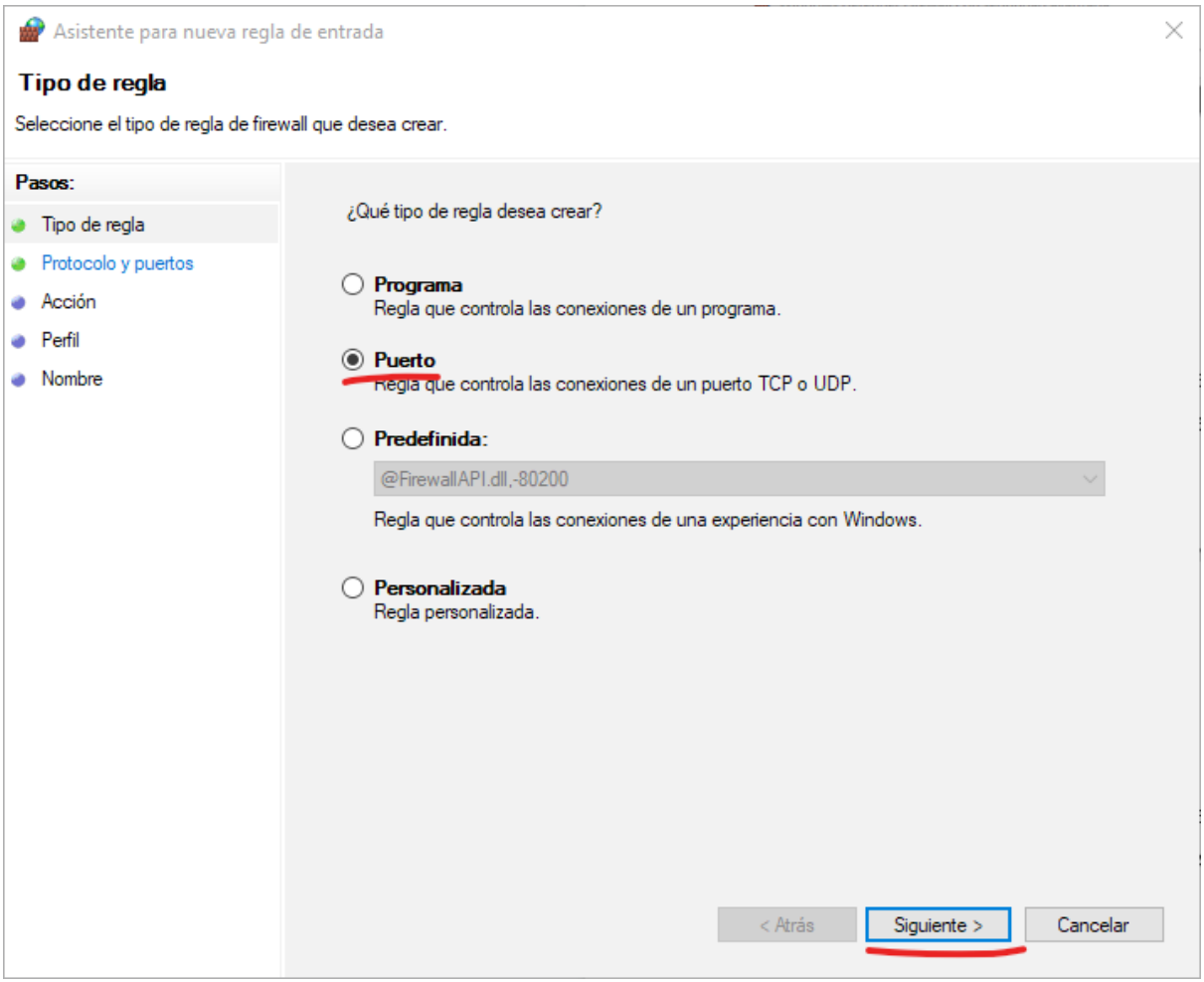


Figura 3.5 (2) Creando una nueva regla del cortafuegos de tipo Puerto.

Se especifica el tipo de puerto en que se elegirá TCP, y los puertos que desean abrirse. Para ello se elige la opción Puertos locales específicos y se teclea 80, 443 (puertos que se necesita abrir al exterior) (figura 3.6).

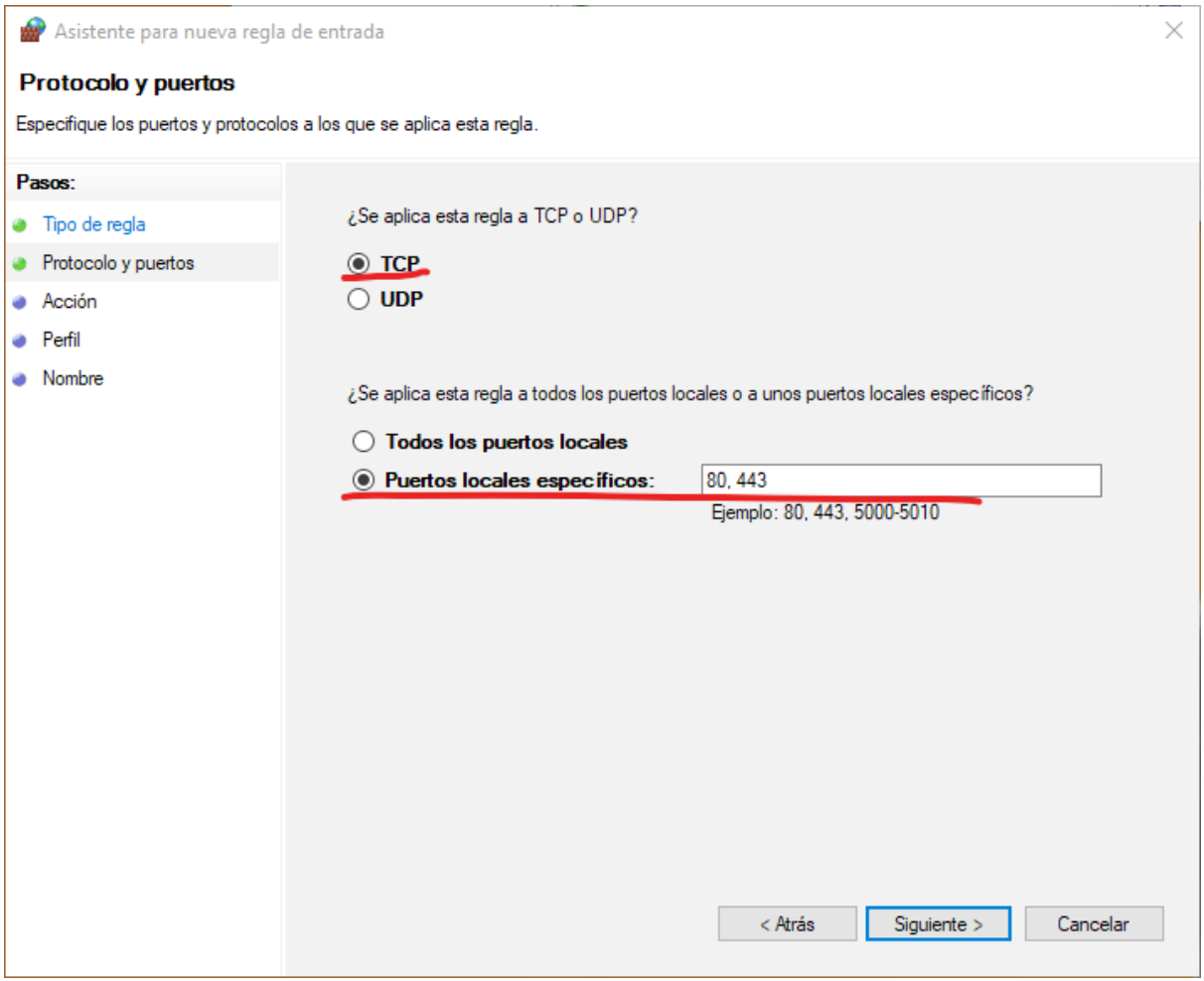


Figura 3.6 (2) Abriendo los puertos 80 y 443 de tipo TCP en el cortafuegos.

Tras pulsar *Siguiente* se elige la opción *Permitir la conexión* (Figura 3.7).

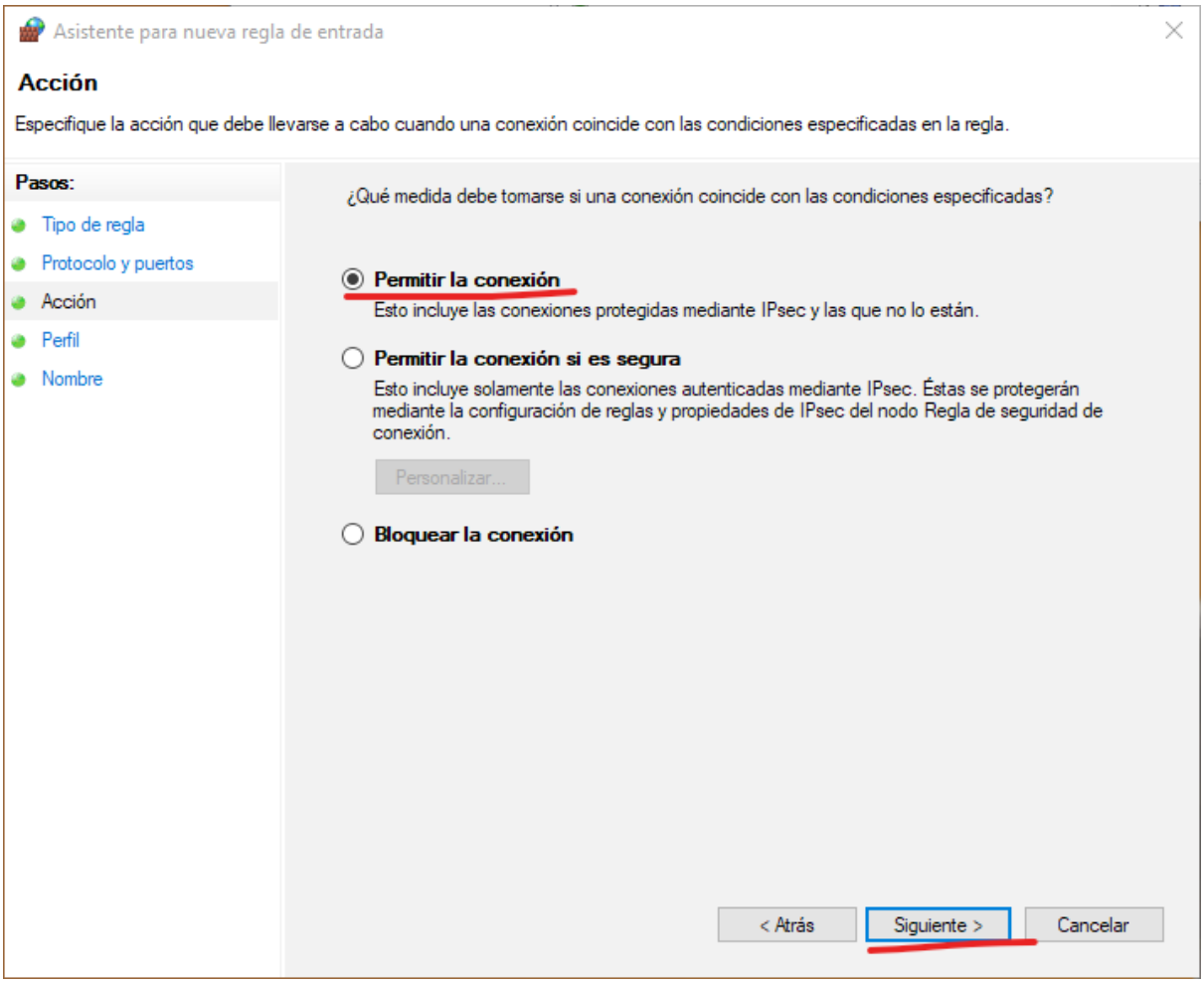


Figura 3.7 (2) Permitir conexiones a los puertos específicos.

En la siguiente etapa del proceso se solicita indicar el contexto de conexión al que se desea aplicar la regla. Como es una regla que debe aplicarse bajo cualquier contexto de conexión, debe tenerse elegidas todas las opciones.

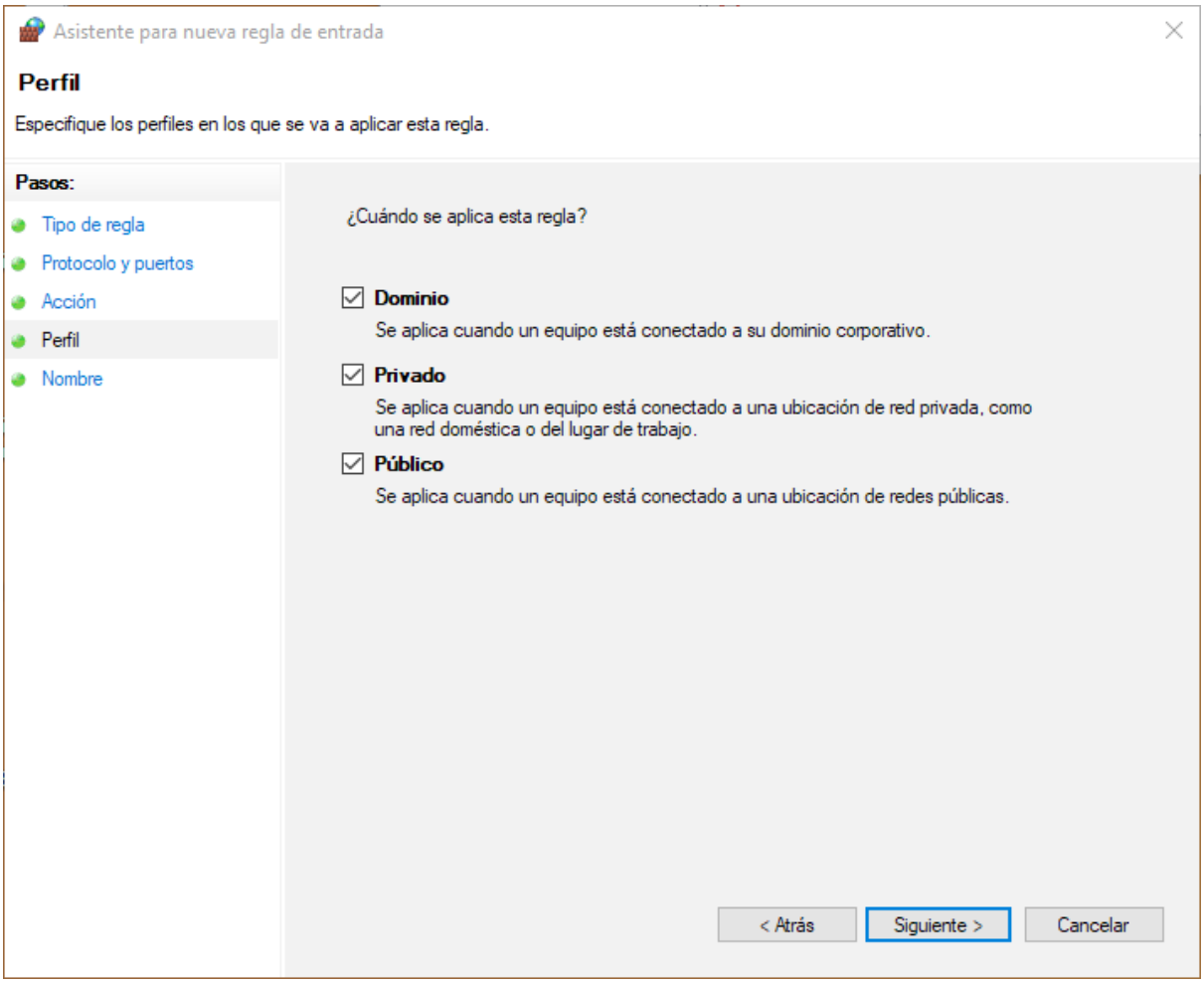


Figura 3.8 (2) ¿Cuándo se aplica la regla?

En la última etapa del proceso se solicita nombrar a la nueva regla e incluir una pequeña descripción (figura 3.9).

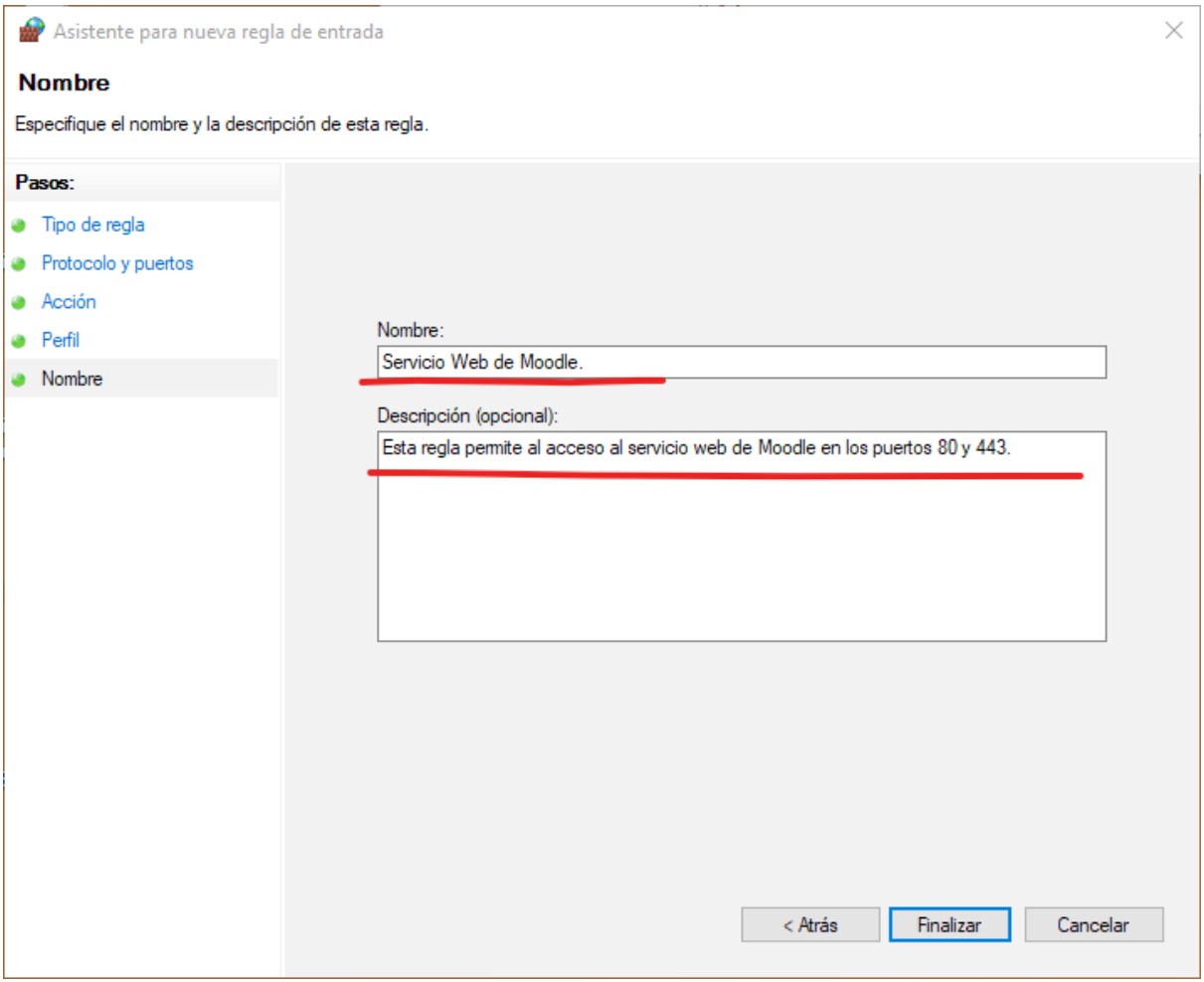


Figura 3.9 (2) Nombre y descripción de la nueva regla.

La nueva regla entrará en funciones. Algunas versiones de Windows solicitarán reiniciar el equipo para que ésta funcione. Ahora se mostrará en el apartado de reglas de entrada del Cortafuegos de Windows Defender (figura 3.10).

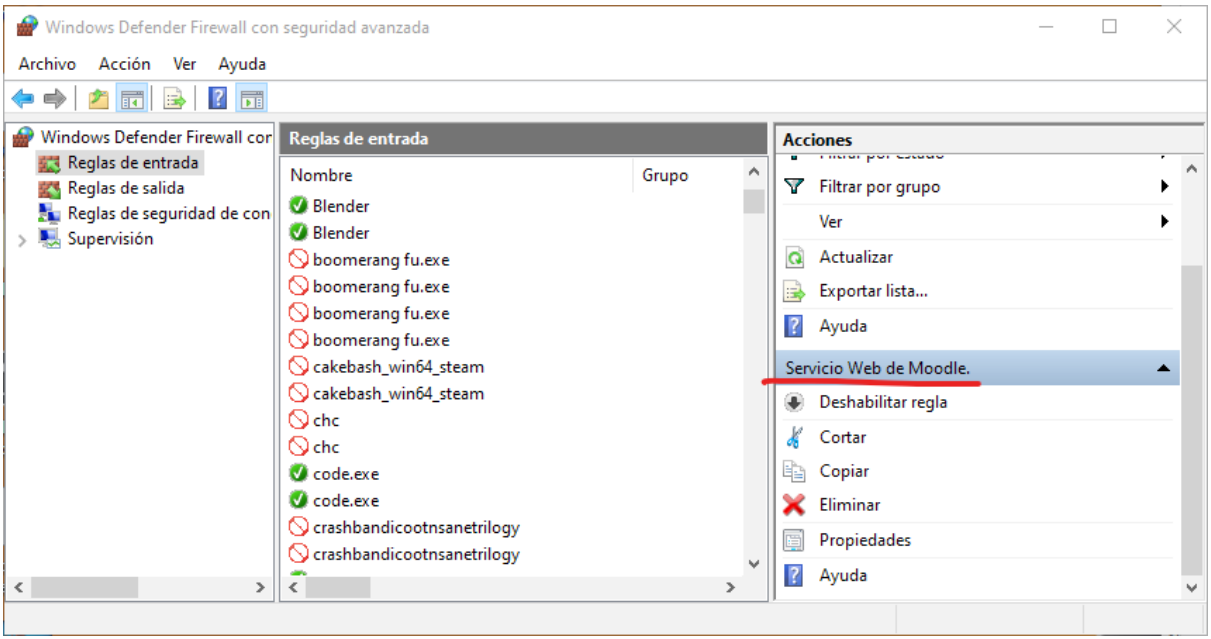
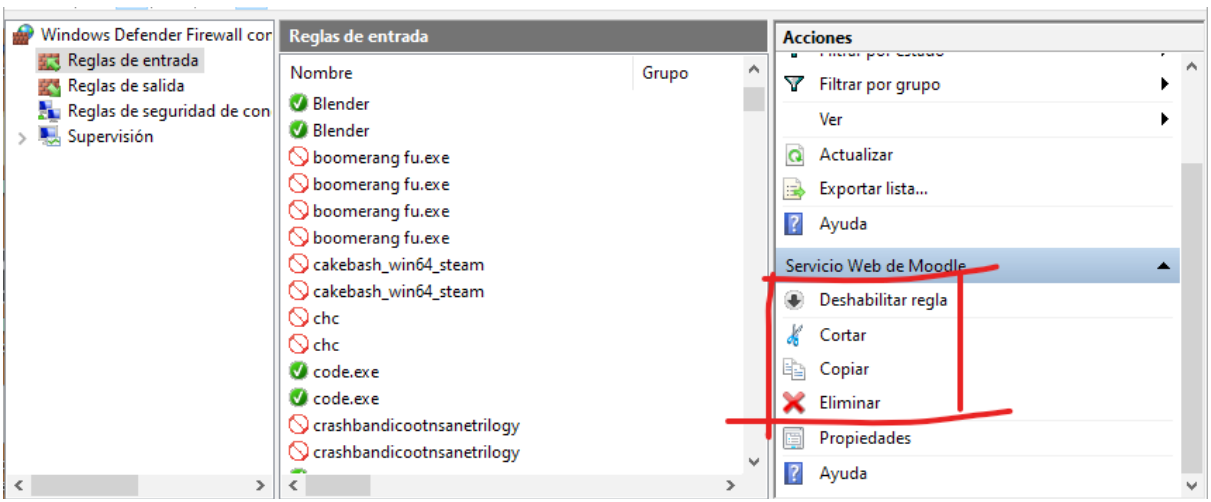


Figura 3.10 (2) Apartado de Reglas de entrada del cortafuegos de Windows Defender.

Si más adelante desea deshabilitar la regla, copiarla, cortarla, eliminarla o verificar sus propiedades, se recurrirá a los apartados correspondientes (figura 3.11).

Figura 3.11 (2) Opciones para alterar las reglas en el cortafuegos de Windows Defender.



Configuración del Firewall en MacOS

Para permitir que se acceda a nuestros servicios http y https (80 y 443) en MacOS, se abre una terminal de comandos y se teclea estos comandos:

```
sudo ipfw add 7000 allow tcp from any to any dst-port 80
```

```
sudo ipfw add 8000 allow tcp from any to any dst-port 443
```

Nota: Los números 7000 y 8000 sirven para identificar las reglas creadas. Es un número de identificación asignado para posteriormente eliminar o modificar estas reglas que llevan como referente dicho número.

Si se desea verificar las reglas añadidas al cortafuegos, teclee este comando:

```
sudo ipfw list
```

Si una regla ya no es necesaria o quiere eliminarse, se recurre a su número de identificación de regla. Por ejemplo, si es necesario eliminar la regla que permite el ingreso al puerto 80 (sudo ipfw add 7000 allow tcp from any to any dst-port 80), creada con el número de identificación 7000, se llevaría a cabo de este modo:

```
sudo ipfw delete 7000
```

Si se desea establecer a la configuración por defecto del firewall para comenzar desde cero, se ingresa en la terminal el comando:

```
sudo ipfw flush
```

Configuración del Firewall en Linux

Dependiendo de la distribución de Linux que se utilice, será el tipo de software para configurar el firewall. Por lo regular Linux utiliza iptables para filtrar sus conexiones. Sin embargo su configuración es demasiado técnica y abrumadora para los usuarios promedio.

Varias distribuciones de Linux ofrecen a sus usuarios diversos front-ends como interfaces más sencillas de usar, que interactúan con el iptables, sin que el usuario tenga que saber programar las reglas del mismo.

Por ejemplo algunas distribuciones ofrecen el ***firewalld*** como interface de iptables; otras distro optan por ***ufw*** (Uncomplicated FireWall o Firewall no complicado). Otras distro simplemente vienen con iptables, sólo por mencionar los más comunes.

Puede instalarse el firewall que más facilite al usuario: Si una distro sólo trae iptables puede instalarse por ejemplo el ufw para facilitar su configuración. Aun así es muy común que actualmente las distros vengan por lo regular con el ufw.

Para configurar el ufw, hay que cerciorarse de que esté instalado. Se ejecuta el comando:

```
$ sudo uwf status
```

Esto informará si está instalado. Si no lo está, el ufw se instala con cualquiera de los siguientes cuatro comandos:

```
$ sudo apt install ufw
```

```
$ sudo  apt-get install ufw
```

```
$ sudo dnf install ufw
```

```
$ sudo snap docker ufw
```

Se comprueba su estado con el comando sudo ufw status.

Para permitir acceso a los puertos 80 y 443, se introduce en el shell:

```
$ sudo ufw allow http
$ sudo ufw allow https
```

La salida de los comandos se muestra en la figura 3.12.

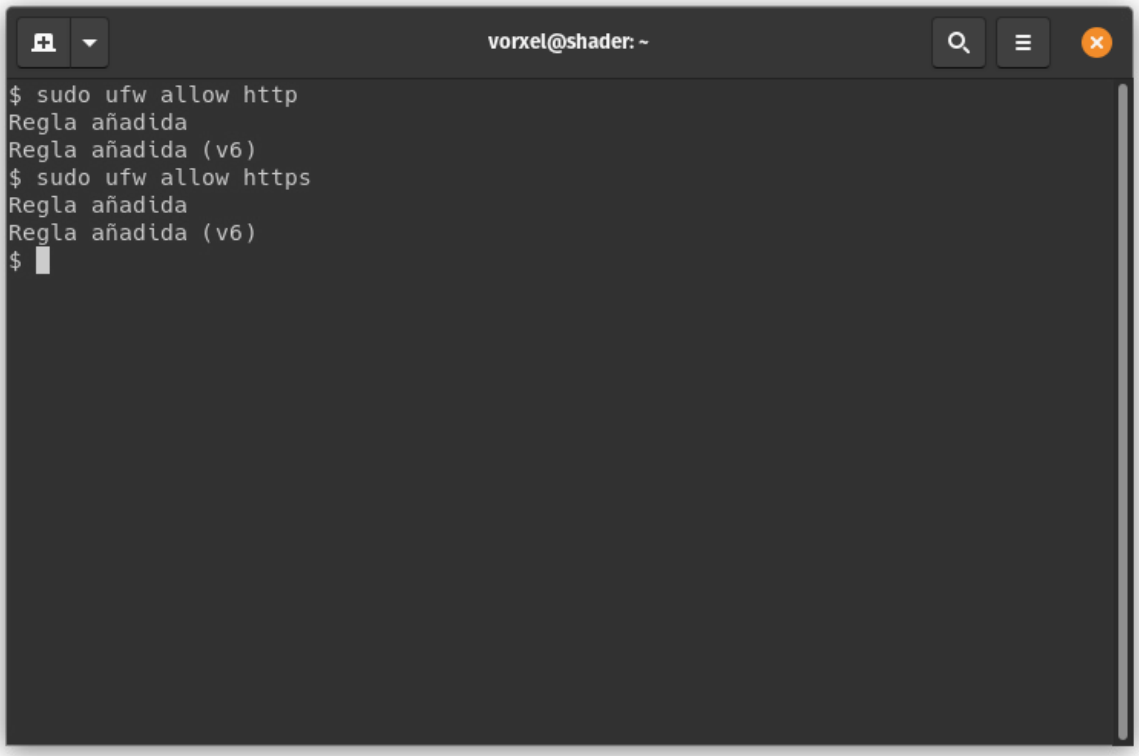


Figura 3.12 (2) Salida de los comandos uwf allow.

El retorno de los comandos muestra Regla añadida y Regla añadida (v6). Esta última dice que se añadió la regla también para el nuevo protocolo IP versión 6, que sustituirá a la versión 4 que se ha usado siempre. Para verificar su estado, se teclea:

```
$ sudo ufw status verbose
```

Esto informará qué puertos (servicios) se tiene abiertos al exterior (figura 3.13).

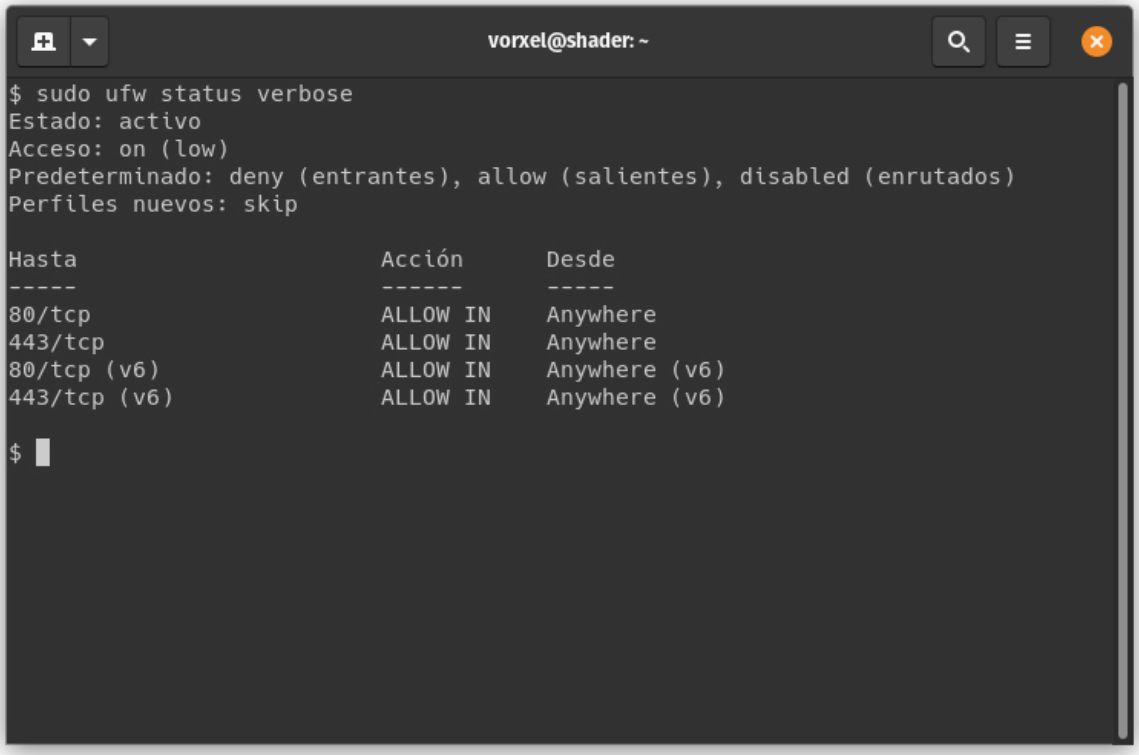


Figura 3.13 (2) Estado del ufw y sus puertos permitidos.

Si ya se instaló un certificado SSL y se desea cerrar el puerto 80 del http, se teclea:

```
$ sudo ufw delete allow http
```

Y se elimina el puerto 80 de los accesos permitidos (figura 3.14).

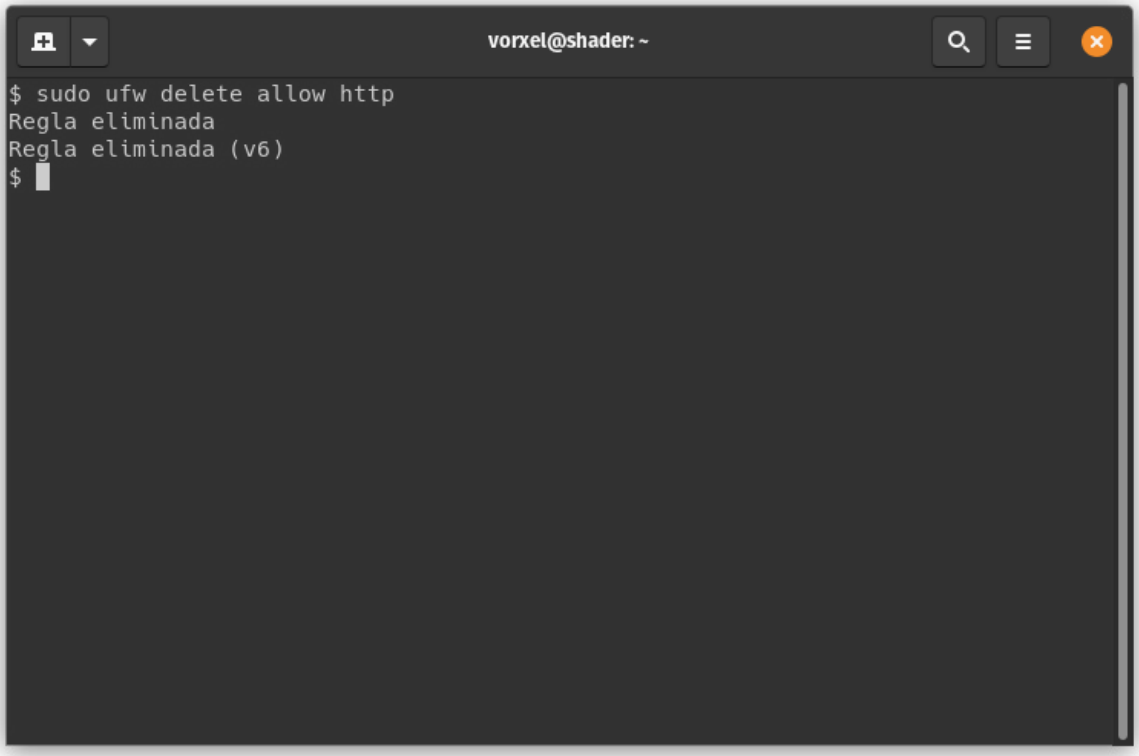


Figura 3.14 (2) Eliminación de acceso al puerto 80.

Protección al interior del S.O.

Debe revisarse la seguridad al interior del Sistema Operativo (S.O.). Por lo regular esto lo hacen usuarios con acceso al servidor: si no están bien establecidas las políticas de seguridad (los derechos en los subdirectorios y los propietarios de los mismos), se corre el riesgo de que el servidor o el servidor mismo sean intervenidos.

Los principios de seguridad básicos en los que está enfocado este capítulo se centran en los derechos de acceso, lectura y ejecución de los programas, archivos y carpetas, así como sus propietarios.

Mantener al día las actualizaciones

En todos los sistemas operativos se tienen activadas por defecto las actualizaciones automáticas. Deben aceptarse siempre y programar reinicios a la hora menos probable de participación de estudiantes. Debe prevenirse también cualquier eventualidad en que el sistema deba ser actualizado o recibir mantenimiento (por ello se recomienda anticipar el evento y avisar a los estudiantes).

Antivirus

Debe mantenerse activo siempre un antivirus: ya sea el «Defender» (instalado por defecto instalado en la versiones recientes de Windows) o alguno de elección personal.

Seguridad en la base de datos

Dentro de los parámetros de seguridad en el servidor donde se ejecuta Moodle destaca que se acceda localmente a su base de datos. El acceso a la base de datos debe hacerse con un usuario que no sea root o administrador, de modo que si se vulnera la base de datos sea más complicado para el atacante asumir dichos roles.

Para crear un usuario diferente al root o administrador, es necesario ingresar al DBMS (DataBase Management System o Sistema Gestionador de Bases de Datos) que se emplee para Moodle. Enseguida se muestra el proceso para las dos bases de datos más usadas en Moodle:

MySQL

MariaDB

Para crear un usuario que no pertenezca al grupo de administradores es necesario ingresar al intérprete de comandos de MySQL o MariaDB (prácticamente idénticos) con el comando:

```
$ mysql -u root -p
Enter password:
```

Será necesario ingresar como root o cualquier otro usuario de nivel administrativo que tenga acceso al DBMS e ingresar la contraseña cuando la pregunte el mysql. Debe conocerse el nombre de la base de datos sobre la que se instaló el Moodle. Suponiendo que se llamó «moodle», se deberá emplear ese nombre de base de datos en el comando que se introducirá. Dentro de la consola interactiva de comandos del mysql se crea un usuario para la base de datos *moodle*, con el que se conectará Moodle de este modo:

```
mysql> CREATE USER moodleuser@localhost
IDENTIFIED BY 'contraseña_aquí';
mysql> GRANT
SELECT,INSERT,UPDATE,DELETE,CREATE,CREATE
TEMPORARY TABLES,DROP,INDEX,ALTER ON moodle.*
TO moodleuser@localhost;
mysql> FLUSH PRIVILEGES;
mysql> quit
```

En el comando anterior se empleó la palabra contraseña_aquí en la primera línea de comandos. Ahí deberá sustituirse dicha palabra por la contraseña que se asignará al usuario que usará Moodle ahora para conectarse a la base de datos. En la segunda línea de comando se deberá sustituir moodle.* por el nombre de la base de datos que está empleando Moodle.

Si se tiene varios Moodle funcionando, hay que asegurarse de hacerlo para las diferentes bases de datos, o crear un usuario para cada una de ellas y realizar los pasos anteriores.

PostgreSQL

Para crear un usuario y darle los derechos necesarios de acceso a la base de datos de Moodle, es necesario ingresar al DBMS con este comando:

```
$ psql -U postgres
Password for user postgres:
```

Se ingresará la contraseña del usuario administrativo del PostgreSQL (en este caso es postgres el usuario administrativo por defecto). Una vez ingresados a la consola interactiva de comandos postgresql, suponiendo que el usuario que empleará Moodle

para conectarse se llamará *moodleuser*, se teclea:

```
postgres=# CREATE USER moodleuser WITH
PASSWORD 'contraseña_aquí';
postgres=# GRANT CONNECT ON DATABASE moodle
TO moodleuser;
postgres=# GRANT ALL PRIVILEGES ON DATABASE
moodle TO moodleuser;
postgres=# quit()
```

En los comandos anteriores se deberá sustituir la frase contraseña_aquí por la contraseña para el nuevo usuario y se deberá usar el nombre de la base de datos de moodle que se está empleando, donde se encuentra la palabra moodle en los comandos anteriores.

Ajustes en config.php

Una vez creado el usuario nuevo para que se conecte el Moodle al DBMS, es necesario realizar cambios al archivo de configuración de Moodle: config.php del directorio donde se instaló Moodle para que a partir de este momento comience a conectarse con el nuevo usuario. Debe localizarse las siguientes líneas dentro de dicho archivo y poner los datos del usuario que se creó:

```
$CFG->dbname   = 'moodle';
$CFG->dbuser   = 'moodleuser';
$CFG->dbpass   = 'contraseña_aquí';
```

Una vez realizados los cambios es necesario reiniciar el servicio web. Esto dependerá del tipo de servidor que se esté ejecutando. Por ejemplo, en Linux puede realizarse esto con el comando:

```
$ sudo systemctl restart httpd.service
```

Seguridad de archivos

Otro punto clave de la seguridad local de un servidor es la seguridad de archivos. Puede leer, ejecutar y/o modificar archivos cualquier usuario que tenga acceso a un equipo. Lo que puede hacer con ellos o su grado de acceso depende de los permisos y derechos que se le otorguen sobre los mismos: a esto se le llama el Access Control System (ACS o Sistema de Control de Acceso). Hay varios tipos, dependiendo del sistema operativo que se utilice.

Control de Acceso Discrecional

Para Linux y MacOS, el Control de Acceso Discrecional (Discretionary Access Control o DAC) es un tipo de protección de acceso basado en la identidad de los usuarios y los grupos a los que pertenecen. Se dice que es discrecional porque un individuo con ciertos permisos es capaz de transferir permisos a otros. Todos los sujetos pertenecen a grupos de usuarios y los permisos que pueden tenerse respecto al sistema de archivos (filesystem) son:

Permisos en archivos:

- Lectura (Read (R)): Permiso de sólo lectura en los archivos. No se permite su modificación.
- Escritura (Write (W)): Otorga la facultad de modificar el contenido de un archivo.
- Ejecución: (Execute (X)): Garantiza ejecutar un archivo. Es un programa o guion ejecutable.

Permisos en directorios:

- Lectura (Read (R)): Permite enlistar los contenidos de un directorio (ver qué contiene un directorio).
- Escritura (Write (W)): Otorga la facultad de crear, renombrar y/o borrar archivos.
- Ejecución: (Execute (X)): Garantiza el ingreso a un directorio.

Las carpetas o directorios donde se encuentra Moodle deben pertenecer al usuario que ejecuta

el servicio web. Por lo regular el usuario es identificado como «apache» o «www-data». También debe establecerse las políticas de acceso de dichos usuarios a los directorios de Moodle.

Para asegurar el directorio donde Moodle almacena sus contenidos (moodledata), es necesario conocer su ubicación al momento de instalar moodle. Suponiendo que está en su ubicación de defecto: /var/www/moodledata y el usuario que ejecuta el servicio web es apache, los comandos para establecer sus permisos serían de la siguiente manera:

```
$ chown -R apache:apache /var/www/moodledata/
$ chmod -R ug=rwX,o= /var/www/moodledata/
```

El primer comando cambia el propietario y grupo a apache para el directorio /www/var/moodledata. El -R garantiza que dicho propietario se propague al interior del contenido del directorio (es decir, que todo lo que contenga también pertenezca a dicho usuario).

En el segundo comando se establecen los permisos del directorio moodledata. Ver ug=rwX implica que el usuario y su grupo tiene derecho a leer, escribir y ejecutar, y o= significa que cualquier otro usuario que no pertenezca al grupo o no sea el usuario que es propietario del directorio no tiene derecho ninguno. Es decir, sin acceso.

Ahora debe establecerse los permisos en el subdirectorio donde se hospeda el motor del Moodle. Suponiendo que está instalado en su carpeta por defecto: /var/www/html y que el usuario con el que se ejecuta el servicio web es apache, la sintaxis de comandos es:

```
$ chown -R apache:apache /var/www/html/
$ chmod -R u=rwX,g=rX,o= /var/www/html/
```

En esta secuencia de comandos se otorga la propiedad del directorio de moodle y su contenido al usuario y grupo apache. En la segunda línea de código se otorgan todos los derechos al propietario (el grupo sólo puede leer y ejecutar, sin modificar y otros usuarios no pueden hacer nada).

La seguridad de archivos en Windows está basada en las Listas de Control de Acceso (Access Control Lists o ACL): acciones y permisos otorgados a los usuarios sobre cualquier objeto del sistema operativo.

Ésta es una lista simplificada estándar de permisos disponibles en Windows para archivos:

- Control completo (Full control): Permiso para realizar cualquier cosa.
- Modificar (Modify): Puede modificar los archivos.
- Leer y ejecutar (Read and Execute): Puede leer y ejecutar archivos mediante las carpetas.
- Lectura (Read): El usuario puede abrir y leer archivos de cualquier tipo.
- Escritura (Write): El usuario puede modificar y almacenar archivos.
- Listar el contenido de una carpeta (List folder content): El usuario puede ver el contenido de la carpeta.

Para establecer los derechos en el Windows para Moodle, es necesario ejecutar una consola de comandos (Shell) como administrador. Suponiendo que el usuario al que se dará derecho se llama moodle y que sus carpetas de instalación son para moodle: c:\inetpub\wwwroot y para moodledata: c:\moodledata, se ejecutarán las siguientes instrucciones:

```
icacls C:\moodledata /Q /T /inheritance:r
icacls C:\moodledata /Q /T /grant Administrators:(OI)
(CI)(F)
icacls C:\moodledata /Q /T /grant moodle:(OI)(CI)(F)
```

```
icacls C:\inetpub\wwwroot /Q /T /inheritance:r
icacls C:\inetpub\wwwroot /Q /T /grant Administrators:(OI)(CI)(F)
icacls C:\inetpub\wwwroot /Q /T /grant moodle:(OI)(CI)(RX)
```

En el primer set de comandos los usuarios que pertenezcan al grupo de Administradores recibirán permiso total sobre el directorio donde Moodle almacena sus datos, mientras que al usuario moodle sólo se le otorga derechos de lectura. Al mismo tiempo se ha configurado ambos directorios para que automáticamente se apliquen dichos permisos a cualquier nuevo subdirectorio que se agregue en esos directorios.

En el segundo set de comandos, las mismas reglas se aplican que el caso anterior, pero al directorio wwwroot (donde reside el motor del LMS Moodle).

3.3. Seguridad al interior del LMS Moodle

En LMS Moodle interactúan los usuarios y comparten documentos y archivos. Mucha información personal debe ser resguardada respecto al exterior. Se puede dotar mayor seguridad y privacidad al respecto.

Autenticación

Moodle puede manejar como mínimo 13 diferentes tipos de fuentes autoritarias de acceso, dependiendo de la versión de que se trate. El más utilizado es el procedimiento Logon: se llena un formulario HTML.

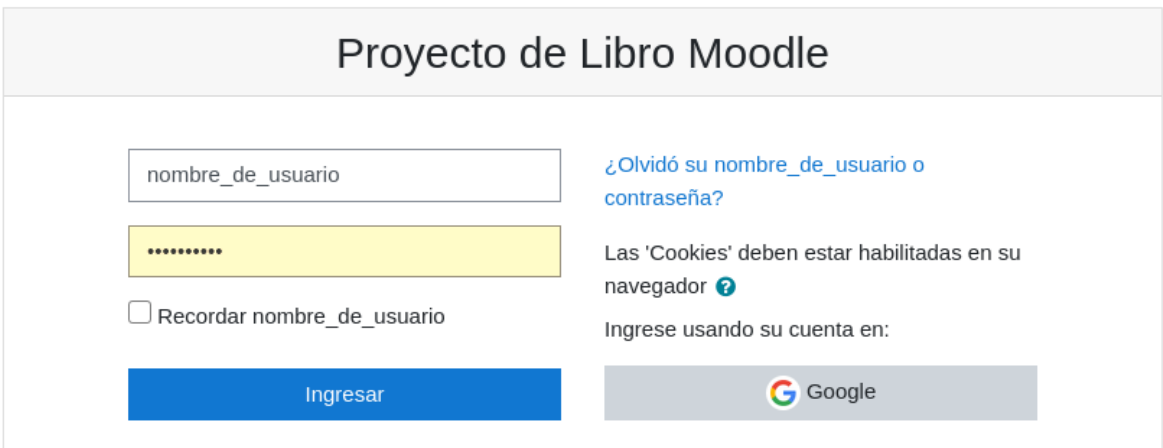


Figura 3.15 (2) Formulario de ingreso a Moodle

Puede recurrirse, también dentro de Moodle, a las políticas de contraseña en Administración del sitio/Seguridad/Políticas de seguridad (figura 3.16).

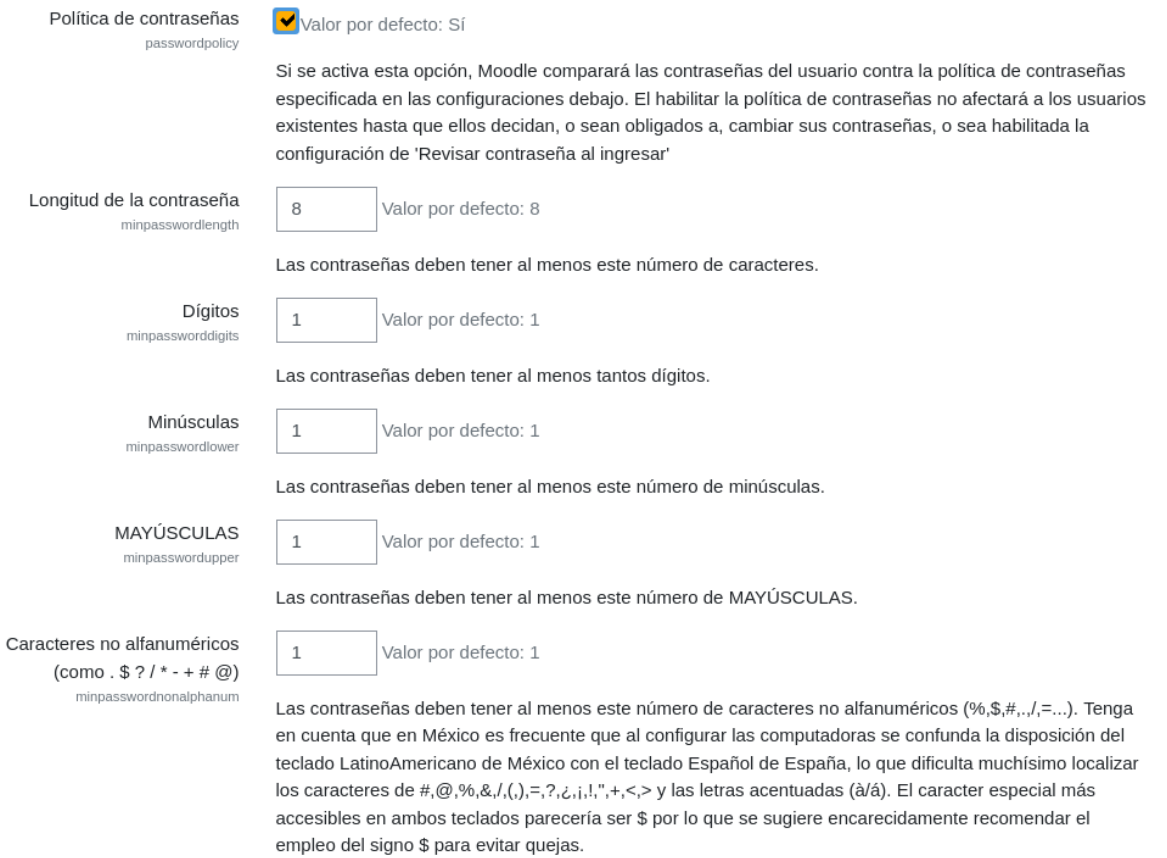


Figura 3.16 (2) Apartado de Políticas de Contraseña.

Certificados de Sockets de Capa Seguros (SSL)

Deben ser adquiridos en alguna compañía con licencia de emitir certificados raíz verificados: Comodo, VeriSign y Thawte, por mencionar algunas, o en sitios que los ofrecen de manera gratuita como www.sslforfree.com.

En última instancia puede generarse uno propio, pero carecerá de validez al no estar verificado por alguna compañía u organización y podría generar más problemas para los usuarios por las advertencias que estarían recibiendo al conectarse al sitio con el certificado no validado.

Uno de los parámetros que deben establecerse al instalar el certificado SSL es *Sólo aceptar cookies seguras*, en Administración del sitio/Seguridad/Seguridad HTTP, y ahí activar *Sólo 'cookies' seguras* (figura 3.17).

Figura 3.17 (2) Permitir sólo las conexiones con cookies seguras de HTTPS.

Protección de los nombres de usuario

Para que Moodle no muestre nombres de usuario en los mensajes de error es necesario ingresar a *Administración del Sitio/Seguridad/Políticas de seguridad del sitio*, y asegurarse de activar la casilla de verificación de Proteger nombres_de_usuarios.

Figura 3.18 (2) Casilla de verificación de protección de nombres de usuario.

Roles y perfiles

Si se sospecha que algún usuario tiene asignados roles que no le pertenecen, vaya a *Administración del sitio/Usuarios/Permisos/Comprobar permisos del sistema*. En la lista que aparece se deberá seleccionar o buscar manualmente al usuario cuyos roles buscan corroborarse. En su defecto, en el campo de búsqueda puede ingresarse el nombre del usuario en específico para que lo localice y corrobore Moodle (figuras 3.19 y 3.20).

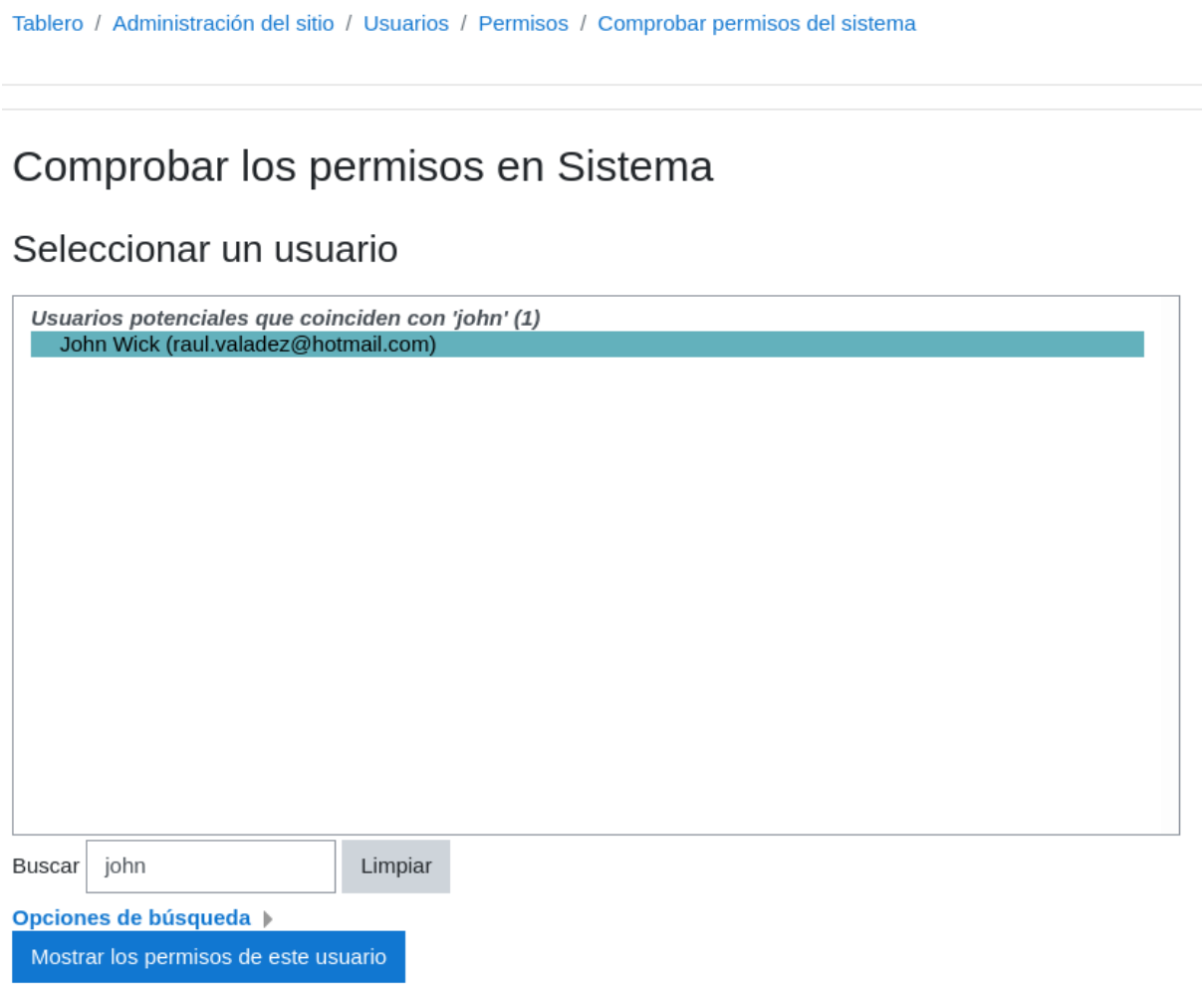


Figura 3.19 (2) Apartado de verificación de permisos en Moodle.

Comprobar los permisos en Sistema

Roles para usuario John Wick

- Usuario autenticado en Sistema

Permisos para John Wick

Filtro [ ] Limpiar

Capacidad	Permitido
Bloque: Administrar marcadores	
Añadir un nuevo bloque de marcadores (bookmarks) del admin a la página del Tablero block/admin_bookmarks:myaddinstance	Sí
Bloque: Insignias recientes	
Añadir un nuevo bloque de Insignias más recientes al Tablero block/badges:myaddinstance	Sí
Bloque: Calendario	
Añadir un nuevo bloque de calendario al Tablero block/calendar_month:myaddinstance	Sí
Bloque: Eventos próximos	
Añadir un nuevo bloque de eventos próximos al Tablero block/calendar_upcoming:myaddinstance	Sí
Bloque: Comentarios	
Añadir un nuevo bloque de comentarios al Tablero block/comments:myaddinstance	Sí
Bloque: Cursos	
Añadir un nuevo bloque de cursos al Tablero block/course_list:myaddinstance	Sí
Bloque: Búsqueda global	

Figura 3.20 (2) Lista de permisos de un usuario en específico.

Protegiendo los perfiles de usuario

Para resguardar la información privada de los usuarios se activa *Forzar a los usuarios a ingresar para ver los perfiles*, en *Administración del sitio/Seguridad/Políticas de seguridad del sitio* (figura 3.21).

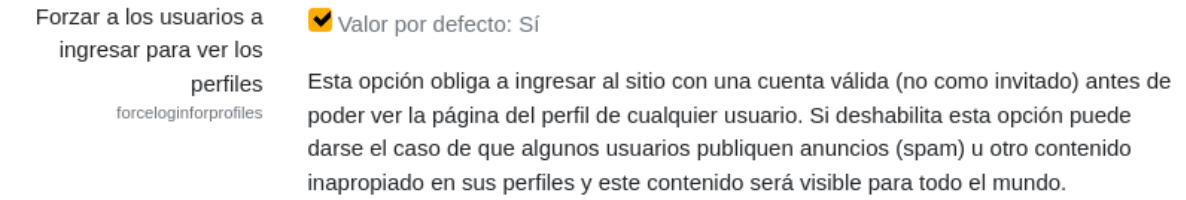


Figura 3.21 (2) Casilla de activación de forzar a los usuarios a ingresar para ver los perfiles.

Limitar la información que se muestra a todos los usuarios

Para ocultar campos de información en los perfiles, vaya a *Administración del sitio/Usuarios/Permisos*. En la parte intermedia se muestra la opción *Ocultar campos de usuario* (figura 3.22).

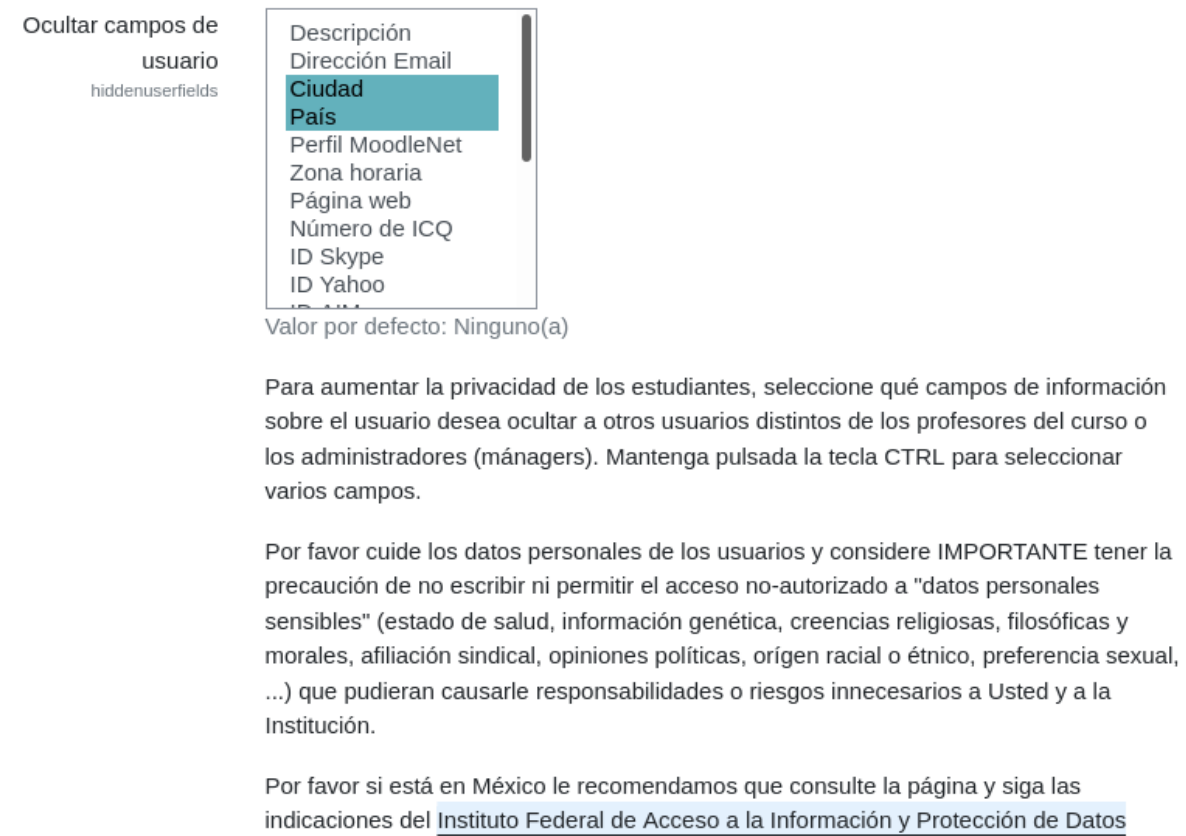


Figura 3.22 (2) Ocultar campos de usuario.

Se recomienda consultar página e indicaciones del Instituto Federal de Acceso a la Información y Protección de Datos, INAI (https://home.inai.org.mx/). También tener visible en todo momento la política de privacidad de datos del sitio Moodle, como lo exige el INAI.

Deshabilitar registrarse a sí mismo en Moodle

Se evita el autorregistro basado en email, en *Administración del sitio/Plugins/Autenticación/Gestionar autenticación*. En Ajustes comunes debe asegurarse que la lista desplegable esté en *Deshabilitar* (figura 3.23).

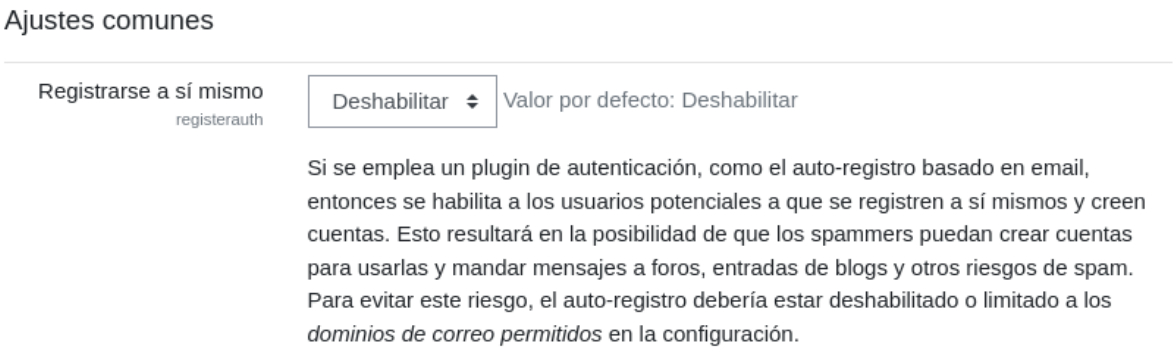


Figura 3.23 (2) Deshabilitado de registro a sí mismo.

Respaldos automáticos

Moodle facilita crear y automatizar periódicamente respaldos del LMS en *Administración del sitio/Cursos/Respaldos/Configuración de respaldo automatizado*.

Aquí se selecciona si están activos o inactivos los respaldos automáticos, qué día de la semana se llevarán a cabo, la hora en que se realizará el respaldo, el lugar donde se almacenará y otros parámetros como el número de respaldos a conservar, entre otros (figura 3.24).

Figura 3.24 (2) Apartado de configuración de respaldos automáticos.

Para que los respaldos automáticos funcionen correctamente, el cron debe estar ejecutando el script CLI de Moodle.