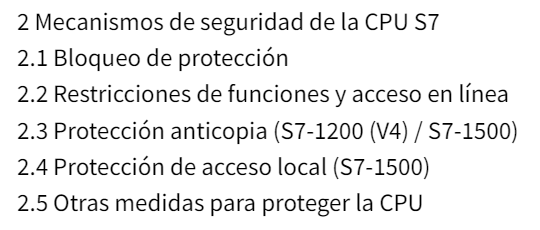
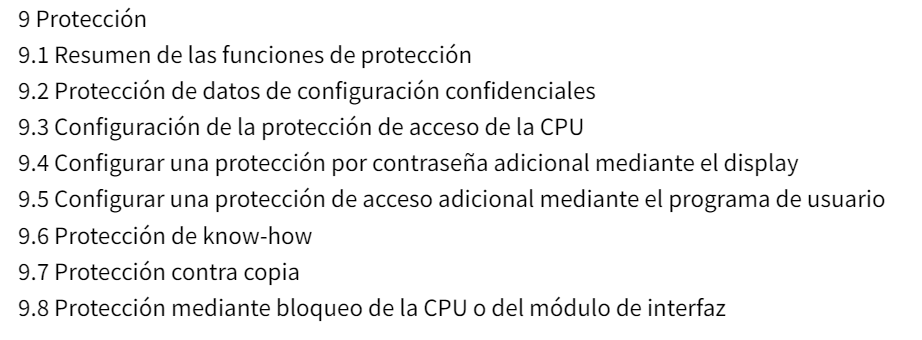
**1- Seguridad con Siemens .**

La modificación de los bloques y los datos de configuración del PLC a través de un acceso en red permite la adaptación rápida de las soluciones de automatización. Por otro lado, la modificación no deseada de los bloques del PLC puede modificar de forma adversa el comportamiento a nivel funcional del PLC. En consecuencia, es importante proteger el sistema de automatización con una aproximación en capas.

Para aquellos clientes preocupados por la alteración del programa o de los datos de configuración, Siemens recomienda el uso de propiedades de protección ofrecidas por los controladores SIMATIC S7-1200 y S7-1500.

Siemens ofrece varios documentos en los que hace mención a los mecanismos de seguridad de la CPU. 



****

**1- Resumen de las funciones de protección**

2- Protección de acceso

3- Protección de know-how

4- Protección contra copia

5- Protección mediante bloqueo de la CPU o del módulo de interfaz

6- Desactivación del servidor OPC UA

7- Desactivación de la comunicación PUT/GET

8- Desactivación de la sincronización horaria a través del servidor NTP

9- Desactivación del servidor web. Si utiliza el servidor web, proteja el sistema de automatización S7-1500/1200 contra accesos no autorizados estableciendo en la administración de usuarios derechos de acceso

10- Actualizar Firmware

**2- Protección de acceso**

La CPU ofrece cuatro niveles de acceso para limitar el acceso a determinadas funciones. Al configurar los niveles de acceso y las contraseñas, se limitan las funciones y las áreas de memoria a las que se puede acceder sin introducir una contraseña. Los niveles de acceso individuales, así como las contraseñas correspondientes, se definen en las propiedades de

objeto de la CPU.

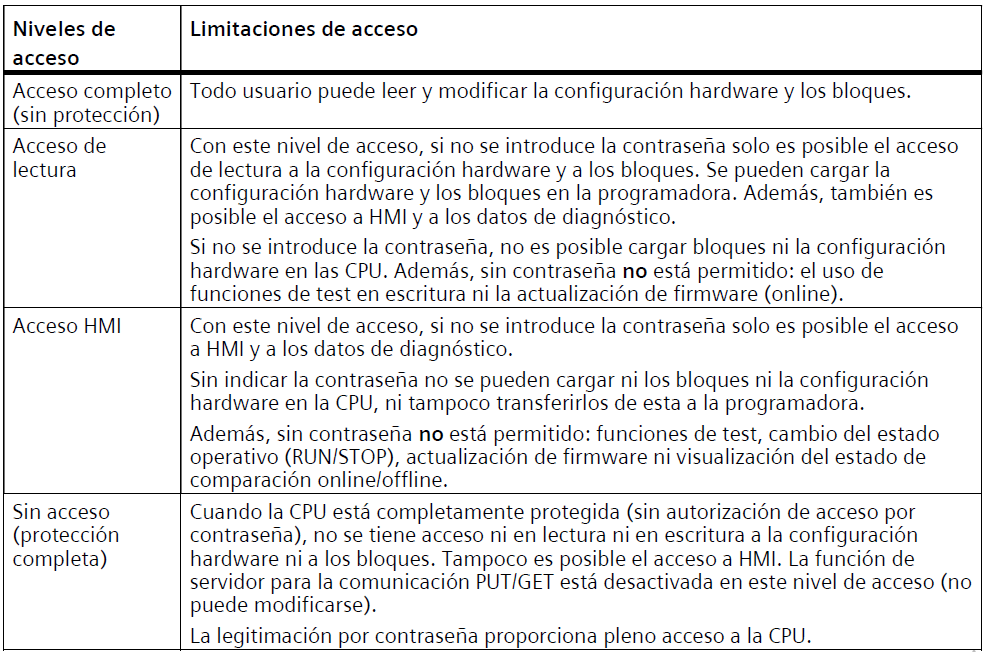
Asegúrese de que la contraseña sea lo suficientemente segura. Para ello, tenga en cuenta las reglas siguientes:

• Asigne una contraseña con una longitud mínima de 8 caracteres.

• Utilice diferentes tipos de grafías: mayúsculas, minúsculas, números y caracteres

especiales.

Niveles de acceso y sus limitaciones de acceso



Nota

La configuración de un nivel de acceso no sustituye la protección de know-how La parametrización de niveles de acceso ofrece una excelente protección contra modificaciones no autorizadas de la CPU a través de un acceso de red. Los niveles de acceso limitan los permisos para cargar la configuración hardware y el software en la CPU. En cualquier caso, los bloques de la SIMATIC Memory Card no están protegidos contra escritura o lectura. Para proteger el código de los bloques de la SIMATIC Memory Card se utiliza la protección de know-how.

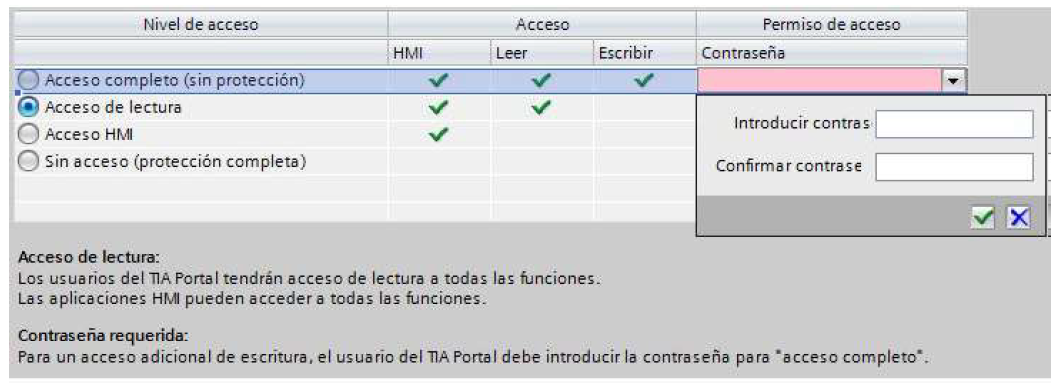
Parametrización de niveles de acceso

Para parametrizar los niveles de acceso de una CPU S7-1500, haga lo siguiente:

1. Abra las propiedades de la CPU S7-1500 en la ventana de inspección.

2. Abra la sección "Protección y seguridad" en la navegación local.

En la ventana de inspección aparece una tabla con los niveles de acceso posibles.



3. Active el nivel de acceso deseado en la primera columna de la tabla. Las marcas de

verificación verdes de las columnas de la derecha del respectivo nivel de acceso indican qué operaciones son posibles sin introducir la contraseña. En el ejemplo (figura: Niveles de acceso posibles), todavía es posible efectuar un acceso de lectura y un acceso a HMI sin

contraseña.

4. En la columna "Introducir contraseña", asigne una contraseña en la primera fila para el nivel de acceso "Acceso completo". Repita la contraseña elegida en la columna "Confirmar

contraseña" por si la ha introducido incorrectamente.

5. En caso necesario, asigne otras contraseñas a otros niveles de acceso.

6. Para que el nivel de acceso sea efectivo, cargue la configuración hardware.

La CPU registra las acciones siguientes con una entrada en el búfer de diagnóstico:

• entrada de la contraseña correcta o errónea;

• cambios en la configuración de los niveles de acceso.

Comportamiento de una CPU protegida por contraseña durante el funcionamiento

La protección de la CPU se hace efectiva para una conexión online una vez que los ajustes se han cargado en la CPU.

Antes de ejecutar una función online, STEP 7 comprueba los permisos y, si existe protección por contraseña, pide que se introduzca la contraseña. Las funciones protegidas por contraseña no pueden ser ejecutadas por más de una programadora o PC al mismo tiempo.

No se permite el acceso desde otra programadora o PC.

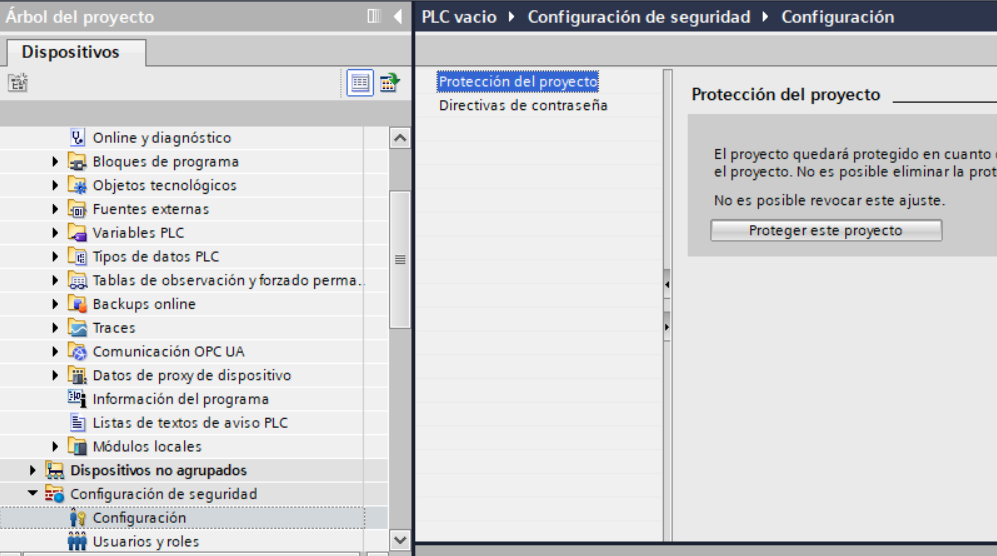
El permiso de acceso a los datos protegidos tiene validez mientras dure la conexión online o mientras STEP 7 esté abierto. Con el comando de menú "

Online > Borrar derechos de acceso" se suprime el permiso de acceso.

El acceso a una CPU protegida por contraseña en estado RUN puede limitarse localmente

desde el display. De este modo no es posible el acceso ni siquiera con contraseña.

**Proteger el proyecto**



**3- Protección de know-how**

Con la protección de know-how se protegen uno o varios bloques del tipo OB, FB, FC y

bloques de datos globales del programa contra accesos no autorizados. Para limitar el acceso a un bloque se introduce una contraseña. La contraseña ofrece una protección mayor contra lectura o modificación no autorizadas del bloque. La CPU no interviene en la protección de know-how (acceso offline en STEP 7).

**3.1 Datos legibles**: En un bloque con protección de know-how pueden leerse únicamente los datos siguientes sin indicar la contraseña correcta:

• Título del bloque, comentarios y propiedades del bloque

• Parámetros del bloque (INPUT, OUTPUT, IN, OUT, RETURN)

• Estructura de llamadas del programa

• Variables globales sin indicación del lugar de uso

**3.2 Otras acciones**

Otras acciones posibles con un bloque con protección de know-how:

• Copiar y borrar

• Llamar en un programa

• Comparación online/offline

• Cargar

**3.3 Bloques de datos globales y bloques de datos Array**

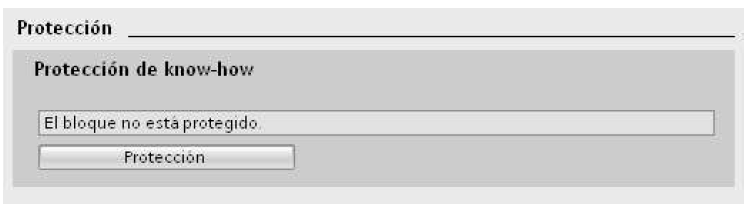
Los bloques de datos globales (DB globales) pueden dotarse de protección de know-how para impedir accesos no autorizados. Si no se dispone de la contraseña correcta puede leerse el bloque de datos global, pero no modificarse. Los bloques de datos Array (DB Array) no admiten la protección de know-how.

**3.4 Configurar la protección de know-how de bloques**

Para configurar una protección de know-how para bloques, proceda del siguiente modo:

1. Abra las propiedades del bloque correspondiente.

2. En "General", seleccione la opción "Protección".

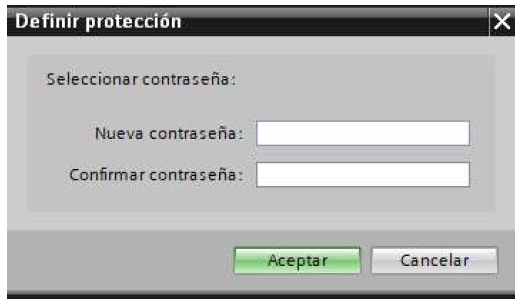


3. Para mostrar el cuadro de diálogo "Protección de know-how", haga clic en el botón

"Protección".



4. Para acceder al cuadro de diálogo "Definir contraseña", haga clic en el botón "Definir".



5. Introduzca la contraseña en el campo "Nueva contraseña". Repita la contraseña en el campo

"Confirmar contraseña".

6. Confirme haciendo clic en "Aceptar".

7. Cierre el cuadro de diálogo "Protección de know how" haciendo clic en "Aceptar".

Resultado: los bloques seleccionados se dotan de una protección de know-how. Los bloques

con protección de know-how están marcados con un candado en el árbol del proyecto. La

contraseña introducida es válida para todos los bloques seleccionados.

**3.5 Abrir bloques con protección de know-how**

Para abrir un bloque con protección de know-how, proceda del siguiente modo:

1. Para abrir el cuadro de diálogo "Protección de acceso", haga doble clic en el bloque.

2. Introduzca la contraseña para el bloque con protección de know-how.

3. Confirme las entradas realizadas con "Aceptar".

Resultado: se abre el bloque con protección de know-how.

Después de abrir el bloque, el código del programa y la interfaz del bloque se pueden editar hasta que se cierren el bloque o STEP 7. Cuando se vuelva a abrir el bloque, será necesario volver a introducir la contraseña. Si el cuadro de diálogo "Protección de acceso" se cierra con "Cancelar", el bloque se abre pero el código del bloque no se visualiza. Por consiguiente, el bloque no se puede editar.

Si el bloque se copia o se inserta en una librería, p. ej., la protección de know-how del bloque no se elimina. En ese caso, las copias también tendrán protección de know-how.

**3.6 Eliminar la protección de know-how de bloques**

Para quitar la protección de know-how de los bloques, proceda del siguiente modo:

1. Seleccione el bloque cuya protección de know-how desea quitar. El bloque protegido no

debe estar abierto en el editor de programación.

2. Para abrir el cuadro de diálogo "Protección de know-how", vaya al menú "Edición" y elija el comando "Protección de know-how".

3. Desactive la casilla de verificación "Ocultar código (protección de know-how)".



4. Introduzca la contraseña.



5. Confirme haciendo clic en "Aceptar".

Resultado: se ha suprimido la protección de know-how del bloque seleccionado.

**4- Protección contra copia**

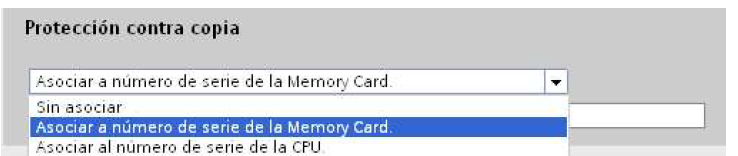
La protección contra copia permite proteger el programa contra una reproducción no autorizada. En la protección contra copia se vinculan los bloques a una SIMATIC Memory Card o CPU determinada. Al vincularlos con el número de serie, el bloque se utiliza únicamente en combinación con la SIMATIC Memory Card o CPU correspondiente.

Para configurar una protección contra copia, proceda del siguiente modo:

1. Abra las propiedades del bloque correspondiente.

2. En "General", seleccione la opción "Protección".

3. Seleccione la entrada "Asociar al número de serie de la CPU" o "Asociar a número de serie de la Memory Card" en el área "Protección contra copia" de la lista desplegable.



4. Active la opción "Número de serie insertado al cargar en un dispositivo o una Memory Card", si desea que STEP 7 inserte automáticamente el número de serie durante la carga (vinculación dinámica). Asigne una contraseña con el botón "Definir contraseña" para vincular el uso de un bloque adicionalmente a la introducción de una contraseña.

Si desea vincular el número de serie de la CPU o de la SIMATIC Memory Card manualmente a un bloque (vinculación estática), active la opción "Introducir número de serie".

5. A continuación, configure la protección de know-how para el bloque en el área "Protección de know-how".

Eliminar la protección contra copia

Para quitar la protección contra copia, proceda del siguiente modo:

1. Elimine la Protección de know-how (Página 228), si la hay.

2. Abra las propiedades del bloque correspondiente.

3. En "General", seleccione la opción "Protección".

4. En el área "Protección contra copia", seleccione la entrada "Sin asociar" de la lista

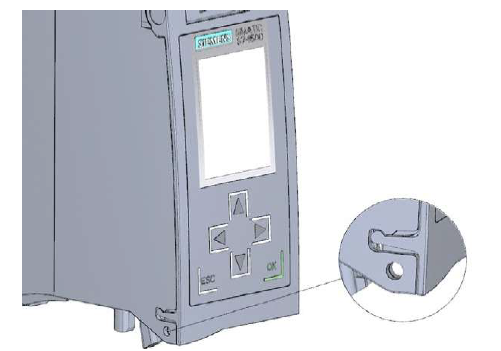
desplegable.

**5- Protección mediante bloqueo de la CPU o del módulo de interfaz**

La CPU/módulo de interfaz debe protegerse adicionalmente contra accesos no autorizados (p. ej., a la SIMATIC Memory Card) mediante una tapa frontal suficientemente segura. Existen, p. ej., las posibilidades siguientes:

• Poner un precinto

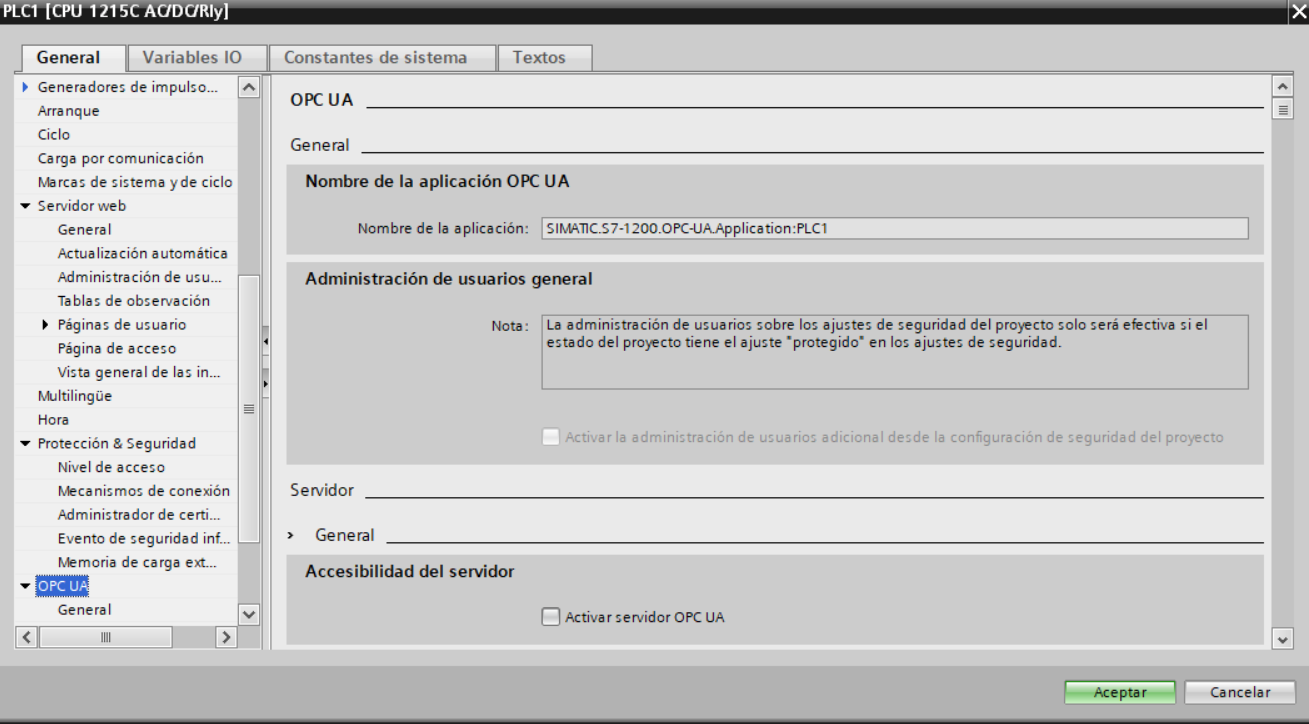
• Asegurar la tapa frontal con un candado (diámetro de estribo: 3 mm)



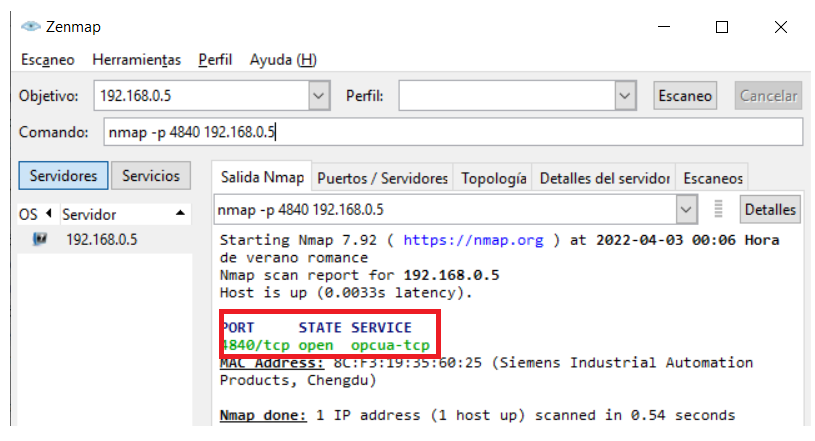
**6- Desactivación del servidor OPC UA**

Garantice accesos de escritura a través de OPC UA solo si los derechos de escritura son realmente necesarios con determinadas variables PLC y variables de bloques de datos.

• Si ha desactivado la opción "Accesible desde HMI/OPC UA" para todos los elementos de un bloque de datos, en el espacio de direcciones del servidor OPC UA de la CPU S7-1200 este bloque de datos dejará de estar visible para un cliente OPC UA.



Por defecto el servidor OPC viene desactivado. Al activar el servidor OPC UA estamos abriendo el puerto 4840



**7- Desactivación de la comunicación PUT/GET**

La CPU puede ser el servidor de una serie de servicios de comunicación. En este modo, otros dispositivos de comunicación pueden acceder a los datos de la CPU sin haber sido configurados o programados explícitamente para la CPU. De igual forma la UCP local no tiene la posibilidad de controlar la comunicación a los clientes.

Por defecto la comunicación PUT/GET viene desactivada.En este caso, el acceso de lectura y escritura a los datos de la CPU sólo es posible para aquellas conexiones de comunicación que requieren programación para la CPU local y para el interlocutor de comunicación.

Las comunicaciones, para las cuales la CPU local es solo servidor (es decir, que no hay configuración/ programación de la comunicación con el interlocutor de la comunicación), no son posibles en el funcionamiento de la CPU.

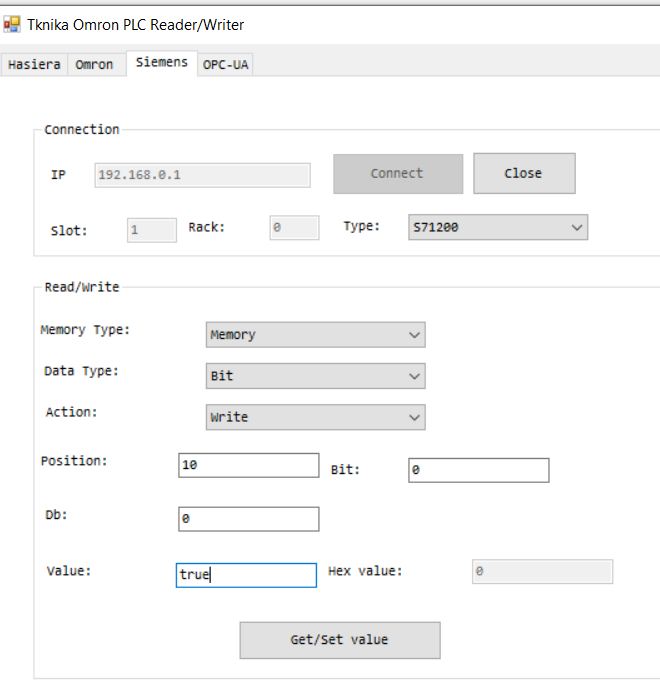
Esto incluye:

PUT/GET, FETCH/WRITE o acceso FTP a través de módulos de comunicación.

Acceso PUT/GET por parte de otras CPU S7.

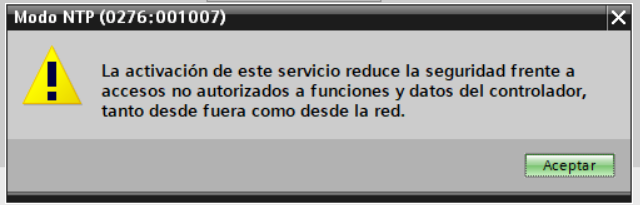
Acceso HMI a través de comunicación PUT/GET.

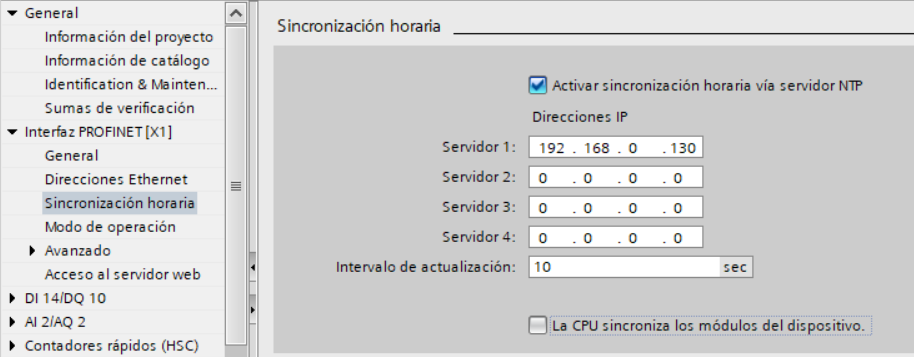
Si habilitamos PUT/GET estamos permitiendo la comunicación desde el exterior . Un usuario con acceso al PLC puede cargarle información o ejecutar un script contra él.



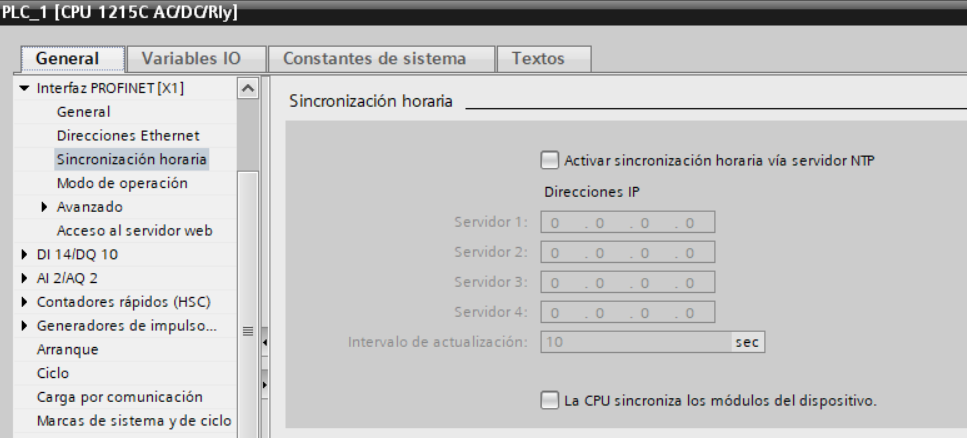
**8- Desactivación de la sincronización horaria a través del servidor NTP**

Para conseguir una buena eficiencia en los servicios y evitar complicaciones, la sincronización de todos los componentes de la red juega un papel notorio. Existen varios mecanismos de sincronización, siendo los tipos *Simple Network Time Protocol* (SNTP), *Network Time Protocol* (NTP) y *Precision Time Protocol* (PTP) los más comunes. El protocolo PTP es el más preciso, con una exactitud del orden de los nanosegundos, mientras que los protocolos SNTP y NTP tienen una precisión menor, del orden de los microsegundos, siendo suficientes para determinadas necesidades industriales y comerciales.





Si no es necesario no habilitar el servidor NTP



**9- Desactivación del servidor web.**

Con el servidor web puede controlar y monitorear remotamente la CPU a través de la Intranet de la empresa.Por lo tanto, las evaluaciones y los diagnósticos son posibles a grandes distancias.

Sin embargo, el riesgo de accesos no autorizados a la CPU puede aumentar al activar el servidor web.

Si desea activar el servidor web, le recomendamos las siguientes medidas:

• no conecte el servidor web de la CPU directamente a Internet proteger el acceso al servidor web mediante el uso de la red apropiada segmentación, DMZ y dispositivos de seguridad.

• proteger el acceso al servidor web mediante el uso de la red apropiada.

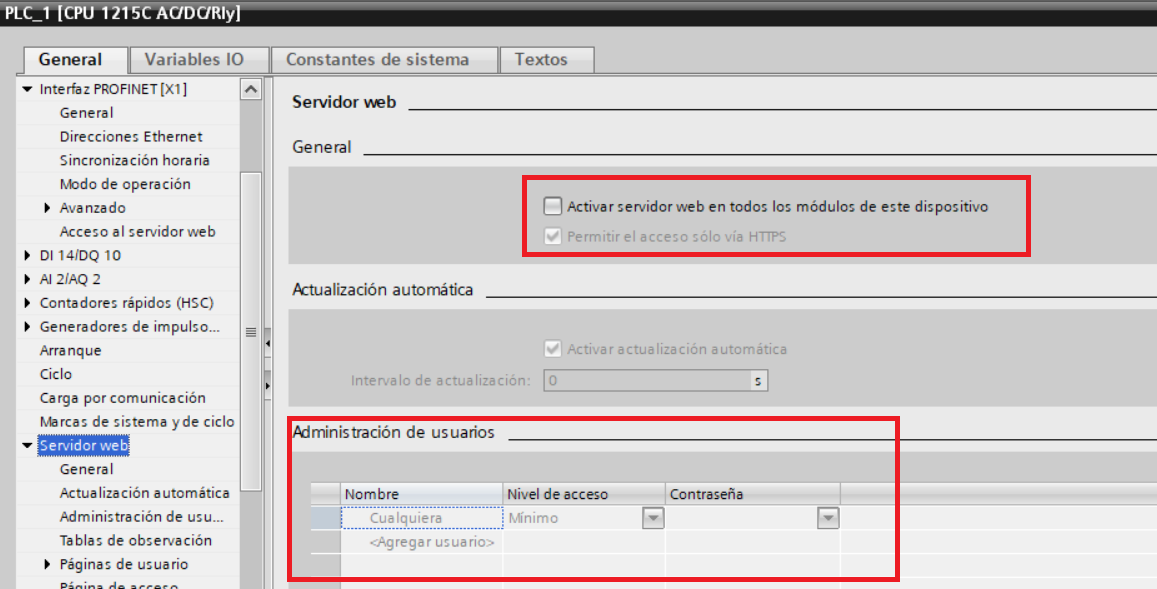
• acceder al servidor web a través del protocolo de transmisión.

• configurar los derechos de usuario y funciones a través de la lista de usuarios

* crear un usuario
* definir los derechos de ejecución
* asignar contraseñas.

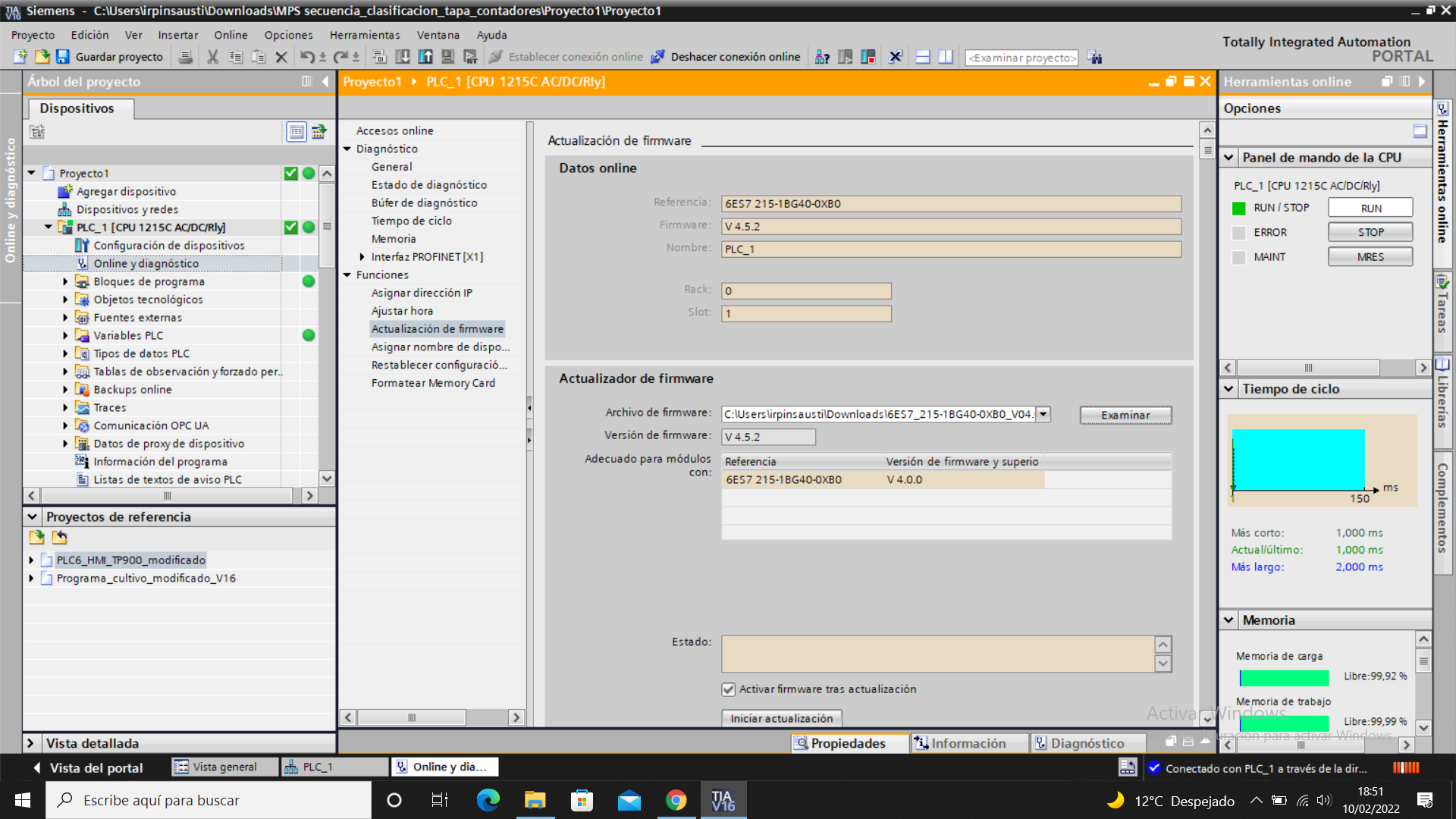
Los usuarios solo pueden realizar las funciones que se han establecido como parte de la configuración de administración de usuarios. Una vez que se ha configurado un usuario, puede iniciar sesión con su contraseña y acceder a los sitios web de acuerdo con sus derechos de acceso. De forma predeterminada, se ha establecido un usuario con el nombre "Todos". Este usuario tiene derechos de acceso mínimos (acceso de lectura a la introducción y la página de inicio). El usuario “Todos” se ha configurado sin contraseña y no se puede modificar.

Nota: En la configuración por defecto de los módulos, estas funciones están desactivadas.



**10 Actualizar Firmware**

Conetarse online y diagnóstico al PLC y actualizar con el fichero descargado. **Atención con la versión** que sea coincidente



Link de [descarga](https://support.industry.siemens.com/cs/document/109771672/versi%C3%B3n-de-firmware-v4-4-liberada-para-el-s7-1200?dti=0&lc=es-ES)  firmware