

Manual de Ciberseguridad

MT / cMTx

Interfaz hombre-máquina (IHM)



Manual de Ciberseguridad

MT / cMTx

Documento: 10014443649

Idioma: Español

Revisión: 00

Fecha de la Publicación: 03/2026

SUMARIO DE LAS REVISIONES

La información abajo describe las revisiones ocurridas en este manual.

Revisión	Descripción
R00	Primera edición.

1	INTRODUCCIÓN	1-1
1.1	SOBRE ESTE DOCUMENTO	1-1
1.2	AVISO IMPORTANTE SOBRE CIBERSEGURIDAD Y COMUNICACIONES	1-1
2	CONCEPTOS FUNDAMENTALES DE CIBERSEGURIDAD	2-1
2.1	VISIÓN GENERAL	2-1
2.2	MUCHO MÁS ALLÁ DE TI: LA NUEVA FRONTERA DE LA CIBERSEGURIDAD	2-1
2.3	DEFENSA EN PROFUNDIDAD	2-2
2.3.1	Entorno externo	2-2
2.3.1.1	Seguridad de planta	2-2
2.3.1.2	Seguridad del entorno de red	2-2
2.3.1.3	Seguridad de la integración de sistemas	2-2
2.3.2	Operación del producto	2-2
2.4	MANTENIMIENTO GENERAL DE SEGURIDAD	2-3
2.5	ANÁLISIS DE RIESGOS Y MECANISMO DE REPORTE	2-3
3	RIESGOS DURANTE LA EDICIÓN DE PROGRAMAS	3-1
3.1	VERIFICACIÓN DEL ARCHIVO DE INSTALACIÓN	3-1
3.1.1	Firma digital	3-1
3.1.2	Directorio de instalación	3-1
3.1.3	Actualización de versión de EasyBuilder Pro	3-2
3.2	CONFIGURACIONES DE SEGURIDAD DEL SOFTWARE	3-3
3.2.1	Habilitar comunicación segura	3-3
3.2.2	Usar el modo de seguridad mejorado	3-3
3.2.3	Usar contraseñas de usuario robustas	3-3
3.2.4	Protección de las configuraciones de contraseña	3-4
3.2.5	Habilitar cierre de sesión automático	3-5
3.2.6	Sincronización de hora mediante servidor NTP	3-5
3.2.7	Seguridad de objetos	3-6
3.2.8	Registro de operaciones	3-6
4	RIESGOS DURANTE LA OPERACIÓN DEL PRODUCTO	4-1
4.1	AUTORIZACIÓN DE INICIO DE SESIÓN	4-1
4.2	SEGURIDAD DE LOS ARCHIVOS DE REGISTRO	4-1
4.2.1	Prolongación de la vida útil de la memoria flash	4-1
4.2.1.1	Recomendaciones para reducir la velocidad de escritura	4-2
4.2.2	Guardar o respaldar los registros en un dispositivo externo	4-2
4.2.2.1	Recomendaciones para el uso de USB y SD	4-3
4.2.2.2	Recomendaciones para el uso de un servidor de bases de datos	4-3
4.2.3	Habilitar checksum para integridad de datos	4-3
5	RIESGOS DURANTE EL MANTENIMIENTO REMOTO	5-1
5.1	SEGURIDAD DE LA COMUNICACIÓN	5-1
5.1.1	Deshabilitar funciones innecesarias	5-1
5.1.2	Servidor Modbus	5-1
5.1.3	MQTT	5-2
5.1.4	Servidor OPC UA	5-3
5.1.5	Servidor de bases de datos	5-3
5.1.6	Correo electrónico	5-4
5.1.7	Monitoreo remoto con cMT Viewer	5-4
5.2	SEGURIDAD DE LA PÁGINA WEB	5-5
5.2.1	Habilitar cifrado HTTPS	5-5
5.2.2	Habilitar reglas de fortaleza de contraseña	5-5
5.2.3	Habilitar caducidad de contraseña	5-6
5.2.4	Bloqueo automático tras intentos de inicio de sesión	5-6

5.2.5	Cambiar la contraseña del sistema	5-7
5.3	ACTIVIDADES REGULARES DE MANTENIMIENTO DE SEGURIDAD	5-7
6	DIRECTRICES PARA LA ELIMINACIÓN SEGURA DEL PRODUCTO	6-1
6.1	RECOMENDACIONES PARA UNA ELIMINACIÓN SEGURA	6-1

1 INTRODUCCIÓN

1.1 SOBRE ESTE DOCUMENTO

WEG trata la ciberseguridad y la seguridad de la información con la máxima seriedad. Reconocemos la creciente necesidad de proteger a nuestros clientes y nuestras operaciones en un entorno cada vez más complejo. Operamos en sectores esenciales donde los ciberataques no son simples inconvenientes, ya que pueden impactar a comunidades enteras y poner vidas en riesgo.

Esta realidad nos impulsa a adoptar un enfoque integral de ciberseguridad, integrando la protección de nuestros productos y servicios con el fortalecimiento de alianzas con otros líderes del sector. El desarrollo y la evolución continua de nuestros productos están guiados por recomendaciones de normas reconocidas internacionalmente, con el fin de cumplir los niveles de protección exigidos por nuestros clientes y por los mercados en los que operan.

De esta manera, este manual tiene como objetivo proporcionar directrices prácticas para la configuración segura, la puesta en marcha y la operación de las IHMs a lo largo de todo su ciclo de vida, abarcando desde la fase inicial hasta la operación continua en campo. El contenido fue desarrollado con enfoque en la línea cMTx, considerando sus funcionalidades y capacidades específicas. Aun así, muchos de los conceptos y mecanismos aquí presentados pueden aplicarse, total o parcialmente, a las IHMs de la línea MT.

Se destaca que pueden existir diferencias en funcionalidades, recursos soportados y capacidades entre las líneas. Por lo tanto, corresponde al usuario evaluar la aplicabilidad de cada recomendación según el modelo específico de IHM utilizado y consultar la documentación técnica correspondiente para validar las características disponibles.

Consolida orientaciones prácticas y medidas de mitigación, con énfasis en la configuración segura de la IHM, la reducción de la superficie de ataque, el endurecimiento de los mecanismos de defensa y la gestión de riesgos cibernéticos a lo largo del ciclo de vida del equipo, contribuyendo a una operación resiliente alineada con las mejores prácticas de seguridad en sistemas de automatización industrial.



¡NOTA!

El texto de este manual fue traducido de la versión original en portugués mediante inteligencia artificial, con revisión técnica realizada por WEG.

1.2 AVISO IMPORTANTE SOBRE CIBERSEGURIDAD Y COMUNICACIONES

Las IHM de WEG, modelos cMTx, son capaces de conectarse e intercambiar información mediante redes y protocolos de comunicación. Aunque han sido diseñadas y probadas para garantizar el correcto funcionamiento con otros sistemas de automatización utilizando los protocolos mencionados en este manual, es esencial que el cliente comprenda las responsabilidades asociadas a la información y a la ciberseguridad al utilizar este equipo.

Por lo tanto, es responsabilidad exclusiva del cliente adoptar estrategias de defensa en profundidad e implementar políticas y medidas para garantizar la seguridad del sistema en su conjunto, incluidas las comunicaciones enviadas y recibidas por el equipo. Estas medidas incluyen, entre otras, la instalación de cortafuegos (firewalls), programas antivirus y antimalware, cifrado de datos, control de autenticación y control de acceso físico de los usuarios.

WEG y sus afiliadas no se responsabilizan por daños o pérdidas derivados de violaciones de ciberseguridad, incluyendo, pero no limitándose a, acceso no autorizado, intrusión, filtración y/o robo de datos o información, denegación de servicio o cualquier otra forma de violación de seguridad. El uso de este producto en condiciones para las cuales no fue específicamente diseñado no es recomendable y puede ocasionar daños al producto, a la red y al sistema de automatización.

En este sentido, es imprescindible que el cliente comprenda que intervenciones externas mediante programas de terceros, como *sniffers* o programas con acciones semejantes, tienen el potencial de ocasionar interrupciones o restricciones en la funcionalidad del equipo.

2 CONCEPTOS FUNDAMENTALES DE CIBERSEGURIDAD

2.1 VISIÓN GENERAL

En una era cada vez más digital e interconectada, las infraestructuras industriales dependen en gran medida de dispositivos de automatización integrados, como variadores de frecuencia, controladores lógicos programables (PLC), interfaz hombre-máquina (IHM), pasarelas industriales, etc. En este escenario, la ciberseguridad deja de ser opcional; es un requisito esencial para la operación segura, confiable y continua de los sistemas.

Con el avance constante de las amenazas cibernéticas, cada vez más sofisticadas y dirigidas—los enfoques tradicionales y puramente reactivos de seguridad se han vuelto insuficientes. A diario surgen nuevas técnicas de ataque, lo que exige que fabricantes, integradores y operadores industriales adopten medidas proactivas y resilientes para proteger sus activos.

Esta complejidad creciente está llevando a los gobiernos a establecer regulaciones que refuercen la resiliencia, es decir, la capacidad de recuperarse de un ataque, adaptarse a amenazas en constante cambio y mejorar los mecanismos de defensa, minimizando los impactos y preservando la continuidad operativa. Esto implica no solo implementar medidas de seguridad robustas, sino también anticipar y responder eficazmente a los incidentes. En este contexto, adoptar una estrategia sólida de ciberresiliencia ya no es una ventaja competitiva; es una necesidad crítica para los negocios y para la protección de las operaciones industriales y de misión crítica.

Diversas jurisdicciones en todo el mundo han desarrollado regulaciones enfocadas en la seguridad de sistemas industriales. En Estados Unidos, el conjunto de normas NERC-CIP establece requisitos rigurosos para la protección de sistemas de automatización en instalaciones críticas. En la Unión Europea, el recientemente aprobado *Cyber Resilience Act* (CRA) impone obligaciones directas a los fabricantes de productos digitales, incluido el equipamiento de automatización industrial.

Estas iniciativas se sustentan en normas y marcos de referencia reconocidos internacionalmente, como la serie ISA/IEC 62443, el marco del NIST, la familia ISO/IEC 27000, así como directrices específicas como la IEC 62351, enfocada en la seguridad de los protocolos de automatización. Adoptar estas referencias ayuda a mitigar riesgos materiales, fortalecer la seguridad de los dispositivos de automatización y garantizar la resiliencia de las operaciones industriales frente a amenazas complejas, salvaguardando la continuidad de servicios esenciales y la integridad de los datos y sistemas involucrados.

2.2 MUCHO MÁS ALLÁ DE TI: LA NUEVA FRONTERA DE LA CIBERSEGURIDAD

Tradicionalmente, el término ciberseguridad se refiere al conjunto de medidas adoptadas para proteger sistemas informáticos y redes contra accesos no autorizados o ataques maliciosos. Sin embargo, cuando se aplica al contexto de tecnologías de automatización y energía, este concepto se amplía significativamente. En este escenario, la ciberseguridad abarca prácticas destinadas a garantizar la fiabilidad, la integridad y la disponibilidad de los sistemas de control y automatización, principios ampliamente conocidos en el ámbito de las tecnologías de la información (TI) por el acrónimo “CIA” (Confidentiality, Integrity, Availability).

En entornos industriales, estas medidas son esenciales para prevenir una serie de riesgos, como la filtración de información sensible, daños físicos a equipos o sistemas, corrupción de datos e interrupciones operativas. Tales incidentes pueden comprometer no solo la eficiencia, sino también la seguridad de procesos críticos.

En TI, la prioridad suele ser la confidencialidad de los datos, seguida de la integridad y, por último, la disponibilidad. En la Tecnología Operacional (TO), este orden se invierte: la disponibilidad es el factor más importante, seguida de la integridad y la confidencialidad, formando el acrónimo “DIC”. Esto se debe a que, en entornos industriales, mantener los sistemas funcionando de forma continua y segura es más crítico que proteger la información contra accesos indebidos.

2.3 DEFENSA EN PROFUNDIDAD

El concepto de defensa en profundidad implica mucho más que confiar en una única medida de seguridad. Consiste en implementar mecanismos de seguridad en múltiples niveles para proporcionar una protección robusta. Este enfoque reduce significativamente los riesgos potenciales, como la filtración de información y los ataques de hackers, mejorando la seguridad general de los productos durante la instalación, operación, mantenimiento y disposición final.

2.3.1 Entorno externo

La IHM debe instalarse y operarse en entornos industriales con infraestructura de red segura para evitar accesos no autorizados. Para asegurar un rendimiento óptimo y minimizar los riesgos de seguridad, siga las recomendaciones a continuación. La estructura de seguridad externa consta de tres capas principales:

- Seguridad de planta
- Seguridad del entorno de red
- Seguridad de la integración de sistemas

2.3.1.1 Seguridad de planta

Garantice el uso seguro de la IHM mediante verificaciones integrales del sistema.

- Instalar perímetros controlados con control de acceso en instalaciones industriales.
- Implementar control de acceso biométrico o sistemas de bloqueo en laboratorios o salas de servidores.
- Utilizar sistemas de alarma o videovigilancia.

2.3.1.2 Seguridad del entorno de red

Un entorno de red seguro es una configuración controlada en la que el acceso se limita a dispositivos, usuarios y servicios autorizados, previniendo accesos no autorizados, fugas de datos y ataques maliciosos.

El producto está diseñado para utilizarse dentro de redes internas protegidas. Evite exponerlo directamente a redes públicas.

Si se requiere conectividad externa, implemente las siguientes medidas de seguridad, que ayudan a separar el tráfico de comunicación interno del externo.

- Monitorizar la comunicación entre redes de oficina y planta utilizando cortafuegos (firewalls).
- Utilizar routers para evitar el acceso directo mediante IP pública.
- Si el producto dispone de dos puertos Ethernet, conecte:
 - LAN 1 a la red externa
 - LAN 2 a los dispositivos internos

2.3.1.3 Seguridad de la integración de sistemas

Asegure que los mecanismos internos de protección se mantengan eficaces durante la integración del sistema.

- Mantener los sistemas actualizados regularmente
- Utilizar antivirus
- Implementar autenticación de usuarios

2.3.2 Operación del producto

La configuración del sistema IHM suele estar gestionada por el personal responsable de la creación de archivos y la integración del sistema. Durante la operación por parte de los usuarios, es esencial impedir cambios no autorizados en parámetros que puedan interrumpir el funcionamiento normal.

Medidas recomendadas:

- Ocultar la configuración del sistema
- Cambiar las contraseñas predeterminadas de inicio de sesión
- Utilizar comunicación HTTPS cifrada en la página de configuración web

La IHM incluye funciones de seguridad integradas habilitadas por defecto, que pueden configurarse según sea necesario para satisfacer los requisitos de la instalación. Esta configuración debe ser realizada únicamente por personal cualificado, ya que cambios incorrectos pueden comprometer la seguridad del sistema y de la red.

2.4 MANTENIMIENTO GENERAL DE SEGURIDAD

Esta sección proporciona directrices y recomendaciones para garantizar la seguridad del producto. Ayuda a los usuarios a planificar y llevar a cabo de manera eficaz las tareas rutinarias de mantenimiento de la seguridad de la información.

- Actualice el producto regularmente para asegurar que tanto el software como el firmware estén siempre al día. Esto incluye aplicaciones, sistemas operativos y otros componentes. Esta práctica evita la explotación de vulnerabilidades conocidas e introduce nuevas funciones de seguridad.
- Realice pruebas rutinarias de vulnerabilidades de seguridad, como escaneos de vulnerabilidades y pruebas de penetración. Este enfoque ayuda a identificar y remediar posibles debilidades.
- Utilice las capacidades de monitoreo del producto para supervisar su operación, identificar comportamientos anómalos y rastrear eventos de seguridad. Además, mantenga registros de todos los eventos de seguridad para su análisis e investigación posterior.
- Emplee mecanismos de cifrado adecuados para el tratamiento de datos sensibles y comunicaciones. Esto garantiza la confidencialidad e integridad de los datos durante la transmisión y el almacenamiento.
- Elabore planes de contingencia para responder eficazmente a posibles eventos de seguridad y ejecutar rápidamente medidas de respuesta. En paralelo, establezca un proceso de gestión de vulnerabilidades para evaluar, realizar seguimiento y remediar vulnerabilidades periódicamente.
- Si este producto permite el acceso a proveedores de servicios externos, asegúrese de que sigan los mismos estándares de seguridad y evalúe regularmente su postura de seguridad. Consulte normas internacionales para la gestión de proveedores externos (por ejemplo, ISO 28000 / ISO 27001).

2.5 ANÁLISIS DE RIESGOS Y MECANISMO DE REPORTE

Al utilizar el producto, si surgen riesgos relacionados con la seguridad, siga el procedimiento a continuación:

- Realizar análisis de riesgos.
- Consultar el manual de seguridad del producto.
- Evaluar la eficacia de las medidas de mitigación.
- Si no es posible resolver el problema, ponerse en contacto con los canales de soporte de la empresa.

3 RIESGOS DURANTE LA EDICIÓN DE PROGRAMAS

3.1 VERIFICACIÓN DEL ARCHIVO DE INSTALACIÓN

3.1.1 Firma digital

Antes de instalar EasyBuilder Pro, verifique que el archivo de instalación (setup.exe) tenga una firma digital válida y que no haya sido manipulado. Haga clic con el botón derecho en el instalador, abra la pestaña *Digital Signatures* y seleccione *Details* para confirmar la integridad de la firma digital. La [Figura 3.1](#) muestra las propiedades del instalador y los detalles de la firma digital.

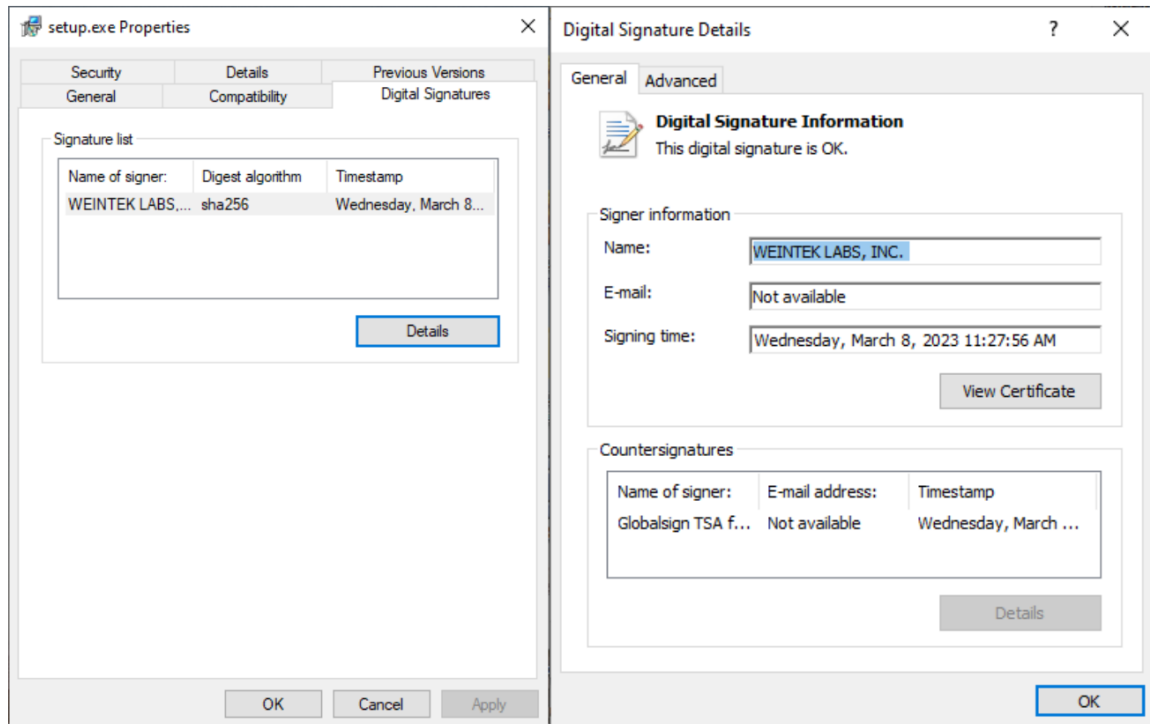


Figura 3.1: Firma digital del instalador.

3.1.2 Directorio de instalación

Instale EasyBuilder Pro en una carpeta con permisos de acceso restringidos (por ejemplo, C:\Program Files (x86)), como se muestra en [Figura 3.2](#).

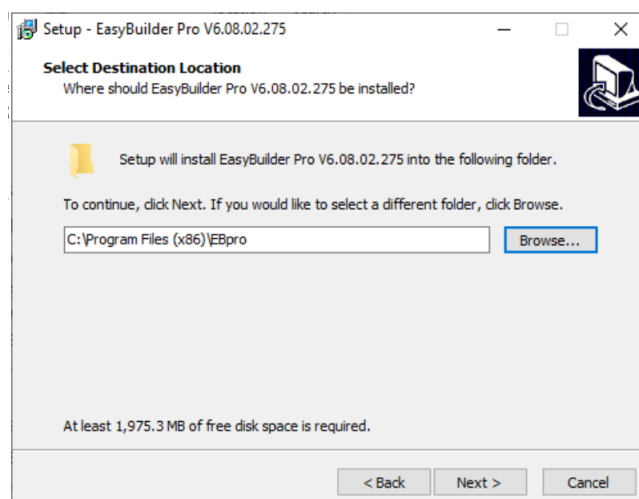


Figura 3.2: Directorio de instalación.

3.1.3 Actualización de versión de EasyBuilder Pro

Asegúrese de que el software esté actualizado a las versiones más recientes que corrigen vulnerabilidades de seguridad. Para comprobar su versión actual y buscar nuevas actualizaciones, abra EasyBuilder Pro y haga clic en *File* → *About* → *Check for updates...*, como se muestra en [Figura 3.3](#).

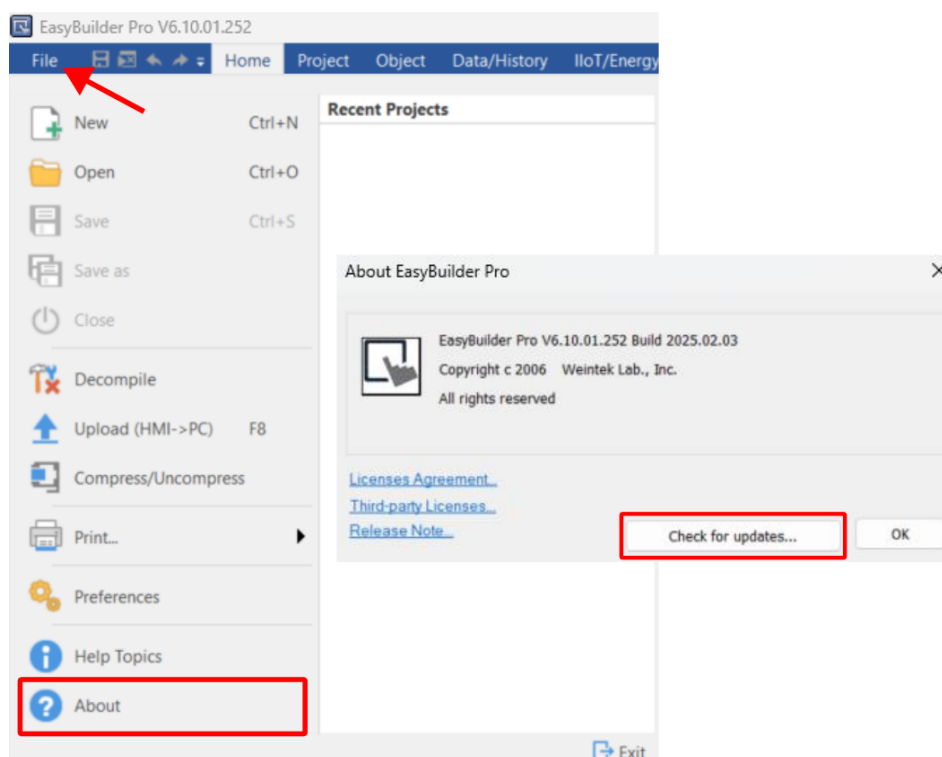


Figura 3.3: Comprobación de la versión actual y de actualizaciones disponibles de EasyBuilder Pro.

Se puede habilitar notificaciones para ser informado automáticamente sobre nuevas actualizaciones al iniciar el programa. Para ello, haga clic en *File* → *Preferences* → *Misc* y active *Notify when new version of EasyBuilder Pro is available*, como se muestra en la [Figura 3.4](#).

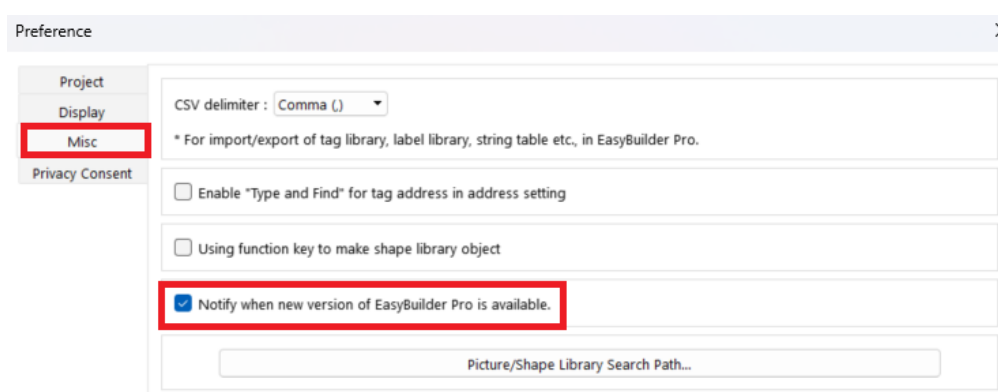


Figura 3.4: Notificar cuando haya una nueva versión de EasyBuilder Pro disponible.

3.2 CONFIGURACIONES DE SEGURIDAD DEL SOFTWARE

3.2.1 Habilitar comunicación segura

Active la comunicación segura para garantizar que la comunicación entre la IHM y otros dispositivos esté cifrada. En un proyecto abierto en EasyBuilder Pro, haga clic en *Home* → *System Parameters*, abra la pestaña *Devices*, seleccione la IHM, haga clic en *Settings/Security* y habilite *Enable secure communication*, como se muestra en Figura 3.5.

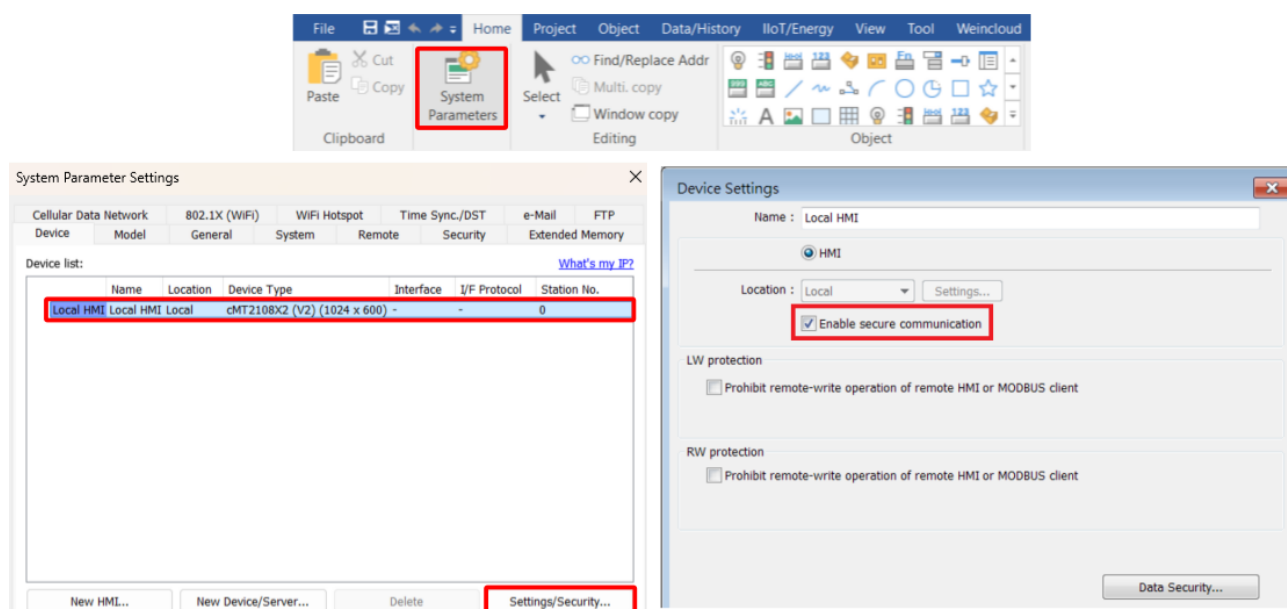


Figura 3.5: Habilitar comunicación segura.

3.2.2 Usar el modo de seguridad mejorado

Se recomienda el modo de seguridad mejorado para que los diseñadores puedan asignar distintos privilegios a diferentes usuarios y controlar el acceso a los objetos. En EasyBuilder Pro, haga clic en *Home* → *System Parameters*, abra la pestaña *Security* y habilite *Enhanced security mode*, como se muestra en la Figura 3.6. Para configuraciones detalladas, consulte el capítulo *User Password and Object Security* del manual de EasyBuilder Pro.

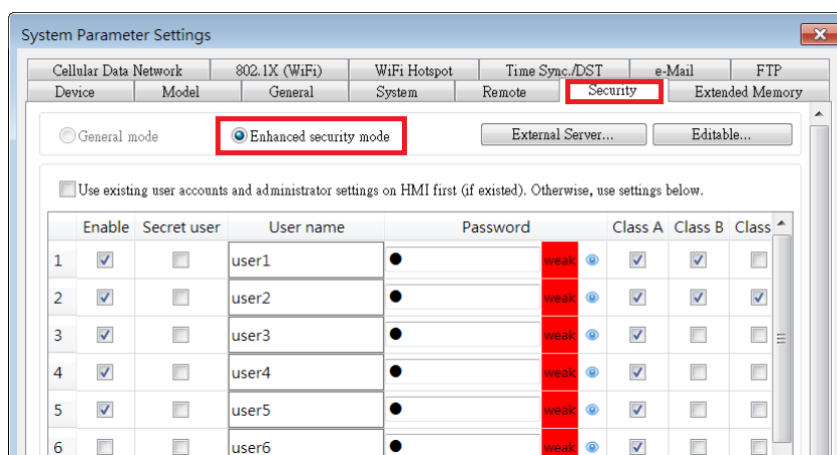


Figura 3.6: Habilitar el modo de seguridad mejorado.

3.2.3 Usar contraseñas de usuario robustas

Las contraseñas robustas son menos vulnerables a intentos de ruptura por actores maliciosos. La robustez de una contraseña está relacionada con la cantidad y la diversidad de caracteres utilizados. Entre los tipos de

RIESGOS DURANTE LA EDICIÓN DE PROGRAMAS

caracteres que pueden emplearse se encuentran:

- Letras mayúsculas
- Letras minúsculas
- Números
- Caracteres especiales

Clasificación de la fortaleza de la contraseña:

- **Fuerte**: tres o más tipos de caracteres y longitud igual o superior a 8 caracteres.
- **Media**: al menos dos tipos de caracteres y longitud igual o superior a 6 caracteres.
- **Débil**: solo un tipo de carácter o longitud inferior a 6 caracteres.

La [Figura 3.7](#) muestra la clasificación de fortaleza de algunos ejemplos de contraseñas.

	Enable	Secret user	User name	Password		Class A	Class B
1	☒	☐	user1	5A@C4@6B5	strong	☒	☒
2	☒	☐	user2	5AC46B	medium	☒	☒
3	☒	☐	user3	3	weak	☒	☐

Figura 3.7: Ejemplos de clasificación de fortaleza de contraseñas.

Directrices para crear contraseñas robustas:

- Utilizar al menos ocho caracteres
- Combinar letras mayúsculas, minúsculas, números y caracteres especiales
- Evitar palabras de diccionario
- Evitar secuencias de teclado como 123456 o asdfg
- Evitar caracteres repetidos como AAAA
- Evitar secuencias alfabéticas como ABCD

3.2.4 Protección de las configuraciones de contraseña

Habilitar el modo *Read-only* evita que usuarios no autorizados modifiquen las configuraciones de seguridad al obtener el archivo original del proyecto. En este modo:

- No se pueden cambiar las configuraciones de seguridad
- Las contraseñas se muestran en forma enmascarada
- El acceso administrativo requiere la contraseña original

Para habilitarlo, abra la pestaña *Security*, haga clic en *Editable* y configure las opciones de *Read-only Settings*, como se muestra en la [Figura 3.8](#).

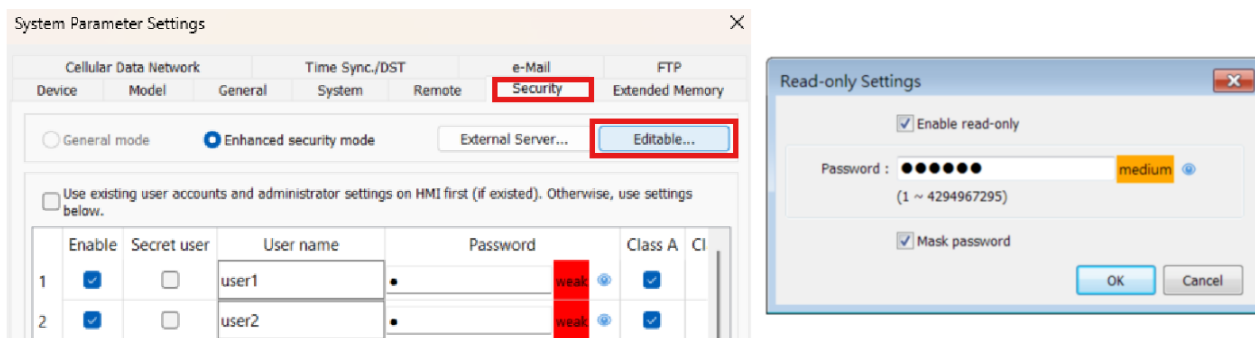


Figura 3.8: Habilitación del modo de solo lectura.

3.2.5 Habilitar cierre de sesión automático

Para evitar accesos no autorizados mediante sesiones abiertas, se recomienda habilitar el cierre de sesión automático en IHM inactivas. En el EasyBuilder Pro, haga clic en *Home* → *System Parameters* → *System* y active *Auto logout*. La [Figura 3.9](#) muestra la pantalla para habilitar el cierre de sesión automático.

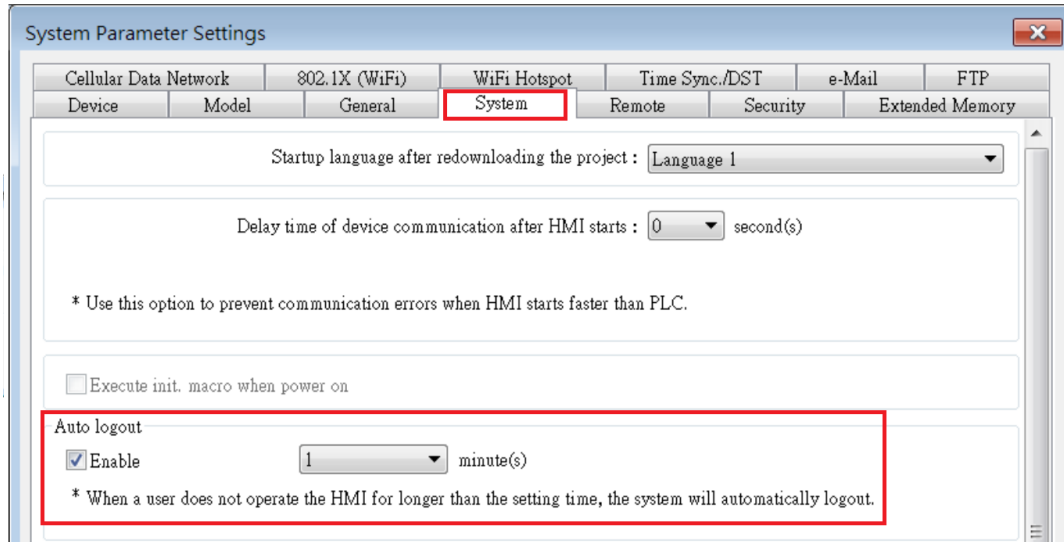


Figura 3.9: Habilitar cierre de sesión automático.

3.2.6 Sincronización de hora mediante servidor NTP

Para mantener registros y logs correctos, se recomienda sincronizar regularmente el reloj de la IHM con un servidor NTP. En EasyBuilder Pro, haga clic en *Home* → *System Parameters* → *Time Sync/DST* y habilite *Enable time synchronization via NTP server*, como se indica en la [Figura 3.10](#).

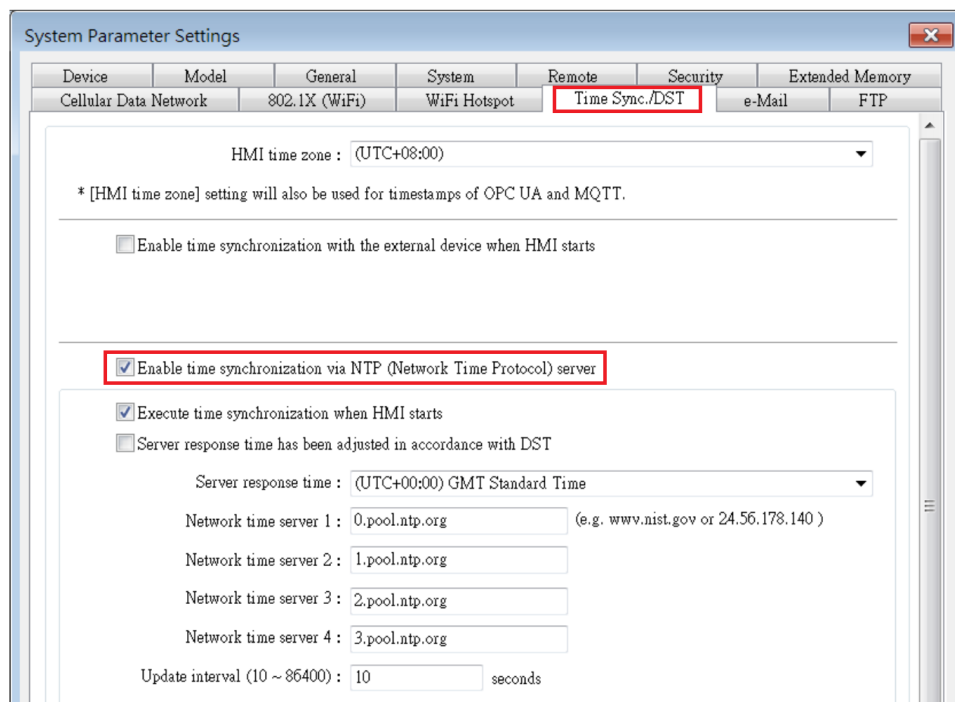


Figura 3.10: Sincronización de fecha y hora.

3.2.7 Seguridad de objetos

El elemento operativo básico de una IHM es el objeto. Se recomienda habilitar el control de seguridad para cada objeto operable, permitiendo la confirmación antes de ejecutar comandos y la restricción según permisos de usuario. Para configurarlo, cree un nuevo objeto o abra las propiedades del objeto haciendo doble clic sobre él, y luego acceda a la pestaña *Security*. La [Figura 3.11](#) muestra la pantalla para configurar la seguridad de los objetos.

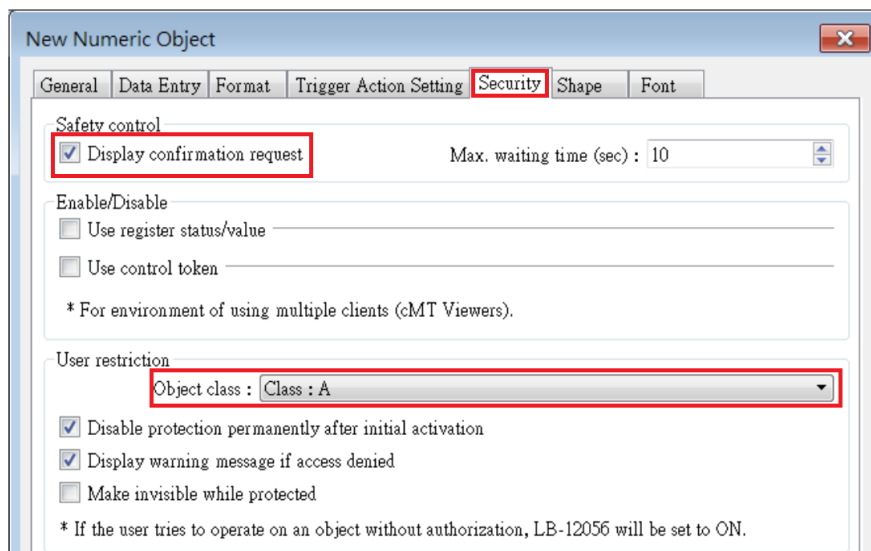


Figura 3.11: Configuración de la seguridad de objetos.

3.2.8 Registro de operaciones

Siempre que se realice una operación sobre objetos de la IHM, el *Operation Log* puede registrar información como:

- Fecha y hora
- Nombre de usuario
- Clase del objeto
- Número de ventana
- Nombre del objeto
- Comentarios definidos por el usuario
- Tipo de acción realizada
- Dirección de memoria
- Cambios efectuados

Por defecto, los registros se almacenan en la memoria de la IHM en formato de base de datos SQLite y también pueden copiarse a dispositivos externos como unidades USB. Para habilitar el registro, haga clic en *Data/History* → *Operation Log Settings* y configure los objetos cuyas operaciones serán registradas, como se muestra en la [Figura 3.12](#).



¡NOTA!

Utilice la función *Object Filter* para definir que objetos deben mostrarse.



¡ATENCIÓN!

Se recomienda precaución al configurar esta página, ya que configuraciones incorrectas pueden causar pérdida de datos. También es aconsejable sincronizar los registros con dispositivos externos si el espacio de la IHM es insuficiente.

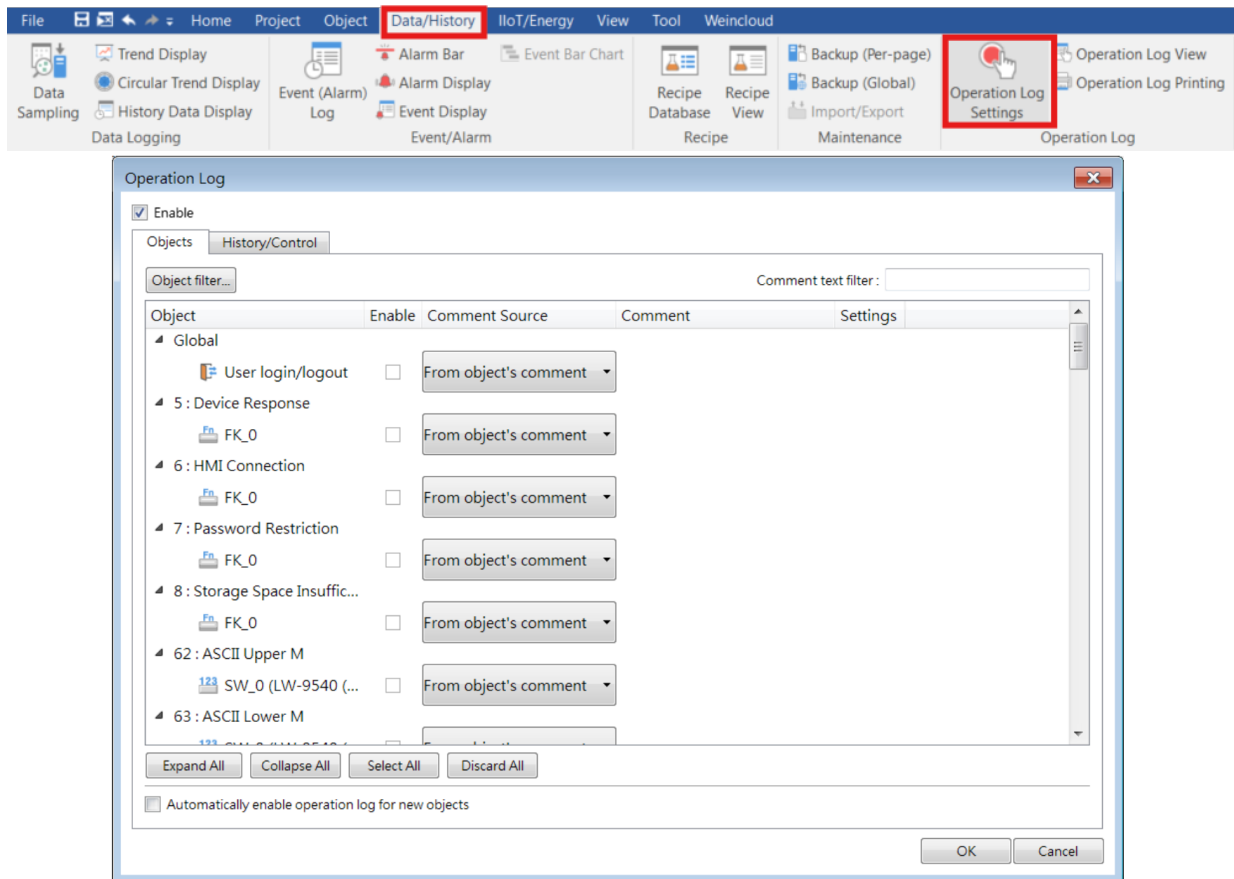


Figura 3.12: Configuración de registros de operaciones.

4 RIESGOS DURANTE LA OPERACIÓN DEL PRODUCTO

4.1 AUTORIZACIÓN DE INICIO DE SESIÓN

Para acceder a la página de configuración web de la IHM de la serie cMTx, abra un navegador (como Edge, Chrome o Firefox) e introduzca la dirección IP del dispositivo. Si la interfaz WebView aparece tras introducir la IP, utilice la dirección: https://<ihm_ip>/admin para acceder a la página de inicio de sesión de parámetros del sistema EasyWeb 2.0.

La autorización dentro del sistema se divide en tres niveles:

- **Admin:** posee el nivel más alto de autorización y puede modificar todos los ajustes.
- **Update:** posee permisos limitados para cambiar configuraciones.
- **History:** posee permisos para acceder a los datos de registro (logs) y a sus copias de seguridad.



NOTA DE CIBERSEGURIDAD!

Se recomienda configurar contraseñas distintas para administradores y operadores, a fin de evitar que cuentas de operador obtengan privilegios administrativos.

Por motivos de seguridad, se requiere confirmación de contraseña antes de acceder a las configuraciones. Además, el acceso a la sección *History* también requiere autenticación de contraseña, permitiendo visualizar los registros almacenados. La [Figura 4.1](#) muestra la página de inicio de sesión del sistema.

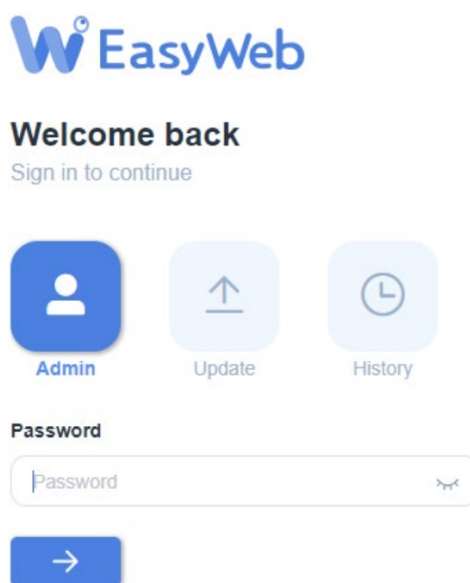


Figura 4.1: Autorización de inicio de sesión en el sistema.

4.2 SEGURIDAD DE LOS ARCHIVOS DE REGISTRO

La seguridad de los archivos de registro generados por *Data Sampling*, *Event Log* y *Operation Log* puede mejorarse utilizando las medidas descritas en las siguientes secciones.

4.2.1 Prolongación de la vida útil de la memoria flash

Debido al número limitado de ciclos de escritura de la memoria flash interna de la IHM, las escrituras frecuentes o un gran volumen de datos pueden reducir la vida útil de la memoria. Esto puede resultar en:

- Datos ilegibles
- Fallo de inicialización de la IHM

Se recomienda mantener la velocidad media de escritura en la memoria flash por debajo de 1200 KB/min. Esta información puede consultarse en los ajustes del sistema de la IHM, como se indica en la [Figura 4.2](#).

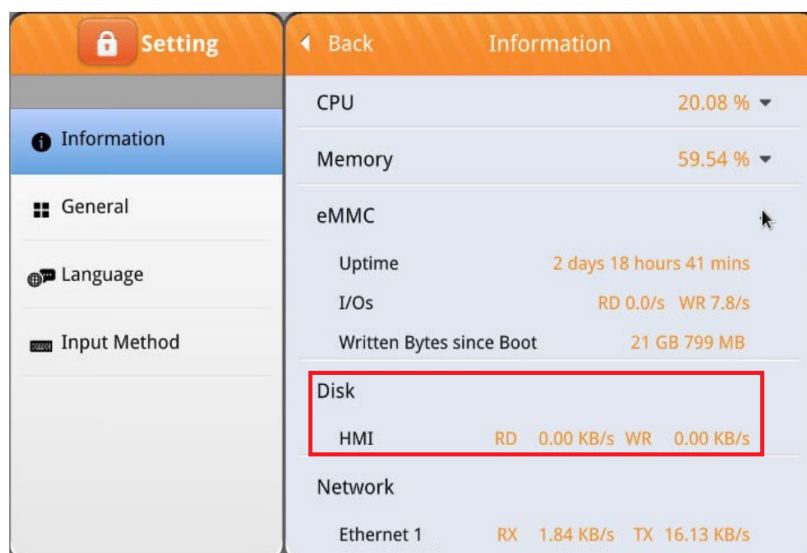


Figura 4.2: Velocidad media de escritura en la memoria flash.

4.2.1.1 Recomendaciones para reducir la velocidad de escritura

Data Sampling

- Si los registros no son necesarios, deshabilite la opción de guardar registros.
- Configure intervalos de muestreo más largos.
- Reduzca la frecuencia de envío de comandos síncronos a direcciones de control.
- Si utiliza tratamiento personalizado de archivos, reduzca la frecuencia de intercambio de archivos.
- Si utiliza sincronización automática periódica, aumente el intervalo de sincronización.

Event Log

- Si los registros no son necesarios, deshabilite el almacenamiento de registros.
- Si no se utiliza para alarmas, evite habilitar la opción *Save to history*.
- Reduzca la frecuencia de envío de comandos síncronos.
- Utilice el modo *Aggregate* para limitar la frecuencia de escritura en la memoria flash.

Operation Log

- Reduzca la frecuencia de envío de comandos síncronos a direcciones de control.
- Utilice el modo *Aggregate* para limitar la frecuencia de escritura.



¡NOTA!

Antes de apagar la IHM, establezca el registro del sistema **LB-9034** en ON para garantizar que los registros se escriban completamente en la memoria flash.

4.2.2 Guardar o respaldar los registros en un dispositivo externo

Se recomienda guardar o respaldar los registros en dispositivos externos, tales como:

- Unidades USB
- Tarjetas SD
- Servidores de bases de datos

Esto ayuda a evitar la pérdida de datos cuando el espacio de almacenamiento de la IHM sea insuficiente. La [Figura 4.3](#) muestra las opciones de almacenamiento disponibles para los registros y la copia de seguridad global de la IHM.

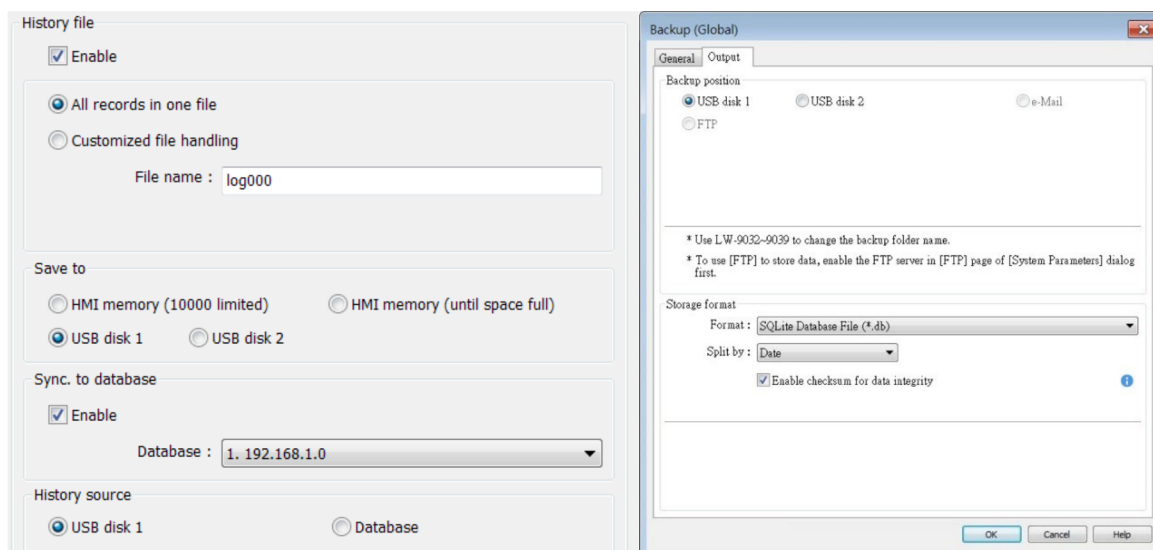


Figura 4.3: Ejemplo de copia de seguridad de registros.

4.2.2.1 Recomendaciones para el uso de USB y SD

Los dispositivos USB y las tarjetas SD también tienen límites de ciclos de escritura.

- Utilice dispositivos de mayor capacidad (por ejemplo, 32 GB).
- Realice copias de seguridad remotas periódicas (por ejemplo, anualmente).

4.2.2.2 Recomendaciones para el uso de un servidor de bases de datos

- Habilitar RAID.
- Realizar copias de seguridad remotas periódicas.

4.2.3 Habilitar checksum para integridad de datos

La herramienta *EasyConverter* permite abrir archivos SQLite en un ordenador y visualizar datos de copia de seguridad, además de exportarlos a formatos Excel o CSV. Si los archivos de copia de seguridad contienen *checksums*, EasyConverter puede verificar la integridad de los datos. Para habilitar esta función, marque *Enable checksum for data integrity* al generar archivos de copia de seguridad, como se indica en la Figura 4.4. Esta función solo es compatible con las series cMTx.

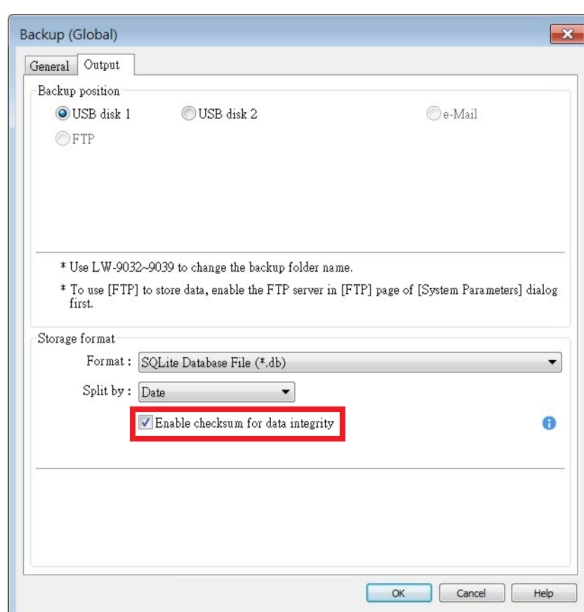


Figura 4.4: Configuración de checksum para archivos de copia de seguridad.

EasyConverter también puede verificar la integridad de los archivos de copia de seguridad. Si se detecta alguna modificación no autorizada durante la verificación, se mostrará una alerta.

5 RIESGOS DURANTE EL MANTENIMIENTO REMOTO

5.1 SEGURIDAD DE LA COMUNICACIÓN

5.1.1 Deshabilitar funciones innecesarias

Al utilizar una IHM, se recomienda deshabilitar las funciones que no se estén usando, o al menos protegerlas con contraseña. Entre las funciones que pueden deshabilitarse se incluyen:

- Remote IHM
- PLC Control (change page)
- Modbus Server
- VNC Server
- cMT Diagnoser (Series cMTx)
- OPC UA Server (en algunos modelos cMTx)

Las funciones de acceso remoto de la IHM—servidor VNC y cMT Diagnoser, pueden habilitarse y deshabilitarse en *System Parameter* → *Remote*, como se muestra en la [Figura 5.1](#).

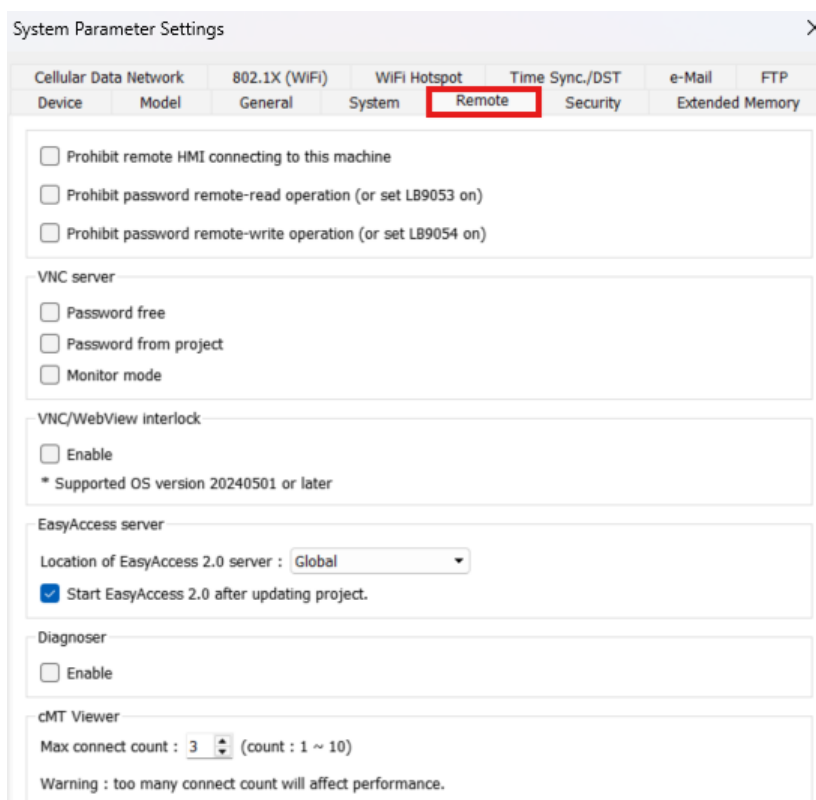


Figura 5.1: Opciones de acceso remoto de la IHM.

5.1.2 Servidor Modbus

Cuando se utilice un servidor Modbus en un proyecto IHM, abra el *System Parameters* → *Device* → *Settings/Security*. Habilite las opciones *LW Protection* y *RW Protection*, como se muestra en la [Figura 5.2](#). Esto evita cambios no intencionados en los registros del sistema durante la comunicación entre la IHM y clientes Modbus.



¡NOTA!

Para configurar el intervalo protegido de LW o RW, consulte el intervalo admitido por los parámetros del sistema.

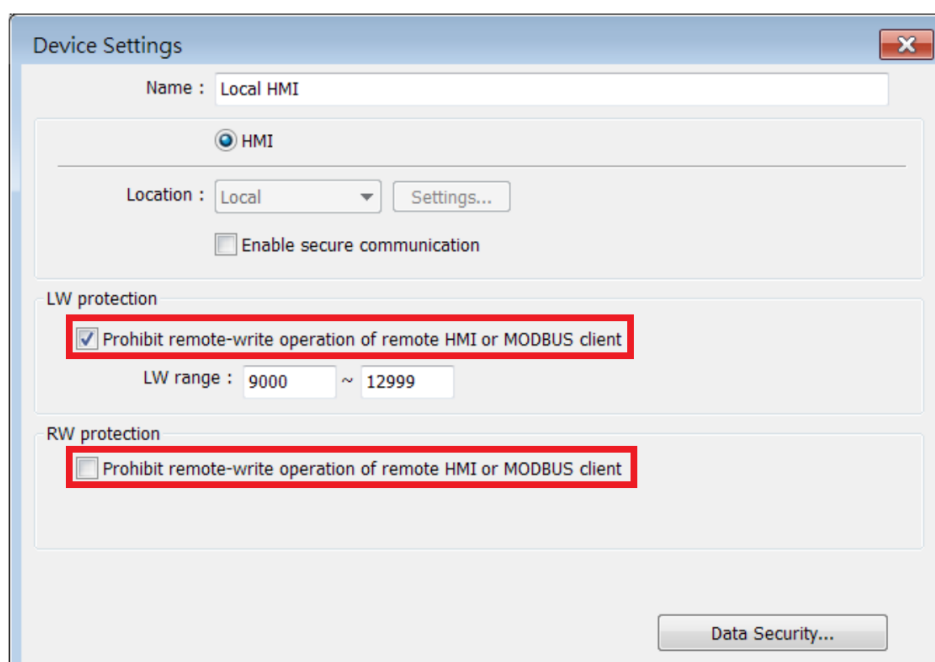


Figura 5.2: Configuración de protección LW para comunicación Modbus.

5.1.3 MQTT

Cuando se utiliza MQTT en un proyecto IHM, se recomienda emplear el cifrado TLS 1.2. También es necesario importar:

- Certificado de la Autoridad Certificadora (CA)
- Certificado del cliente
- Clave privada

En la configuración del objeto MQTT Server, habilite el cifrado y la verificación en la pestaña *TLS/SSL*, como se indica en la Figura 5.3.

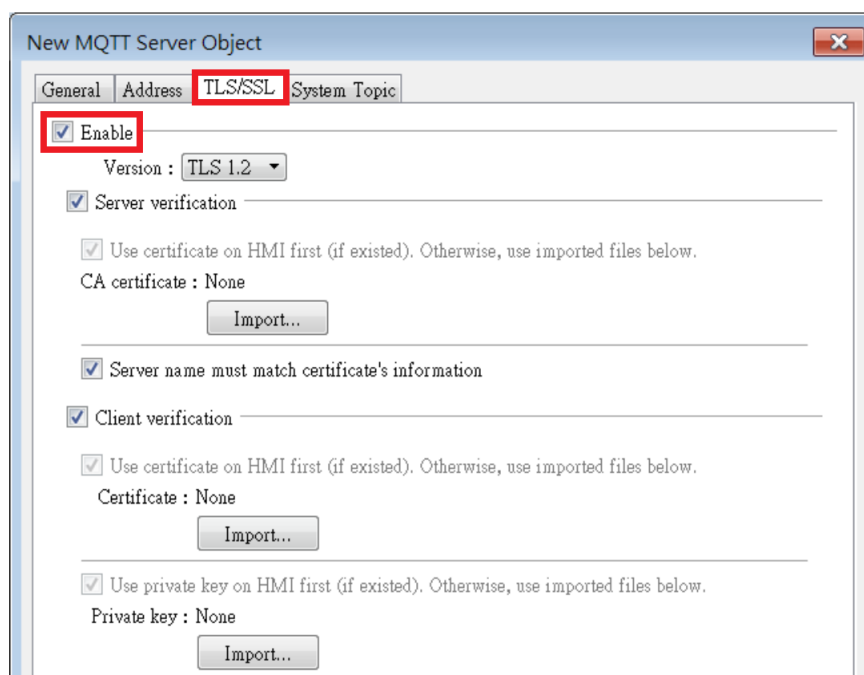


Figura 5.3: Configuración de cifrado TLS/SSL para MQTT.

5.1.4 Servidor OPC UA

Si se utiliza un servidor OPC UA en el proyecto de la IHM, se recomienda deshabilitar la comunicación en texto plano y utilizar solo comunicación cifrada. En la pestaña *General* de la configuración del servidor OPC UA, *deshabilite* la opción *None* en la política de seguridad, como se muestra en la [Figura 5.4](#). Esto garantiza que los clientes se comuniquen solo con datos cifrados.

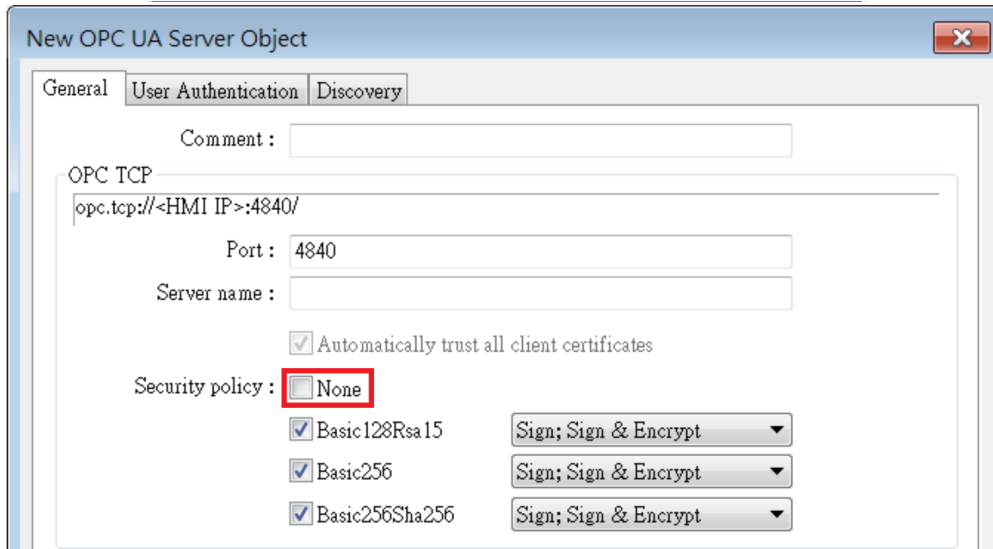


Figura 5.4: Configuración de la política de seguridad del servidor OPC UA.



NOTA DE CIBERSEGURIDAD!

Las políticas de seguridad Basic128Rsa15 y Basic256 ya no se consideran seguras debido al algoritmo de hash SHA-1. Estas políticas solo se admiten por compatibilidad.

5.1.5 Servidor de bases de datos

Cuando se utilice un servidor de bases de datos en un proyecto con IHM, se recomienda habilitar el cifrado TLS 1.2. También debe importarse el certificado de la autoridad certificadora (CA). En la configuración del objeto Database Server, habilite el cifrado y la verificación en la pestaña *TLS/SSL*, como se muestra en la [Figura 5.5](#).

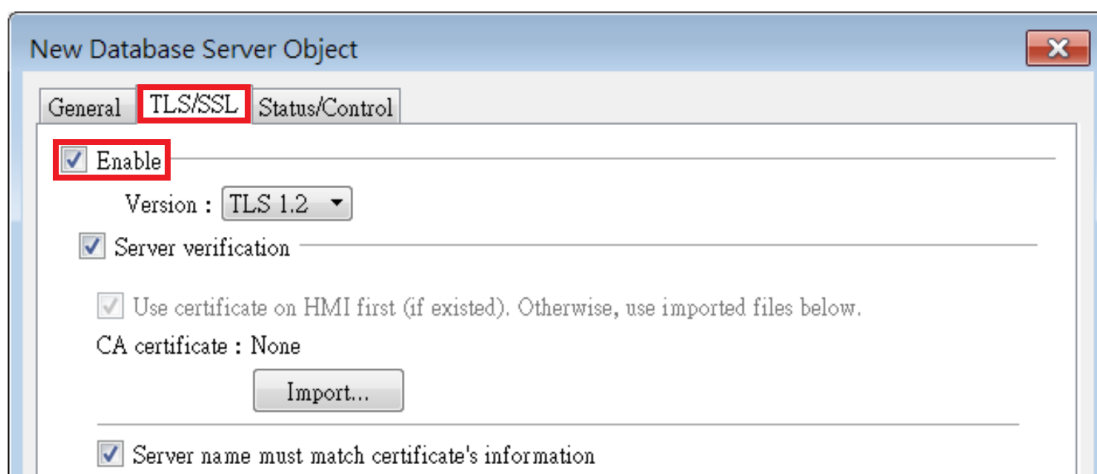


Figura 5.5: Configuración de cifrado TLS/SSL para servidor de bases de datos.

5.1.6 Correo electrónico

Cuando se utilice la función de envío de correos en el proyecto de la IHM, se recomienda:

- Utilizar un servidor SMTP que requiera autenticación
- Utilizar una conexión cifrada TLS/SSL

Tras habilitar la función de correo en los ajustes del sistema, marque las opciones *SMTP server requires authentication* y *Use the following type of encrypted connection*, como en la [Figura 5.6](#).

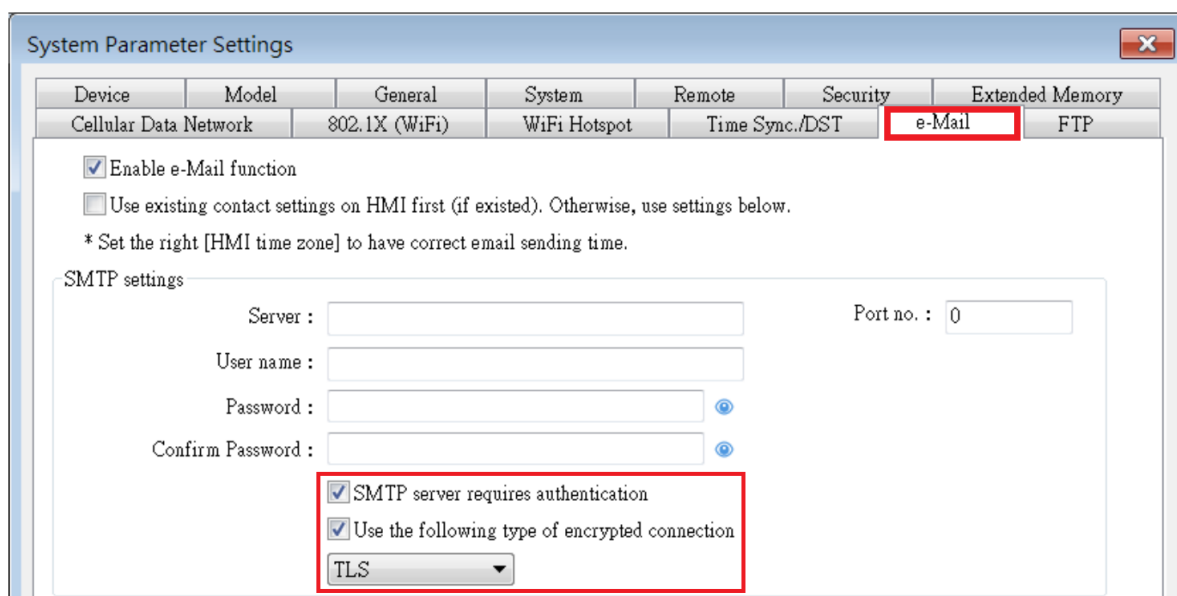


Figura 5.6: Configuración de cifrado para envío de correos.

5.1.7 Monitoreo remoto con cMT Viewer

Si se requiere monitoreo remoto de IHM de las series cMTx, puede utilizarse la aplicación *cMT Viewer*. Se recomienda configurar contraseñas para distintos niveles de permiso en los ajustes del sistema de la IHM, como se muestra en la [Figura 5.7](#). Estas mismas contraseñas deben utilizarse en *cMT Viewer* para acceder a las pantallas.



Figura 5.7: Configuración de contraseña del sistema para acceso remoto.



¡NOTA!

El número máximo de accesos simultáneos a la IHM mediante *cMT Viewer* puede limitarse en *System Parameters* → *Remote*, como se muestra en la [Figura 5.1](#).

5.2 SEGURIDAD DE LA PÁGINA WEB

Cuando se utiliza una IHM de las series cMTx, el usuario puede acceder a la interfaz EasyWeb 2.0 mediante un navegador. En esta interfaz es posible:

- Configurar la dirección IP de la red
- Cargar o descargar proyectos
- Realizar copias de seguridad de datos

Dado que estas funcionalidades implican operaciones críticas, se recomienda aplicar las siguientes configuraciones de seguridad.

5.2.1 Habilitar cifrado HTTPS

Se recomienda habilitar la comunicación HTTPS cifrada. Tras acceder a EasyWeb 2.0, abra el menú *Administration*, abra la página *Security* y habilite la opción *Force HTTPS*, como se muestra en la [Figura 5.8](#).

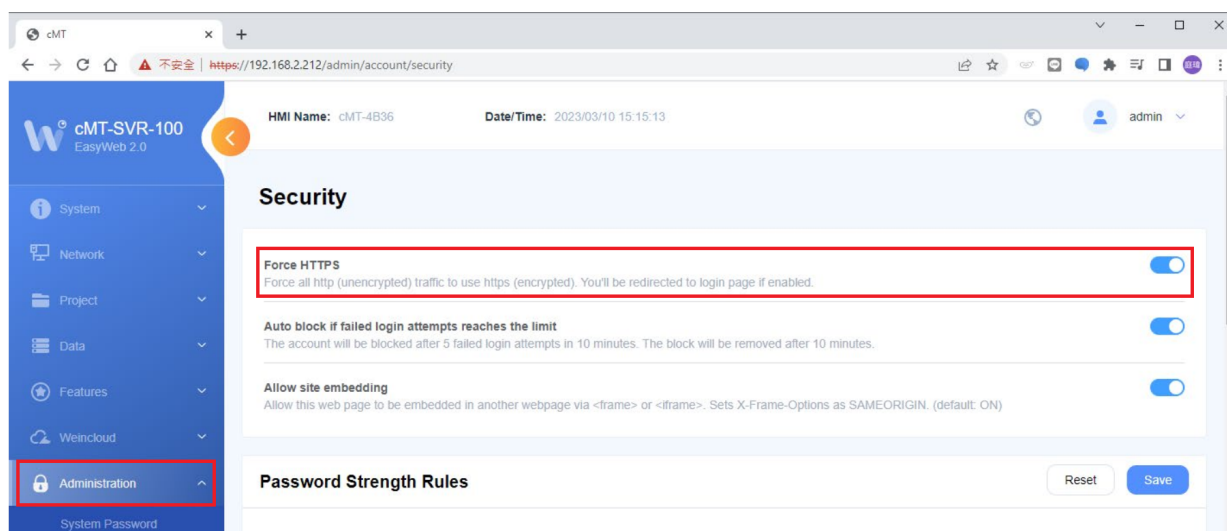


Figura 5.8: Ajuste para forzar el uso de HTTPS.

5.2.2 Habilitar reglas de fortaleza de contraseña

Se recomienda habilitar reglas de fortaleza de contraseña para imponer requisitos de:

- Longitud mínima
- Uso de letras mayúsculas y minúsculas
- Números
- Caracteres especiales

En la sección *Password Strength Rules*, configure las opciones destacadas en la [Figura 5.9](#) y haga clic en *Save*.

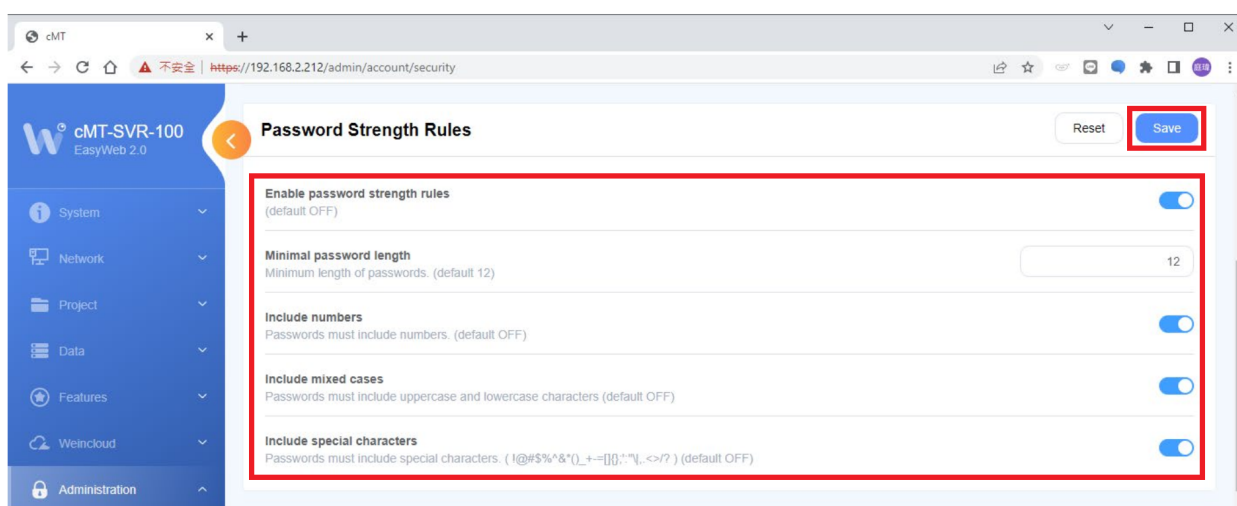


Figura 5.9: Configuración de reglas de fortaleza de contraseña.

5.2.3 Habilitar caducidad de contraseña

Se recomienda habilitar la caducidad de la contraseña para exigir actualizaciones periódicas de credenciales. En la sección *Password Expiration*, configure el número de días de validez de la contraseña, como se indica en la Figura 5.10, y haga clic en *Save*.

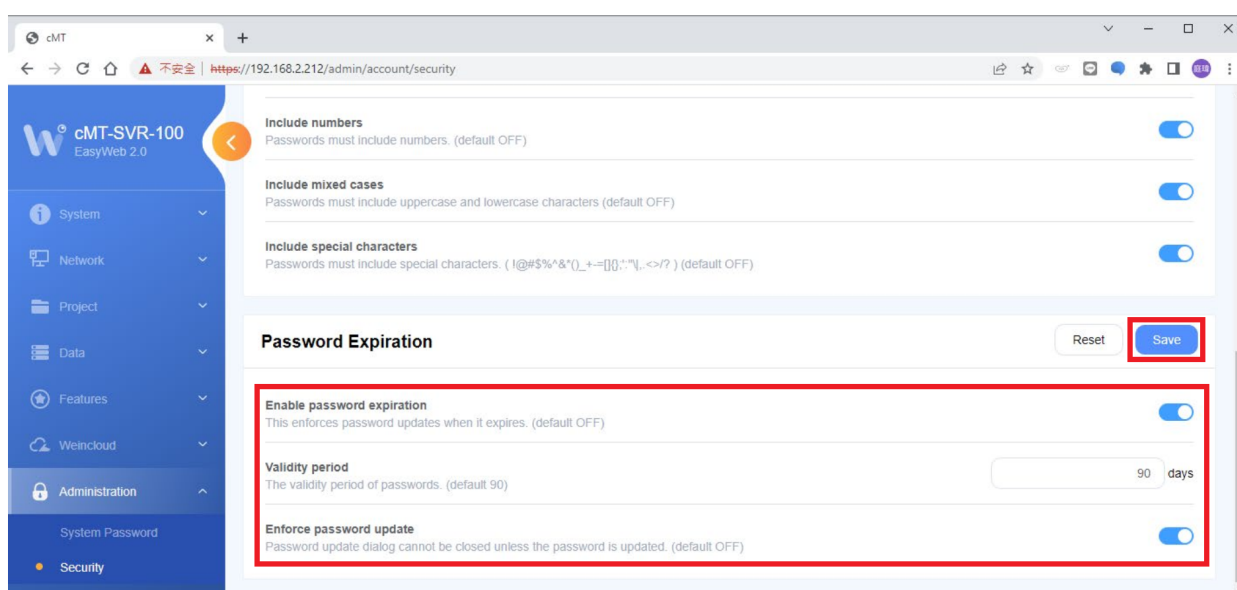


Figura 5.10: Configuración de caducidad de contraseña.

5.2.4 Bloqueo automático tras intentos de inicio de sesión

Se recomienda habilitar el bloqueo automático cuando se produzcan múltiples intentos de inicio de sesión con contraseña incorrecta. Cuando esta opción está habilitada, el sistema se bloquea tras 5 intentos consecutivos inválidos y el bloqueo permanece activo durante aproximadamente 10 minutos. El ajuste puede configurarse en la página *Security* del menú *Administration*, como se muestra en la Figura 5.11.

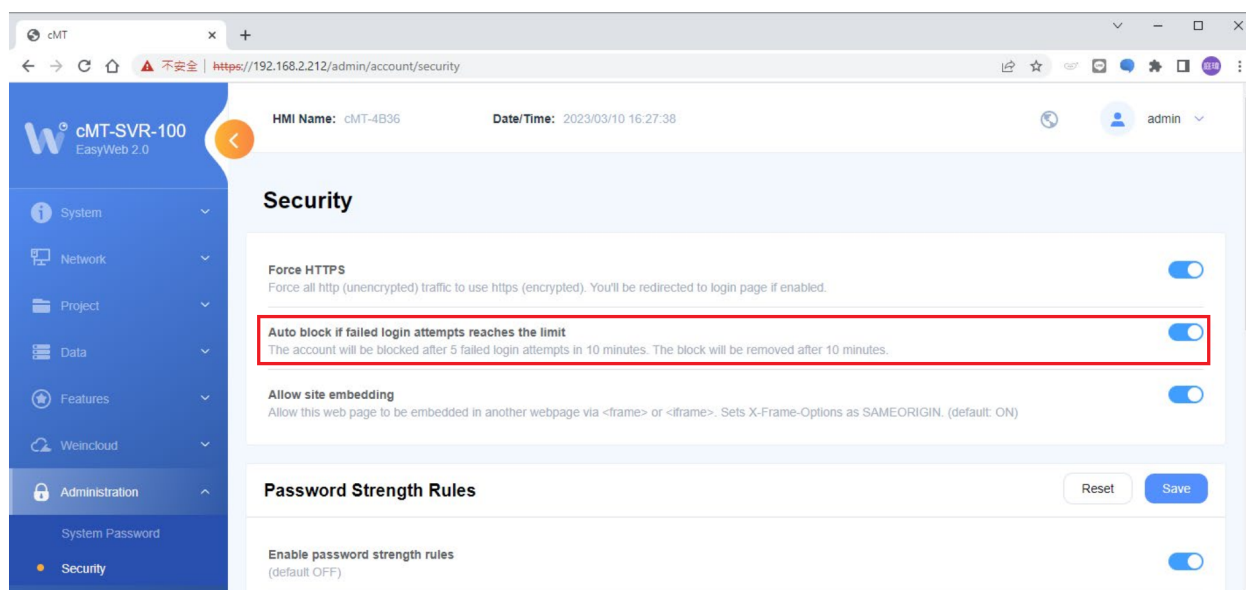


Figura 5.11: Configuración de bloqueo automático tras fallos de inicio de sesión.

5.2.5 Cambiar la contraseña del sistema

Tras configurar las opciones de seguridad de la interfaz web, se recomienda cambiar la contraseña del sistema por una más robusta. Para cambiarla, vaya a *Administration*, abra la página *System Password* y establezca la nueva contraseña, como se muestra en la Figura 5.12.

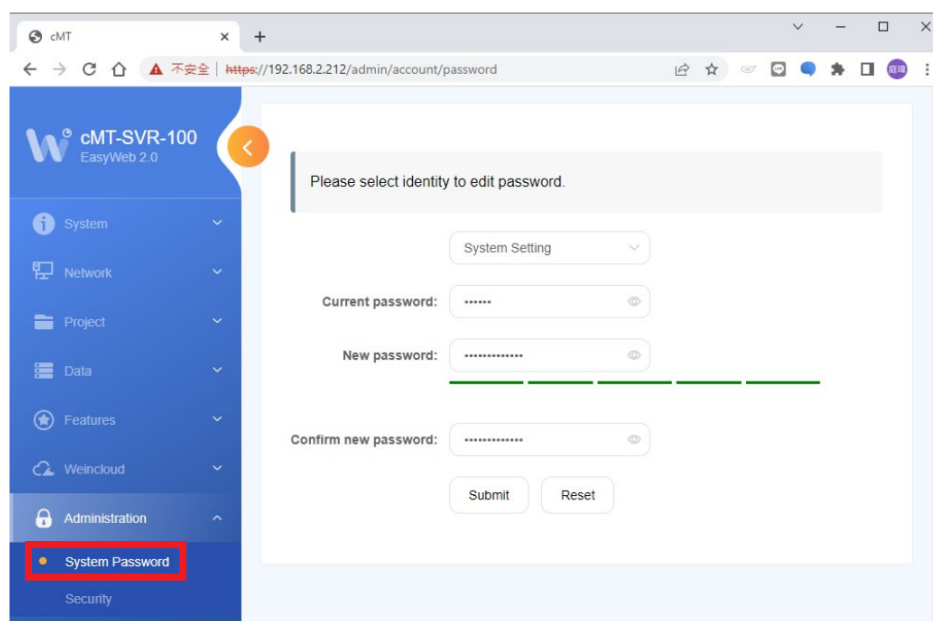


Figura 5.12: Configuración para cambiar la contraseña del sistema.

5.3 ACTIVIDADES REGULARES DE MANTENIMIENTO DE SEGURIDAD

La realización de actividades regulares de mantenimiento de la seguridad de la información es esencial para mantener la protección continua del sistema y los datos. Las prácticas recomendadas incluyen:

- Actualizaciones periódicas de software para asegurar que sistemas operativos, aplicaciones y firmware estén al día con los últimos parches de seguridad.
- Cambios periódicos de contraseña utilizando combinaciones robustas de letras, números y caracteres especiales.
- Realización de copias de seguridad periódicas de los datos y almacenamiento en ubicaciones seguras.

RIESGOS DURANTE EL MANTENIMIENTO REMOTO

- Endurecimiento de cortafuegos y sistemas de prevención de intrusiones.
- Ejecución periódica de escaneos de vulnerabilidades y pruebas de seguridad.
- Revisión periódica de permisos de acceso para garantizar que solo los usuarios autorizados tengan acceso a recursos sensibles.
- Monitoreo regular de registros del sistema y de aplicaciones para detectar incidentes o comportamientos anómalos.
- Realización de auditorías de seguridad internas o externas para verificar el cumplimiento de las mejores prácticas y estándares de seguridad.

6 DIRECTRICES PARA LA ELIMINACIÓN SEGURA DEL PRODUCTO

Esta sección describe los procedimientos para la eliminación segura del producto, a fin de evitar problemas de seguridad de la información, como la filtración de datos sensibles, cuando un producto HMI se retira de operación o se da de baja.

6.1 RECOMENDACIONES PARA UNA ELIMINACIÓN SEGURA

Al dar de baja de forma permanente una HMI, se recomienda seguir las prácticas que se indican a continuación para garantizar que la información almacenada en el dispositivo no quede expuesta.

- Retirar la HMI del equipo o sistema sin causar daños físicos al dispositivo.
- Borrar por completo los programas y los datos de configuración almacenados en la HMI realizando un restablecimiento del sistema.
- Eliminar de forma segura los *logs* almacenados tanto en la HMI como en dispositivos de almacenamiento externos.
- Realizar la eliminación física segura del equipo—si es necesario mediante destrucción física—para prevenir posibles filtraciones de datos que no puedan eliminarse completamente del dispositivo.



BRASIL

BWEG DRIVES & CONTROLS - AUTOMAÇÃO LTDA.

Av. Prefeito Waldemar Grubba, 3000

89256-900 - Jaraguá do Sul - SC

Teléfono: 55 (47) 3276-4000

Fax: 55 (47) 3276-4060

www.weg.net