Guía de seguridad KNX

Edición del manual: b

www.zennio.com

MANUAL DE USUARIO

CONTENIDO

Contenido 2
Actualizaciones del documento 3
1 Introducción 4
2 Configuración 5
2.1 Seguridad en el Bus KNX 5
2.1.1 Puesta en marcha segura 6
2.1.2 Comunicación de grupo segura 9
2.2 Seguridad KNX IP 10
2.2.1 Puesta en marcha segura 11
3 Restablecimiento de valores de fábrica 14
4 Observaciones 15

ACTUALIZACIONES DEL DOCUMENTO

Versión	Modificaciones	Página(s)
b	Se añaden las indicaciones para realizar un reinicio de fábrica.	14

1 INTRODUCCIÓN

Hasta el momento, los datos transmitidos en una instalación domótica KNX eran abiertos y podían ser leídos y manipulados por cualquier persona con conocimientos al respecto que tuviera acceso al medio KNX, de esta forma, la seguridad se garantiza impidiendo el acceso al bus KNX o a los dispositivos. Los nuevos protocolos de seguridad **KNX Secure** añaden una seguridad adicional a las comunicaciones en una instalación KNX, para evitar este posible tipo de ataques.

Los dispositivos que cuenten con seguridad KNX tendrán la capacidad de comunicarse de forma segura con ETS y con cualquier otro dispositivo KNX Secure, ya que incorporarán un sistema de autentificación y cifrado de la información.

Se distinguen dos tipos de seguridad KNX que pueden ser implementadas de manera simultánea en una misma instalación:

- **KNX Data Secure:** asegura la comunicación dentro de una instalación KNX.
- **KNX IP Secure:** para instalaciones KNX con comunicación IP, asegura la comunicación a través de la red IP.

El uso de la seguridad depende de dos ajustes significativos en el proyecto de ETS:

- Seguridad en la puesta en marcha: establece si, durante la puesta en marcha, el dispositivo debe comunicarse con ETS de forma segura y abre la posibilidad de activar la seguridad en el funcionamiento.
- Seguridad en el funcionamiento: permite elegir si durante la ejecución, la comunicación entre dispositivos debe ser segura o no. Es decir, determinar qué direcciones de grupo serán seguras. Para activar la seguridad en el funcionamiento debe estar activada la seguridad en la puesta en marcha.

La activación de la seguridad en dispositivos KNX Secure es opcional. Si se activa, se establece de forma individual en las direcciones de grupo, por lo que se pueden asegurar todos sus objetos o solo una parte de ellos, funcionando el resto con normalidad con dispositivos no seguros. Es decir, dispositivos con y sin KNX Secure pueden convivir en una misma instalación.

2 CONFIGURACIÓN

A partir de la versión 5.7 de ETS, se permite el uso de seguridad KNX y todas sus funcionalidades para trabajar con dispositivos seguros. Hay dos tipos de seguridad, la seguridad KNX, es decir, en el bus KNX, y la seguridad KNX-IP, que corresponde al medio IP.

En esta sección se expone una guía para la configuración de la seguridad KNX en proyectos ETS.

2.1 SEGURIDAD EN EL BUS KNX

Su implementación asegura la comunicación entre dispositivos en el medio TP, los cuales trasmitirán telegramas cifrados a otros dispositivos que dispongan también de seguridad KNX.

Será posible elegir para cada dirección de grupo, si la comunicación será de forma segura o no.

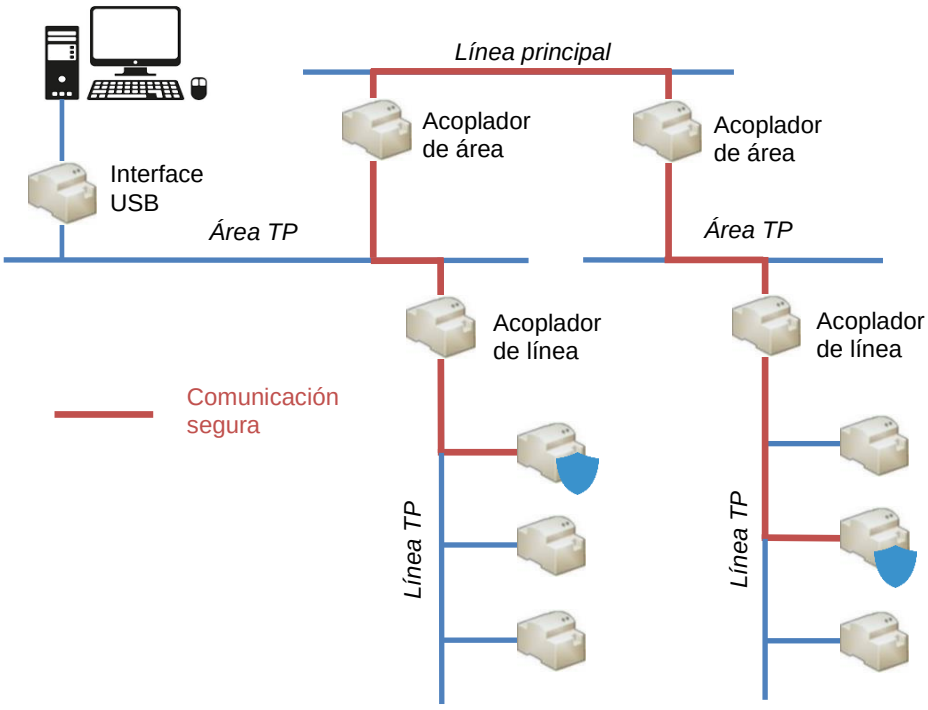


Figura 1. Esquema de seguridad en el bus KNX.

2.1.1 PUESTA EN MARCHA SEGURA

Cuando un dispositivo cuenta con una puesta en marcha segura, la comunicación entre ETS y el dispositivo se llevará a cabo en modo seguro.

Un dispositivo deberá tener configurada una puesta en marcha segura siempre que exista seguridad durante el funcionamiento, es decir, que alguno de sus objetos sea asociado a una dirección de grupo segura (ver sección 2.1.2).

Nota: *Téngase en cuenta que la presencia de un dispositivo seguro dentro de un proyecto ETS, supone la protección del propio proyecto con una contraseña.*

PARAMETRIZACIÓN ETS

La configuración de la seguridad en puesta en marcha se establece desde la pestaña "Configuración", dentro de la ventana de "Propiedades" del dispositivo.

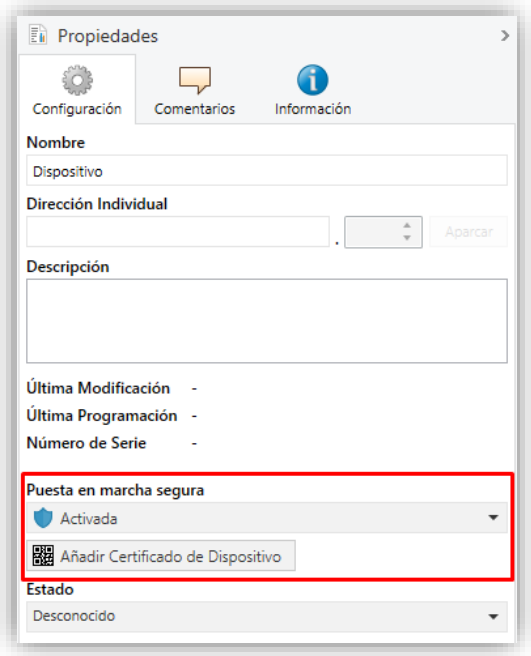


Figura 2. Seguridad en el bus KNX - Puesta en marcha segura.

- **Puesta en marcha segura** [*Activada / Desactivada*]: permite elegir si ETS debe comunicarse con el dispositivo en modo seguro o no, es decir, permite habilitar o inhabilitar la seguridad KNX en el dispositivo.

  Si se selecciona la opción "*Activada*", será necesario **establecer contraseña para el proyecto**, sin ella no se permite descargar con seguridad.

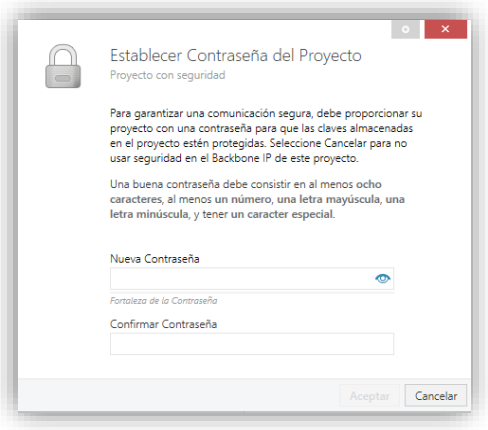


Figura 3. Proyecto – Establecer contraseña.

Un modo adicional de establecer contraseña en un proyecto es a través de la ventana principal ("Visión general") de ETS. Al seleccionar el proyecto, se mostrará una sección en la parte derecha donde, en "Detalles", se podrá incluir la contraseña deseada.

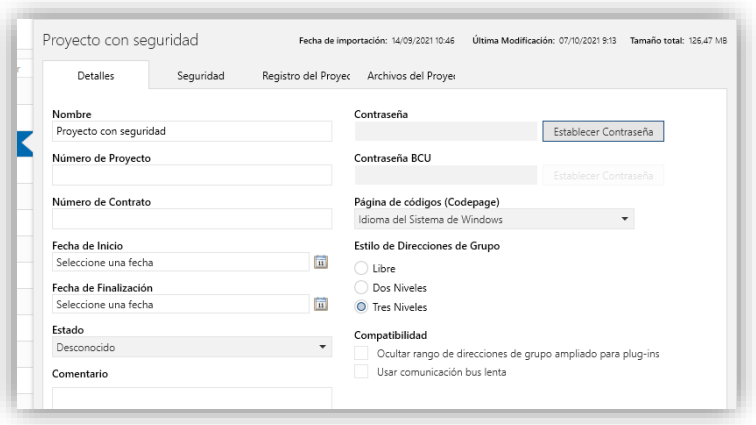


Figura 4. ETS - Establecer contraseña.

- **Añadir Certificado de Dispositivo:** siempre que la **puesta en marcha segura** esté "*Activada*", ETS, además de la contraseña, solicitará un certificado único para el dispositivo.

El **certificado** a añadir [*xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx*] consta de 36 caracteres alfanuméricos generados a partir del número de serie y la clave de fábrica o *FDSK* (*Factory Default Setup Key*) del dispositivo. Se incluye junto con el dispositivo y contiene el código QR correspondiente para poder escanearlo de manera sencilla.

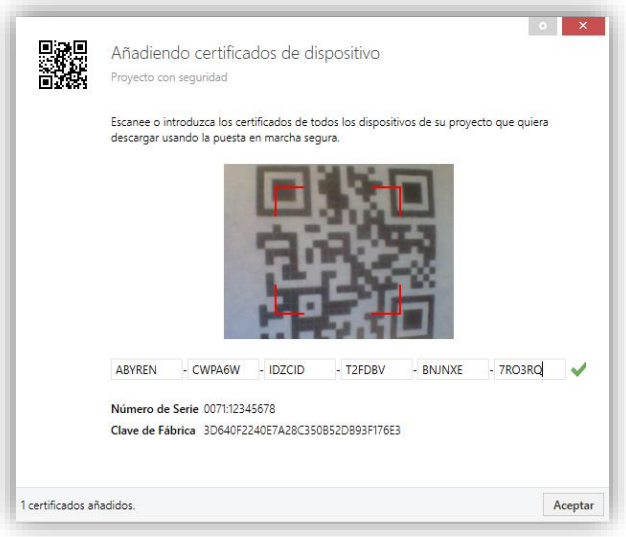


Figura 5. Proyecto - Insertar certificado de dispositivo.

El certificado del dispositivo también podrá ser añadido desde la ventana principal de ETS ("Visión general"), accediendo a la sección "Seguridad" de la nueva ventana que se visualiza en la parte derecha al seleccionar el proyecto.

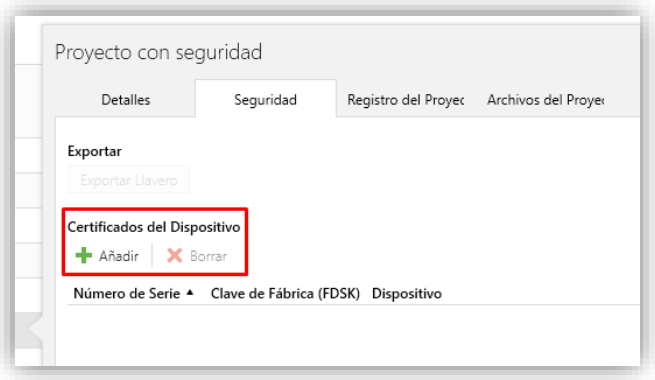


Figura 6. ETS - Añadir certificado de dispositivo.

Durante la primera puesta en marcha segura, ETS sustituye la FDSK del dispositivo por una nueva clave, la clave de herramienta (*Tool Key*) que se genera individualmente para cada dispositivo que se ponga en marcha de forma segura.

Si el proyecto se perdiese, todas las claves de herramienta se perderán con él. Por lo que los dispositivos no se podrán reprogramar. Para poder recuperarlos, hay que reestablecer la clave de fábrica (FDSK).

La FDSK puede ser restituida de dos maneras: con una desprogramación, siempre que se realice desde el proyecto en el que se llevó a cabo la puesta en marcha, o tras un restablecimiento manual de los valores de fábrica (ver sección 3).

2.1.2 COMUNICACIÓN DE GRUPO SEGURA

Cada objeto de un dispositivo seguro podrá transmitir su información de forma encriptada, estableciendo así seguridad en la comunicación o funcionamiento.

Para que un objeto cuente con seguridad KNX, esta tendrá que ser configurada desde la propia dirección de grupo, es decir, aquella dirección a la que irá asociado el objeto.

PARAMETRIZACIÓN ETS

La configuración de la seguridad en la comunicación se establece desde la subpestaña "Configuración", dentro de la ventana de "Propiedades" de la dirección de grupo.

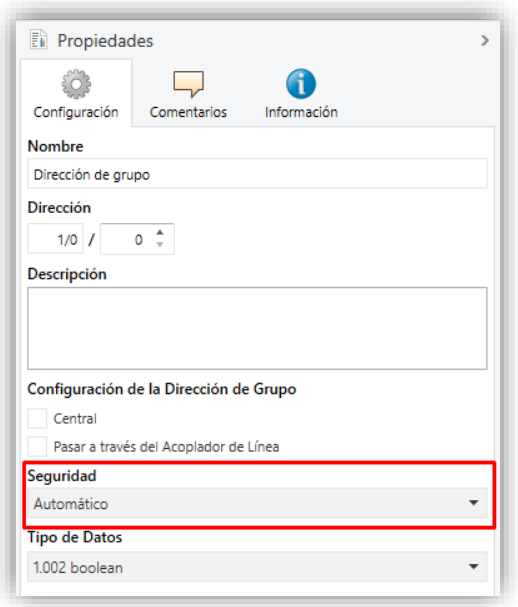


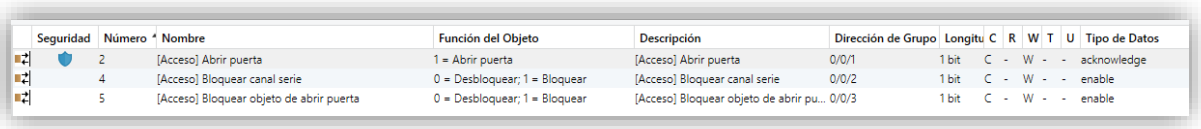
Figura 7. Seguridad en el bus KNX - Seguridad en las direcciones de grupo.

- **Seguridad** [*Automático / Encendido / Desactivado*]. Si se selecciona la opción "*Automático*", ETS será quien decida si se activa o no la seguridad dependiendo de si los dos objetos enlazados pueden comunicarse de manera segura.

Notas:

- *Todos los objetos asociados a una **dirección de grupo segura** van a ser **objetos seguros**.*
- *Un mismo dispositivo puede tener direcciones de grupo seguras y no seguras.*

Los objetos seguros pueden identificarse con un "escudo azul".



Seguridad	Número	Nombre	Función del Objeto	Descripción	Dirección de Grupo	Longitu	C	R	W	T	U	Tipo de Datos
	2	[Acceso] Abrir puerta	1 = Abrir puerta	[Acceso] Abrir puerta	0/0/1	1 bit	C	-	W	-	-	acknowledge
	4	[Acceso] Bloquear canal serie	0 = Desbloquear; 1 = Bloquear	[Acceso] Bloquear canal serie	0/0/2	1 bit	C	-	W	-	-	enable
	5	[Acceso] Bloquear objeto de abrir puerta	0 = Desbloquear; 1 = Bloquear	[Acceso] Bloquear objeto de abrir pu...	0/0/3	1 bit	C	-	W	-	-	enable

Figura 8. Objeto seguro.

2.2 SEGURIDAD KNX IP

La seguridad KNX IP ha sido ideada para instalaciones KNX con comunicación IP. Su implementación garantiza el intercambio de datos KNX de forma segura entre instalaciones a través de dispositivos KNX seguros con conexión IP.

Este tipo de seguridad se aplica en interfaces de bus y únicamente en el medio IP, es decir, los telegramas seguros se transmiten entre acopladores, dispositivos e interfaces KNX IP seguros.

Para que la transmisión de los telegramas en una línea principal o sub-línea también sea segura, se deberá activar la seguridad en el bus KNX (ver sección 2.1).

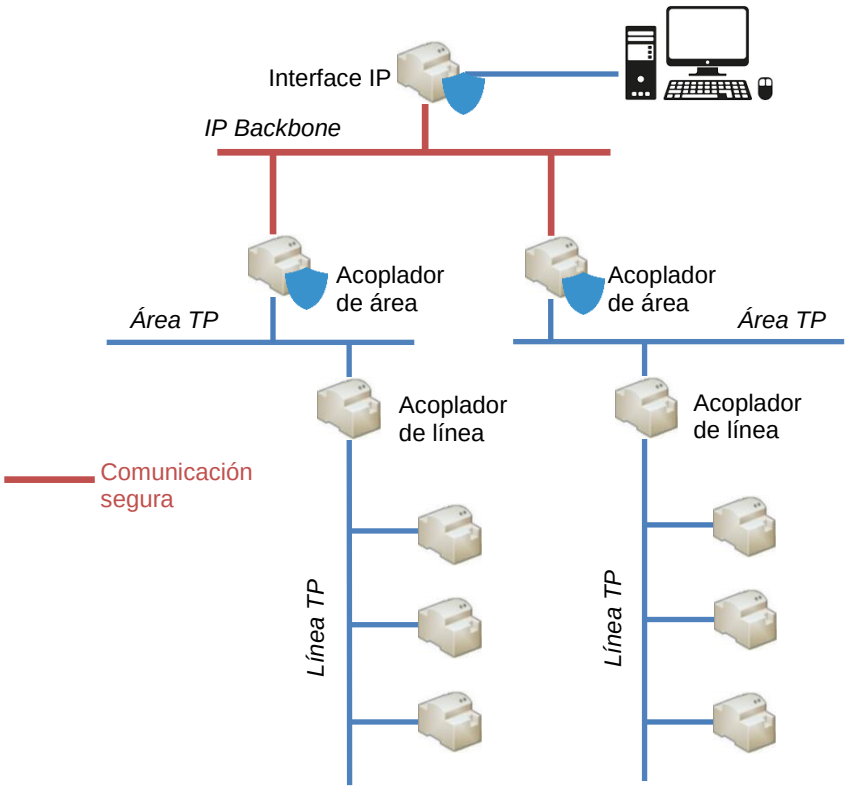


Figura 9. Esquema de seguridad KNX IP

2.2.1 PUESTA EN MARCHA SEGURA

En este tipo de seguridad, a parte de la puesta en marcha segura de la sección 2.1.1, también se puede activar el "*Tunneling* seguro". Este parámetro se encuentra en la pestaña de "Configuración" de la ventana de propiedades de los dispositivos seguros con conexión IP, en la parte derecha de la pantalla de ETS.

PARAMETRIZACIÓN ETS

La configuración de la seguridad en puesta en marcha y en el *tunneling* se establece desde la pestaña "Configuración", dentro de la ventana de "Propiedades" del dispositivo.

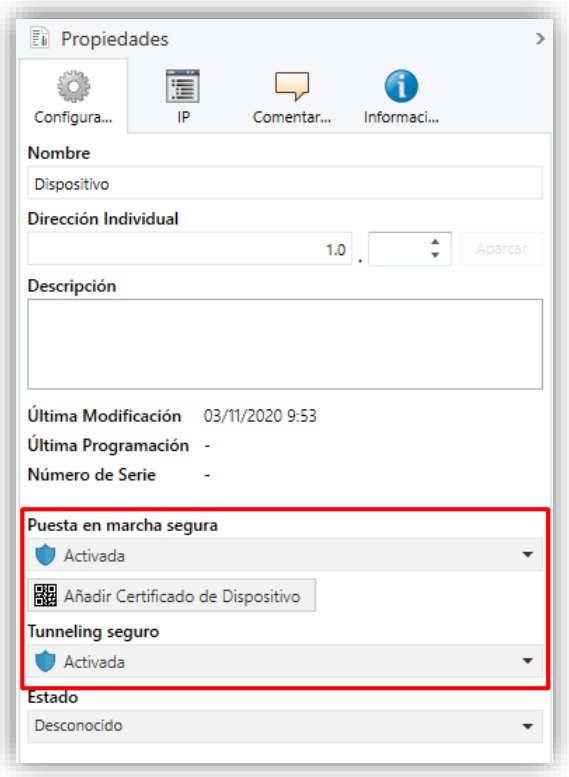


Figura 10. Seguridad KNX IP - Puesta en marcha y *Tunneling* seguro.

Además de la **Puesta en marcha segura** y el botón **Añadir Certificado de Dispositivo**, explicados en la sección 2.1.1, también aparecerá:

- ***Tunneling* seguro** [*Activada / Desactivada*]: parámetro solo disponible si se tiene activada la **puesta en marcha segura.** Si esta propiedad está "*Activada*", los datos transmitidos a través de las conexiones de túnel, serán seguros, es decir, la información irá cifrada por el medio IP. Cada dirección de túnel tendrá su propia contraseña.

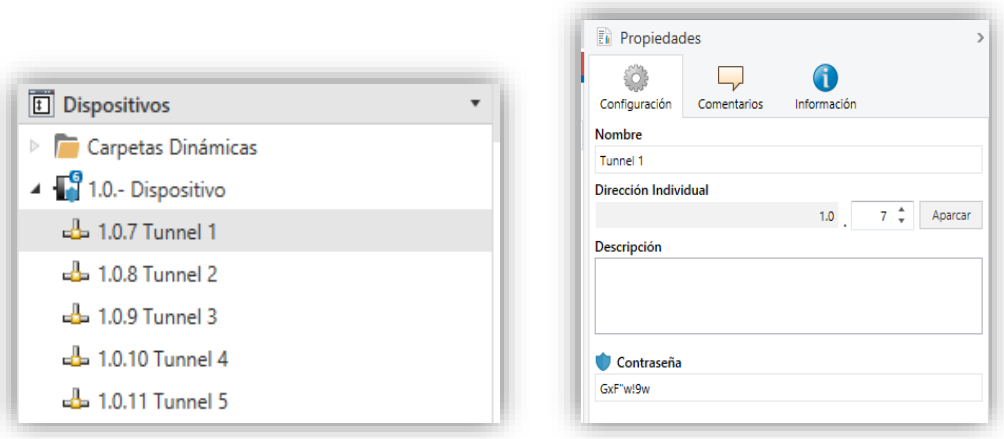


Figura 11. Contraseña de la dirección de túnel.

La pestaña "IP" contiene la **Contraseña de puesta en marcha** y **Código de Autenticación**, necesarios para realizar cualquier conexión segura con el dispositivo.

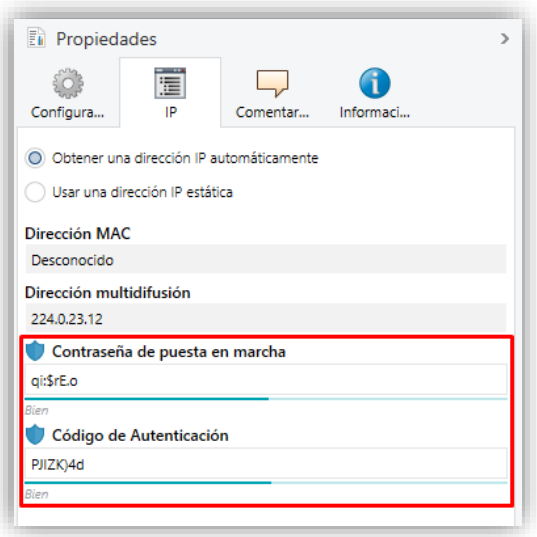


Figura 12. Contraseña de puesta en marcha y Código de Autenticación.

Importante: *Se recomienda que el código de autentificación de cada dispositivo sea individual (y preferiblemente el establecido por defecto en ETS).*

La contraseña de puesta en marcha se solicitará al seleccionar la interfaz IP en ETS para conectarse a ella (el código de autenticación es opcional):

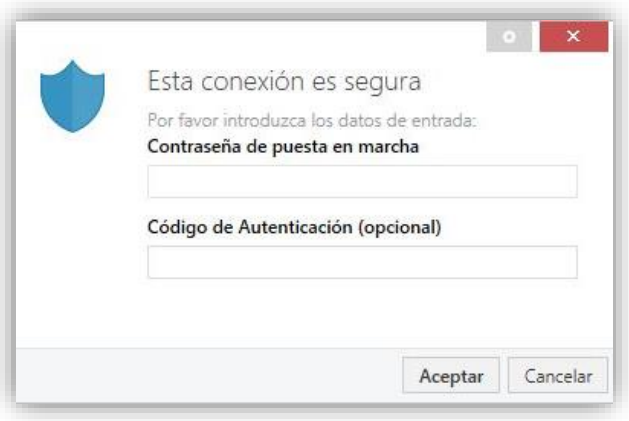


Figura 13. Petición de contraseña de puesta en marcha al seleccionar una interfaz IP segura.

3 REINICIO DE FÁBRICA

Como medida para no dejar inutilizado un dispositivo, en el caso de perder el proyecto y/o la clave (*Tool Key*) con la que está programado, se puede volver al estado de fábrica restituyendo la clave FDSK mediante los siguientes pasos:

1. Poner el dispositivo en modo seguro. Se consigue alimentándolo con el botón de programación pulsado hasta ver que el led de programación parpadea.
2. Soltar el botón de programación. Ver que sigue parpadeando.
3. Realizar una pulsación de 10 segundos sobre el botón de programación. Durante la pulsación el botón quedará encendido en rojo. Se observará el reinicio cuando se apague el led momentáneamente.

Este proceso, aparte de la ***Tool Key***, borra también la **contraseña BCU** y restaura la dirección individual al valor 15.15.255.

Una desprogramación del programa de aplicación también borra la *Tool Key* y la contraseña de BCU, aunque en este caso es necesario el proyecto de ETS con el que se ha programado para realizarla.

4 OBSERVACIONES

Algunas consideraciones para el uso de seguridad KNX:

- **Cambio de dirección individual:** en un proyecto con varios dispositivos seguros ya programados que comparten direcciones de grupo entre ellos, el cambio de la dirección individual en uno de ellos hace que sea necesario reprogramar el resto de dispositivos que comparten direcciones de grupo con él.

- **Programación de un dispositivo reseteado:** al intentar programar un dispositivo restaurándolo a valores de fábrica, ETS detecta que se está usando la *FDSK* y pide confirmación para generar una nueva *Tool Key* para poder reprogramar el dispositivo.

- **Dispositivo programado en otro proyecto:** si se intenta descargar un dispositivo (de forma segura o no) que ya ha sido programado con seguridad en otro proyecto, no se podrá realizar la descarga. Habrá que recuperar el proyecto original o realizar un reinicio de fábrica.

- **Contraseña de BCU:** esta contraseña se pierde tanto con el reinicio de fábrica manual como con una desprogramación.

Únete y envíanos tus consultas sobre los dispositivos Zennio:

https://support.zennio.com

Zennio Avance y Tecnología S.L.
C/ Río Jarama, 132. Nave P-8.11
45007 Toledo. España

Tel. +34 925 232 002.

www.zennio.com
info@zennio.com