

KNX SECURE

MANUAL DE USUARIO ETS

ÍNDICE

1 SEGURIDAD KNX 3
2 SEGURIDAD EN EL BUS KNX 4
2.1 PUESTA EN MARCHA SEGURA 5
2.1.1 CONTRASEÑA DEL PROYECTO 6
2.1.2 CERTIFICADO DEL DISPOSITIVO 7
2.2 COMUNICACIÓN DE GRUPO SEGURA 8
3 KNX IP SECURE 9
3.1 PUESTA EN MARCHA Y TUNNELING SEGURO 10
3.2 CREDENCIALES Y CONEXIÓN CON LA INTERFAZ 11
3.3 ROUTING Y CLIENTES EXTERNOS 12
4 REINICIO DE FÁBRICA 13
5 OBSERVACIONES 14

I SEGURIDAD KNX

Este manual describe la puesta en marcha de dispositivos DINUY compatibles con KNX Secure y la protección de sus comunicaciones. Prepare el proyecto, active la puesta en marcha segura, incorpore los certificados y descargue la configuración. Para equipos IP Secure, configure también los accesos y, cuando corresponda, la seguridad del routing.

Antes de comenzar, compruebe las funciones Secure de la referencia DINUY y de su programa de aplicación. Importe el archivo de producto adecuado y utilice una versión de ETS compatible. Las capturas corresponden a ETS 6.3 en español; la disposición y algunos rótulos pueden variar entre versiones.

Qué seguridad debe configurar

- **KNX Data Secure:** protege los datos de grupo entre dispositivos compatibles, también cuando atraviesan distintos medios KNX. Se configura mediante la puesta en marcha segura del dispositivo y la seguridad de las direcciones de grupo asociadas a sus objetos.
- **KNX IP Secure:** protege el acceso por túnel o la comunicación por routing en el tramo IP. No activa por sí solo Data Secure en las líneas TP. Los dos mecanismos pueden utilizarse conjuntamente.

Orden de trabajo

1. **Preparar el dispositivo:** añádalo al proyecto, compruebe su referencia y asígnele una dirección individual sin duplicidades.

2. **Activar la puesta en marcha segura:** seleccione el ajuste en las propiedades del dispositivo.

3. **Establecer la contraseña del proyecto:** complete la solicitud de ETS y conserve la contraseña.

4. **Añadir el certificado:** lea el QR o introduzca el código suministrado con ese equipo.

5. **Configurar los grupos:** asocie los objetos y seleccione la seguridad de cada dirección de grupo.

6. **Programar y comprobar:** descargue los equipos afectados y pruebe las funciones configuradas.

La puesta en marcha segura protege el acceso de programación desde ETS. La seguridad de las funciones durante el servicio se configura por separado: en las direcciones de grupo para Data Secure y en el túnel o el medio IP para IP Secure. Activar un único ajuste no completa toda la configuración.

2 SEGURIDAD EN EL BUS KNX

La figura 1 muestra una función protegida entre dos dispositivos KNX Data Secure. Todos sus participantes deben ser compatibles. La interfaz de programación y los acopladores del recorrido deben admitir las tramas ampliadas necesarias, tanto durante la descarga como durante el funcionamiento.

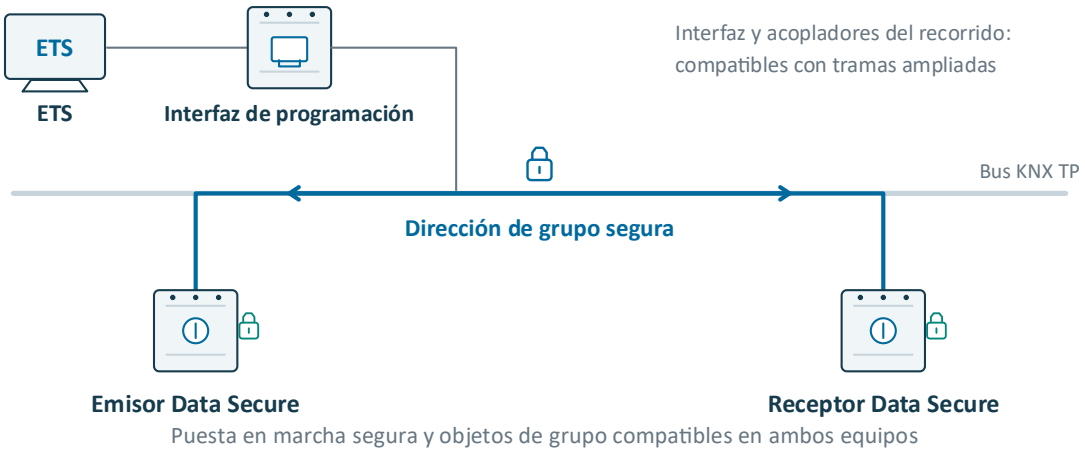


Figura 1. Esquema de una instalación con dispositivos KNX Data Secure

Preparación del proyecto

1. **Añada los equipos DINUY** desde el catálogo e identifique su ubicación y referencia.

2. **Asigne las direcciones individuales** de acuerdo con la topología de la instalación.

3. **Localice el certificado de cada unidad** antes de descargarla. Mantenga la relación entre etiqueta, número de serie y equipo instalado.

Conserve los certificados: registre el número de serie y la ubicación de cada unidad. No publique los códigos QR ni las claves de fábrica en planos de acceso general.

4. **Seleccione la conexión de ETS** que alcanza la línea. Verifique la compatibilidad con tramas ampliadas de la interfaz y de cada acoplador intermedio; no basta con que los dispositivos finales admitan Secure.

Continúe con la activación de la puesta en marcha segura en las propiedades del dispositivo.

2.1 PUESTA EN MARCHA SEGURA

1. **Seleccione el dispositivo DINUY** en el proyecto.

2. Abra el panel «**Propiedades**» y la pestaña «**Configuración**».

3. Abra la lista «**Puesta en marcha segura**» y seleccione «**Activada**». La figura 2 muestra el ajuste que debe seleccionar; el cambio todavía deberá descargarse al dispositivo.

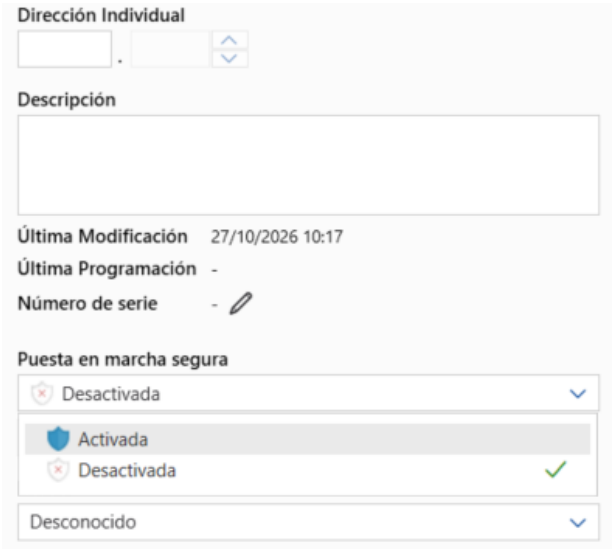


Figura 2. Selección de la puesta en marcha segura en las propiedades del dispositivo

4. Si ETS solicita proteger el proyecto, establezca su contraseña como se explica en el apartado 2.1.1. La contraseña es obligatoria para incorporar certificados y utilizar KNX Secure.

5. Pulse «**Añadir Certificado de Dispositivo**» e incorpore el certificado de esa unidad, según el apartado 2.1.2.

Resultado esperado: la puesta en marcha segura queda activada en el proyecto y el dispositivo tiene asociado su certificado. La configuración debe descargarse al equipo para completar su puesta en marcha.

Si el ajuste no aparece, compruebe que ha seleccionado el dispositivo correcto y que su aplicación admite KNX Secure. Si una referencia permite trabajar sin seguridad y se selecciona «**Desactivada**», no se podrá utilizar esa configuración como participante de una comunicación de grupo protegida que requiera Data Secure.

2.1.1 CONTRASEÑA DEL PROYECTO

Cuando ETS muestre la ventana de la figura 3, introduzca una contraseña para el proyecto en «**Nueva contraseña**» y repítala en el campo de confirmación. Respete los requisitos que indique la propia ventana y confirme la operación.

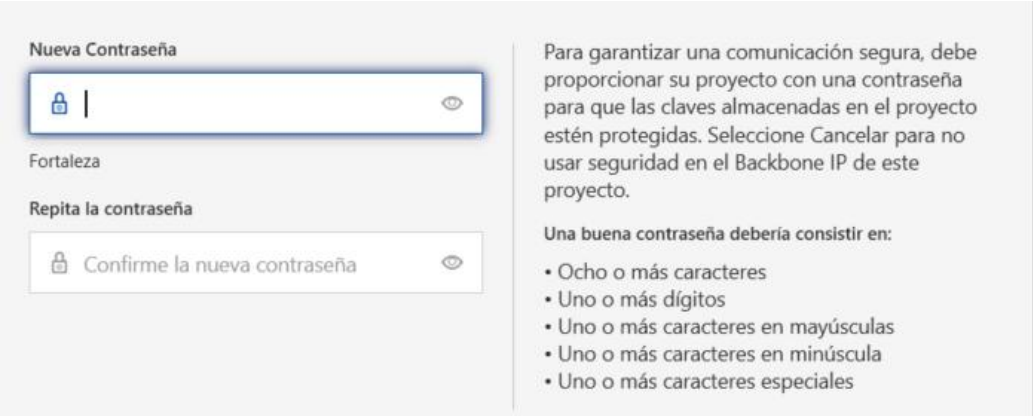


Figura 3. Solicitud para establecer la contraseña del proyecto

Ruta alternativa: desde la visión general, abra los detalles del proyecto. En «**Detalles**», utilice la opción de contraseña. La figura 4 identifica el acceso a ese apartado; la contraseña se establece en la pantalla siguiente.

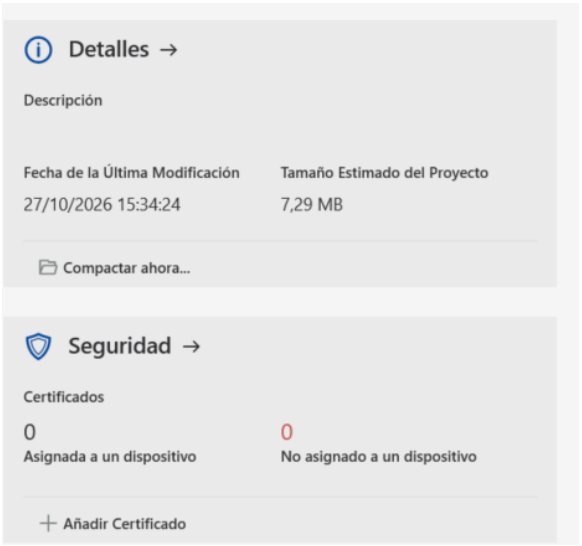


Figura 4. Acceso a los detalles del proyecto desde la visión general

Resultado esperado: el proyecto queda protegido y ETS permite continuar con la incorporación de certificados y la configuración Secure.

Conserve la contraseña junto con una identificación inequívoca del proyecto y entréguela al responsable autorizado por un canal seguro. Esta contraseña abre el proyecto; no es la contraseña de una interfaz IP ni la de una dirección de túnel.

2.1.2 CERTIFICADO DEL DISPOSITIVO

1. En las propiedades del dispositivo, pulse «**Añadir Certificado de Dispositivo**».

2. **Por QR:** sitúe la etiqueta ante la cámara seleccionada y encuadre su código en la zona de lectura.

3. **Por escritura:** introduzca el código del certificado en los seis bloques de seis caracteres. ETS utiliza 36 caracteres Base32 y no admite los dígitos 0 y 1. Copie el código completo de la etiqueta; el número de serie por sí solo no es el certificado.

4. Compruebe que ETS reconoce el certificado y que el número de serie corresponde al dispositivo instalado. Acepte su incorporación.

Si ETS rechaza el código: compruebe la transcripción, la lectura completa del QR y el número de serie. Si el certificado ya está asociado a otro dispositivo, revise esa asignación antes de aceptar una reasignación.

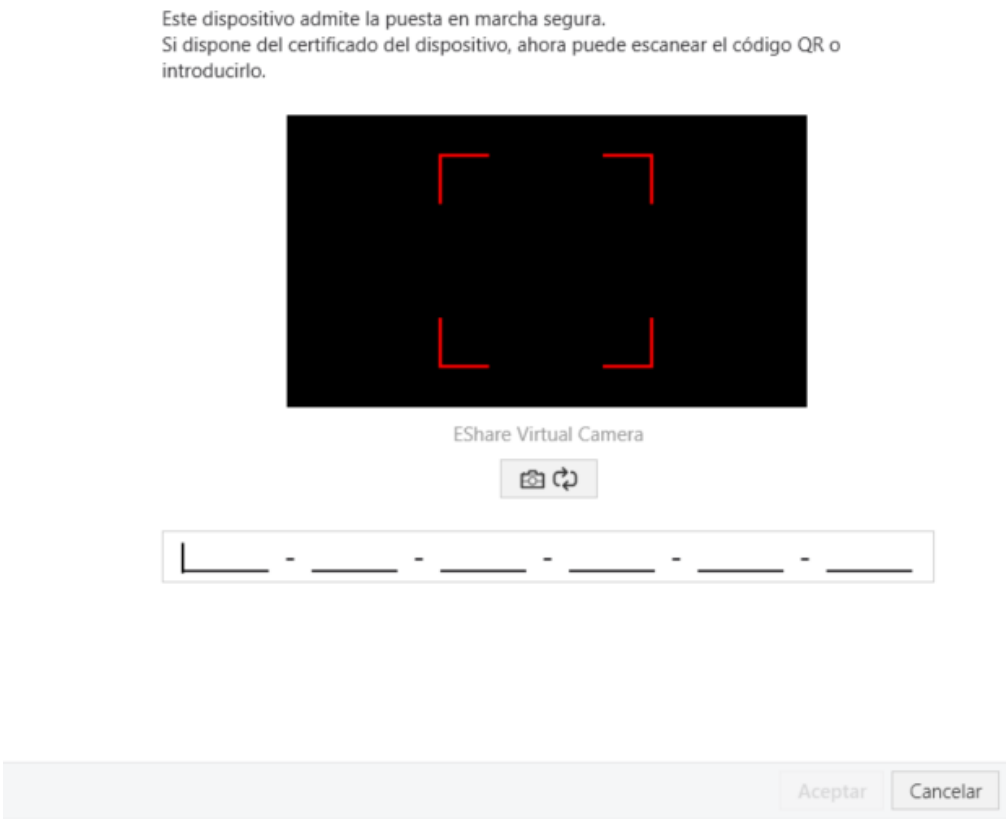


Figura 5. Lectura del QR o introducción del certificado

Después de la primera descarga segura: ETS establece las claves operativas; en Data Secure, la clave de programación se denomina Tool Key. El certificado contiene la clave inicial de fábrica (FDSK), que debe conservarse para recuperar el equipo tras un reinicio de fábrica. El certificado no sustituye al proyecto con sus claves actuales.

2.2 COMUNICACIÓN DE GRUPO SEGURA

1. Cree o seleccione la dirección de grupo y asocie los objetos que deben intercambiar la función.

2. Seleccione esa dirección y abra «**Propiedades**» > «**Configuración**».

3. Localice «**Seguridad**» y elija el ajuste correspondiente, como se muestra en la figura 6.



Figura 6. Seguridad de la dirección de grupo

- **«Automático»:** ETS determina la seguridad según los objetos asociados. Revise el estado efectivo después de añadir o modificar participantes.
- «**Encendido**» o «**Activada**», según la versión: solicita comunicación segura. Todos los objetos enlazados deben admitirla y sus dispositivos deben tener activada la puesta en marcha segura. Resuelva cualquier incompatibilidad indicada por ETS antes de descargar.
- **«Desactivado» o «Desactivada»:** la dirección funciona sin Data Secure, cuando la aplicación permite esa opción.

4. **Descargue la configuración:** seleccione los equipos y abra «**Programar**». En la primera puesta en marcha, descargue dirección individual y aplicación. Pulse el botón de programación solo cuando ETS lo solicite. Espere a que finalice y compruebe los indicadores de descarga; actualice también los participantes y acopladores afectados.

5. **Pruebe la orden y su estado** entre los participantes reales. Un dispositivo puede tener funciones seguras y convencionales en objetos distintos. Un mismo objeto no puede combinar direcciones de grupo seguras y sin seguridad: revise todas sus asociaciones, incluidas las direcciones de recepción.

3 KNX IP SECURE

Utilice este procedimiento cuando el equipo DINUY admita KNX IP Secure. Distinga sus funciones: el tunneling conecta ETS o un cliente con una interfaz; el routing comunica líneas a través de routers. Una interfaz de tunneling no puede asumir la función de router si no la incorpora.

La figura 7 diferencia ambos recorridos. El tramo azul representa la protección IP Secure; el gris identifica la línea TP, cuya seguridad de grupo se configura por separado mediante Data Secure. Para routing y clientes externos, complete el apartado 3.3.

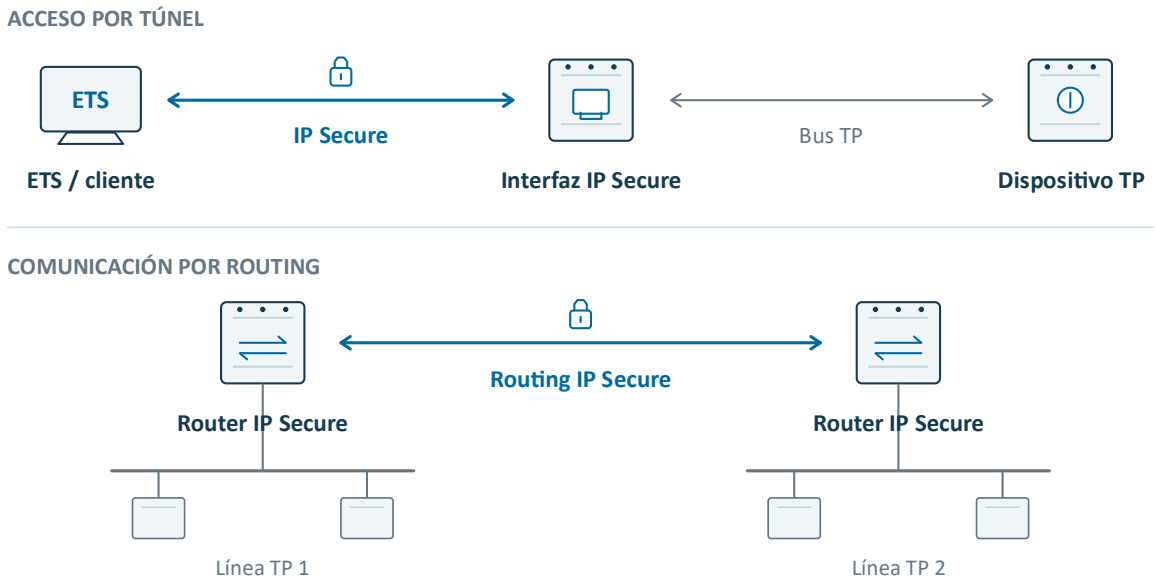


Figura 7. Ámbito de protección de KNX IP Secure en tunneling y routing

Preparación de la interfaz

1. Añada la referencia IP correcta al proyecto y asígnele su dirección individual.

2. Configure el direccionamiento IP conforme a la red de la instalación. Compruebe que ETS puede alcanzar el equipo y que no existen direcciones IP ni individuales duplicadas.

3. Active la puesta en marcha segura e incorpore el certificado del equipo, siguiendo el mismo procedimiento utilizado para los dispositivos del bus.

4. Configure el tunneling seguro y sus accesos, como se explica en el apartado 3.1.

3.1 PUESTA EN MARCHA Y TUNNELING SEGURO

1. Seleccione la interfaz o el dispositivo IP Secure y abra «**Propiedades**» > «**Configuración**».

2. Establezca «**Puesta en marcha segura**» en «**Activada**» e incorpore su certificado.

3. Si el equipo ofrece «**Tunneling seguro**», seleccione «**Activada**». La figura 8 muestra ambos ajustes. La configuración solo será efectiva en la interfaz después de descargarla.



Figura 8. Activación de la puesta en marcha y del tunneling seguro

4. Despliegue los accesos o direcciones de túnel del dispositivo y seleccione el que utilizará el cliente.

5. En sus propiedades, localice la contraseña del acceso de túnel, como muestra la figura 9. Asigne a cada cliente un acceso disponible y compruebe el número de conexiones simultáneas que admite la interfaz.

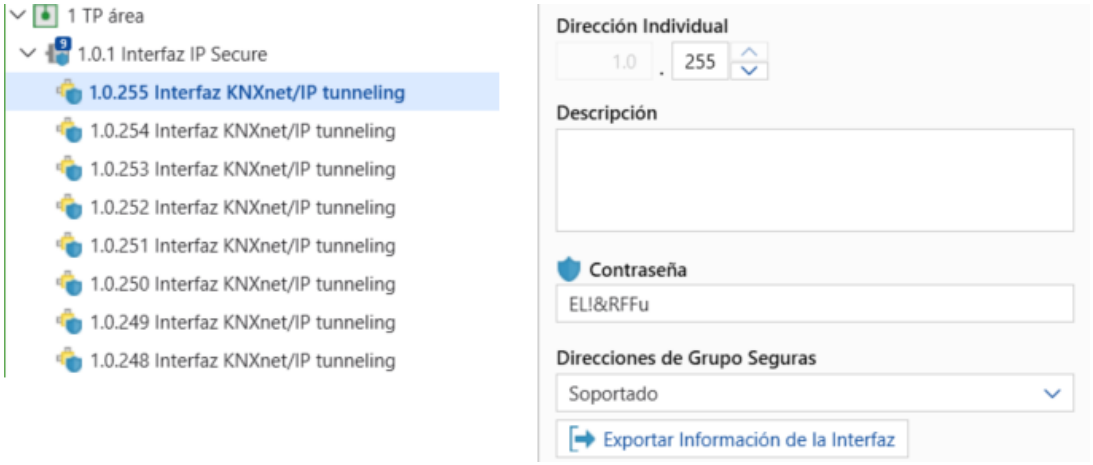


Figura 9. Contraseña del acceso de túnel

Comprobación: cada acceso debe tener una dirección individual libre de su línea. La contraseña del túnel corresponde al cliente de ese acceso; la contraseña de puesta en marcha permite el acceso de gestión de ETS. No utilice en su lugar la contraseña del proyecto.

Continúe con las credenciales de puesta en marcha de la pestaña «**IP**» y la selección de la interfaz en ETS.

3.2 CREDENCIALES Y CONEXIÓN CON LA INTERFAZ

1. Con el dispositivo IP seleccionado, abra la pestaña «**IP**» de sus propiedades.

2. Localice «**Contraseña de puesta en marcha**» y «**Código de Autenticación**», mostrados en la figura 10. Son credenciales del dispositivo. Conserve las generadas para cada equipo y evite reutilizarlas. Los valores de las capturas pertenecen a un ejemplo de configuración.



Figura 10. Credenciales IP del dispositivo

3. **Descargue la interfaz** con sus ajustes de red y seguridad. Compruebe previamente el procedimiento de puesta en marcha del fabricante y la conexión disponible; las credenciales del proyecto no están aplicadas al equipo hasta que la descarga termina correctamente.

4. Abra las conexiones de ETS y seleccione la interfaz IP Secure. Si solicita identificación, introduzca su contraseña de puesta en marcha y el código de autenticación cuando corresponda. Si ETS ya dispone de las credenciales correctas, puede utilizarlas sin mostrar la solicitud.

5. Confirme la conexión y pruebe el acceso a un dispositivo de la línea prevista. Después, compruebe las funciones de grupo que vaya a utilizar el cliente y sus respuestas.

Si la conexión falla: revise la interfaz seleccionada, las direcciones IP e individual, la configuración descargada y las credenciales de ese equipo. Verifique también que queda un túnel disponible. No desactive la seguridad para resolver un error de identificación.

3.3 ROUTING Y CLIENTES EXTERNOS

Routing IP Secure

1. Compruebe que los routers del recorrido admiten KNX IP Secure. En «**Topología**», seleccione la línea o red troncal de medio IP y revise su propiedad «**Seguridad**». Seleccione «**Encendido**» o «**Activada**», según la versión, y resuelva las incompatibilidades de los participantes.

2. Configure una dirección multicast común para los routers que deban comunicarse. Compruebe el paso del tráfico multicast en la red. ETS gestiona la clave compartida del backbone; no equivale a la contraseña de un acceso de túnel.

3. Descargue los routers y demás equipos que ETS marque como afectados. Pruebe una función entre líneas y su respuesta. Un router sin seguridad no puede intercambiar telegramas de routing seguro con los participantes protegidos.

Preparación de la red

Mantenga KNX en una red controlada y limite los accesos mediante la segmentación y el cortafuegos de la instalación. No exponga los puertos KNX directamente a Internet; para acceso remoto, utilice una VPN. Coordine el direccionamiento y el multicast con el responsable de la red.

Clientes externos y exportación de claves

1. Confirme qué mecanismo admite el cliente: túnel IP Secure, routing IP Secure o direcciones de grupo Data Secure. Configure el acceso y las direcciones necesarias en el proyecto.

2. Si el cliente utiliza un archivo de claves, abra el proyecto, acceda a su apartado «**Seguridad**» y exporte el keyring. Proteja el archivo .knxkeys con la contraseña solicitada por ETS e impórtelo según las instrucciones del cliente. Si utiliza credenciales individuales, facilite las del acceso asignado.

3. Entregue únicamente los datos necesarios a personal autorizado; el keyring puede contener claves de más equipos y grupos que los utilizados por ese cliente. Pruebe el cliente y genere una exportación actualizada si cambian las claves o los accesos. Un cliente que utilice grupos Data Secure necesita también las claves de esos grupos.

4 REINICIO DE FÁBRICA

Si se ha perdido el proyecto que programó el dispositivo o sus claves operativas, intente recuperar primero una copia válida. El certificado original no permite acceder por sí solo a un equipo que ya utiliza otras claves. Si no puede recuperarlas, consulte el procedimiento de reinicio de fábrica de la referencia.

Procedimiento para un dispositivo DINUY

1. **Identifique la referencia exacta** y consulte sus instrucciones de uso. Localice el procedimiento de reinicio de fábrica, las condiciones de alimentación y las indicaciones del LED.

2. **Prepare el certificado original** de esa unidad y el proyecto desde el que volverá a programarla.

3. **Ejecute la secuencia indicada para esa referencia.** Siga sus tiempos de pulsación y sus señales de confirmación. No hay una secuencia única que pueda aplicarse a todos los dispositivos DINUY.

4. **Añada o verifique el certificado en ETS** y active la puesta en marcha segura en el proyecto de destino.

5. **Realice la nueva programación** de la dirección individual y la aplicación. Compruebe los grupos, las claves y el funcionamiento de los participantes afectados.

Antes de intervenir: el reinicio puede borrar configuración y claves y detener la función controlada. Confirme sus efectos en las instrucciones de la referencia, conserve el certificado y coordine la interrupción del servicio antes de ejecutarlo.

Con el proyecto original disponible: puede utilizar las operaciones de desprogramación que admita ETS y el dispositivo. Compruebe en la documentación de la referencia sus efectos sobre aplicación, dirección individual, claves y contraseña BCU antes de ejecutarlas.

Un corte de alimentación o un reinicio de ejecución no equivale necesariamente a un reinicio de fábrica.

5 OBSERVACIONES

Cambio de dirección individual

Si cambia la dirección de un dispositivo que ya participa en comunicaciones seguras, revise los equipos que comparten esas funciones. Descargue los participantes y acopladores que ETS marque como afectados y vuelva a comprobar las órdenes y los estados.

Nueva programación después de un reinicio de fábrica

Confirme que el equipo ha recuperado el estado de fábrica previsto por el fabricante. Incorpore el certificado de esa unidad al proyecto de destino, verifique el número de serie y realice de nuevo la puesta en marcha segura. La nueva configuración debe descargarse también a los participantes afectados.

Dispositivo programado desde otro proyecto

Un proyecto distinto puede no disponer de las claves necesarias para acceder a un equipo que ya se ha puesto en marcha con seguridad. Recupere el proyecto que lo programó. Si no es posible, aplique el procedimiento de reinicio de fábrica de la referencia y vuelva a incorporarlo con su certificado.

Sustitución de un dispositivo

Exporte primero una copia del proyecto. El equipo de sustitución tiene su propio número de serie y certificado: no reutilice los de la unidad retirada. Configure la aplicación compatible, la dirección y los grupos previstos; incorpore el nuevo certificado y realice la descarga segura. Actualice los demás participantes que ETS marque como afectados, pruebe las funciones y conserve una nueva copia del proyecto.

Contraseña BCU

La contraseña BCU, cuando el dispositivo la admite, es un mecanismo de control del acceso de programación distinto de KNX Secure. Consulte las instrucciones DINUY antes de desprogramar o reiniciar: la eliminación de una clave no debe deducirse de lo que ocurre con la otra.

Conservación del proyecto

Al terminar una puesta en marcha o una modificación, exporte el proyecto como archivo .knxproj protegido y conserve una copia fuera del ordenador de trabajo. Guarde por separado los certificados originales, las contraseñas y, cuando se utilice, el archivo .knxkeys actualizado. El keyring no sustituye al proyecto ETS.

Identifique la fecha y la versión entregadas. Verifique la apertura de la copia exportada y facilite al responsable de mantenimiento las instrucciones y credenciales mediante un canal seguro. No entregue contraseñas en capturas ni en documentación pública.