Smart home and building solutions.
Global. Secure. Connected.

KNX SECURE
LISTA DE VERIFICACIÓN

LISTA DE VERIFICACIÓN PARA AUMENTAR LA SEGURIDAD Y LA PRIVACIDAD EN LAS INSTALACIONES KNX

1. ¿Se tomaron en cuenta las siguientes medidas durante la instalación?

¿Se han montado los dispositivos y las aplicaciones de forma fija? ¿Se garantiza la debida protección de los dispositivos contra el desmontaje (por ejemplo, instrumentando medidas antirrobo)?	☐
¿Se garantiza la restricción del acceso a las personas no autorizadas a los cuadros de distribución con instalaciones KNX montadas (por ejemplo, siempre cerrados o ubicados en salas cerradas)?	☐
¿Es difícil acceder a los dispositivos en las áreas externas (por ejemplo, montados a una altura suficiente)?	☐
En el caso de que la instalación KNX pueda operarse desde áreas en edificios públicos y no vigilados, ¿se ha considerado el uso de entradas binarias (montadas en los cuadros de distribución) o interfaces de pulsadores?	☐
¿Están los paneles táctiles KNX protegidos mediante contraseña (usuario, grupo o modo invitado)?	☐

2. ¿Se usan cables de par trenzado como medio de comunicación?

¿Están los cables —en cualquier lugar dentro o fuera de la casa o edificio— protegidos contra accesos no autorizados?	☐
En el caso de que se usen cables de par trenzado en áreas que necesiten medidas de protección adicionales, ¿se han instrumentado las medidas recogidas en el punto 6?	☐

3. ¿Se utilizan líneas de potencia como medio de comunicación?

¿Se han instalado filtros de supresión de banda?	☐
Si las líneas de potencia también se usan fuera del edificio, ¿se han instrumentado las mismas medidas para el acoplador de medios como se recoge en el punto 6?	☐

4. ¿Se utiliza el protocolo de internet (IP) como medio de comunicación?

¿Se ha documentado la configuración de la red o se ha entregado al propietario de la vivienda o al administrador de la red de área local (LAN)?	☐
¿Se han configurado los conmutadores y los enrutadores de tal manera que solo las direcciones MAC conocidas puedan acceder al medio de comunicación?	☐
¿Se usa una red de área local (LAN) o una red de área local inalámbrica (WLAN) separada con hardware propio para las comunicaciones KNX?	☐
¿Está limitado el acceso a las redes IP (KNX) a las personas autorizadas mediante nombres de usuario apropiados y contraseñas seguras?	☐
En lo que respecta a las comunicaciones multidifusión IP KNX, debe usarse otra dirección IP como dirección por defecto (por lo general, 224.0.23.12). ¿Se ha cambiado esta dirección multidifusión IP?	☐
¿Se ha cambiado el nombre de la red wifi (SSID) del punto de acceso inalámbrico? ¿Se ha desactivado la transmisión periódica del nombre de la red wifi (SSID) tras la instalación?	☐
¿Se han cerrado los puertos de los enrutadores para KNX hacia internet y se ha establecido en 0 la puerta de enlace por defecto del enrutador KNXnet/IP utilizado? ¿Se ha protegido la instalación (W) LAN mediante un cortafuegos apropiado? En el caso de que una instalación KNX requiera acceso a internet, compruebe si es posible instrumentar: 1. El establecimiento de una conexión VPN al enrutador de internet 2. El uso de servidores de objetos KNX específicos del fabricante	☐

5. ¿Se usa la radiofrecuencia como medio de comunicación?

¿Se han instrumentado las mismas medidas para el acoplador de medios que se recogen en el punto 6?	☐
¿Tiene cada dominio RF una dirección de dominio diferente?	☐

6. ¿Ha utilizado acopladores en la instalación?

¿Se han asignado direcciones individuales en función de su ubicación en la topología?	☐
Mediante la configuración de parámetros apropiados en los acopladores, ¿evita que las direcciones de origen incorrectas no se reenvíen fuera de la línea?	☐
¿Bloquea la comunicación punto a punto y de difusión en todos los acopladores?	☐
¿Se han cargado correctamente las tablas de filtros y se ha realizado la configuración de tal manera que los acopladores tengan en cuenta las tablas de filtros?	☐
¿Ha tenido en cuenta las medidas recogidas en el punto 7 en lo que respecta a los acopladores?	☐

7. ¿Se han bloqueado los dispositivos contra posibles reconfiguraciones?

De lo contrario, introduzca la clave 1 BCU en el proyecto ETS.	☐

8. ¿Utiliza dispositivos KNX Secure[2]?

En lo que respecta a las comunicaciones de grupos que requieren protección, utilice la autenticación prevista y los mecanismos de cifrado del dispositivo. ☐

9. ¿Sospecha de accesos no autorizados al bus?

Registre el tráfico de telegramas y analícelo. En el caso de los dispositivos KNX Secure, lea los registros de errores.
Documente la hora y los efectos observados (lo que sucede, lo que no sucede, cuándo sucede y dónde sucede)
Desactive la conexión a internet del sistema KNX y compruebe si los efectos desaparecen o no desaparecen. ☐
Póngase en contacto con el fabricante a través de su línea de atención: ¿conoce el fabricante los efectos o los problemas de seguridad?, ¿hay actualizaciones disponibles?

Lea el PID_Device_Control[3] de los dispositivos y compruebe si estos usan la misma dirección física. ☐

Lea el PID_Download_Counter[3] de los dispositivos y compruebe que estos se hayan descargado otra vez una vez realizada la configuración. ☐

10. ¿Se han bloqueado los dispositivos contra posibles reconfiguraciones?

¿Al acoplar KNX a las instalaciones de seguridad, se hizo de alguna de las siguientes maneras?

1. ¿Mediante puertas de enlace o dispositivos KNX certificados por empresas aseguradoras nacionales de pérdidas?
2. ¿Mediante contactos libres potenciales (entradas binarias, interfaces de pulsadores, etc.)? ☐
3. Mediante interfaces apropiadas (RS232, por ejemplo) o puertas de enlace: ¿se garantiza que las comunicaciones KNX no puedan desencadenar las funciones de seguridad pertinentes en la parte correspondiente a la seguridad de la instalación?

11. Medidas generales de seguridad

¿Está el software de herramientas de ingeniería (ETS) actualizado?

1. ¿Es seguro el PC (detección de virus y sistema operativo más reciente actualizados) en el que está instalado el ETS? Se recomienda usar un dispositivo dedicado para el diseño y la puesta en marcha en materia de KNX.
2. Durante la instalación, debe evitarse enlazar otros dispositivos de almacenamiento de datos que no sean de confianza al PC (USB, unidad de disco duro externo, etc.). ☐
3. Preferiblemente, los complementos (plug-ins) y las aplicaciones ETS (Apps) deben descargarsed antes de realizar la instalación física.
4. Haga una copia de seguridad del archivo del proyecto tras la instalación (idealmente en una memoria USB segura que debe guardarse cuidadosamente) y elimine el proyecto del PC.

¿Está actualizado el firmware de los dispositivos utilizados? ☐

12. Medidas adicionales de privacidad (RGPD)

Tanto el instalador como el cliente deben firmar una declaración de privacidad. ☐

Con miras a cumplir con el Reglamento General de Protección de Datos (RGPD), el instalador debe entregar una copia del archivo del proyecto ETS al cliente. ☐

[2] Disponible a partir del ETS 5.5 / [3] No compatible en todos los dispositivos