Guía importante para clientes: Garantizar el cumplimiento de las leyes y normativas europeas sobre privacidad de datos

Como proveedor de sistemas digitales de alarma social que implementan las normas PD CLC/TS 50134-9:2018 y SS 91100:2014 (Digital social alarm – Social care alarm internet protocol (SCAIP) – Specification), estamos comprometidos a ayudar a nuestros clientes a cumplir con la legislación europea aplicable, en particular con el Acto Delegado de la Directiva 2014/53/UE sobre equipos radioeléctricos (RED).

Nuestros sistemas de alarma social están diseñados para utilizar el Protocolo de Internet para Alarmas Sociales (SCAIP) y se basan en las normas SS 91100:2014 y PD CLC/TS 50134-9:2018. Estas especificaciones definen el uso de un formato XML para los códigos de alarma e información, transmitidos a través de una red de comunicaciones IP, como puede ser internet. El protocolo se apoya en SIP (Session Initiation Protocol) para la gestión de sesiones.

Para garantizar el cumplimiento de la legislación europea, especialmente en lo relativo a la protección de datos personales y la privacidad en las comunicaciones electrónicas, es fundamental que todos los mensajes de alarma, así como las comunicaciones de voz o multimedia asociadas, se transmitan mediante un canal seguro.

Si bien nuestros productos pueden configurarse para transmitir mensajes de alarma en texto plano (clear text), con el fin de adaptarse a infraestructuras existentes de los Centros Receptores de Alarmas (ARC) que aún no implementan Transport Layer Security (TLS), este método de transmisión no se considera seguro para el manejo de información sensible.

La norma PD CLC/TS 50134-9:2018 establece de forma explícita que tanto la Unidad Local de Control (LUC) como el ARC deben admitir cifrado, y que el LUC no debe transmitir información personal o sensible por conexiones no seguras sin cifrado. Además, estipula que los datos personales y sensibles solo podrán transmitirse mediante SIP seguro (SIPS). Esto incluye el uso de SIP seguro incluso sobre conexiones no seguras y, en el caso de sesiones de voz, el empleo de Secure Real-time Transport Protocol (SRTP) con un cifrado mínimo de AES-128.

Por tanto, para cumplir con los requisitos legales europeos en materia de protección de datos y seguridad de las comunicaciones electrónicas, los clientes deben asegurarse de implementar una de las siguientes opciones en sus despliegues de sistemas de alarma social:

Utilizar SIP seguro (SIPS) con TLS 1.2 o superior: Esta es la opción preferente para proteger tanto los mensajes de alarma como las comunicaciones de voz y multimedia en redes IP. Nuestros productos son compatibles con esta funcionalidad. El ARC deberá presentar un certificado X.509 válido emitido conforme a la norma ITU, y el LUC deberá verificar la identidad del servidor mediante un certificado raíz (Root CA Certificate) local.

Transmitir los mensajes de alarma y las comunicaciones de voz a través de un canal seguro independiente (por ejemplo, una Red Privada Virtual – VPN): Si el cifrado directo mediante SIP TLS no es viable debido a limitaciones en la infraestructura actual del ARC, deberá establecerse un túnel

seguro como una VPN, para cifrar todas las comunicaciones entre el LUC (emisor de la alarma) y el ARC (receptor).

El no implementar las medidas de seguridad adecuadas para la transmisión de mensajes de alarma y comunicaciones de voz puede derivar en un incumplimiento de la normativa europea sobre protección de datos y comunicaciones electrónicas. **Es responsabilidad del cliente configurar y operar el sistema de manera que se garantice dicho cumplimiento.** Recomendamos encarecidamente consultar con sus equipos legales y de seguridad informática para asegurarse de que el despliegue cumpla con todos los requisitos regulatorios aplicables.