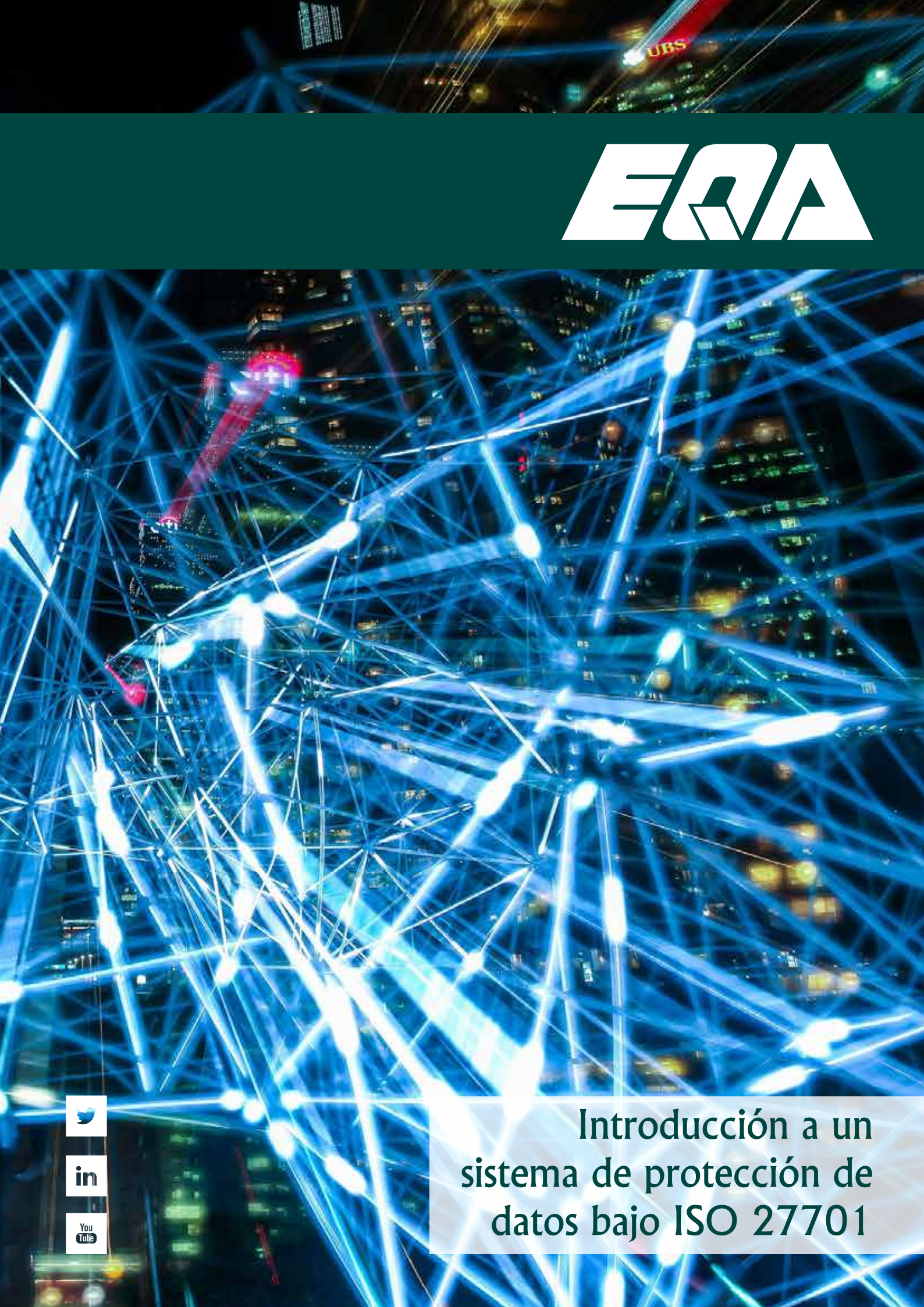


Introducción a un sistema de protección de datos bajo ISO 27701

Introducción al estándar ISO/IEC 27701

La norma ISO 27701:2019 publicada el 6 de agosto de 2019 es un estándar que desarrolla un Sistema de Gestión cuyo fin es la salvaguarda de la privacidad de los datos dentro de una organización. Dentro de nuestro ámbito nacional y europeo, esto implica cumplir con lo dispuesto por el Reglamento Europeo de Protección de Datos y la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales. Por ello, desde su misma concepción, este estándar se creó con vistas a que aquellas organizaciones que lo implementen puedan dar cumplimiento a los requisitos de la legislación, evidenciándose este enfoque en el anexo D, en el que se realiza un cruce de requisitos entre estándar y Reglamento.

El texto se configura en parte como una extensión de ISO/IEC 27001 e ISO/IEC 27002, modificando y ampliando algunos de sus requisitos y en parte como un estándar autónomo, al incorporar los nuevos anexos A y B de carácter normativo. Así, nos encontramos frente a un Sistema de Gestión de Privacidad de la Información (SGPI) enfocado en el cumplimiento en materia de protección de datos que se construye sobre un Sistema de Gestión de Seguridad de la Información (SGSI) del que tomará las buenas prácticas relativas a protección de la información. Establece un marco para que los Responsables y Encargados del tratamiento de datos de carácter personal gestionen los controles de privacidad, a fin de reducir el riesgo para los derechos vinculados a la privacidad de las personas. Así mismo, se constituye como una hoja de ruta que los DPO podrán utilizar como referencia para el desarrollo de sus funciones.

La certificación ISO/IEC 27701 está pensada para organizaciones que dispongan de la certificación ISO/IEC 27001, y para aquellas que, sin contar con un SGSI, deseen implantar un Sistema de Gestión de Seguridad de la Información y de la Privacidad integrado como un único proceso.

¿El estándar ISO/IEC 27701 sigue la estructura de alto nivel de las normas ISO?

No, al menos formalmente. El documento introduce en el punto 5 las modificaciones a ISO 27001, en el 6 las modificaciones a ISO 27002 y en los puntos 7 y 8 las indicaciones para la implementación de los nuevos controles de privacidad.

Sin embargo, en la medida en que el documento es una extensión de ISO 27001, describe un Sistema de Gestión que sí sigue la estructura de alto nivel. En una primera lectura del índice del documento se puede ver como, por ejemplo, el punto 5.2 se corresponde con el 4 de la estructura de alto nivel o el punto 5.8 equivale al punto 10.

¿Existe una versión traducida de ISO/IEC 27701 al castellano?

No, por el momento no se ha realizado una traducción al castellano. Sin embargo, la terminología en inglés utilizada dentro del texto del estándar es la misma que la empleada en el texto legal del Reglamento en su versión en inglés, por lo que aquellos términos técnicos vinculados a la protección de datos que pudieran presentar alguna dificultad de interpretación son fácilmente asimilables al castellano a través de la lectura del propio Reglamento.

Implementando un SGPI

El proceso de diseño e implantación de un Sistema de Gestión de Privacidad de la Información es similar al de cualquier otro Sistema de Gestión y no existen unos pasos marcados para realizarlo. La organización deberá, en base a su realidad y conocimientos en otros Sistemas de Gestión, evaluar cómo abordar esta labor.

Sin embargo, EQA propone el siguiente modelo a modo ilustrativo, de forma que la organización pueda contar con una referencia a la hora de plantearse los principales hitos del proceso de implantación de un SGPI.

01 Identificar a los responsables

02 Definir el alcance

03 Crear una Política de Privacidad

04 Realizar un análisis de riesgos

05 Realizar una análisis de impacto

06 Realizar un plan de tratamiento de riesgos

07 Elaborar una declaración de aplicabilidad

08 Elegir e implantar controles

09 Realizar una auditoría interna

10 Realizar una revisión por la Dirección

11 Tratar las no conformidades y desarrollar la madurez

12 Realizar una auditoría de certificación

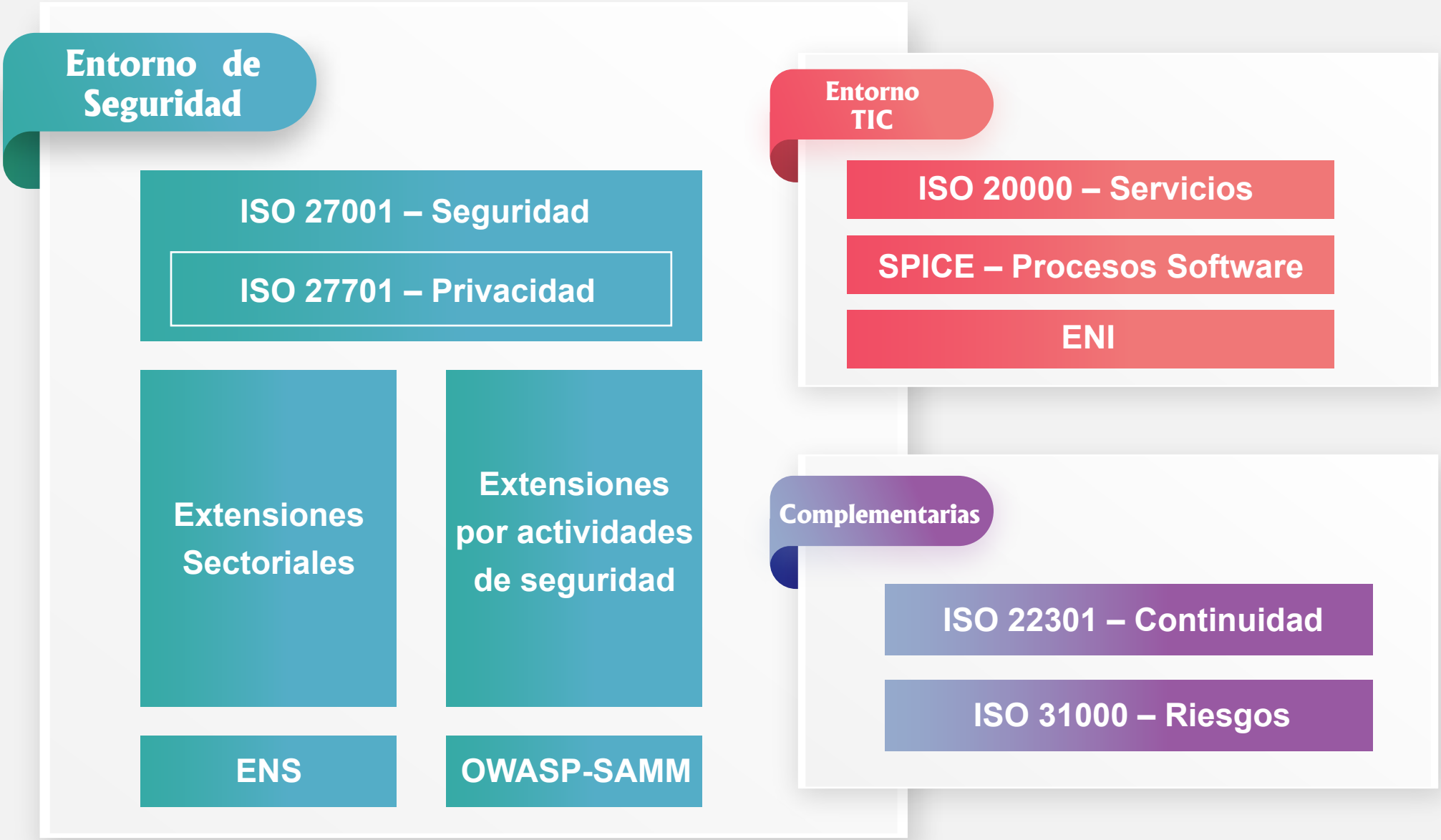
¿Este modelo cubre todos los requisitos del estándar?

No, tanto en el modelo propuesto como en el desarrollo de este manual únicamente tratamos los aspectos más relevantes y característicos de ISO/IEC 27001 y ISO/IEC 27701. Aunque no lo mencionemos, la organización sigue debiendo cumplir con el resto de los requisitos de la estructura de alto nivel, como, por ejemplo, realizar un análisis del contexto (punto 4) o establecer pautas relativas a la gestión documental (punto 7.5) por citar algunos.

¿Es necesario contar con el asesoramiento de una empresa consultora?

No, en ningún momento el contar con la asistencia de una empresa consultora se ha establecido como un requisito para la obtención de un certificado ISO/IEC 27701. En cualquier caso, sí que es recomendable contar con esta ayuda cuando la organización no cuente con suficientes conocimientos y experiencia como para abordar la tarea de implementación del sistema por sí mismos o requieran de ayuda externa para abordar algún aspecto concreto. En cualquier caso, es la organización quien debe valorar esta necesidad.

El modelo de seguridad de EQA



El departamento de Seguridad de la Información cuenta con un equipo de profesionales especializados en seguridad, privacidad y tecnología. Nos esforzamos en ofrecer a nuestros clientes servicios de auditoría flexibles y personalizados a través de nuestro Modelo de Seguridad. Si tenéis cualquier necesidad en materia de seguridad, tecnológica o deseáis ampliar esta información, estamos a vuestra disposición para ofreceros una solución a medida.

Camino de la Zarzuela, 15 | Bloque 2, 1ª Planta | 28023 Madrid
902 44 9001 · +34 91 307 86 48 | Fax: 91 357 40 28
www.eqa.es | info@eqa.es