

Es frecuente encontrarse con planteamientos en los que el Esquema Nacional de Seguridad y las normas de la serie UNE - ISO/IEC 27000 se ponen en pie de igualdad e incluso se comparan como si fueran alternativas en el mismo plano de igualdad. Conviene tener presente que estos instrumentos se encuentran en planos diferentes:

- El Esquema Nacional de Seguridad, materializado en el Real Decreto 3/2010, de 8 de enero, es un texto legal que desarrolla lo previsto al respecto en la Ley 11/2007 y se encuentra, por tanto, vinculado a la creación de condiciones de confianza y de seguridad que permitan el ejercicio de derechos, el cumplimiento de deberes y el acceso electrónico de los ciudadanos a la información y al procedimiento administrativo. Tiene que ver en definitiva con la realización del derecho de los ciudadanos a relacionarse por medios electrónicos con las Administraciones Públicas.

Es un texto legal, de aplicación por parte de todas las Administraciones Públicas, que llega en su nivel de concreción hasta donde puede llegar, sin comprometer ciertos espacios de decisión que han de quedar para las propias Administraciones, ni llegar a un excesivo nivel de detalle que podría quedar vinculado a tecnologías concretas o dar lugar a una rápida obsolescencia. En relación con este último aspecto, la formulación de sus contenidos se realiza con un nivel de abstracción tal que le facilite una cierta longevidad en el tiempo, por encima de vaivenes a los que puedan estar sometidos normas procedentes de la normalización voluntaria y elementos tecnológicos.

El Esquema impulsa que debe haber una gestión continuada de la seguridad, necesaria para poder satisfacer ciertos principios básicos y requisitos mínimos, relativos, en general, a la implantación de la seguridad, a la gestión de los riesgos y a la mejora continua del proceso de seguridad.

- Dicho esto, en el ámbito de la normalización voluntaria hay instrumentos disponibles de posible aplicación a la citada gestión continuada de la seguridad, tales como la norma UNE ISO/IEC 27001 que, en resumen, especifica un sistema de gestión certificable; aunque tal certificación no es obligatoria en el Esquema Nacional de Seguridad.
- Por otra parte, la norma UNE ISO/IEC 27002 especifica un conjunto de controles de seguridad para sistemas de información genéricos, en su origen orientado al ámbito comercial.
- Si bien hay coincidencias entre el Esquema Nacional de Seguridad y la norma UNE ISO/IEC 27002, las medidas de seguridad del primero se han seleccionado y estructurado atendiendo a las condiciones y necesidades de las Administraciones Públicas, incorporando un mecanismo de proporcionalidad para racionalizar la implantación de las medidas de seguridad. No obstante, la Guía 804 - Medidas de implantación del Esquema Nacional de Seguridad de la serie CCN-STIC, a la fecha en estado de borrador, contempla una tabla de correspondencias entre las medidas de seguridad del Anexo II del Esquema Nacional de Seguridad y los controles de la norma UNE ISO/IEC 27002.