Resumen de la entrevista realizada a Paloma García (Asociación Española de Normalización, UNE) el 5/6/2017

*(El siguiente artículo es un extracto de la entrevista realizada por el CPIICM a **Paloma García López de la Asociación Española de Normalización, UNE**, sobre normalización y estándares que puedan afectar a la profesión de Ingeniería Informática. No pretendemos dar una exposición detallada, sino simplemente ayudarnos a comprender algunos aspectos básicos que a menudo nos resultan lejanos a los perfiles técnicos).*

…

CPIICM - … y hablando de normas y estándares, ¿Podrías decirnos cuál es la diferencia?

PG -- Básicamente una norma y un estándar vienen a ser lo mismo, y lo importante es señalar

que es un "acuerdo entre partes, con un amplio reconocimiento, fruto del consenso a nivel de país, y publicado por un organismo de normalización reconocido", lo cual es garantía de su transparencia y legitimidad. La Asociación Española de Normalización, UNE, es la entidad legalmente responsable del desarrollo de las normas técnicas en España, poniendo a disposición del tejido económico uno de los catálogos más completos del mundo, con más de 32.000 normas con soluciones eficaces al alcance de todos. Las partes que normalmente intervienen en la generación del acuerdo (norma) suelen ser el conjunto de todas las organizaciones y entidades (públicas, privadasy académicas, entre otras) afectadas por su contenido y que por lo tanto tienen algo que decir al respecto. En España, más de 12.000 expertos expertos participan cada año en la elaboración de normas técnicas en alguno de los 215 Comités Técnicos de Normalización de UNE, bajo los principios de consenso, apertura y transparencia.

Las normas son de adopción voluntaria. En algunos casos, se vuelven obligatorias cuando el legislador, convencido de su conveniencia, las utiliza como documentos de referencia para cumplir una determinada regulación, o por ejemplo para la contratación pública.

CPIICM.- Y de cara los profesionales, en concreto a los titulados e ingenieros en informática, ¿Dónde pueden encontrar las normas que les atañen y por cuales deben preocuparse?

PG – Hay infinidad de normas, es importante conocer que hay 3 tipos que pueden ser herramientas de conocimiento y ayuda a la profesión: Hablando en general, existen básicamente tres tipos de normas:

Normas sobre terminología y fundamentos de un sector o actividad determinados.

a) **Normas de especificación y requisitos técnicos**: son las que hacen referencia por ejemplo a todo lo que tiene que ver con requisitos o especificaciones, en el caso delas

TIC, por ejemplo las de ingeniería SW, la arquitectura o realización de pruebas SW, o la evaluación del producto, y modernamente por ejemplo lo relativo a la impresión 3D…

b) **Normas de sistemas de gestión**: que tienen como finalidad guiar y ayudar en los procesos de control interno de una organización a la hora de elaboración del producto o servicio que vamos a ofrecer. Éstas son por ejemplo importantes en la contratación pública. Tenemos por ejemplo la conocida norma ISO 9001 sobre gestión de la calidad , la 14001 de gestión ambiental o la 27001, gestión de la seguridad de la información, , etc.

Junto a esta clasificación podemos añadir las:

c) **Normas legales**: aquellas que son obligatorias porque así lo establece el regulador en el desarrollo de la legislación de un determinado ámbito.

También debemos conocer que existen las **normas armonizadas**, que son aquellas que dan presunción de conformidad a directivas europeas, y normalmente incluyen en sí mismas definición de ensayos y metodologías de forma que cuando una organización dice que las cumple tienen presunción de conformidad y no se necesita una acreditación de un tercero (aunque lo que realmente da garantía de cumplimiento es la evaluación por un tercero, un laboratorio, un organismo de certificación…).

En lo que respecta a temáticas concretas podemos hablar de comités con actividad en ámbitos como CLOUD COMPUTING, BIGD DATA, INTERNET Of THINGS, INDUSTRIA CONECTADA, SMART CITIES o BLOCKCHAIN

CPIICM.- ¿Y que diferencia hay entre una norma "certificable" y una que no lo sea?

PG -- La diferencia es que las normas que pueden ser certificables son aquellas que establecen **requisitos a cumplir** que se pueden verificar de forma objetiva. Estas normas nos dicen lo que se "**debe**" implementar para estar de acuerdo con ellas.

Las normas "no certificables" simplemente nos dicen lo que "**deberíamos**" hacer o tener en cuenta, pero no nos proporcionan requisitos medibles.

Para poder acreditar el cumplimiento de una determinada norma hay que seguir un proceso de evaluación de la conformidad, el cual puede ser de varios tipos en función del caso:

a) De 1ª parte: realizado mediante una auditoría interna en la organización.
b) De 2ª parte: cuando lo hace por ejemplo el propio cliente del producto o servicio.
c) De 3ª parte: es lo que realmente se conoce como "**certificación**", y lo debe hacer un tercero reconocido y acreditado para hacerlo. La entidad encargada en España de reconocer a estos posibles certificadores es ENAC, y la legislación aplicable es el *"Real*

Decreto 2200/1995, de 28 de diciembre, por el que se aprueba el Reglamento de la Infraestructura para la Calidad y la Seguridad Industrial" (https://www.boe.es/buscar/act.php?id=BOE-A-1996-2468)

CPIICM.- ¿Cómo podemos los profesionales manejar adecuadamente las normas y cuáles son las que debemos conocer?

PG – En general las normas siempre nos dicen el "qué" debemos hacer, pero no "como" hacerlo, salvo algunas normas armonizadas que sí lo hacen y ya hemos mencionado.

Por ello existen multitud de metodologías que nos pueden ayudar a cumplir con las normas. También existen normas que son guías de aplicación o informes técnicos que nos ayudan a saber cómo podemos estar de acuerdo a una determinada normativa para el caso concreto de un sector o una disciplina.

En estos momentos por ejemplo se está trabajando a nivel nacional y europeo en todo lo relativo a la ciberseguridad y privacidad, y en particular en lo relacionado al nuevo reglamento sobre protección de datos (RGPD). Por ejemplo, la Norma UNE-EN ISO/IEC 27001 que establece los requisitos para desarrollar un sistema de gestión de la Seguridad de la Información en las organizaciones.

Un profesional de la ingeniería informática por supuesto debería conocer al menos los estándares internacionales y nacionales que se aplican a su ámbito de trabajo, saber dónde se encuentran las normas y como acceder a ellas, y disponer de un sistema de seguimiento de las mismas, y en qué forma se utilizan, es decir, cuales son susceptibles de certificación o evaluación, etc.

No deberíamos olvidar nunca el componente de conocimiento y capacidad de gestión que aporta el ser capaz de implementar y llevar a la práctica los estándares que nos afectan al ejercicio profesional, y de hecho en algunos entornos esto es ya una competencia más a destacar en el CV del ingeniero.

CPIICM.- Muchas gracias, el tema da para mucho más, y ojalá podamos continuar charlando al respecto en el futuro. Desde el CPIICM queremos agradecer encarecidamente a Paloma García y Gustavo Granero su atención y disponibilidad en esta colaboración.