

OCDE: hacia una cultura de seguridad

Debido a los avances registrados en las tecnologías de la información y las comunicaciones, y también al modelo y generalización de uso de los sistemas de información y redes, la OCDE (Organización para la Cooperación y el Desarrollo Económico) ha revisado la primera edición de sus Directrices para la Seguridad de la Información y de las Redes, vigente desde 1992.

El nuevo documento (hay un enlace al mismo en el web del MAP), aunque no vinculante, es sin embargo producto del consenso entre los países miembros de la OCDE, y en su elaboración han participado representantes de la industria TI, de los usuarios empresariales y de otras organizaciones.

Las Directrices están enfocadas al desarrollo de una «Cultura de Seguridad» (así se titulan) en las administraciones públicas, las empresas y los particulares, cada colectivo en función de sus responsabilidades. La finalidad es la reducción del riesgo en un mundo interconectado.

A tal fin se han establecido los siguientes nueve principios: concienciación, responsabilidad, actuación cooperativa frente a incidentes de seguridad, conducta ética, compatibilidad entre la seguridad de los SI y las redes, y los valores esenciales de una sociedad democrática, evaluación del riesgo, diseño e implantación de seguridad, administración de seguridad y revisión.

La cooperación política, normativa y técnica entre los países miembros de la OCDE (y otros), basada en estos principios superestructurales, sería muy beneficiosa para todos: sector público, privado y ciudadanos, y especialmente para el ramo de seguridad TIC, a cuyo mercado se está dotando de fundamentos de peso.

Protección de datos personales

La OCDE no ha sido la única organización que ha tenido que revisar documentos para evitar su obsolescencia. Así, el 12 de julio se publicó la esperada Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), que deroga y sustituye a la Directiva 97/66/CE, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, que complementaba a la Directiva 95/46/CE.

Queda claro que la consolidación de Internet en la mayoría de países avanzados (en el nuestro, aunque nos duela, estamos aún en vías de desarrollo, porque nos faltan usuarios de la Red, que es lo peor que puede pasar) está propiciando renovaciones legislativas importantes. Esta Directiva es una prueba fehaciente de ello.

Firma electrónica

El 26 de julio se publicó en el web del Ministerio de Ciencia y Tecnología un nuevo borrador de anteproyecto de ley de firma electrónica, más pulido que el anterior (acreditación voluntaria, constitución de garantía por parte de los PSC que emitan certificados reconocidos...), y en el que se mantienen, entre otras, dos novedades: las bases para la regulación del DNI Electrónico y la emisión de certificados a nombre de personas jurídicas.

Con independencia de que el proyecto de DNI Electrónico, pionero en el mundo, pudiera despegar más ampliamente a finales de año o principios del que viene, y sin entrar en polémicas sobre la diferencia entre autenticación y firma, hay que reconocer que tras la ya mítica iniciativa de la AEAT (presentación telemática de la declaración de la renta, entre otros impuestos), se necesita un nuevo hito para la implantación de la firma electrónica en España. Se necesita, por tanto, el DNI Electrónico. No es la única razón, pero sí una de las más importantes.

Además –y como indica un gran experto español en seguridad y protección de la información, que representa a nuestro país en foros internacionales–, algo está cambiando en las sensibilidades europea y norteamericana en lo concerniente al registro de identidad de las personas y a la verificación de su identidad en el contexto telemático. Parece que se está pasando de la liberalización más descarnada (cualquiera que cumpla una serie de requisitos puede realizar estas misiones) a una posición, digamos, más restrictiva. De ser así, no pocos PSC deberán reconsiderar sus estrategias de futuro. |