ISO–27001, ¿y las AA.PP.?

NO HAY DUDA DE QUE ESPAÑA ESTÁ HACIENDO BIEN LOS DEBERES EN CUANTO AL AVANCE DE SUS SISTEMAS DE INFORMACIÓN, PERO FALTA IMPLANTAR LA NORMA DE SEGURIDAD POR EXCELENCIA

Alejandro Corletti
DIRECTOR DIVISIÓN SEGURIDAD INFORMÁTICA
NCS

Carmen de Alba Muñoz
RESPONSABLE ISO-27000
NCS

Desde que empezamos hace tiempo a asistir a los encuentros Dintel y algunos otros, nos está llamando la atención las exposiciones de Organismos Públicos. Evidentemente, no hay duda de que España está haciendo bien los deberes en cuanto al avance de sus Sistemas de Información. La Administración Pública está incorporando de forma adecuada la tecnología a sus procesos, los trámites ciudadanos son cada vez más ágiles e integrados, los procesos funcionan, la Agencia Tributaria conoce hasta el menú que comemos en casa, la Justicia incorpora nuevos métodos para sus pleitos y hasta ya tenemos el DNI electrónico, etc., pero... con total sinceridad, la palabra "seguridad" es de las que menos se escucha. No creemos que se esté dejando de lado, pues hay hechos que demuestran que no es así, pero... cuando la "seguridad" se la tiene presente en todo desarrollo, sale a la luz permanentemente, cosa que no está sucediendo.

Tanto sale a la luz, que por ejemplo la **Ley 11** del 22 de junio de 2007 **"Acceso electrónico de los ciudadanos a los Servicios Públicos"**, la menciona cuarenta y dos veces. Desde el Objeto mismo hace referencia en el punto 2. *"Las Administraciones Públicas utilizarán las tecnologías de la información de acuerdo con lo dispuesto en la presente Ley, asegurando la disponibilidad, el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias"*, así le sigue asignando relevancia a lo largo de sus diecisiete folios.

> Cuando la "seguridad" se la tiene presente en todo desarrollo, sale a la luz permanentemente, cosa que no está sucediendo

Otra regulación en cuanto a AA.PP. es la ***"Resolución de 26 de mayo de 2003, de la Secretaría de Estado para la Administración Pública"***, por la que se dispone la publicación del Acuerdo del Pleno de la Comisión Interministerial de Adquisición de Bienes y Servicios Informáticos, de 18 de diciembre de 2002, por el que se aprueban los Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas por la Administración General del Estado en el ejercicio de sus potestades. Esta regulación es tan específica en sus párrafos que expresa textualmente *"la Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones sobre seguridad de las redes y de la información: insta a los Estados miembros a fomentar el uso de mejores prácticas basadas en instrumentos existentes, tales como la norma* **UNE ISO/IEC 17799** *'Código de buenas prácticas para la gestión de la seguridad de la información', que constituye un término de referencia fundamental de los criterios y recomendaciones incluidos en este documento"*. Esto lo menciona en la Propuesta para un enfoque político europeo. Se debe considerar que para esa fecha aún no existía la ISO–27001, por eso se hace referencia a su antecesora.

Por otra parte, dentro de la misma ley, en su ***"Estructura y contenidos"*** se describen los diecinueve capítulos que la componen: *"Gestión Global de la Seguridad de la Información, Política de Seguridad, Organización y Planificación de la Seguridad, Análisis y Gestión de Riesgos. etc".* Son exactamente lo que comprenden los once grupos de la ISO–27001 y su análisis de riesgo.

Siguiendo con la Unión Europea, desde el año 97, la ***"Directriz VI/661/97 rev. 2 CE"*** sobre la ***"Seguridad de la Información de los Sistemas de Información de los Organismos Pagadores"***, exige la necesidad de garantizar la seguridad de la información. Se establece que los organismos pagadores deberán basar la seguridad de sus sistemas de información en los criterios establecidos en una versión aplicable de una de las normas siguientes, que gozan de aceptación internacional: Organización Internacional de Normalización 17799/Norma británica 7799: *'Code of practice for Information Security Management'*.

Podríamos también hacer referencia a su versión más reciente que es el ***"Reglamento (CE) Nº 885/2006 de la Comisión"***, de 21 de junio de 2006 por el que se establecen las disposiciones de aplicación del Reglamento (CE) nº 1290/2005 del Consejo en lo que se refiere a la autorización de los organismos pagadores y otros órganos y a la liquidación de cuentas del FEAGA (Fondo Europeo Agrícola de Garantía) y del FEADER (Fondo Europeo Agrícola de Desarrollo Rural). En su ANEXO I – CRITERIOS DE AUTORIZACIÓN – 3. Información y comunicación – B) Seguridad de los sistemas de información, también expresa textualmente: *"La seguridad de los sistemas de información estará basada en los criterios fijados en una versión aplicable en el ejercicio financiero considerado de una de las siguientes normas aceptadas internacionalmente: i) Organización Internacional de Normalización 17799/Norma británica 7799: Code of practice for Information Security Management (Código de prácticas para la gestión de la seguridad de la información) (BS ISO/IEC 17799)"*.

En este tema hay que anotarle un punto a la **Consejería de Agricultura y Agua de la Comunidad Autónoma de Murcia**, que, conociendo estas regulaciones, apostó por la ISO–27001 **y acaba de ser la primera Entidad Pública Española en certificarse** (¡muy bien, así se hace!), eso se llama ser vanguardista (y sobre todo astuto). La UE establece una serie de requisitos para la concesión de ayudas, vieron la necesidad, una regulación, y obraron de acuerdo a lo que el mundo les exigía... y lo lograron.

Por su parte, el Ministerio de Administraciones Públicas, a través del consejo Superior de Informática y para el empleo de la Administración Electrónica, el 24 de junio de 2004, también publicó sus ***"Criterios de Seguridad"*** exponiendo los requisitos, criterios, y recomendaciones relativos a la implantación de las medidas de seguridad, organizativas y técnicas, en el diseño, desarrollo, implantación

Comentario: Nos encantaría que en los próximos eventos y publicaciones, podamos empezar este 2008 con ISO–27001 como una palabra que figure cotidianamente en el léxico de las AA.PP., de esta forma le estaremos deseando a los SS.II. un próspero año nuevo, sobre todo con mayor Paz para sus contenidos y aplicaciones.

y explotación de las aplicaciones **cuyo resultado sea utilizado para el ejercicio por los órganos y entidades del ámbito de la Administración General del Estado** de las potestades que tienen atribuidas. Dentro de este documento, reitera una vez más ***"Propuesta para un enfoque político europeo"*** que *"insta a los Estados miembros a fomentar el uso de mejores prácticas basadas en instrumentos existentes, tales como la norma* ***UNE ISO/IEC 17799*** *'Código de buenas prácticas para la gestión de la seguridad de la información', que constituye un término de referencia fundamental de los criterios y recomendaciones incluidos en este documento"*.

Existen otras iniciativas para fomentar la seguridad en España a través de la norma ISO–27001, como el proyecto PYMETICA en Andalucía, el

> No existe una determinación clara y precisa por parte del Estado de abordar esta norma

CAMERSEC en Málaga, por su parte INTECO hace su esfuerzo en León, pero no existe una determinación clara y precisa por parte del Estado de abordar esta norma. Aunque por ejemplo RENFE, en un pliego de licitación que venció en septiembre de 2007, ya hacía mención al estándar ISO–27001. (Esto corrobora el hecho del "Lobby" que pueden hacer las empresas certificadas, tal cual mencionamos en artículos anteriores).

Es triste que esta determinación estatal no se haga manifiesta. Pero volviendo al inicio de este texto, no nos debería llamar la atención, pues "seguridad", no es una palabra que suene en sus discursos. Y si empezara a sonar, a esta altura de la vida, no puede ser de otra forma que bajo los "armónicos" de **ISO–27001**, pues hacia allí va todo el mundo, lo recalca la Unión Europea, y hasta las regulaciones españolas, así que no cabe otra "melodía" que la de este estándar.

No nos gustaría dejar latente este triste mensaje en los lectores. Este texto no es una recriminación, **es un humilde y sincero llamamiento de atención a las AA.PP.** por parte de gente que viene evaluando y trabajando con esta norma, la vive de cerca y está convencida que es el mejor camino. Para ello basta con mirar las tendencias mundiales, las leyes y regulaciones que mencionamos, que son sólo algunas. **El presente y futuro en Seguridad se llama ISO–27001** (es el único camino)**, y las AA.PP. están obligadas a asumirlo**. Es una cuestión de astucia hacerlo antes o después, como lo hicieron en Murcia. Y por supuesto de costes, pues cualquiera que lleve algún tiempo en esta viña del Señor, sabe perfectamente que si la seguridad no se piensa desde el vamos, luego cuesta el triple o más, es decir, **HOY** las **AA.PP.** deben comenzar a ser motores de este estándar en España, es la mejor forma de hacer las cosas como es debido, y de impulsar las nuevas tecnologías hacia un futuro correcto. Pero sobre todo de ofrecer a sus ciudadanos un Sistema de Gestión de la Seguridad de SU Información (SGSI), pues en definitiva, todo servidor público en estos temas, no hace más que velar por la mejor forma de "cuidar" de nuestra información.