III FORO DATA PRIVACY INSTITUTE

Problemas actuales de la privacidad y la seguridad de la información

"la *identidad* es el elemento clave para entender el futuro de internet"

- **En el marco de la web 2.0 el individuo ha pasado de ser un receptor pasivo de información a emitir información activamente, de allí que la identidad sea un elemento clave para entender el futuro de Internet.**

- **Las organizaciones tienen el reto de definir lo que se considera "uso razonable" de los medios informáticos de la empresa para así delimitar la "expectativa de privacidad" del trabajador en su entorno laboral.**

- **La aparición del Cloud Computing implica un cambio en la forma de gestionar los riesgos de seguridad y cumplimiento normativo en las organizaciones.**

- **La privacidad no es viable sin una estrategia en seguridad de la información.**

- **Las certificación Certified Data Privacy Profesional (CDPP) está aportando a las organizaciones, ciertas garantías sobre el nivel de conocimientos en materia de privacidad.**

Madrid, 11 de noviembre de 2010.- Bajo el título ***Problemas actuales de la Privacidad y de la Seguridad de la Información,*** el **Data Privacy Institute (DPI)**, celebró el pasado **3 de noviembre** su tercer foro donde los expertos abordaron temas tan importantes como el Impacto del Cloud Computing en la privacidad; la Seguridad de la información en el sector sanitario; el uso privado de los medios informáticos por parte de los trabajadores en las organizaciones, entre otros.

El evento aglutinó a expertos y profesionales en privacidad de organizaciones públicas y privadas, representantes de la Agencia Española de protección de Datos (AEPD), el Consejo General de Colegios de Médicos de España, el Servei Català de la Salut, el Servicio Madrileño de Salud, y de empresas como Bankinter, Check Point y Grupo FCC; así como algunos de los primeros Certified Data Privacy Professionals, que debatieron sobre los retos de los profesionales del sector.

El foro comenzó con una llamada de atención sobre el nuevo paradigma al que asiste la Sociedad de la Información: Ricard Martínez Martínez, Coordinador del Área de Estudios de la Agencia Española de protección de Datos (AEPD), señaló el concepto de *identidad* como el elemento clave para entender el futuro de Internet: "el individuo ha pasado de ser un receptor pasivo de información a emitir información activamente." Para Martínez, el reto es la gestión

de la identidad y la necesidad de identificar a los sujetos en Internet. Martínez incidió en las cuestiones que afectan a los menores y resaltó la existencia de un "reto normativo" en este sentido que les proteja de riesgos asociados a "supuestos amigos, que no son ni amigos ni menores".

La AEPD, en palabras de Martínez, ha insistido en la formación y la creación de espacios educativos para los menores a la hora de utilizar las nuevas tecnologías.

Esta necesidad de formación fue también apuntada por Antoni Bosch, Director de Data Privacy Institute (DPI), quien aseguró que "en la actualidad se dispone de más datos, aunque no de mayor información".

Uso privado de los medios informáticos por parte del trabajador en la empresa

Con relación a este particular, Ricard Martínez, centró su discurso en un aspecto clave como "la expectativa de privacidad del trabajador". El trabajador debe poder responderse a cuestiones tales como "¿se me permite consultar el periódico online o se van a rastrear mis consultas en Internet?". Los controles por parte de la empresa son necesarios, pero ésta debe previamente definir el ámbito de los mismos y trasladárselo al empleado para su conocimiento. Asimismo, añadió que la empresa u organización deberá tener en cuenta la proporcionalidad del control en función del tipo de puesto de trabajo y definir qué es "secreto de las comunicaciones" en el seno de la misma.

La confianza de los pacientes: una cuestión de seguridad y privacidad

Juan José Rodríguez, presidente del Consejo General de Colegios de Médicos, enfatizó la necesidad de una regulación específica que garantice la privacidad de la información clínica. "La confidencialidad de la información es una de las claves de la relación con el médico y el paciente debe saber que se va a respetar" aseguró.

En este sentido, para Anna García Martínez, responsable de los sistemas de información para la evolución de servicios sanitarios del Servei Català de la Salut, la utilización de medidas como los Certificados Digitales, confieren una percepción de transparencia y seguridad para el ciudadano en el acceso a su información clínica.

Para Joan Camps, director de Proyectos y de la Unidad Tecnológica del Consejo General de Colegios de Médicos, la problemática reside en el hecho de que la información médica se encuentre repartida entre diferentes entidades, como mutuas, clínicas privadas o el Sistema Público de Salud, y considera que "la meta tiene que ser que el profesional pueda acceder a toda la información dispersa en diferentes entidades".

La implantación de estándares para la gestión de la seguridad de la información fue otro de los temas tratados en este apartado del Foro. Todos reconocieron la importancia de los estándares, si bien, José Manuel Laperal, responsable de Seguridad e Innovación Tecnológica del Servicio Madrileño de Salud, comentó que la

heterogeneidad existente, hace necesaria la puesta en marcha de estándares propios que permitan afrontar necesidades particulares de los distintos servicios de salud.

¿Privacidad versus seguridad?

La armonización de las políticas internas de privacidad y seguridad en las organizaciones fue también tema discutido en el Foro, donde los participantes expusieron sus experiencias profesionales al respecto, dejando de manifiesto que la privacidad no es posible sin la seguridad de la información que manejan las organizaciones. En este sentido, se aludió al Data Loss Prevention (DLP), como una herramienta útil para disminuir el número de incidencias en materia de fugas de información cuya implantación se debe alinear con la privacidad de los trabajadores.

Julio San José, gerente de Seguridad de Bankinter, puntualizó la importancia de educar a los usuarios como parte del proceso, para lograr un sistema que garantice la privacidad y la seguridad de la información. Por otro lado, Miguel Cebrián, gerente de Riesgo y Cumplimiento normativo del Grupo FCC, reconoció que existen diferentes grados de monitorización y que es fundamental hacer entender al empleado la necesidad de estos controles. Según Cebrián, "la privacidad no es viable sin una estrategia en seguridad de la información". En la misma línea, Adolfo Hernández, Governance, Risk & Compliance manager de Écija, manifestó que el empleado debe entender y aplicar el "uso razonable de los sistemas de información", pero es la empresa la que tiene que marcar los criterios y directrices para que esto sea posible.

A juicio de los participantes, los escasos recursos económicos de algunas empresas a la hora de implantar sistemas de protección de la información que sean acordes con su negocio no es obstáculo para llevar a cabo iniciativas en formación o utilizar recursos como ***www.protegetuinformacion.com***, el nuevo portal para fomentar la seguridad de la información, enmarcado en el Plan Avanza, y creado gracias a la colaboración entre ISMS Forum Spain y el Ministerio de Industria, Turismo y Comercio. En palabras de Miguel Cebrián, este portal, inaugurado el pasado 1 de noviembre, "es una maravillosa iniciativa para todas las empresas que no cuenten con los suficientes recursos para invertir en políticas de seguridad".

Privacidad en la nube

Carlos Alberto Sáiz, socio director del Área Governance, Risk & Compliance de Écija, vicepresidente de ISMS Forum Spain y subdirector del DPI, expuso las ventajas y los inconvenientes del Cloud Computing, señalando la reducción de costes que supone tanto para el proveedor como para el cliente que puede acceder a su información a través de una infraestructura externa. Sin embargo, explicó que en el Cloud Computing la información es "líquida" y se mueve de unos servidores a otros por todo el mundo y esto conlleva una serie de riesgos que afectan al cumplimiento normativo y a la seguridad de la información.

Sáiz considera fundamental analizar los riesgos que corre la información de cualquier empresa que contrate un servicio de Cloud Computing. Además, destaca la necesidad de que las entidades seleccionen la información que puede ser almacenada y procesada a través de este servicio en función de su sensibilidad.

El camino de las certificaciones y el CDPP

Los últimos minutos del Foro se centraron en analizar las garantías de calidad existentes en los servicios, la formación y la cualificación de los profesionales de la privacidad.

Por este motivo, ante la creciente necesidad de poder contar con profesionales cualificados en materia de privacidad, el DPI puso en marcha la certificación Certified Data Privacy Professional (CDPP), que permite aportar a las organizaciones algunas garantías sobre el nivel de conocimiento en la materia, a la hora de contratar personal interno, abogados, consultores y auditores.

Los CDPP Gonzalo Salas, senior manager del Área de Cumplimiento Normativo en SIA, Antonio Ramos, consultor independiente, y Rocío Troyano, directora de Auditoría Informática en BDO Auditores, reconocieron la gran utilidad de esta certificación en un mercado que necesita de expertos cualificados en la materia. “El DPI ha puesto sobre la mesa una herramienta para ayudar a los que tienen que tomar decisiones a que encuentren a la persona adecuada”, aseguró Salas.

Sobre ISMS Forum Spain

La creación del Foro Data Privacy Institute es el resultado de la iniciativa de ISMS Forum Spain, asociación española sin ánimo de lucro, cuyo principal objetivo es fomentar la seguridad de la información. Se constituye como foro especializado para que todas las empresas, organismos públicos y privados y profesionales del sector colaboren, intercambien experiencias y conozcan los últimos avances y desarrollos en materia de seguridad de la información.

La Asociación está respaldada por algunas de las más representativas empresas y organizaciones comprometidas con la seguridad de la información. Los socios fundadores ejercen su labor en muy diversos ámbitos que van desde la enseñanza superior y la I+D hasta la Consultoría, pasando por los sectores de Banca, Seguros, Sanitario, Construcción, Servicios Jurídicos Tecnologías de la Información o Telecomunicaciones. Hoy en día cuenta con el respaldo de más de 100 empresas y 700 profesionales asociados, lo que la convierte en la mayor red activa española de Seguridad de la Información.

Para más información:
Laura Esteban
Gabinete de Prensa ISMS Forum Spain
Tel. 91 594 18 09
laura.esteban@poweraxle.es