LLUCH CONSULTING & TRAINING, S.L.

Las 10 normas que deberían cumplirse según la AEPD

Los 10 errores típicos de una PYME en materia de seguridad

Protección de datos

Lluch Consulting & Training
01/06/2013

Las 10 normas que deberían cumplirse según la AEPD (Agencia Española de Protección de Datos)

La normativa en protección de datos la han de cumplir todas las entidades tanto públicas como privadas, los partidos políticos, comunidades de vecinos, asociaciones, fundaciones y todo tipo de entidades que traten datos de carácter personal en el ejercicio de su actividad.

Estas recomendaciones son:

1. Inscribir los ficheros de datos personales es la primera obligación de una empresa en materia de protección de datos. Es un trámite que se realiza online a través de la web de la AEPD. Qué ficheros se inscriben es decisión de cada empresa. Los más habituales son Clientes, Proveedores, Nóminas y recursos humanos, Prevención de riesgos laborales, Videovigilancia, Página web, etc.

2. Su empresa debe chequear que cumple los principios de información y consentimiento en todos sus ficheros y tratamientos de datos personales, y que estos principios se reflejan correctamente en sus cláusulas y leyendas informativas.

3. Los datos personales que contiene un fichero se clasifican en tres niveles: básico, medio y alto. Según el nivel del fichero, deberá aplicarle el nivel correspondiente de medidas de seguridad (a mayor nivel, mayor complejidad de las medidas). Las medidas las establece la normativa, y deberá tenerlas reflejadas por escrito en el Documento de Seguridad, con el que obligatoriamente deberá contar su empresa.

4. Su empresa debe informar a las personas de las que recabe sus datos del derecho que tienen a ejercer sus derechos ARCO (acceso, rectificación, cancelación y oposición). Y además debe establecer en su empresa los procedimientos adecuados que le permitan atenderlos dentro de los breves plazos que marca la ley para ello. No atenderlos o atenderlos fuera de plazo es una infracción sancionable.

5. Su empresa no necesita el consentimiento de sus trabajadores para tratar sus datos personales estrictamente necesarios para llevar a cabo la propia relación laboral, pero sí debe cumplir la obligación de información. Por lo tanto, al iniciarse la relación laboral deberá incorporar una cláusula informativa específica dentro del contrato laboral. Si no lo hubiera hecho en su momento, con sus trabajadores ya en plantilla puede firmar esa cláusula en cualquier momento posterior.

6. En las campañas promocionales que realice su empresa deberá cumplir la regla general de informar y obtener el consentimiento para crear cualquier fichero o base de datos con fines publicitarios. Y estar muy atento a atender correctamente el derecho de cancelación de quienes solicitan dejar de recibir mensajes publicitarios de su empresa (sean éstos por correo postal, correo electrónico o por teléfono).

7. Su empresa puede permitir el acceso a los datos personales de sus ficheros a los proveedores que obligatoriamente lo necesiten para prestar el servicio que su empresa ha contratado con ellos. Pero ¡atención!: para ello deberá haber formalizado un contrato de especial de prestación de servicios con acceso a datos personales. Si no lo hiciera así, el acceso del proveedor a los datos personales de los ficheros de su empresa se consideraría una cesión no consentida y tendría graves consecuencias tanto para su empresa como para el proveedor.

8. Para incluir a un cliente en un fichero de solvencia patrimonial (que tiene importantes consecuencias en su vida, como limitarle su acceso al crédito, por ejemplo), su empresa debe cumplir exquisitamente los requisitos legales que se exigen para poder hacerlo. Además, también deberá poner cuidado a la hora de comunicarse con el "moroso" para que no trascienda su condición en su entorno (por ejemplo, al dejar recados en su casa, en su trabajo, etc., nunca se debe dejar constancia en los mensajes de las cantidades que se adeudan o dar pie a que piensen que se le reclama deuda alguna al "moroso").

9. Una web corporativa puede estar cometiendo infracciones en la LOPD y en la LSSI (Ley de Servicios De La Sociedad de la Información y De Comercio Electrónico en varios puntos (por ejemplo, instalación de cookies sin el consentimiento del usuario, formularios de obtención de datos personales sin las leyendas informativas adecuadas…), por lo que es conveniente que chequee todos los puntos "problemáticos" y se asegure de que cumple la normativa.

10. La videovigilancia es un sistema de seguridad muy intrusivo para la intimidad de las personas. Pero eso no significa que la seguridad no sea un fin legítimo y que su empresa no pueda instalar cámaras; de lo que se trata es de hacerlo correctamente, cumplimiento bien todos los requisitos legales.

Si su empresa incumple alguna de estas 10 normas de la LOPD podría ser sancionada.

Recordamos que las sanciones económica oscila entre 900,00€ y 600.000,00€, según el actual régimen sancionador.

Los 10 errores típicos de una PYME en materia de seguridad

No cabe duda de que en los últimos años hemos avanzado mucho en Seguridad de la Información. Poco a poco, entre las empresas comienza a implantarse la idea de que la seguridad es un ámbito al que hay que prestar una atención específica e independiente, más allá de lo que muchos consideran "los informáticos". Sin embargo, si no es bueno caer en el catastrofismo, no debemos ser demasiado indulgentes: queda mucho camino por recorrer y los avances no siempre se producen a la velocidad a la que, afortunadamente para los delincuentes, serían recomendables o deseables. A diario se producen noticias de empresas u organizaciones con una fuerte inversión en seguridad cuya infraestructura tecnológica es vulnerada, lo que da una idea del desequilibrio de fuerzas existente.

En esta línea, aún persisten muchos errores y creencias que podemos identificar como los diez errores típicos de las Pymes en materia de seguridad y que marcan el camino a seguir estos próximos años.

1. Pensar que su información o sus sistemas no interesan a nadie. Este es, sin duda alguna, el principal escollo en la mejora de la seguridad de la información de una organización: pensar que no son el objetivo de nadie. Existen varios poderosos argumentos para desmontar esta creencia. En primer lugar, cualquier equipo es útil para las "botnets" o redes de "PC´s zombies" controlados remotamente, sea un PC corporativo o el portátil de un adolescente; mientras pueda controlarse remotamente puede ser utilizado, con otros miles, para divulgar "spam" o atacar sistemas. En segundo lugar, quizá nadie esté interesado en nuestros sistemas, pero un escaneo por parte de un gusano puede detectar por simple casualidad un equipo vulnerable. Por último, muchas organizaciones infravaloran el valor de su información, tanto para la competencia externa como interna: balances contables, tarifas de precios, márgenes, procesos de producción, innovaciones, etc.

2. Creer que la seguridad es sólo técnica y por tanto sólo compete a los informáticos. Limitar la seguridad a los controles técnicos, evidentemente necesarios, conduce a descuidar aspectos tan importantes como los legales y organizativos. Gestionar las incidencias, definir responsabilidades o abordar los requerimientos de carácter legal son aspectos vitales para evitar amenazas como la ingeniería social o el phishing.

3. Un antivirus y un firewall son suficientes. Este es, principalmente, el progreso con el que introducíamos esta entrada: pocas organizaciones actualmente carecen de un antivirus e incluso de un cortafuego. Sin embargo, esto conduce a una falsa sensación de seguridad que hace olvidar que existen otras muchas amenazas, tanto técnicas como no técnicas, que requieren la adopción de medidas más específicas.

4. Pensar que la seguridad es un producto y no un proceso. Este error persiste de épocas lejanas en las que la seguridad era un aspecto más dentro de las muchas tareas del personal del área de informática. Sin embargo, las cosas han cambiado significativamente y la seguridad ha adquirido un estatus propio.

Cualquier persona que trabaje en un departamento de RRHH, producción, logística o contabilidad tiene que llevar a cabo un mantenimiento diario, ya sea actualizando sus conocimientos, manteniendo los sistemas, implantando nuevos procesos o adaptando su funcionamiento a nuevos requerimientos legales; las áreas y departamentos se adaptan a los cambios constantemente. Sin embargo, la seguridad sigue considerándose un ámbito que no requiere mantenimiento o seguimiento alguno. Nada más lejos de la realidad.

5. La confidencialidad es algo de espías y grandes multinacionales. Es cierto que los espías y las grandes multinacionales firman acuerdos de confidencialidad. Y aunque a muchas empresas todavía le suenan a ciencia ficción, eso no los hace innecesarios en el ámbito de la PYME. Tanto con proveedores, clientes como con trabajadores y en definitiva cualquier persona física o jurídica que vaya a acceder a la información de la empresa, es vital firmar acuerdos de confidencialidad cuya finalidad no es otra que proteger la información de la organización. Pocas veces un esfuerzo tan pequeño trae unos beneficios tan grandes. Ni más, ni menos.

6. No contemplar la seguridad en los contratos corporativos. Hoy en día, la hoja de pedido, sin más, sigue siendo en muchos casos el procedimiento para contratar servicios. No existe un contrato de servicios ni cláusulas de confidencialidad. No se contemplan requerimientos legales como la Ley Orgánica de Protección de Datos ni se tienen en cuenta, por ejemplo, las medidas que el proveedor puede estar aplicando sobre la información que le

proporcionamos. En definitiva, la seguridad, en cualquiera de sus ámbitos, todavía brilla por su ausencia en los contratos que muchas PYME´s firman con sus proveedores y/o clientes.

7. La Ley Orgánica de Protección de Datos, esa gran desconocida. A pesar de que la LOPD lleva en marcha desde 1999 y que incluso existía un reglamento de una ley anterior que concretaba, con mayor o menor detalle, las medidas a implantar en el ámbito de protección de datos, casi catorce años después muchas empresas ignoran sus obligaciones en esta materia y algunas de las que las conocen deciden no llevar a cabo acción alguna. Ya sea por evitar sanciones o por responsabilidad social con las personas que nos confían sus datos, cualquier empresa debería adoptar las medidas necesarias para garantizar la seguridad de los datos de carácter personal de sus clientes, empleados, proveedores…

8. Mirar hacia fuera pensando que las amenazas siempre son externas. Sin ánimo de criminalizar y a pesar de lo que las noticias pueden a menudo hacernos pensar, es bien sabido en el ámbito de la seguridad que la mayor parte de los problemas de seguridad provienen de dentro de las propias organizaciones. En algunos casos, por usuarios malintencionados con los que se deben adoptar las medidas que subsanan muchos de los errores anteriores. Sin embargo, en muchos otros casos se trata de simple desconocimiento: un empleado que utiliza un USB infectado, abre un adjunto o pincha en un enlace que le llega en un correo o simplemente tira a la papelera información confidencial. En este caso, se hace imprescindible adoptar una estrategia permanente de concienciación en seguridad de la información, incluyendo al personal directivo que maneja información sensible, que evite y mitigue comportamientos peligrosos tanto para la organización como para el propio empleado.

9. Ofrecer servicios a través de Internet sin tener en cuenta su seguridad. Un servicio ofrecido a Internet es accesible virtualmente por miles de millones de personas, algunas de las cuales no tendrán desde luego buenas intenciones. Sin perder de vista los requerimientos legales necesarios (y en muchos casos bastante sencillos de cumplir) que ya hemos visto, la historia se repite una y otra vez: entre otros, servicios que contienen formularios vulnerables a ataques que ya existían hace una década o servidores web incorrectamente configurados… o directamente sin configurar.

10. Descuidar la gestión de la red y los sistemas. Por último, pero no menos importante, muchas empresas todavía descuidan de manera continuada el mantenimiento de la seguridad de sus servidores y redes, lo que conduce a dispositivos de red vulnerables, puntos WiFi que permiten a una persona al otro lado de la calle acceder a nuestra red corporativa, bases de datos de uso interno accesibles desde Internet, o servidores sin actualizar desde hace años. Sin entrar en que esto además conduce a la ignorancia más absoluta sobre lo que sucede en las infraestructuras de la organización, donde un intruso puede por tanto campar a sus anchas. El resto queda a la imaginación.

Este decálogo de errores típicos, más habituales de lo que cabría pensar, podría sin duda ser completado con muchos otros problemas más específicos que las Pymes cometen a diario. Sin embargo, si en unos años pudiésemos tachar al menos la mitad de estos errores, ya habríamos avanzado mucho en la seguridad de nuestras empresas.