



Pag. 1

¿Y cuánto cuesta?

Pag. 2

Llamadas de
publicidad y LOPD
versus LSSI-CE

Pag. 2

Como usar el correo
electrónico, con
garantías legales.
Email y LOPD

¿Y cuánto cuesta?

¿Qué pasa cuando se pierde el portátil, el móvil o el dispositivo USB? ¿Cuanto cuesta perder datos? La **pérdida de datos** cuesta el tiempo que perdemos de vista nuestro dispositivo: segundos. Y esa pérdida genera un impacto con un coste, que suele ser siempre muy elevado, aunque al final el conformismo y el que le vamos a hacer o el no podemos hacer ya nada, solapan los costes asociados de la pérdida y los convierte en inexistentes.

Ante la pérdida de un equipo asociamos los costes únicamente al coste del elemento resumido con un "me han robado el portátil, necesito uno nuevo, mi presupuesto es de 1.000 euros para reponer el equipo y seguir trabajando".

El coste de la pérdida de un elemento que contiene información es el mismo que el **valor de la información** contenida, mas el coste del dispositivo. Y la suma da un total cuantificable previamente pero muy difícil de cuantificar posteriormente.

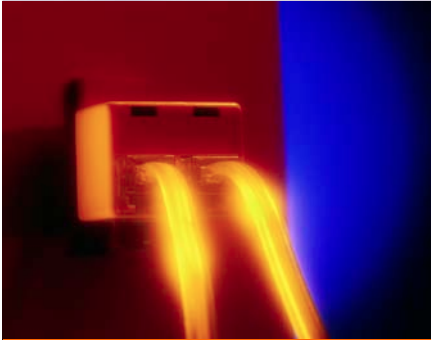
Al coste del equipo hay que añadir el coste de la pérdida de confianza de los clientes si los datos perdidos contenían información de clientes.

El coste de notificación si teníamos almacenada información de tarjetas de crédito o números de cuentas bancarias, es un coste de tiempo, siempre que no hayamos sido víctimas de un delito de sustracción económico.

También hay que añadir el coste que supone dejar de trabajar un tiempo no solo sin nuestro equipo si no también sin la información, el coste de recuperación de la información siempre que tengamos copias de seguridad existe y el coste de rehacer la información para dejarla en el mismo estado que la teníamos el ultimo momento que trabajamos, tiene un valor.

Añadiremos el coste de una o varias personas para que puedan acceder a recuperar y reconstruir el equipo, ya sea sincronizando de nuevo el teléfono móvil con el correo y traspasando nuestra información o volcando datos de nuestra agenda de contactos o recuperando la ultima copia de seguridad que habrá que comprobar si tiene toda la información o le faltan datos que deberemos rehacer. El impacto de la pérdida de un dispositivo no es trivial, si los datos contenidos son revelados y publicados habrá que añadir el coste de la posible sanción de la agencia de protección de datos por no haber sometido la información al nivel de seguridad y formación al usuario que le corresponde.

Y todo ello, excepto el coste asociado al propio dispositivo, podría haber sido quizás no evitado, pero si minimizado con tres elementos unidos, sea cual sea el tamaño de la organización propietaria de la pérdida: una correcta implantación de la LOPD a todos los usuarios de la empresa, acompañada de elementos físicos de seguridad como son la encriptación y DLP: las protecciones que permiten bloquear los movimientos de la información y evitar extraerla cuando no se trata de una persona autorizada a ello.



Llamadas de publicidad y LOPD versus LSSI-CE

El artículo 30 de la ley de protección de datos establece que, cuando no se cuenta con un consentimiento inicial para la utilización de los datos personales del receptor de la llamada comercial, esos datos solo pueden provenir de fuentes accesibles al público. De este modo, en cada llamada deberían decirle al receptor de dónde han obtenido sus datos, quién es la entidad responsable de la

llamada y el derecho que tiene a oponerse a que sigan usando sus datos.

Ciertamente, en la práctica no suelen cumplirse esas normas, y el modo más inmediato de librarse del acoso suele ser o no coger el teléfono o colgar el mismo inmediatamente.

Pero existe otra posibilidad, informarse de qué empresa es la que va a

facturar el producto o servicio. Obtenida esa información, hay que advertir al interlocutor de que presentaremos una denuncia a la Agencia Española de Protección de Datos (AEPD) por no haberle informado de sus derechos.

Para cualquier consulta o dudas se puede poner en contacto con nuestras oficinas.

Cómo usar el correo electrónico, con garantías legales. Email y LOPD

El uso del correo electrónico en las empresas y en el día a día es fundamental. Sin duda ha pasado a ocupar, junto con el teléfono móvil, un lugar en las comunicaciones privilegiado.

Sin embargo debemos tener en cuenta una serie de medidas para que no vulneremos ciertos aspectos normativos.

El primero de ellos hace referencia a la necesidad de incorporar una cláusula de protección y confidencialidad que nos ayude a informar las personas destinatarias de nuestros emails, del uso que pueden hacer de la información que les suministramos y del empleo que haremos de los datos que nos hayan podido suministrar. El segundo aspecto sin duda, afecta a nuestra agenda de contactos. Debemos ser muy conscientes de que las cuentas de correo electrónico que tenemos de las demás personas, son al fin y al cabo, datos personales que disponemos y debemos salvaguardar con el mismo recelo que cualquier otro dato del que dispongamos de terceras personas.

Respecto al envío de correos electrónicos a varios destinatarios, la Agencia Española de Protección de Datos ha emitido varias resoluciones dejando clara su postura y las medidas de salvaguardia que debemos adoptar. El correo electrónico que permite la identificación o hace identificable a una persona física, es un dato personal, esto es, cuentas de correo compuestas de nombre y apellidos – nombreakellidos@cuenta.es – y por ello deben adoptarse las medidas de seguridad que prescribe la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal. El acceso y comunicación de datos personales de terceros queda sometido a la normativa, por lo que sólo con la autorización "expresa e inequívoca" dada por su titular se podrá realizar el tratamiento de sus y la comunicación a terceros.

Es muy común incluir en correos electrónicos varios destinatarios, que bajo el campo "para" pueden visualizar el resto de personas que reciben la información que remitimos. Esta práctica tan habitual, es sin duda la manera más común de difundir datos personales por lo que se está incurriendo en una vulneración de la norma legal. Su corrección es sencilla, emplear el campo "CCO" evitando que se visualicen las cuentas de correo a las que se envía en correo electrónico. En caso contrario estaremos incurriendo en una infracción, tipificada como tal en la normativa de protección datos –Artículo 44.2.e) de la Ley 15/1999–, cuya sanción podría oscilar entre los 600 € y los 3000 €, por accesos in consentidos a la información personal vulnerando el deber de secreto del Artículo 10 de la Ley 15/1999.