20190809, Nota Informativa, Sobre las recomendaciones de la Agencia Española de Protección de Datos para el periodo de vacaciones.

En cumplimiento de mis funciones, seguidamente le traslado una serie de recomendaciones sobre el uso de dispositivos móviles en periodo de vacaciones, publicadas por la Agencia Española de Protección de Datos.

Se debe recordar que los dispositivos móviles almacenan información privada (no sólo del usuario del dispositivo, sino también de sus contactos y allegados) que debe protegerse. Uno de los principales motivos para proteger los dispositivos móviles es salvaguardar información personal y la de aquellas personas con las que se establezcan comunicaciones: contactos, fotografías, vídeos, correos electrónicos, etc., y que no nos gustaría perder o que llegaran a manos de terceros.

En primer lugar, la AEPD hace hincapié en que, en el caso de compartir en las redes sociales cualquier tipo de información, se debe comprobar si lo que se comparte puede comprometer su cumplimiento con la normativa vigente sobre Protección de Datos. En concreto, se recomienda que no se comparta información sobre su localización y que, dado que los códigos de billetes y tarjetas de embarque contienen datos personales, se debe evitar su publicación.

A fin de evitar que se compartan datos sensibles, privados o confidenciales, se debe evitar acceder a redes WIFIs abiertas o públicas, sobre todo cuando se vaya a acceder a servicios de bancos online o realizar compras online. Igualmente, se debe evitar acceder a cuentas protegidas mediante usuario y clave cuando se haga uso de esas redes. Esto se debe a que las redes WIFI públicas (aeropuertos, cafeterías, bibliotecas, etc.) pueden no ser seguras ya que, o no cifran la información que se transmite a través de ellas, por lo que cualquier usuario conectado con ciertos conocimientos podría hacerse con ella, o

porque desconocemos quién está conectado a esa misma red y con qué fines

En caso de que se utilicen ordenadores compartidos, se recomienda el uso de ventanas de incógnito del navegador, que no se guarden contraseñas y que, cuando se termine el uso de los mismos, se cierren todas las sesiones que se hayan abierto.

Por último, dado que siempre existe el riesgo de robo o pérdida de los dispositivos móviles, se recomienda que se utilice un sistema de patrón o clave para desbloquearlos. Además, la AEPD estima que se debe hacer una copia de seguridad de la información que contienen sus dispositivos. Se debe hacer uso de herramientas de seguridad que te ayudarán a localizar el dispositivo, bloquearlo e incluso eliminar la información almacenada en él.

Como conclusión, se recomienda que cuando se haga uso de los dispositivos móviles se tenga en cuenta la importancia de los mismos y su conexión con la protección de datos. Se entiende que el deber de responsabilidad proactiva se cumple si se siguen las recomendaciones previamente expuestas así como aquellas otras que se hayan proporcionado en previas notas informativas.

Hecho, conforme a mi leal saber y entender, en Manilva a 9 de agosto de 2019.

ZOTANO SANCHEZ SALVADOR - 32028277H

Firmado digitalmente por ZOTANO SANCHEZ SALVADOR - 32028277H
Fecha: 2019.08.09 19:18:10 +02'00'