09/05/2023

La AEPD, ISMS Forum y APEP publican unas orientaciones para validar el cifrado como medida de seguridad de los datos personales

• El documento aborda cómo evaluar si esta técnica está adecuadamente implementada en los tratamientos de datos personales • La mitad de las brechas de datos personales notificadas ante la Agencia el mes pasado se debieron a exfiltración de datos, pérdida



(9 de mayo de 2023). La Agencia Española de Protección de Datos (AEPD) ha publicado, en colaboración con la Asociación Española para el Fomento de la Seguridad de la Información (ISMS Forum) y la Asociación Profesional Española de Privacidad (APEP), la guía Orientaciones para la supervisión de sistemas criptográficos como medida de seguridad en protección de datos.

El cifrado es un procedimiento mediante el cual una información se transforma en un conjunto de datos aparentemente ininteligible mediante diversas técnicas. El Reglamento General de Protección de Datos lo menciona como una **medida que forma parte de las condiciones para la conformidad del tratamiento y como ayuda para mitigar los riesgos ante una posible brecha** de datos personales. El aspecto característico del cifrado es que, sin acceso a la clave adecuada, debería resultar inviable acceder al contenido de la información cifrada o alterar la misma sin que los cambios fueran detectados.

El documento recoge que el cifrado será una medida adecuada de seguridad para la protección de datos siempre que su implementación se ajuste a las características e impacto del tratamiento en los derechos y libertades de los afectados. Las Orientaciones recogen que, en caso contrario, se convierte en una medida que genera una sensación de falsa seguridad que relaja la aplicación de otras medidas complementarias en el tratamiento, en particular, garantías de privacidad desde el diseño, y que limitar la cuestión del cifrado a la selección de un algoritmo deja de lado aspectos esenciales que pueden hacer inútil dicha medida. Asimismo, pone de manifiesto que las organizaciones que llevan a cabo el tratamiento de datos deben verificar, evaluar y valorar todos los elementos que intervienen en el proceso de cifrado para que este sea una medida efectiva.

Esta guía analiza los elementos que es recomendable evaluar en el diseño y validación de un sistema de cifrado que se utiliza en un tratamiento de datos personales, y especialmente en aquellos casos en los que el cifrado se emplea para preservar la confidencialidad. Solo en marzo de este año, la Agencia recibió casi **170 notificaciones de brechas de datos personales que afectaban a la confidencialidad de la información**

y un 50% de ellas se debieron a la exfiltración de datos, pérdida de dispositivos o comunicaciones de datos personales que no estaban adecuadamente cifradas. Además, el documento propone una lista de controles para facilitar al delegado o asesor de protección de datos la selección de aquellos que pudieran ser los más oportunos en su labor de supervisar la validación del sistema de cifrado en el marco de un tratamiento específico.

La guía está dirigida principalmente a responsables y encargados de tratamiento que aplican criptografía en sus tratamientos de datos personales, así como a los delegados, asesores y auditores de protección de datos y especialistas y responsables de seguridad. También a desarrolladores de soluciones de cifrado destinadas al tratamiento de datos personales y, en general, a los desarrolladores de productos y servicios de la economía digital.