ESCURA

Telf. +34 902 702 037
escura@escura.com
www.escura.com

¿Cómo actuar ante un virus en materia de Protección de Datos?

En las últimas semanas, en **Escura** hemos tenido varios avisos de clientes que han sufrido un ciberataque a su base de datos.

Hoy en día hay infinidad de virus que pueden afectar de manera significativa a los sistemas informáticos de las empresas, desde virus que pueden interferir en el normal funcionamiento del sistema, provocando la corrupción de archivos y programas, hasta secuestros por parte de un tercero que procede a encriptar todos los archivos de la base de datos y pide un "rescate" económico a cambio de liberarlos.

Es por ello que debemos recordar qué pasos hemos de seguir ante una intrusión de un virus o de un tercero y que puede afectar a datos de carácter personal:

1. Detectar la amenaza y saber a qué nos estamos enfrentando.
2. Determinar el alcance de los archivos dañados o encriptados y si hay datos personales afectados.
3. Adoptar las medidas de contención y solución/erradicación de la amenaza (en el caso de suplantación de identidad mediante correo electrónico se recomienda como medida de contención el realizar una comunicación a los titulares de los datos informando de dicha situación a efectos de prevenir mayores daños a los mismos).
4. Reforzar las medidas de seguridad técnicas y organizativas, para garantizar la seguridad de los datos.

Hay que tener en cuenta que, si se han visto afectados datos personales, el ataque puede constituir una brecha de seguridad y que, de ser así, se deberá informar en un plazo no superior a **72 horas** ante la Agencia Española de Protección de Datos desde la toma de conocimiento del hecho.

Asimismo, cuando la brecha de seguridad pueda entrañar un alto riesgo para los derechos y libertades de las personas físicas entonces, se deberá, comunicar a los afectados dicha brecha de seguridad sin dilación indebida.

Si procede, se recomienda realizar una denuncia a la Policía sobre el ciberataque ocurrido ya que a través de un organismo especializado como es la Unidad de Investigación Tecnológica se encargará de paliar estas amenazas cibernéticas.

Según el principio de responsabilidad proactiva que establece el Reglamento (UE) 679/2016 y la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales las empresas deberán ser proactivas y participar más en el ámbito de protección de datos.

Por lo tanto, se tienen que ir actualizando esas medidas de seguridad con el fin de frenar los ciberataques ya que no sólo puede afectar al funcionamiento de la empresa, sino que puede llegar a afectar a los datos de carácter personal.