Protección de los activos de información de una empresa

Actualmente las empresas afrontan un reto clave: la protección de sus activos de información que comprenden básicamente los siguientes tipos de datos:

Secretos empresariales y/o profesionales: deben protegerse por el conocimiento o *know–how* que incluyen. Éstos tienen un gran valor porque:

- Permite añadir al producto o productos características, funcionalidades y prestaciones que son muy valoradas por el mercado, por tanto, generan un impacto beneficioso en el negocio.
- Se trata de un factor diferenciador de otras empresas de la competencia.
- Es fuente de generación de prestigio y buen posicionamiento de la empresa en el mercado, fortaleciendo sus marcas, nombres comerciales y otros signos distintivos.

Datos personales: están protegidos en la UE por el Reglamento 679/2016 General de Protección de Datos (RGPD) y en España por la Ley Orgánica 3/2018 de Protección de Datos Personales y Derechos Digitales (LOPD), que afectan a la esfera de intimidad de las personas físicas y que son tratados habitualmente en el propio desarrollo de la actividad empresarial. La empresa debe protegerlos garantizando su confidencialidad, integridad y disponibilidad, por tratarse de un derecho fundamental y porque el no cumplimiento de la legislación vigente lleva aparejado sanciones económicas importantes.

La intensificación en el uso de tecnologías TIC, la progresiva digitalización de los datos tratados en los sistemas de información, el incremento de los flujos internos y externos y número de usuarios en el seno de las empresas, han ocasionado la aparición de nuevos riesgos y la necesidad de **proteger estos datos aplicando controles y medidas que consigan mitigarlos**.

La realidad demuestra que la gran mayoría de las empresas han afrontado este reto:

- Diseñando e implementado medidas y controles de seguridad informáticos, sobre la base de que los ciberataques pueden afectar principalmente a los sistemas de información que están conectados a Internet y otras redes abiertas.
- Evaluando los riesgos inherentes al tratamiento de cada dato por su nivel de criticidad, teniendo en cuenta, la propia naturaleza del dato por su valor en sí mismo.

Desde RSM Spain proponemos abordar este reto:

- Elaborando un registro de todos los datos que son objeto de tratamiento identificando cada categoría de datos, su nivel de criticidad, qué áreas y cuántos empleados tratan cada categoría de datos y cuál es su perfil de uso. Si los datos son tratados por empleados en la nube o en PC's con posibilidad de copia en disco duro o en tablets y teléfonos móviles, qué proveedores tratan cada categoría o tipo de datos y si lo hacen de forma remota o en los equipos propios de la empresa.
- Evaluando los riesgos inherentes al tratamiento de cada categoría de datos teniendo en cuenta su nivel de criticidad y otros factores como quién los trata, cómo se tratan, qué flujos internos y externos existen.
- Analizando qué controles y medidas de seguridad son necesarios para mitigar los riesgos inherentes hasta alcanzar unos riesgos residuales aceptables, que no pongan en riesgo su confidencialidad, integridad y disponibilidad. En este punto, se analizan las políticas, protocolos, normas y procedimientos de seguridad lógica y perimetral o de accesos de la empresa y se ajustan, adaptan o, caso de no existir, se elaboran e implementan.
- Analizando todas las cláusulas, pactos, procedimientos y normas que son necesarias en las relaciones con los empleados y con los proveedores externos, a fin de garantizar la existencia de un compromiso de deber de secreto. En el caso de proveedores que tratan secretos empresariales o datos personales sensibles, se contempla la posibilidad de realizar auditorías de seguridad periódicas, así como exigir certificaciones que acreditan el cumplimiento de determinados estándares de seguridad (normas ISO 27001 e ISO 27002).
- Realizando sesiones de formación dirigidas a empleados que tratan secretos empresariales o datos personales sensibles, a fin de que conozcan los riesgos inherentes y sus funciones y deber de secreto en el tratamiento de éstos.

Para más información puede contactar con nuestro equipo de derecho digital.
Javier Albouy, Associate Lawyer
jalbouy@rsm.es
T.+34 93 418 47 47 | M. 607 542 392