LA IMPORTANCIA DE LA PROTECCIÓN DE LOS SECRETOS EMPRESARIALES EN TIEMPOS DEL COVID-19

Cuando se cumple poco más de un año de la entrada en vigor de la Ley 1/2019 de Secretos Empresariales (LSE), la llegada del Covid-19 ha obligado a las empresas a tener que recurrir al teletrabajo para poder seguir operativas.

El trabajo en remoto supone un cambio radical en el modo en el que por parte de los empleados se accede a los contenidos y materiales de la empresa. De este modo, la empresa, entendida como un único espacio físico de trabajo, ha dado paso a una multitud de espacios de trabajo, que en su mayoría son los domicilios de los empleados.

Como consecuencia de la declaración del estado de alarma, el teletrabajo se ha implementado en muchos casos de manera precipitada, sin que las empresas hayan tenido tiempo de adoptar medios y protocolos de seguridad. En muchos casos el acceso por parte de los empleados a los contenidos de sus empresas se hace a través de sus ordenadores y dispositivos particulares, que son compartidos en muchos casos con otros familiares, y sin las necesarias medidas de seguridad.

Todo ello supone una **mayor exposición de la información** de carácter reservado de la empresa, con el consiguiente **riesgo de que dicha información pueda ser accesible por terceros no autorizados**.

Estas circunstancias ponen en riesgo la protección que la LSE otorga a las empresas, en tanto que titulares de secretos empresariales.

Conviene recordar cualquier información o conocimiento puede ser un secreto empresarial, cuando esta información sea fruto del trabajo desarrollado en el seno de la propia empresa y suponga un activo que lo diferencie de la competencia. Nos referimos, por ejemplo, a invenciones no patentadas, procedimientos de fabricación, listas de clientes y proveedores, información sobre precios y costes, planes de negocio, estrategias de marketing, etc. Incluso determinados elementos de un programa de software pueden considerarse secretos empresariales.

El hecho de poder gozar de protección como secretos empresariales no es una cuestión baladí. La LSE establece un amplio abanico de acciones a favor de su titular, no sólo contra quien hubiese revelado de los secretos empresariales, sino también contra los terceros adquirentes de la información, como podrían resultar los competidores a quienes se les hubiesen facilitado los secretos empresariales, aun cuando dichos competidores hubiesen obrado de buena fe, con desconocimiento de su obtención de forma ilícita.

Ahora bien, la LSE establece que para que estemos ante un secreto, es necesario que su titular pueda acreditar el cumplimiento de manera cumulativa de 3 requisitos:

(1) que la información **sea secreta**,

(2) que tenga **valor empresarial** y

(3) que haya sido **objeto de medidas razonables** por parte de su titular para mantener su carácter reservado.

Es precisamente este tercer requisito el que entraña una mayor complejidad (en tanto que se requiere de la adopción de medidas por el titular) y en el que tiene una incidencia clara el actual contexto de teletrabajo.

¿Cómo mantener el carácter reservado de la información de la empresa cuando ésta se puede acceder de manera remota por parte de los empleados, a través de sus propios dispositivos?

Las empresas deben implementar **medidas técnicas de seguridad** para que el acceso en remoto no pueda menoscabar el carácter reservado de su información. Si bien dichas medidas dependerán del tipo de empresa y de la tipología de información, existen determinadas actuaciones a tener en consideración:

- Implementación de sistemas de trabajo “cloud”, con los que se logra desvincular los contenidos de la empresa a los equipos físicos y se permite que el acceso a dichos contenidos se realice con sujeción a unos filtros de seguridad.
- Entrega de ordenadores y dispositivos propios de la empresa, desde el que los trabajadores puedan acceder en remoto a la documentación de la empresa.
- Creación de claves de acceso personalizadas para permitir el acceso por parte de los empleados (i) a los equipos que tuviesen asignados, (ii) a los contenidos ubicados en el “cloud” y (ii) a sus cuentas de correo electrónico profesional.
- Implementación de un sistema de actualización de contraseñas para el acceso a equipos, “cloud” y cuentas de correo electrónico.
- Bloqueo del uso externo de dispositivos USB o discos duros externos no validados por la empresa.
- Implementación de políticas de seguridad en el acceso a internet desde los equipos y/o “cloud” de la empresa, bloqueando el acceso a páginas webs que pudiesen permitir la transmisión de virus.
- Restricción del acceso de la documentación de carácter secreto a una serie de empleados y bajo las preceptivas claves de seguridad personalizadas.
- Implementación de filtros por parte de los departamentos de IT para impedir la entrada de correos malicioso e información de aquellos que habiendo entrado resultasen maliciosos.
- Elaboración de manuales de uso dirigidos a los empleados para trabajar en remoto, sin comprometer la seguridad de la empresa y salvaguardando el carácter secreto de los contenidos a los que se les permita acceder.

Asimismo, dichas medidas técnicas deben complementarse con **medidas legales** que son **igualmente necesarias**. Dichas medidas van dirigidas a informar a los empleados sobre el carácter reservado de la información a la que tendrán acceso, advirtiéndoles a su vez de su obligación de actuar salvaguardando dicho carácter reservado. Respecto de los empleados dichas medidas pueden consistir en la creación de cláusulas de confidencialidad para los empleados, la firma del código ético de la compañía, el desarrollo de una política de *compliance,* etc. Respecto de los socios o colaboradores dichas medidas pueden consistir en la creación de acuerdos de confidencialidad o NDA's.

Si desea obtener más información sobre **Secretos Empresariales** haga clic aquí.

El equipo de Propiedad Industrial e Intelectual de March & Fieldfisher queda a su disposición por si tuviera alguna duda que deseara consultar.

Eduardo Vila, Asociado
March & Fieldfisher
marchtrademark@march-asociados.com