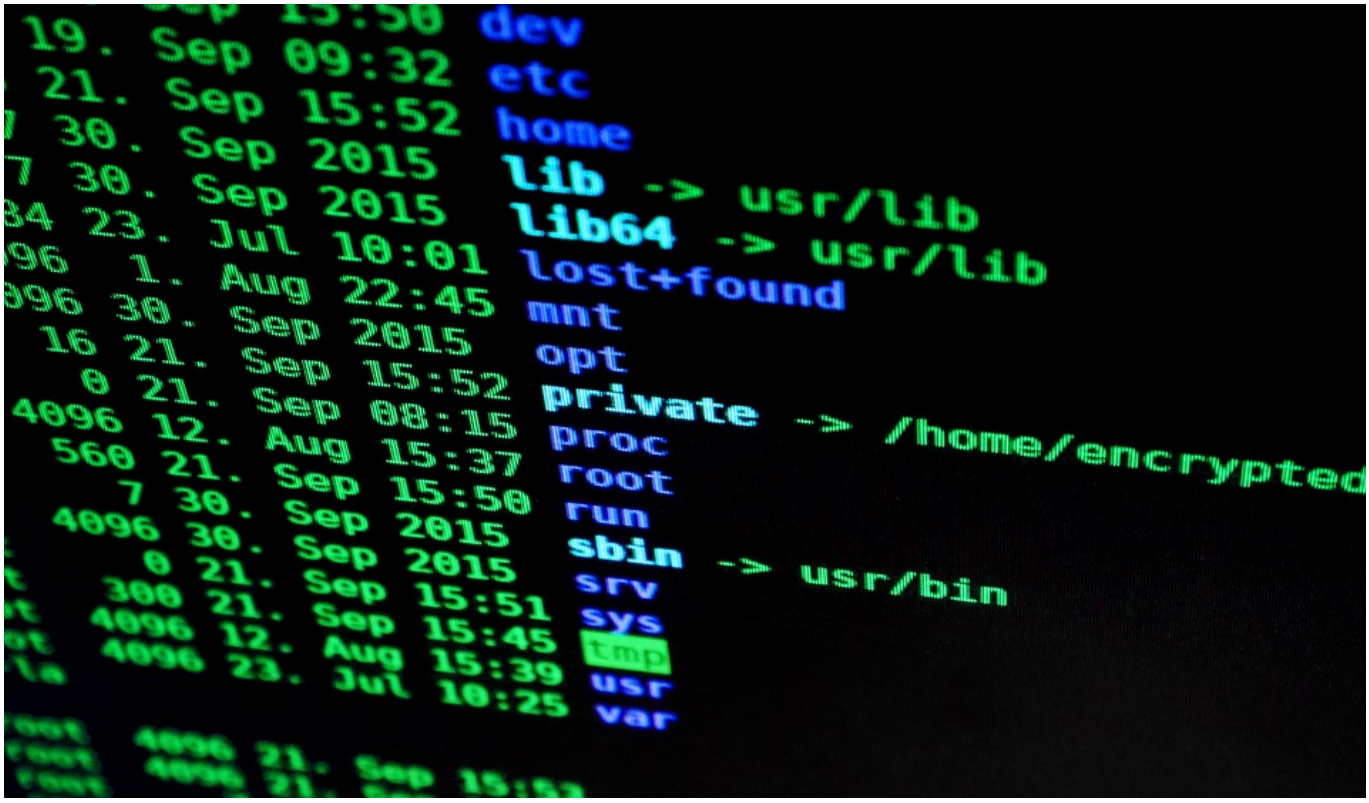
Análisis de la actualidad internacional

CYBERSECURITY SOFTWARE DEVELOPERS: Descifrando las opciones legales

AUTORA: María Martínez, Abogada especialista en derecho tecnológico



Que el software, en todas sus dimensiones, se ha convertido en algo esencial para toda empresa considerada exitosa en la actualidad, salvo raras excepciones, no es noticia. Que la creciente demanda de soluciones de ciberseguridad y ciberdefensa supone una oportunidad de negocio para los desarrolladores de software, tampoco. La mejora de la capacidad y gestión operativa tanto interna como externa, y su incidencia directa en la competitividad, lo han convertido en un *must*. Lo que, tal vez, sea más discutible es que todas las empresas que gozan de sus múltiples ventajas, ya sea como desarrolladores, comercializadores o consumidores de soluciones tecnológicas de ciberseguridad, tengan claras las **implicaciones legales y operativas derivadas** de las múltiples opciones que existen en cada uno de los escenarios de explotación de software.

A continuación, repasaremos las principales implicaciones derivadas del uso de componentes de **código abierto para el desarrollo de soluciones de ciberseguridad**, las opciones de **protección del desarrollo** así como de **comercialización** del software.

La creciente demanda de soluciones de ciberseguridad y ciberdefensa supone una oportunidad de negocio para los desarrolladores de software

Desarrollo: Componentes del software

Empecemos por el principio. A la hora de comenzar con el desarrollo de una solución de software, ya sea de forma interna o externalizada, el principal riesgo y, por tanto, la principal necesidad que debe asegurarse es **el soporte que ofrece cada uno de los componentes que van a formar parte del desarrollo**.

En este punto, se vuelve a plantear la dicotomía coste/riesgo, cuanto más garantías ofrezca un componente (o software base) más elevados serán los royalties que la compañía/desarrollador deba pagar para poder utilizarlos. Una de las soluciones más comunes por las que se está optando hoy en día, incluidas las Administraciones Públicas, es el uso de soluciones de *free software (FS)* o software *open source (OSS)*, que, a simple vista soluciona todos los problemas, al menos, desde la perspectiva económica directa.

Ejemplos reales de esta tendencia son los múltiples proyectos que se están desarrollando en varias Comunidades Autónomas desde hace varios años:

1. En Extremadura, comunidad pionera en este campo, la distribución GNU/Linux, gnuLinEx, inició su camino en el año 2001 y se instaló en miles de ordenadores de la Junta, institutos y escuelas extremeñas.

2. En Andalucía se lleva implantando, también, desde el año 2004, su propia distribución Guadalinex (http://www.guadalinex.org/) en administraciones y centros públicos.

3. Otro caso a destacar es el del Ayuntamiento de Zaragoza, que desde 2005, lleva a cabo un proyecto para migrar todos los ordenadores de la administración local a software libre con el objetivo de ser el primer ayuntamiento español en trabajar 100% con software libre.

No sólo en el ámbito público es práctica habitual el uso de **código abierto**. El uso de este tipo de licencia es una tendencia en auge ya que posibilita el estudio y la modificación del software con total libertad, salvo excepciones expresas.

Prácticamente todas las compañías desarrollan sus productos y servicios utilizando componentes procedentes de este entorno. Existen más de 5 millones de librerías de código abierto y se espera que millones de desarrolladores liberen hasta 500 millones en la próxima década.

La ventaja principal del software OSS/FS, además de su acceso gratuito, es la posibilidad de que, de forma colaborativa, los usuarios puedan compartir, modificar y estudiar el código fuente de, por ejemplo, una solución de seguridad, lo que permite el desarrollo continuo de nuevas funcionalidades.

Sin embargo, desde la perspectiva del soporte, los programas *open source*, en la mayoría de los casos, no tienen ninguna empresa detrás que proporcione soporte o a la que se le pueda realizar ningún tipo de reclamación.

Por tanto, en caso de experimentar algún tipo de problema, el usuario se vería obligada a buscar la solución en la comunidad o bien practicar un *insourcing del mantenimiento*, lo que puede suponer un gasto inesperado tanto económico como productivo.

> En términos generales, desde el punto de vista de la seguridad, el *open source* es una aproximación colaborativa, en constante actualización y utilizado de forma masiva, las compañías tienden a no verificar su seguridad con el mismo detenimiento que si se tratase de un software desarrollado internamente.

El *open source* es una aproximación colaborativa, en constante actualización y utilizado de forma masiva, las compañías tienden a no verificar su seguridad con el mismo detenimiento que si se tratase de un software desarrollado internamente.

Protección de la Propiedad Intelectual

Un aspecto a veces olvidado, es el de la protección de la propiedad intelectual de la creación. El ámbito de la protección vía propiedad intelectual de las soluciones de software de ciberseguridad es, cuanto menos, un ámbito complejo debido a la falta de armonización de las legislaciones a nivel mundial. Un claro ejemplo de las diferencias de protección que nos ofrece este ámbito es el caso de las soluciones software de ciberseguridad desarrolladas en Europa versus las desarrolladas en USA. Pongamos un ejemplo práctico, un mismo desarrollador crea un software con una funcionalidad innovadora en el mercado en Madrid (España) y en California (USA), mientras que en España únicamente podrá proteger el código que soporte dicha funcionalidad a través de la propiedad intelectual, en USA podrá proteger tanto el código como la funcionalidad en si misma a través de una patente. La principal consecuencia es que, protegiendo la funcionalidad per se y no el código, evita que terceros puedan desarrollar funcionalidades similares con códigos distintos al original, situación que estaría permitida en España y el resto de Europa.

Como en toda inversión, la principal motivación a la hora de invertir en un desarrollo de una solución software de ciberseguridad, es conseguir una ventaja competitiva sobre el resto de actores en el mercado y, esta idea, también es aplicable a los casos en los que la empresa decida embarcarse en el desarrollo e implementación de un programa informático en las que, el principal riesgo es que un competidor pueda tener acceso dicho código, copiarlo y lucrarse de la misma manera sin la inversión inicial.

La vía legal de mitigar este riesgo, o al menos proteger nuestras acciones frente a terceros que utilicen nuestro desarrollo es a través de la propiedad intelectual. En el caso de que la adaptación de la organización al desarrollo de software sea “suficientemente original e innovadora en el mercado”, conviene llevar a cabo una de las dos opciones siguientes para dejar evidencia de dicha creación:

1. Depositar el código fuente de la parametrización, adaptación o desarrollo base ante notario.
2. Registrar ese código en el Registro de Propiedad Intelectual.

Los efectos de ambos son muy parecidos ya que la principal protección que ofrecen es frente al uso de terceros, si tenemos nuestro desarrollo correctamente depositado o registrado ante un oficial público, no tenemos que presentar mayor evidencia al tercero cuando le solicitemos que no haga uso de nuestro desarrollo. Sí que podrá valorarse como criterio decisorio la diferencia de coste de los trámites en un caso u otro, siendo más conveniente en este sentido la opción de optar por el Registro de Propiedad Intelectual, ya que el depósito notarial a largo plazo puede traducirse en unos costes considerables.

Además, a la hora de plantearnos proteger nuestro desarrollo frente al uso de terceros, también entra en juego el ámbito de las marcas o nombres comerciales. Antes de decidir bajo qué nombre vamos a comercializar nuestro producto

de ciberseguridad conviene comprobar si en el mercado-en nuestro caso en el ámbito europeo- no existe ya una denominación similar registrada o con un uso notorio que pueda derivar en reclamaciones de terceros y, de nuevo, a afrontar nuevos costes.

Es importante tener en consideración que la necesidad de protección puede venir no solo cuando somos los creadores originales, sino también cuando nuestra necesidad de adaptación o parametrización del software tiene una dimensión tal que puede considerarse una creación nueva. Esto último deberá quedar claramente determinado en el contrato de prestación de servicio, donde la propiedad intelectual tanto de la "obra derivada" como de la "obra preexistente" deberá acordarse entre las partes. La práctica habitual que el desarrollador conserve los derechos sobre la preexistente a fin de poder proseguir con la comercialización del mismo.

Comercialización: el licenciamiento

Una vez el software está desarrollado y apropiadamente protegido, llega el momento de plantearse cuál es la mejor forma de comercializar nuestro producto. Tanto si somos proveedor como si somos cliente, éste resulta un punto crucial donde los aspectos a prever pueden devenir críticos.

A pesar de que esta pregunta parece tener estrictamente consecuencias a nivel comercial, la estructura jurídica que empleemos tiene mucha relevancia a la hora de controlar el uso y obtener las garantías necesarias sobre nuestro desarrollo. A priori, las dos opciones más comunes bajo las que comercializar/adquirir el software son bien la licencia o bien la cesión. Sin entrar en detalles sobre las modalidades de licencia y/o cesión, que pueden ser tantas como queramos, a continuación se exponen los pros y contras de ambas fórmulas.

Los contratos de **licencia** (ya sean licencias temporales o por uso) presentan la ventaja principal de que, como regla general, el coste económico es menor al no requerir una inversión inicial, el desarrollo está sujeto a mejoras evolutivas, siempre a cargo del propietario o licenciante, y, además, permiten desistir del contrato si finalmente la organización decide que el software no cumple con las expectativas. Adicionalmente, cuando el propietario del software es una empresa con cierta reputación en el sector, optar por una licencia ofrece muchas garantías de cumplimiento (por ejemplo, en materia de protección de datos o de seguridad), al estar en constante mejora compitiendo con el mercado.

En el caso de los contratos de **cesión**, la ventaja principal es el absoluto control del desarrollo por parte de la empresa. Una vez se complete su desarrollo, el software podrá irse adaptando a las necesidades de la empresa a lo largo de su implementación y uso sin necesidad de incurrir en costes adicionales, el control y supervisión se gestiona por el departamento interno de IT.

La principal desventaja en los contratos de **licencia** es, por el contrario, la absoluta dependencia del proveedor del software. El licenciatario (la organización) nunca tendrá acceso al código fuente por lo que toda mejora, modificación o adaptación que la empresa detecte sobre el software-salvo la corrección de meros errores- deberá siempre ser canalizada a través del propietario. En este punto, una opción a tener en cuenta en el caso en el que seamos el adquirente de la licencia es optar por un contrato de *escrow* o depósito del código fuente que nos permita acceder al mismo en situaciones excepcionales (por ejemplo, la disolución de la empresa propietaria) que nos asegure una continuidad a nuestro negocio.

Por otro lado, la desventaja en el contrato de **cesión** es el riesgo de incurrir en la inversión inicial sin asegurar la utilidad o rentabilidad de la implementación del software y tener que asumir, por defecto, toda la gestión de mejoras, mantenimiento, soportes,.. Además de los potenciales riesgos en casos de incumplimientos que no se podrán externalizar a terceros (por ejemplo en el caso de brechas de seguridad).

Adicionalmente, en torno a ambas fórmulas, podemos encontrar todos los servicios asociados de soporte y mantenimiento, así como aquellas conocidos como servicios de valor añadido, que en ocasiones se convierten en el *core* del negocio de desarrolladores de código abierto o de empresas que, siendo proveedoras de estos servicios respecto a softwares de terceros, en cuyo caso podrían complementarse con servicios de reselling de las licencias de terceros respecto de las cuales se prestan estos servicios asociados.

Conclusiones:

La necesidad de una **evaluación de las implicaciones jurídicas** de un desarrollo de soluciones software de ciberseguridad ha de llevarse a cabo **desde el momento de la concepción de la iniciativa**, de forma que podamos prever aquellos aspectos que puedan tener incidencia y que, a posteriori, pueden ser mucho más costosos de solucionar. Por ejemplo, no basta con identificar una necesidad en el mercado, sino validar que no existe una similar, debidamente protegida, que podría anular nuestro *business plan*. Tener en consideración la tipología de cliente potencial, prestando especial atención a los requisitos que pueden imponer determinados sectores, por estratégicos, o administraciones públicas por su naturaleza, que podrían imponer requerimientos tales como la puesta a disposición del código fuente o la cesión de los derechos sobre éste, al amparo de un interés público son cuestiones al menos tan trascendentales como el plan de viabilidad del proyecto.

> Una adecuada protección de nuestro producto puede evitar una pérdida competitiva y con ello reforzar la continuidad de nuestro negocio asegurando nuestra inversión.

Por último, y no menos importante, la posibilidad de definir colaboraciones con *partners* autorizados para la prestación de servicios de valor añadido respecto de nuestro software conviene igualmente evaluarla desde la fase inicial, o al menos previa al lanzamiento del producto siendo una relevante oportunidad de mercado.

La necesidad de una evaluación de las implicaciones jurídicas de un desarrollo de soluciones software de ciberseguridad ha de llevarse a cabo desde el momento de la concepción de la iniciativa