El papel de las tecnologías de la información en el proceso de *Due Diligence*

IVAN CASTELLTORT
Universitat Rovira i Virgili

Fecha recepción: 30/01/2022
Fecha aceptación: 26/02/2022

RESUMEN

Es inevitable que la Tecnología de la Información o IT tenga un papel relevante hoy en día en el funcionamiento de cualquier empresa. Inevitable también que cualquier proceso de *Due Diligence* deba considerar la tecnología de la empresa que evalúa como un factor que puede alterar el resultado final de la inversión necesaria para la compra.

De todas las operativas que IT representa hoy en la mayoría de las empresas, destacaremos aquellas que pueden ser más relevantes para la *Due Diligence*. Empezando por las personas que conforman el departamento de IT con sus roles y talentos, para seguir con aspectos que pueden impactar reputacionalmente si no se tienen como una política de seguridad tecnológica que blinde en la medida de lo posible contra ciberataques o una infraestructura que permita la continuidad del negocio en base a unos excelentes niveles de servicio y arquitectura redundada en puntos clave de los sistemas. Estos puntos y algunos más son objeto de la primera parte del artículo.

En la segunda parte comentaremos sobre las oportunidades que las diferentes aplicaciones comerciales disponibles en el mercado pueden ofrecer para reducir el esfuerzo necesario para completar un proceso de *Due Diligence*.

Y terminamos ofreciendo una serie de conclusiones relativas al papel de IT en el proceso de *Due Diligence*.

Clasificación JEL: G34, K42, H25, M14, M40.

PALABRAS CLAVE

IT (Tecnología de la Información), Ciberseguridad, Plan y Mapa de Sistemas, Virtual *Data Rooms*.

ABSTRACT

There is no chance to find a company where Information Technology is not relevant for the core business operations. For this reason, there is no way for a *Due Diligence* Process cannot consider what IT is supplying to the business health and future. On the other hand, IT has its own impact in what could be the final figures of the investment required to purchase.

Among a vast number of operational procedures which IT implements in most of the modern companies, we will highlight a bunch of outstanding ones. Beginning with the IT people IT and their talents and moving on to a set of policies that will assure a good protection against cyberattacks and a reliable platform able to provide the required business continuity with no lacks of IT architecture redundancy. We will cover this in the first two chapters of the article.

Chapters three will discuss about some opportunities to make *Due Diligence* process easier to run. In particular, we will have a look to some tools which can be deployed to handle in a more efficient way the data and procedures required for a right development of the *Due Diligence* process.

Last but not least, we will be settling what should be the paramount points no one can miss when talking about the role of IT in the *Due Diligence* process.

JEL classification: G34, K42, H25, M14, M40.

KEYWORDS

IT (Information Technology), Cybersecurity, Systems Plan and Map of IT Services, Virtual Data Rooms.

1. IT en el proceso de Due Diligence

El proceso de *Due Diligence*, en su función de investigación de las distintas áreas de negocio de la empresa a valorar debe de tener muy en cuenta aquellos aspectos tecnológicos que puedan generar riesgos o significar sinergias en el cálculo final de la inversión necesaria para la operación. En el mundo de la empresa actual, la dependencia de la tecnología de la información o IT, en adelante, suele ser relevante. La mayoría de las empresas apoyan sus operaciones diarias en un componente tecnológico que se ha ido complicando tras la irrupción de Internet hace ya más de 20 años.

Hay varios aspectos tecnológicos clave que un riguroso proceso de *Due Diligence* debe de analizar para valorar luego potenciales impactos. El objetivo de este artículo en este punto no es ser exhaustivo sino más bien aportar al lector una perspectiva de aquello que puede ser importante con un lenguaje que trata de huir del tecnicismo habitual de muchos textos. Dichos aspectos se enumeran en los siguientes apartados de forma clasificada y secuencial sin que el orden implique una escala de mayor a menor riesgo o impacto.

Existen a lo largo de todo el texto diversas menciones a aspectos particulares de empresas puramente tecnológicas. Nos referimos a empresas de servicios o productos informáticos o también a las famosas *start ups* tecnológicas. Es evidente que esta categoría de empresas incorpora características IT que empresas de otros sectores no requieren en la misma medida. Para mayor claridad para el lector, dichas menciones son siempre referenciadas en el texto de tal manera que no den lugar a confusión alguna.

Finalmente, nos ha parecido interesante incorporar al texto un apartado independiente donde se comenta brevemente el ecosistema de aplicaciones orientadas a dar soporte al propio proceso de *Due Diligence*. Esto es debido a que parece recomendable usar este tipo de herramientas en el proceso de *Due Diligence* para mantener la información recogida, que es a menudo mucha y diversa, estructurarla adecuadamente y permitir una versión centralizada de toda la información acumulada para todos los participantes en el proceso en todo momento. Estas herramientas se han popularizado en los últimos años y han proliferado diversas versiones de varios fabricantes.

2. Aspectos claves de IT en el proceso de la Due Diligence

Ciertamente son muchos y variados los aspectos en los que casi todas las empresas dependen de la tecnología hoy en día. No es el ánimo de este artículo ser exhaustivos en este apartado sino aportar al lector una visión global, clara y concisa, de los principales puntos que deberían ser valorados. En aras de tal claridad clasificaremos los diferentes aspectos en las siguientes categorías:

- **Estructura, Estrategia y Talento del departamento de Tecnología de la Información**. Especial atención despertará la existencia de la función de Innovación en el departamento reflejada en la aparición de un CTO (*Chief Technological Officer*) o quizás de un CDO (*Chief Data Officer*) que nos permita identificar inequívocamente que la compañía cuenta con una estrategia a largo plazo para su departamento de IT y, por tanto, un alineamiento con el Plan Estratégico de la empresa.
  Fundamentalmente, la existencia de estas dos figuras, CDO y CTO, merecen una especial atención por parte del responsable de la *Due Diligence*, ya que tanto en control de los datos como de las nuevas tecnologías pueden ser un factor diferencial para la compañía y tanto el talento de las personas que ocupan tales posiciones como su estrategia a medio y largo plazo serían un factor clave para conseguir los objetivos futuros de la empresa.
  En este punto cobra especial importancia la revisión del Plan de Sistemas de la entidad (a veces Plan Estratégico de Sistemas) donde debe encontrarse no solo la fórmula para rentabilizar los costes de IT sino también aquellas tecnologías claves que deben incorporarse a futuro en el Mapa de Sistemas y que han de permitir no solo el crecimiento del negocio sino también, a menudo, la propia supervivencia de la empresa frente a los competidores directos. El alineamiento que el responsable de la *Due Diligence* pueda detectar entre Plan de Sistemas y Plan Estratégico de la Empresa, así como los diferentes comités establecidos entre CEO e IT para medir el avance de tareas y consecución de resultados parciales será un factor relevante a la hora de medir la importancia de las personas, procesos y herramientas de IT en el futuro de la compañía.
- **Riesgo Operacional especialmente a todo aquello que se refiera a la continuidad del negocio y a los procedimientos de *Disaster Recovery* que se hayan establecido**. Este es quizás el apartado más tradicional en IT y que engloba aquellos aspectos operacionales, téc-

nicos y económicos relacionados con la propia función de IT y que son comunes a la mayoría de las empresas modernas:

- Las **licencias y suscripciones de productos y aplicaciones** deben de estar bajo control y nunca exceder los volúmenes contratados. Es cierto que muchos contratos de fabricantes de *software* permiten una cierta variación respecto a aquello contratado, pero normalmente se esperan regularizaciones periódicas en caso de ampliación significativa. Aquí será relevante no solo conocer el contrato de licencias suscrito por las partes sino además verificar las últimas facturas de compra en el capítulo de licencias al menos con los *partners* tecnológicos relevantes. En particular, hay que prestar atención a las suscripciones de *software* donde el coste suele ir asociado a un *pay per use*. Esto es muy habitual en productos desplegados en *cloud* que utilizan un modelo de *Software as a Service* (*SaaS*) como es el caso de la mayoría de los productos de Microsoft.
  Uno de los principales problemas es el empleo de usuarios genéricos para el acceso a aplicaciones donde un grupo de usuarios comparte acceso al servicio. Afortunadamente, esta es una práctica que se está abandonando progresivamente ya que, además de estar específicamente prohibido por la mayoría de los fabricantes, impide la debida trazabilidad de las operaciones en el sistema.
- Desde la perspectiva de la continuidad del negocio, hay que prestar atención a la existencia de una implementación **madura de los procesos de ITIL**. El ITIL o *Information Technology Infrastructure Library* es un conjunto de buenas prácticas vastamente aceptado entre los profesionales de IT como una forma sencilla y estructurada de organizar las operaciones IT de la empresa. El ITIL organiza y regula los principales procesos de las operaciones IT, como la Gestión del Cambio (*Change*), Incidental (*Incident*), de los Problemas (*Problem*) o la monitorización (*Event Management*). Especial mención a la gestión de la capacidad (*Capacity Planning*) y configuración (*Configuration*) que, en caso de tener carencias en el momento de la *Due Diligence*, significarán un coste de adaptación posterior.
- La **obsolescencia de la tecnología** es otro de los problemas graves que pueden aparecer. En este caso, la no implementación de nuevas versiones de *hardware* o *software* de forma duradera sobre los sistemas de la empresa puede significar un riesgo de obsolescencia que el nuevo propietario deberá afrontar antes pronto que tarde. Esta obsolescencia, caso de no ser subsanada, puede acarrear graves problemas de disponibilidad de las aplicaciones que afecten al normal desarrollo del negocio.

- En cuanto **a la disponibilidad**, es necesario revisar la arquitectura de los centros de proceso de datos (*Datacenters*) y la disponibilidad teórica que aportan. Un registro razonable para empresas con sistemas críticos de negocio sería de un 99,9 % de disponibilidad anual, lo que representa menos de 10 horas de caída al año, normalmente descontando las paradas planificadas por mantenimiento u otras razones. Normalmente, los profesionales que realicen la *Due Diligence* solicitarán los RTOs (*Recovery Time Objective*) para recuperación del servicio en caso de incidente y RTOs (*Recovery Point Objective*) para recuperación de datos en cada servicio crítico. Dichos indicadores están íntimamente vinculados a los niveles de servicio (*Service Level Agreements*) contratados con lo diferentes proveedores y, por lo tanto, un cambio en la disponibilidad global suele necesitar de inversión económica que debe conocerse y calcularse durante la *Due Diligence*.
- Finalmente, **la existencia de patentes o estrategias de incorporación al mercado** de un nuevo producto o servicio deben ser medidas minuciosamente analizando el *business plan* correspondiente. Por supuesto, esto ocurrirá principalmente en empresas cuya actividad esté relacionada con la propia tecnología como es el caso de las *start ups* tecnológicas. No es objeto de este artículo ahondar en las especiales características que una *Due Diligence* de una empresa emergente debe contemplar, pero parece evidente que necesita de unas particularidades específicas derivadas de su particular condición de empresa «nueva» en el mercado y del riesgo que este punto pueda significar.

• **Funcionalidad de las aplicaciones y servicios**. Especialmente del ERP (*Enterprise Resource Planning*) entendido como el sistema central (*core*) de la compañía y del CRM (*Customer Relationship Management*) como plataforma única de relación con el cliente requerirán de un análisis en profundidad por parte del responsable del proceso de *Due Diligence*. La existencia de un ERP que agrupe la mayoría de los procesos de la empresa, tanto en áreas financieras, logísticas o comerciales hace de este servicio uno de los más relevantes de la compañía. El caso del CRM es también relevante. Se supone que el CRM concentra todo el conocimiento que la empresa posee sobre sus clientes. Desde sus datos personales y administrativos a sus ciclos de compras y sus particularidades operativas, logísticas o técnicas. El CRM es un repositorio centralizado de toda la información que los diferentes ejecutivos de ventas necesitan para poder realizar un buen trabajo. Ambos sistemas son, por lo tanto, capitales para el funciona-

miento de la empresa y serán objeto de estudio particular por parte de la *Due Diligence* como componentes fundamentales del mapa de sistemas IT.

En particular y además de la potencial obsolescencia del producto y de su debido mantenimiento a nivel de versiones y contratos de mantenimiento con el fabricante, deberá de revisarse su estructura básica de datos a nivel de tablas principales y relaciones entre ellas para verificar que presentan un diseño funcional adecuado y pueden responder a las preguntas o informes que se soliciten por parte del comprador. Cualquier carencia en este aspecto debe de anotarse como un *gap* a subsanar que, obviamente, tendrá un impacto económico dependiendo de la gravedad del problema y de las posibles alternativas.

Es probable que, además del CRM y el ERP, existan en el mapa de sistemas de la empresa otros servicios IT que merezcan igualmente dicho tratamiento especial. Su número y complejidad dependerá de la empresa, sector, mapa tecnológico e historia de la compañía y es difícil de precisar de forma genérica.

- **Arquitectura Tecnológica**. Revisaremos en este apartado la estrategia tecnológica de la compañía en el sentido sobre si su apuesta es firme hacia el *Cloud Computing* y el mundo del *software* como servicio (SaaS) o, por el contrario, mantiene una arquitectura híbrida donde conviven los servicios externos con los despliegues *onpremise* en los *datacenters* de la compañía. Una estrategia o la contraria puede acarrear grandes costes recurrentes (costes operativos o OPEX) que pueden amortiguarse con la debida inversión.

  Otro capítulo relevante es el de las capacidades de integración tecnológica de la compañía, a menudo olvidadas a pesar de su capital importancia para el funcionamiento IT de la empresa moderna. En este caso, es especialmente relevante valorar la capacidad de la tecnología de la empresa para asumir futuras operaciones de *Merge & Acquisition* a corto o medio plazo. Si se prevé que estas operaciones puedan acontecer, este capítulo cobra gran relevancia para la *Due Diligence*, ya que la plataforma tecnológica y los equipos de trabajo IT deben de estar preparados para asumirlo. Aquí es importante a nivel tecnológico la existencia de un bus de servicios que aglutine los diferentes servicios tecnológicos disponibles en una plataforma ágil y sencilla de usar para una tercera parte que participe en futuras integraciones dentro de futuros escenarios de M&A.

  Finalmente, en este apartado de Arquitectura y aunque quizás sea menos relevante que los anteriores, no quiero dejar de mencionar la importancia de como se ha abordado en la compañía el tema de la multi-

canalidad. En concreto y si existen *apps* desarrolladas *inhouse,* habría que analizar su uso y determinar si la empresa las está usando adecuadamente para llegar de la mejor manera posible a su mercado y clientes. Otro punto interesante para comprobar es si existe una estrategia de desarrollo de aplicaciones web en modo *responsive,* entendido el término como aplicaciones capaces de adaptarse al dispositivo que las requiera, sea este un *smartphone,* una *tablet* o un ordenador personal. Si no es así, los costes de adaptación de tales aplicaciones deben ser considerados como un potencial riesgo tras la compra.

- **Seguridad Informática y Ciberseguridad**. Pocos aspectos tan relevantes hoy en día como este. Aquí, la figura del CISO (*Chief Information Security Office*) y la existencia de una política de seguridad sólida y respaldada por la dirección son fundamentales. Por supuesto, la sensibilidad de una compañía y el impacto reputacional que pueda soportar en caso de ciberataque tienen que ser muy tenidos en cuenta. Desafortunadamente, el *ransomware* ha demostrado ser común en nuestros días y difícil de predecir o incluso de detener habida cuenta de la larga lista de grandes y conocidas empresas e instituciones, públicas o privadas, que han sido víctimas de los cada vez más sofisticados *hackers* en el pasado reciente.

  Por lo tanto, **la ciberseguridad** se convierte en un pilar imprescindible en el funcionamiento diario de las empresas conectadas a la red. Debemos de partir de la base de que la única empresa segura cien por cien es hoy en día aquella empresa que no está conectada a Internet, la simple conexión con el mundo exterior implica un cierto riesgo que hay que asumir y contar después con las herramientas que permitan defenderse de los ciberataques y sus *hackers*. Esta circunstancia se ha agravado después de la crisis de la COVID-19 en marzo de 2020 con la llegada del teletrabajo masivo. Las herramientas de videoconferencia y mensajería instantánea han evolucionado notablemente en los últimos dos años y se han convertido en la penúltima revolución silenciosa que IT ha aportado a la empresa. El proceso de *Due Diligence* debe de tener en cuenta la estrategia de teletrabajo en la compañía, no solo por la posibilidad de nuevos confinamientos parciales o incluso estrictos (en el peor de los casos) sino también por la aportación de estos métodos de trabajo a la conciliación de la vida familiar y a conseguir, por tanto, empleados más satisfechos y por eso más productivos. Por supuesto, la concurrencia necesaria en términos de ancho de banda de comunicaciones y dispositivos móviles debe de ser objeto de atención para garantizar que la contingencia potencial será cubierta por la tecnología disponible llegado el momento.

La existencia y seguimiento de un plan de seguridad encaminado a auditar internamente los potenciales riesgos y vulnerabilidades para corregirlos con las debidas implementaciones, tanto *software* como *hardware*, son buenas pistas para ayudar a determinar la salud de la seguridad IT de la compañía. Otros aspectos que pueden ayudar al responsable de la *Due Diligence* a determinar el grado de madurez de la seguridad IT en la compañía es la existencia de lo que se ha dado en llamar «*hacking* ético», donde los ciberataques son provocados por un *third party* contratado por la compañía que hace las veces de «hacker» para encontrar vulnerabilidades y alertar al responsable de seguridad para su corrección antes que los *bad boys* del ciberespacio lo hagan a su vez. En otros casos, la propia compañía ha lanzado «anzuelos» de *phishing* entre sus propios empleados para concienciar sobre la necesidad de estar siempre alerta y no atender a determinados cantos de sirena digitales. Esta es una práctica que tiene sus detractores, ya que en muchas ocasiones este *phishing* ético se asocia a campañas internas donde se ofrece un premio, simulando al departamento de Recursos Humanos de la compañía, por ejemplo, un *smartphone*, a cambio de contestar una simple encuesta o similar. Esta última categoría se conoce también como Ingeniería Social en algunas empresas.

- **Data y Automatización.** En apartados anteriores hemos mencionado al *Chief Data Officer* o *CDO* como figura clave del departamento de tecnología. Efectivamente dicha figura es el garante interno tanto de la calidad de los datos como del *reporting* proporcionado a las diferentes áreas de negocio. No es solo una cuestión de forma sino de unicidad de los datos y homogeneidad transversal de dichos datos. Esta es una cuestión trascendental hoy en día para la toma de decisiones así que se convierte en un aspecto para tener en cuenta por parte de la *Due Diligence*. Los servicios tecnológicos asociados a este punto y que deben por tanto ser muy tenidos en cuenta son los sistemas operacionales, *Data Marts, Data Warehouse* y más recientemente los *Data Lakes*, y las herramientas de *Business Intelligence*.

  Quizás todavía más importante que esta responsabilidad del CDO es la función predictiva que el análisis de datos acumulados en sus sistemas puede (y debe) proporcionar a las diferentes áreas de negocio. En los últimos años, compañías como Facebook o Google han demostrado que existen pautas nuevas en los hábitos de compras de los consumidores. Dichas tendencias, una vez detectadas en base a lo que llamamos el *Big Data* y convenientemente adiestradas en los sistemas con técnicas de *Machine Learning* (una de las muchas ramas de la Inteligencia Artificial) pueden significar un nivel superior de ventas futuras

para la compañía. Estas pautas o tendencias son las que el CDO con sus *Data Architects* debe ser capaz de destilar de los datos acumulados por la compañía en toda su historia y canalizar debidamente hacia las áreas de negocio para certificar la bondad de la predicción. Es evidente que es una tarea ardua que requiere inversión, pero también es evidente que otras empresas pioneras han recorrido un camino que está ahí para ser recorrido también. Desde el punto de vista de la *Due Diligence*, la maduración de este proceso *de Big Data* debe de poder medirse y evaluarse como un activo más de la empresa valorada.

Finalmente, y para cerrar este capítulo de *Data*, nos referiremos a la automatización de los procesos operativos o de negocio de la compañía. Si bien es cierto que esta es una actividad transversal en la empresa que suele ser liderada por un grupo de la Organización fuera de IT normalmente, no es menos verdad que el papel de IT es fundamental en la implementación técnica y funcional de todo aquello que la Organización pretende. En este caso, el profesional que realiza la *Due Diligence*, debe de buscar las herramientas de *Workflow*, también llamadas por sus siglas en inglés, *BPM o Business Process Management,* que serán las que le llevarán a entender hasta qué punto los procesos de la empresa han sido analizados, cómo se han implementado y cómo se están utilizando por parte de los departamentos usuarios. Cuantos más procesos hayan sido identificados y mecanizados, más eficiente es la compañía.

Por supuesto y para terminar, hay otras formas de automatización en el campo tecnológico más allá del BPM. Desde los habituales *procesos batch* de carga de datos y los servicio web que sincronizan datos *online* hasta una de las tecnologías que con más fuerza se han asomado al mercado de la IT empresarial en los últimos años, el RPA o *Robotic Process Automation.* Dicho de otro modo, el uso de *robots* tecnológicos (los *chatbots* que nos atienden ahora en muchos servicios online son un buen ejemplo) para simular el desempeño de humanos sin que el cliente lo detecte de ningún modo. Esta es una tecnología relativamente nueva, que ha madurado de forma rápida en los últimos años y que permite sustituir tareas operativas sobre servicios IT realizados por un usuario por un *robot.* Este *robot* necesita un cierto entrenamiento, pero una vez lo consigue y en teoría, es tan eficiente como el humano, pero infinitamente más rápido por lo que la eficiencia está servida. De nuevo un apartado a considerar dentro de la *Due Diligence*.

En definitiva, la parte operacional de cualquier *Due Diligence* requiere de un análisis en detalle de todas o casi todas las componentes IT que hemos

enumerado en los apartados anteriores. Esto puede significar la recopilación y gestión posterior de una gran cantidad de datos. Es aquí donde la tecnología también aporta soluciones para hacer el trabajo del auditor más sencillo. Las aplicaciones diseñadas específicamente para el tratamiento de *Virtual Data Rooms* se adaptan perfectamente a la problemática generada durante la *Due Diligence* como vamos a ver en el siguiente apartado.

3. Aplicaciones informáticas para el Soporte al proceso de *Due Diligence*

Dentro de las innumerables familias de *software* que han aparecido en los últimos años nos interesan especialmente para este artículo aquellos productos que pueden englobarse dentro de la familia de *Vendor Risk Management Tools.*

El proceso de *Vendor Risk Management* es responsable de asegurar que el uso de servicios externos de IT proporcionados por otras compañías (*third party*) no nos creará un inaceptable potencial para una disrupción del negocio o impacto negativo en el rendimiento del negocio. Estas aplicaciones ayudan a la monitorización, gestión y asesoramiento de determinados procesos críticos de IT o para IT, gestionando a la vez la exposición al riesgo y aportando indicadores para controlar dicho riesgo. En general se asocian a todo lo relacionado con el cumplimiento normativo (*Compliance*) de la empresa moderna. La mayoría de ellas han desarrollado módulos específicos para el control y seguimiento de la *Due Diligence*. La facilidad para crear *Virtual Data Rooms* basados en espacios en *cloud* que cuentan con la debida facilidad es otra de las características fundamentales de estas aplicaciones.

En general se trata de aplicaciones de propósito específico cuyo objetivo es minimizar el esfuerzo necesario y maximizar el tiempo para el análisis. El objetivo es huir de un proceso focalizado en un conjunto poco estructurado de correos, *PDF, Word* y *Excel* unidos por un único documento maestro realizado, a su vez, con otra herramienta microinformática como *Word* o *Power Point.* Por supuesto esta forma de trabajar no es la más adecuada debido a la ingente cantidad de datos que se manejan durante los procesos de *Due Diligence*.

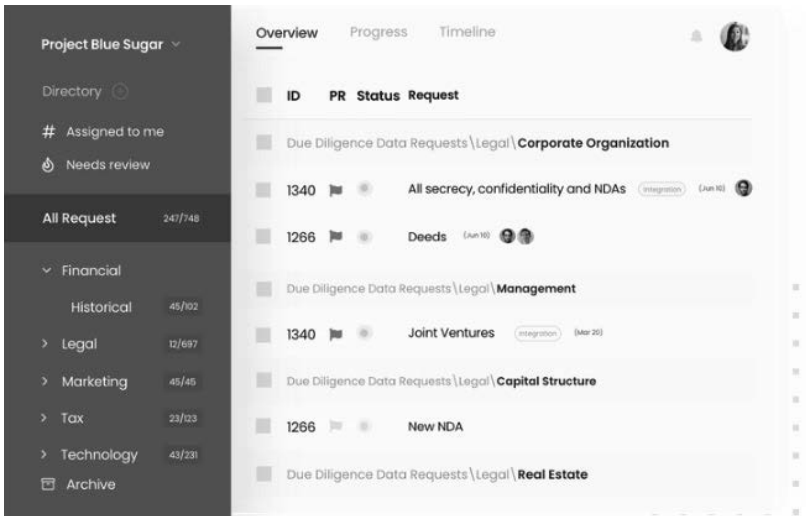
Una mucho mejor solución es disponer de un *software* diseñado específicamente para la *Due Diligence* que guie a través del proceso de principio a fin. Esto facilitará la compartición de formularios, *checklist* y cualquier otro contenido. En general, un proceso de *Due Diligence* es secuencial y ordenado, por lo que desde un punto de vista funcional puede resumirse en

una lista de tares ordenada. El formato de *checklist* donde cada tarea de la lista queda convenientemente marcada una vez completada proporcionará el soporte perfecto al proceso. De esta forma y contando con alguna de estas herramientas desde el principio, es posible monitorizar, controlar e informar del progreso de las tareas en cualquier momento y con la garantía que la actualización es óptima.

En muchos casos, estas herramientas incorporan flujos de trabajo (*o workflows*) que permiten una mínima y simple programación de pasos (*steps*) y autorizaciones (*grants*) para conseguir la confluencia de todas las partes implicadas en un mismo frontal sobre una base de datos común para acabar con emails y otros tipos de incómoda información poco estructurada.

Al lector ávido de mayor detalle en este campo no le será nada difícil tras una rápida búsqueda en Internet, hallar buenos ejemplos de este tipo de aplicaciones. En general, todas las herramientas que se pueden encontrar en Internet están ligadas al mundo del *Compliance* y, como ya hemos dicho, tecnológicamente incorporadas en la familia de productos asociados al *Vendor Risk Management.*

En la siguiente Figura 1, puede verse como ejemplo la apariencia de una de estas aplicaciones con el característico *checklist* ya comentado y un sencillo código de colores (semáforo) que permite a primera vista una impresión del grado de avance de la tarea evaluada.



Fuente: www.dealroom.net

Figura 1. Ejemplo de check list.

4. Conclusiones

La componente operacional de la *Due Diligence* es un proceso exhaustivo de investigación de la compañía objetivo que debe definir cómo lo hace primero y cómo de bien lo hace después. La intersección de este proceso con la tecnología sobre la que la compañía despliega sus procesos de ventas y operativos es inevitable si se desea un producto final completo.

La mayoría de los aspectos tecnológicos (Ciberseguridad, Mapa y Plan de Sistemas, Infraestructura, Arquitectura y aplicaciones, etc.) son comunes a casi cualquier empresa y deberán ser tratados por el experto IT dentro del equipo responsable de la *Due Diligence*. Este experto será el responsable de evaluar los aspectos claves de IT para la *Due Diligence* y valorar los posibles riesgos que puedan existir.

Cada compañía tendrá sus propias particularidades que harán cada *Due Diligence* diferente de las anteriores. Esta diversidad hace recomendable contar con aplicaciones desarrolladas específicamente para dar una estructura a un proceso que puede llegar a ser fácilmente difícil de manejar.

Referencias bibliográficas

Blokdyk, G. (2020) «Vendor Risk Management Practices: A Complete Guide». Ed. Emereo Publishing.

Dewey, R. (2018) «Valuing Data: An Open Framework». Ed. CRC Press.

Langer, A. M. (2018) «Strategic Information Technology: Best Practices to Drive Digital Transformation». Ed. Wiley.

Small, M. J. (2019) «A Quick Guide to Understanding IT Security Basics for IT Professionals». Ed. RMS Consulting.

Soisco, M. (2015) «IT Due Diligence: merger and acquisition discovery process». Ed. MDE Enterprises.