El sector biotecnológico continúa despertando un enorme apetito inversor, pero al mismo tiempo atrae el interés de ciberdelincuentes buscando obtener codiciados datos sensibles sobre patentes, licencias o propiedad intelectual. Tener herramientas de seguridad adecuadas en todos los procesos, desde el fundraising hasta la due diligence, resulta fundamental para proteger el tiempo y el dinero invertido.

CIBERSEGURIDAD, EL TALÓN DE AQUILES DEL SECTOR BIOTECH

// Pese al entorno macro actual hemos seguido viendo apetito por el sector biotech, ¿a qué se debe el fuerte interés inversor en este sector?
La pandemia ha puesto de relieve la importancia de la investigación y el desarrollo en áreas como la biotecnología, la atención médica y las vacunas, lo que generó una mayor atención y demanda de inversores. Estamos hablando además de un sector considerado refugio, que no se ha visto afectado tan negativamente por la incertidumbre macroeconómica como otros sectores económicos. Las cifras hablan por sí solas, tras dos ejercicios alcanzando niveles de inversión récord en el sector biotecnológico español, en 2022 el volumen se ha estabilizado, pero sigue estando por encima de los años previos a la crisis sanitaria. El sector se encuentra en un buen momento, gracias a la solidez y competitividad de las startups y scaleups, el talento de sus equipos, y la irrupción de inversores especializados y sofisticados como Asabys, Ysios Capital, Alta Life Sciences, o Invivo Capital, entre otros.

// La tecnología y la digitalización siempre ha jugado un papel importante en este sector, ¿en qué punto estamos actualmente?
La ciberseguridad sigue siendo uno de los grandes talones de Aquiles en España. El 89% de las organizaciones sufrió un intento de ataque de ransomware el año pasado, mientras que el 72% fue infectado con éxito, según un informe de Proofpoint, y la situación se vuelve crítica si se habla del sector sanitario. España fue el tercer país más afectado del mundo en este sector con aproximadamente 3.300 ataques al sistema de salud en el primer trimestre de 2022. Estamos hablando de un sector que maneja una gran cantidad de información confidencial, incluyendo no sólo datos personales sensibles, sino también financieros e incluso propiedad intelectual e industrial. Son datos muy codiciados por los ciberdelincuentes por lo que su protección se ha vuelto una necesidad crítica y requiere de medidas de seguridad sólidas por parte de las compañías. Una de las soluciones tecnológicas son los Data Room

Clara Càmpas y **Josep Lluis** Sanfeliu
Socios Fundadores de **Asabys.**

"LA TECNOLOGÍA NOS AYUDA A MEJORAR EL FLUJO DE INFORMACIÓN CON NUESTROS LPs"

Desde su fundación en 2018, Asabys Partners se ha consolidado como una de las gestoras españolas de capital riesgo de referencia en el sector salud. Acaba de completar el primer cierre de €100M de su segundo fondo, el Sabadell Asabys Health II, con el que esperan alcanzar un tamaño objetivo de entre €150M y €200M a medida que se vayan incorporando nuevos inversores. "2023 está siendo un año complejo para el levantamiento de capital a nivel global, sin embargo, hemos conseguido captar €100M en este contexto tan complejo, y más aun viendo que una gran parte de nuestros inversores en el fondo I han repetido/aumentado en el fondo II validando así la actividad realizada por Asabys hasta ahora", nos cuentan Josep Sanfeliu y Clara Càmpas, Socios Fundadores de la firma. En 2023 han realizado 3 nuevas inversiones, 2 en compañías de dispositivos médicos, DeepUll y Gradient Denervation Technologies, y 1 en una compañía biotecnológica, OrikineBi, operaciones que han sido lideradas por Asabys junto con gestoras de capital riesgo líderes en Europa, como Sofinnova Partners y Kurma, e inversores corporativos como Werfen y BioMerieux. "Buscamos compañías de los sectores de biotecnología y tecnología médica `healthtech´, que desarrollen y comercialicen soluciones innovadoras para resolver necesidades médicas no cubiertas actualmente. Esto incluye desde tecnologías para diagnosticar enfermedades, como herramientas de monitorización y prevención, así como el desarrollo de nuevos fármacos y terapias", según explican desde la firma. Para Asabys resulta fundamental invertir en ciberseguridad y en tecnología por el desafío que supone trabajar constantemente con información sensible y para mejorar sus vías de comunicación con sus LPs, entre los que destacan Alantra y Sabadell. "La tecnología nos ayuda a mejorar el flujo de información con nuestros LPs, y en especial la VDR de Multipartner, nos permite que nuestros LPs tengan toda la documentación relativa a la inversión disponible en todo momento, de manera que cuando la necesitan pueden disponer de ella al instante. Nos ayuda mucho en los procesos de fundraising y en los de due diligence", nos explican los Socios Fundadores de Asabys.

asabys

Virtuales, que son una herramienta indispensable en los intercambios de documentos confidenciales en las diferentes fases del negocio: investigación y desarrollo, fundraising, gestión de licencias y patentes, pruebas clínicas, etc.

// ¿Cómo ayuda la plataforma de Multipartner a las biofarmacéuticas en sus rondas de financiación? ¿En qué otras fases o procesos ayudáis a este tipo de compañías?

La mayoría de las empresas nacen como proyectos científicos en el entorno universitario con recursos modestos. Suelen contratar un proveedor de Data Room cuando necesitan abordar las primeras rondas de financiación con inversores para seguir desarrollando el producto de forma más segura, rápida y eficiente. Por ejemplo, recientemente, Nuage Therapeutics (portfolio Asabys) ha utilizado nuestra plataforma para su ronda seed de 12M€, y Carthera (portfolio Panakes Partners) para su ronda Serie B de €37,5M. Otro momento crítico es cuando la start up ya tiene productos en desarrollo preclínico y clínico, y llega el primer acuerdo de licencia con una multinacional farmaceútica, momento en el que es imprescindible que inviertan en una VDR. En fases de desarrollo posterior, el departamento regulatorio necesita nuestros servicios para proteger la propiedad intelectual de la compañía y el departamento legal para dar soporte a sus due diligences en procesos de M&A, ofreciendo un acceso rápido a documentos sensibles. En cuanto a salidas a Bolsa, las compañías farmacéuticas y de biotecnología son las segundas más numerosas en el BME Growth sólo por detrás de las tecnológicas, para lo que es imprescindible estar en fase clínica (fase II o III) y, por supuesto, tener una plataforma digital sólida y segura que permita compartir y manejar grandes volúmenes de información. Además, los fondos de private equity y venture capital utilizan la VDR para comunicarse con sus LPs, presentando toda la información relativa a sus distintos vehículos de inversión en un espacio seguro de trabajo virtual; y también para su actividad relativa al proceso de inversión de forma más rápida, segura y eficiente. Por último, las compañías biotech más maduras usan la VDR para intercambiar sus dosieres y cerrar acuerdos de licencia. Un ejemplo es el caso de Palobiofarma, que utilizó nuestro VDR para cerrar un acuerdo comercial con Novartis.

// ¿Qué ventajas ofrece utilizar la tecnología a la hora de realizar fundraising por parte de un fondo que opera en este sector?

Uno de los momentos de mayor vulnerabilidad del proyecto es cuando se comparte la información confidencial de la empresa con terceros, ya que es primordial hacerlo de forma segura. Si la competencia consigue ser más rápida y conseguir los derechos sobre un determinado descubrimiento, patente o medicamento antes que nuestro cliente, perdemos la oportunidad de negocio. Nuestras soluciones facilitan la seguridad y eficiencia necesaria en las rondas de financiación, apoyando y optimizando los acuerdos de licencia y venta, y dando soporte a las posteriores operaciones de inversión y crecimiento vía adquisiciones. Cuando los datos están en "reposo" utilizamos la anonimización de los datos a través de nuestro propio sistema de cifrado, Enigma. El cifrado es una de las herramientas más poderosas disponible, ya que, si pierde o le roban los datos, serán ilegibles y no tendrán sentido. Y cuando los datos están en "tránsito" usamos un nivel de cifrado como TLS 1.3. Además, es importante preguntar siempre al proveedor de la nube dónde se encuentran localizados los servidores, ya que en regiones como la UE existe una mayor protección de los datos. En el caso de las soluciones SaaS (Software as a Service) como la de Multipartner, los proveedores de la nube se encargan de proteger la infraestructura a través de auditorías internas y externas continuas, controles de infraestructura recurrentes y parches continuos.

Mª del Mar García Rodero
Manager Spain & Latam de **Multipartner**

// ¿Qué otras herramientas y qué valor añadido ofrece vuestra plataforma en el sector en un momento actual donde la digitalización es esencial?

La pandemia supuso, por un lado, el boom en investigación que ha multiplicado los proyectos científicos, la necesidad de digitalización y conectividad, lo que ha hecho aumentar la demanda de nuestra plataforma *Workspace Data Room*, utilizada para compartir y administrar documentos y proyectos de manera segura y eficaz entre colegas, socios, clientes e inversores de todo el mundo, y que es posible integrar con un sistema de *Workflow* para la organización de actividades y flujos de trabajo. Además, gracias al nuevo módulo *AGENDA* diseñado para una organización avanzada del calendario. Crear eventos y órdenes del día, convocar reuniones e invitar a los participantes son algunas de las funciones disponibles para facilitar la gestión de las numerosas actividades asociadas a los Consejos. Permite mejorar la transparencia, la eficiencia en el trabajo y la productividad en el contexto del gobierno corporativo.

Por otro lado, han aumentado también los ciberataques, lo que nos ha llevado ha desarrollar varias soluciones de protección para las empresas: la capa de cifrado adicional *ENIGMA,* la activación de varios modos de acceso como la *Autenticación a Dos Factores* o el *Single Sign On* (SSO), y el *Sincronizador Unidireccional* que sincroniza en tiempo real archivos/carpetas de red con las del VDR, para asegurar en todo momento que se tiene siempre la copia actualizada, eliminado así los efectos negativos de cualquier pérdida de datos debida a ciberataques o problemas técnicos. &