“No debemos hacernos trampas al solitario porque los ciberdelincuentes no entienden de esto y todo lo que no esté convenientemente protegido, simplemente no existirá”

José Miguel Ruiz Padilla

Director de Ciberseguridad y Servicios Gestionados de INGENIA (a BABEL company)

>Por **Luis Fernández Delgado**
>Fotografía: **Carlos Bentabol**

Entre las referencias indiscutibles de proveedores de servicios de ciberprotección para entornos corporativos, incluyendo la provisión gestionada, en España figura Ingenia por méritos propios. Su bagaje y especialización, exitoso foco en el ámbito público y generación de producto propio viable, confieren a la compañía de origen andaluz un pujante marchamo que justo ahora acaba de ser refrendado por la operación de adquisición de la misma protagonizada por Babel.

– ¿Qué es hoy Ingenia?

– Ingenia nació en 1992 en Málaga Tech Park, y, en este tiempo, se ha convertido en una multinacional TI que ha acompañado a sus más de 2.000 clientes en 25 países en la digitalización segura de sus operaciones y procesos a través de tres grandes unidades de negocio, que son: ciberseguridad y servicios gestionados, soluciones digitales y soluciones e-Learning. El año 2020, a pesar de la pandemia, batimos nuestro récord de facturación con 21,8 millones de euros, y esperamos superar en 2021 esa cantidad, porque seguimos creciendo y teniendo éxito con nuestra apuesta por la calidad de servicio frente al precio.

Pero algo trascendental ha ocurrido. Después de estos casi 29 años de trayectoria, ahora comenzamos una nueva andadura, ya que en julio, la consultora tecnológica de origen español BABEL adquirió la compañía. De esta manera, los casi 400 profesionales del grupo Ingenia nos incorporamos a un grupo líder que estará formado por cerca de 2.000 profesionales, con presencia en siete países y una facturación que superará los 110 millones de euros.

Las sinergias que esta unión va a producir se traducirán sin duda en los próximos meses en oportunidades de negocio en el ámbito de la ciberseguridad con nuevas capacidades y servicios de valor para nuestros clientes.

– Y, en el contexto histórico, representativo y de actividad, ¿cuál es el alcance del área de negocio de la ciberseguridad y en qué dimensiones tecnológicas y de servicios opera y atiende?

– Ingenia ha sido pionera en redes, Internet y ciberseguridad en Andalucía cuando era cosa de pocos, pero es cierto que hasta no hace demasiado no existía en la organización una unidad de negocio global de ciberseguridad, que además trabaja distribuida entre España y Latinoamérica. La visión 360º de la ciberseguridad que adoptamos hace años nos ha dado muy buenos resultados porque estamos convencidos de que es lo que necesitan la mayoría de nuestros clientes objetivo.

Tenemos equipos de especialistas software, de integración de infraestructura y gestión de

sistemas, de consultoría, de formación y concienciación, equipo azul, equipo rojo, equipo de gestión de incidentes, un SOC 7x24, especialistas en vigilancia digital y ciberinteligencia, así como producto propio GRC como ePULPO, muy empleado en las AAPP españolas, y otros que estamos desarrollando para mejorar la prestación de servicios. Actualmente unas 130 personas entre España y Latinoamérica.

Y todo ello con unos altos niveles de calidad que medimos proyecto a proyecto, e incorporando y formando todo el talento que podemos. Además, estamos certificados según el ENS en nivel alto en los servicios de ciberseguridad, que ya cumplían con la ISO 9000, 27000 y 20000. Y nos ha costado casi 15 años montar todos estos equipos, talento, formación, certificaciones, procesos, herramientas, producto propio para dar un servicio global de alta calidad.

– Porcentualmente, ¿qué parcela corresponde a su actividad en el mercado público y cuál en el privado, y su evolución?

– En Ciberseguridad y Servicios Gestionados está aproximadamente en un 75% privado y un 25% público y en el global de la compañía 60% y 40%. Nuestra filosofía es lograr trabajar con clientes con recorrido y a largo plazo, y no renunciamos por supuesto al sector público que tiene clientes y proyectos super importantes para nosotros, pero pensamos que es muy sano estar por encima del 50% de cliente privado.

– Ya que mencionamos el ámbito público, la casuística española de actores, su interrelación más o menos fluida y el modelo de servicio de ciberseguridad TIC al que se tiende, ¿cómo los valora?

– Cuando una organización está sujeta a las leyes de mercado está obligada a funcionar bien, a mejorar, a ser productiva y eficiente porque si no, la competencia te elimina. Esto no es así en el sector público que tiene sus propias reglas de juego y que cuenta con grandísimos profesionales muy comprometidos pero sujetos a esas diferentes reglas, y esto hace que en ocasiones haya cosas que funcionan muy bien y otras que no. Todos tenemos muy presentes recientes ciberataques cuyos datos nos indican que el impacto no debería haber sido el que ha sido, y ser valiente en el sector público a veces penaliza.

Además, en el ámbito público hay un *gap* importante entre los anuncios presupuestarios de inversión, la verdadera inversión, el posterior gasto recurrente, que es el quid de la cuestión, y la capacidad de rápida adaptación a la realidad que exige lo digital. Todo esto dificulta las cosas, y, aun así, en España creo que hemos avanzado muchísimo en los últimos años y el papel que desempeñan CCN e INCIBE en su colaboración con el sector privado, ha contribuido de manera importante a mejorar la ciberseguridad en el ámbito público, y en el ámbito de pymes y personas físicas respectivamente. Ahí están los resultados en los rankings internacionales en ese aspecto.

En Andalucía se ha creado la Agencia Digital de Andalucía (ADA), que tiene un propósito valiente de coordinar y poner en marcha políticas digitales que actualmente estaban distribuidas entre diferentes Consejerías y otros organismos. Y bajo ese paraguas se ha anunciado el Centro de Ciberseguridad de Andalucía con una inversión inicial importante. Con la dirección y gestión adecuada y un presupuesto, no sólo inicial sino de posterior gasto recurrente, adecuado para lo que se quiere abordar, contribuirá a una mejor gestión de la ciberseguridad no sólo en Andalucía sino a nivel nacional coordinándose con los distintos CSIRTs públicos y privados, donde además espero que se tenga muy en cuenta lo que se hace en otros países para impulsar a la empresa nacional. No podemos pretender que con un mercado tan fragmentado como el europeo, cuando las principales potencias europeas ayudan desde el sector público a sus empresas, sean pequeñas, medianas o grandes, que aquí hagamos lo contrario y nos pasemos el día como en "Bienvenido, Mr Marshall".

"Perdemos bastantes proyectos porque nos negamos a no ganar dinero. Un buen CISO debe exigir que sus proveedores ejecuten proyectos rentables porque si no, no va a poder retener el talento y está perdiendo tiempo con ese proveedor que más pronto que tarde le va a fallar cuando más lo necesite"

– En cuanto a la transformación digital, ¿cómo entiende Ingenia el rol de la ciberprotección en su devenir y qué rol de acompañamiento desempeña o debería desempeñar?

– Las organizaciones llevan años transformándose digitalmente. Es cierto que unos sectores han sido más precoces que otros pero la pandemia lo ha acelerado todo de manera exponencial y se nos echa encima el 5G, la automatización y robotización, sensores e IoT, inteligencia artificial y *machine learning*, analítica de datos avanzada...Todo lo que no esté convenientemente protegido, simplemente no existirá. Digamos que no podemos gastar dinero en arreglar nuestra casa y dejarnos las puertas abiertas. Muchas organizaciones lo están sabiendo ver y están actuando rápido pero también hay todavía un gran porcentaje que siguen pensando en simplemente cumplir o en contratar el servicio más barato posible sin hacer un análisis profundo de cómo mejorar su negocio protegiendo de manera adecuada sus principales activos con un proveedor de total confianza y calidad. No debemos hacernos trampas al solitario porque los ciberdelincuentes no entienden de esto. La ciberseguridad total es imposible, pero con un buen análisis, un buen equipo interno, un buen proveedor y una inversión razonable y sostenida, se pueden evitar muchas situaciones, y si somos atacados, que el impacto sea mínimo. La seguridad debe ser un parámetro de diseño y de funcionamiento de todos los desarrollos y procesos de una organización que pretenda tener futuro porque ese futuro va a ser digital y global.

– En líneas generales, el gran usuario corporativo con quien Ingenia interactúa ¿cómo cree que está actualmente pertrechado en cuanto a recursos, disposición de especialistas y refrendo de la alta dirección en estas materias?

– Según nuestra experiencia y estudios de mercado propios las grandes compañías en España están, en general, bastante bien preparadas en el ámbito de la seguridad IT. Tienen presupuesto, suelen tener un CIO y un CISO, con un equipo especializado propio y proveedores certificados, y les suele costar menos la retención del talento. Es después, cuando damos el salto a compañías, que siguen siendo medianas o grandes pero están en sectores menos digitalizados o que tienen departamentos de IT más pequeños, a los que se les ha dado también la responsabilidad de la seguridad recientemente, las que tienen bastantes problemas para llegar a todo. Y en algunos casos nos llega que el freno les viene de arriba, que tienen limitaciones presupuestarias o que desde la alta dirección comprenden que hay que invertir en

activos más directamente relacionados con el negocio pero no tanto en digitalización, y menos en ciberseguridad, porque es difícil demostrar el ROI de no tener ciberincidentes. Es necesario dar la vuelta a ese concepto y mostrar el impacto reputacional y coste de sufrir un solo ataque donde logren una penetración importante e incluso llegue a afectar a los clientes.

En el ámbito de la seguridad OT seguimos percibiendo que aún hay un *gap* importante, no hay profesionales formados en el mercado para todo el trabajo que se debe llevar a cabo y hay que empezar a afrontarlo ya porque el impacto de los ataques es muy diferente, ya sabemos que crítico en muchos casos, y con afectación de la población y posible riesgo incluso de vidas humanas en ocasiones.

– ¿Cree usted que está aflorando en la sociedad un sentimiento creciente de inquietud y desconfianza ante lo digital dada la fragilidad percibida ante la abultada oleada de agresiones a las instituciones públicas y privadas por todo tipo de ciberataques, brechas, exfiltraciones y *ransomware* mayormente?

"La inversión pública en I+D debería dedicarse más a investigación básica y desarrollo, y después tener buenos mecanismos de colaboración público-privada para que las empresas sean las que innoven en todo aquello que les haga más competitivas, de manera que la financiación y fiscalidad de esa innovación sea muy ventajosa"

– Desafortunadamente con la pandemia hemos vivido en primera persona como, por un lado, el ser humano sólo aprende a base de repetir y repetir el mensaje, y por el contrario, ese mismo mensaje repetitivo y exagerado, abruma, cansa y termina por generar el perverso efecto contrario. No hay día en el que muchas personas que estamos en este mundillo estemos comentando en las redes sociales múltiples ataques y sus consecuencias, mientras sorprende cuando vas a determinadas organizaciones y cómo están a pesar de "la que está cayendo". Especialmente vemos muy confiados a la alta dirección y Consejos de Administración, pero no deberían estarlo. Deberían asegurarse, porque tienen la responsabilidad final, de que han velado por la mejor ciberseguridad posible en sus negocios, activos, personal, clientes, proveedores, etc. También hay que decir que hablamos mucho del concepto de "nativo digital" pero precisamente nuestra visión es que los nativos digitales se preocupan muy poco en general de su privacidad, de la confidencialidad, de los datos, de las contraseñas, etc. Quizás hay incluso hasta cierta polarización en personas y organizaciones, los que están tremendamente preocupados y ven peligro ante el más mínimo intento, y los que viven demasiado despreocupados. Lo ideal sería un término medio. Con las medidas adecuadas, se puede vivir relativamente seguro, no 100% seguro, pero puedes trabajar que si ocurre algo el impacto sea bajo, lo que no puedes hacer es cerrar los ojos y como la seguridad total no es posible, pues que pase lo que tenga que pasar. Esto se ve aún demasiado.

– La extorsión y chantaje de las abrumadoras oleadas del *ransomware* están desbocadas atenazando incluso al sector oferente asegurador de ciberpólizas. ¿Cómo valora esta fragilidad actual y cuál es su visión para tratar de solucionarlo, más allá de la obvia insistencia en la concienciación?

– Es una pregunta muy relevante y tremendamente complicada de abordar. Posiblemente sea sencillo hablar teorizando pero cuando sufres un secuestro y no te queda otra que pagar para salvarlo todo, también hay que intentar entender la situación. No es lo que se debe hacer, sería colaborar con criminales y provocar que el delito sea rentable y les merezca la pena continuar y expandirlo, por tanto, agravamos el problema. Las organizaciones están dispuestas a pagar cantidades razonables si no hay consecuencias y si no sale a la luz pública. Bajo mi punto de vista la mejor solución es dejarse asesorar por la Policía y cumplir la ley, y ponerse en manos de expertos para solucionar el problema.

– En el ámbito específico del trabajo en remoto de la actividad empresarial laboral, ¿cómo dimensiona la situación derivada de la pandemia y en qué media y qué porcentaje ha aumentado su facturación centrada en afrontar estos aspectos en sus clientes?

– Ha sido sin duda un antes y un después en España, donde aún había poca flexibilidad en muchos sectores, con bastante presencialidad y la ciberseguridad adaptada a ello. A nosotros afortunadamente nos pilló preparados y pudimos ir a teletrabajar todos inmediatamente de manera segura, pero ha habido organizaciones, algunas muy grandes, que han tenido pérdida de productividad durante meses, afrontado riesgos de seguridad. En nuestro caso en 2020 el impacto en la facturación aún no fue demasiado relevante por el decalaje de los proyectos y presupuestos, y contentos estamos de haber crecido frente a 2019 sin pérdida relevante de proyectos importantes, pero en 2021 sí que esperamos que ya tenga un impacto cercano al 10-15%.

– ¿De qué proyectos realizados recientemente o en plena inmersión actual en colaboración con clientes están ustedes más satisfechos? ¿Pueden dar algunas referencias y foco concretos?

– Tenemos especial interés y buenos resultados en proyectos y clientes que cuentan con Ingenia para acompañarlos durante todo el proceso de mejora de la ciberseguridad. Clientes que confían en nosotros para diagnosticar su situación actual, establecer objetivos de mejora y trazar una hoja de ruta ajustada a sus necesidades. Combinando siempre que sea posible y aplique la seguridad estratégica, con la gestionada y la integración de soluciones tecnológicas para mejorar la protección. En este sentido, cabe destacar, entre otras muchas referencias, a Globalvia, una organización que contempla la ciberseguridad como proceso clave en la gestión estratégica y operativa, con quienes colaboramos desde 2016 prestando servicios de SOC 24x7 para corporativo y concesionarias nacionales e internacionales (Portugal, EE.UU., Costa Rica y Chile), seguridad defensiva con nuestro Blue Team y ampliando alcance este año para cubrir también las infraestructuras OT. Igualmente, como referencia relevante contamos con el Senado de la República de Chile, donde también prestamos servicios de SOC 24x7, bastionado y respuesta a incidentes de seguridad, entre otros.

En el sector público, contamos además con perfiles altamente especializados y certificados que nos permiten acometer proyectos de cumplimiento normativo y legal (ENS, ISO 27001, RGPD, etc.) con una metodología propia y muy adaptada a las necesidades de los distintos tipos de organismos, enfocada a conseguir la certificación junto con la mejora tangible de la ciberseguridad, como son los casos de la Universidad Complutense de Madrid, múltiples organismos de la Junta de Andalucía, Dirección General de Seguros y Fondos de Pensiones, Instituto de Crédito Oficial, Autoridad Portuaria de Baleares y otros. Recientemente hemos conseguido contratos relevantes con empresas privadas que aún no estamos en disposición de desvelar.

– La prestación de servicios de ciberseguridad es una de sus principales señas de

identidad. ¿Qué bazas diferenciadoras esgrimen?

– Como parte de la filosofía de Ingenia, nuestro diferencial es la alta exigencia de calidad en cada uno de nuestros proyectos, entendiendo muy bien la situación de nuestro cliente, de nuestro interlocutor y de su negocio. No en vano llevamos años exigiéndonos proyecto a proyecto una calidad percibida por encima de 8 sobre 10, y una visión de la tecnología y de la seguridad como medio y no como fin, desde un punto de vista 360. De nada vale estar super protegidos en un aspecto descuidando otros, es fundamental ir con un plan global adaptado a la realidad de cada cliente y su negocio, y además hay que defender que los servicios de calidad tienen un precio. Diría que perdemos bastantes proyectos porque nos negamos a no ganar dinero. Un buen CISO debe exigir que sus proveedores ejecuten proyectos rentables porque si no, no va a poder retener el talento y está perdiendo tiempo con ese proveedor que más pronto que tarde le va a fallar cuando más lo necesite.

– En estos tiempos abocados, al fin, a poner el ojo en la I+D+i europea en ciberseguridad, ¿cómo valoran la tesitura española en cuanto a apoyo y venideras inversiones, mayormente vía fondos europeos, en la materia? Ustedes ya desarrollaron con contrastado éxito ePULPO…

– Es cierto que tenemos cierto éxito en el desarrollo y comercialización internacional de producto propio, aunque nos gustaría que fuera más (en 2020 representó aproximadamente el 10% de la facturación y pretendemos llegar al 15% en 3 años). En el ámbito de la ciberseguridad con ePULPO, adquirido por más de 50 organizaciones nacionales e internacionales para realizar la gestión de sus activos IT y ciberseguridad, pero también con productos como eRLS para la gestión RFID de bibliotecas o la familia de soluciones para emergencias eCALLER, que actualmente se usa para gestionar las emergencias en el Servicio Cántabro de Salud, en El Salvador y Bolivia, así como la principal aseguradora médica de Argentina. Para aumentar esas ventas por innovación y producto propio implantamos hace año y medio un sistema de gestión de la innovación basado en metodología "lean startup" que nos está dando magníficos resultados, donde puede participar cualquier empleado en base a retos, y donde colaboramos con el ecosistema a la hora de realizar los desarrollos, siempre orientados a negocio, al cliente, y no a la tecnología.

Creo que la inversión pública en I+D debería dedicarse más a investigación básica y desarrollo, y después tener buenos mecanismos de colaboración público-privada para que las empresas sean las que innoven en todo aquello que les haga más competitivas, de manera que la financiación y fiscalidad de esa innovación sea muy ventajosa. Ahí están los resultados pasados de toda la inversión en I+D+i "regada" con dinero público de la UE y no sólo en España. Las mayores innovaciones y grandes empresas digitales del mundo siguen surgiendo y desarrollándose en Estados Unidos. Nos guste o no, debe ser que su modelo de innovación funciona mejor.

– La sede corporativa de Ingenia radica en Málaga, un lugar hoy de máxima proyección tecnológica en tanto nodo de referencia territorial y en el que una de sus principales bazas aplica precisamente a la acumulación de actores de peso en ciberseguridad…

"En ciberseguridad ahora mismo todos nos estamos intentando posicionar, pero al negocio le falta madurez y si los clientes siguen apostando exclusivamente por el precio más bajo sin tener en cuenta la calidad del servicio, y las empresas aceptamos ese juego, volveremos a repetir errores del pasado que generarán frustración de todos"

– Efectivamente, Málaga ha sido durante años tierra de oportunidades de negocio en el sector IT porque reúne una serie de requisitos muy atractivos. Es una ciudad grande en su ámbito metropolitano pero lejos de las masificaciones de Madrid o Barcelona. Tiene buen clima todo el año, buenos equipamientos culturales y servicios, toda la Costa del Sol para residir y muy buenas comunicaciones nacionales e internacionales con uno de los principales aeropuertos de España. A todo ello se le une la visión estratégica y voluntad desde hace más de 30 años de una serie de personas, organizaciones públicas y empresas que ya estaban instaladas en la ciudad, para impulsar tanto las Escuelas de Telecomunicación e Informática en la Universidad de Málaga y el Parque Tecnológico de Andalucía. Como resultado de este trabajo continuado tenemos hoy un *hub* de tecnología e innovación de los más importantes de Europa con empresas muy relevantes en ciberseguridad y sector IT en general.

Pero la pandemia y el teletrabajo también está cambiando esto, y las organizaciones y las ciudades se van a tener que adaptar. Hay que continuar siendo competitivos en todos los aspectos para atraer y retener el talento, y con el teletrabajo este talento puede decidir vivir hoy en Málaga y mañana en cualquier otro sitio. No podemos confiarnos en que todo lo consigue el buen clima y hay que seguir trabajando todos en los parámetros que más valora el talento para trabajar en una organización y vivir en un territorio.

– Una última pregunta: ¿Cómo se las apañan para disponer del suficiente personal experto para atender la nada trivial y creciente demanda del mercado? ¿Bastan buenos sueldos? ¿Formación continua? ¿Teletrabajo de mar y sol…?

– Como todas las empresas que estamos en el sector ahora mismo compitiendo por atraer y retener el talento más adecuado para nuestros proyectos y clientes. Ingenia se ha visto siempre como una compañía seria y reconocida en Andalucía, con unos valores de estabilidad y permanencia en el mercado que son atractivos. No muchas empresas de tecnología pueden decir que llevan 29 años pagando la nómina puntualmente a pesar de diversas crisis y dando carrera profesional a profesionales que llevan en la compañía desde su fundación y todo esto se va a ver reforzado por la integración en el Grupo BABEL, y su apuesta fuerte por el equipo y la cultura deportiva, donde las personas son el centro. Su modelo cooperativo, beneficios sociales y planes de carrera sin duda atraeran talento.

Evidentemente trabajar en Málaga o Sevilla puede resultar atractivo pero la evolución salarial y profesional y poder aprender múltiples tecnologías y trabajar en proyectos interesantes, es determinante. Además, las personas necesitamos aprender y desarrollarnos profesionalmente en un buen ambiente donde casi siempre está muy bien puntuada la relación con los compañeros y, tengo que decirlo, incluso con los jefes. Tenemos vínculos con distintas universidades, pero también colaboramos estrechamente con centros de Formación Profesional y para acelerar la adaptación a proyectos concretos, lanzamos *bootcamps* propios con compromisos de contratación.

También sucede que se está "recalentando" más el mercado salarialmente que lo que los clientes están dispuestos a pagar por los servicios. Aún escucho que se está ganando mucho dinero en ciberseguridad y esto no es así. En ciberseguridad ahora mismo todos nos estamos intentando posicionar, pero al negocio le falta madurez y si los clientes siguen apostando exclusivamente por el precio más bajo sin tener en cuenta la calidad del servicio, y las empresas aceptamos ese juego volveremos a repetir errores del pasado que generarán frustración de todos. ■