“En ciberseguridad, si se tiene vocación de permanencia, hay que apostar por la calidad de los servicios”

Félix Muñoz

Director General de Entelgy Innotec Security

>Por **José de la Peña Muñoz**
>Fotografía: **Jesús A. de Lucas**

Buen conocedor del sector de la ciberseguridad desde hace más de dos décadas, Félix Muñoz ha participado en muchos proyectos públicos y privados, en España y fuera de ella. Ha ido, paso a paso, y codo con codo con su equipo de colaboradores, haciendo de Entelgy Innotec Security uno de los grandes proveedores del sector. Como persona de pocas palabras, este informático de profesión ha utilizado las justas para brindarnos en esta entrevista la visión de su compañía y su estilo de competir.

– ¿Cómo desea que la demanda perciba a Entelgy Innotec Security?
– Como una empresa española especializada en ciberseguridad que dispone de expertos con una competencia técnica muy alta y que sólo trabaja en proyectos con retorno para sus clientes.
– ¿Qué hace su compañía que no puedan ejecutar otras?
– No nacimos como una gran marca, y llevamos diecinueve años en la ciberseguridad. Hemos ido creciendo con mucho esfuerzo y muy apegados a la calidad de nuestro trabajo, de tal suerte que los grandes usuarios nos tienen en cuenta y estamos ya en las grandes licitaciones. El secreto ha sido la constancia, cuidar mucho al equipo y, por ende, disponer de capacidades muy bien estudiadas y en continuo refinamiento.
Hay otro factor importante: la agilidad. Somos una compañía poco jerarquizada, lo que nos permite adaptarnos a la velocidad y profundidad de las demandas de las organizaciones en transformación digital. Le puedo decir que yo tengo contacto con todos nuestros clientes.
Obviamente, seguimos ampliando capacidades, consolidando la presencia en España y fortaleciendo nuestra vocación exportadora de productos y servicios.
– ¿Cuántas personas forman el equipo de Entelgy Innotec Security?
– Actualmente, 450. Como ve, somos un jugador grande en el nicho de la ciberseguridad. Y vamos a seguir creciendo.
– ¿Cómo balancean los trabajos de consultoría, los de servicios TIC y el desarrollo de herramientas?
– En nuestra organización hay un director de operaciones. Y por cada especialización un gerente, que tutela los proyectos y evoluciona nuestras capacidades.
Tenemos un área de consultoría de alto nivel, cumplimiento y GRC. El objetivo aquí es ayudar al cliente, según su nivel de madurez, en la definición e implantación de medidas y controles efectivos para la mejora.
Por su parte, el área de servicios está dividida en Blue Team y Red Team. En la de Red Team, Hacking Ético y Análisis de Vulnerabilidades, su gerente va definiendo las líneas de evolución y diferenciación; en tanto que en la de Blue Team, tenemos diferentes subáreas: SOC (o MDR), Cyber Threat (ciberinteligencia, amenazas en redes sociales, *Deep* Web, antifraude); y, debido a las necesidades, hemos fortalecido la subárea de anti*malware* y gestión de incidentes, que tiene un gerente dedicado y nutre al resto de áreas.
En lo que toca a productos, disponemos de dos líneas: una es la relacionada con nuestro papel de integrador de ciberseguridad IT y OT. Antes se ubicaba en el Blue Team; pero este año hemos decidido hacer un cambio, y en la parte de productos de terceros nombrar un gerente, cuyos objetivos pasan por crear nuevas alianzas, conocer productos y presentarlos.
La otra línea es la de productos propios, con dos orientaciones: la de desarrollo para venta, y la que se incardina más en nuestro ADN, que es el desarrollo de esos productos para incorporarlos al ciclo completo de nuestros servicios, de tal suerte que contribuyan a su diferenciación.
– ¿Cómo va la compañía? ¿Ganan dinero?
– Malo sería si no lo hiciéramos. El año pasado, a pesar del frenazo general en algunos segmentos del mercado, crecimos un 16% sobre las cifras de 2019. Y en todas las áreas.
De todas formas, no estoy obsesionado con los números. Siempre hay que caminar por la senda de la viabilidad financiera. Pero si se tiene vocación de permanencia y mejora, algunos años toca invertir en capital humano, mejoras organizativas, capacidades, herramientas… En dicho año, bajan los márgenes.

"Somos actualmente 450 personas en la compañía. En el ejercicio pasado, a pesar del frenazo general que se registró en algunos sectores de la economía, crecimos un 16% sobre las cifras de 2019. Y en todas las áreas".

– ¿Les preocupa el I+D+i?
– Adolecemos de un marco nacional para gestionar las iniciativas y, por supuesto, culminar el itinerario hasta el último tramo, el de la comercialización aquí y en el exterior.
Prácticamente solo se subvenciona el desarrollo de productos. Pero no parece que se entienda que hay que aplicar una gran inversión para su venta: implantarse en los mercados, conocer sus peculiaridades domésticas, encontrar buenos socios, … Muchas grandes ideas, convertidas en herramientas técnicamente excelentes, no han fructificado por la imposibilidad de llegar al ciclo comercial.
– ¿Cómo hacen ustedes para conservar a sus empleados y para fichar a nuevas personas con perfiles de interés?
– Retener y captar talento es una de mis principales preocupaciones. Las personas tienen que sentirse bien en el equipo y saber que tienen carrera profesional. Y parece que por el índice de rotación vamos por buen camino, porque nos situamos entre un 7% y 8%, porcentajes inferiores a la media del mercado español. Los factores psicológicos de arraigo a una compañía en el trabajo presencial

han cambiado con el teletrabajo, por lo que hemos tenido que idear nuevos métodos para mantener el contacto entre todos y potenciar la sensación de pertenencia al grupo. No obstante, mi filosofía siempre ha sido tener el teléfono abierto para cualquier compañero de la empresa y mi despacho, también.

– ¿Qué perfiles son los más codiciados?

– La joya de la corona es el perfil de buen técnico con, a la vez, capacidades de gestión. Y, por supuesto, los analistas especializados.

Pero en este punto me gustaría remarcar que en España tampoco se pagan grandes dinerales en salarios, y las tarifas que tenemos los prestadores, en un mercado tan competitivo, son limitadas. Por añadidura, las áreas de compras de las grandes empresas son implacables. Esta es la situación actual del mercado. ¿La culpa? Pues de ambas partes, oferta y demanda.

– Trabajar a pérdidas no es buen negocio…

"Adolecemos de un marco nacional para gestionar el I+D+i y culminar el itinerario hasta el último tramo, el de la comercialización. Generalmente solo se subvenciona el desarrollo de productos. Pero no parece que se entienda que hay que aplicar una gran inversión para su venta".

– A pérdidas o con márgenes desproporcionadamente bajos. Es malo para los clientes y para los proveedores. Sin embargo, el desequilibrio persiste. Nosotros no estamos en esto.

– ¿Cómo se va a ir desarrollando la ciberseguridad OT?

– Los proveedores de servicios de ciberseguridad TIC hemos partido de un gran desconocimiento de la ciberseguridad OT. Para entrar en OT se necesitan expertos que vengan de OT y que dominen la práctica de la ciberseguridad. Eso es lo que hemos hecho nosotros al fichar a un especialista con experiencia contrastada y que conoce bien las áreas de ingeniería OT, Alejandro Villar.

¿Por dónde van a ir los dos mundos, IT y OT? Pues por eficiencia, se integrarán en materia de servicios. Y a efectos tecnológicos, deberemos profundizar en estándares bien establecidos que hagan posible la ciberseguridad por diseño.

– ¿Se abre hoy una vía para modernizar de verdad a las Administraciones Públicas, ciberseguridad incluida?

– Hay recorrido. El problema que le veo es el modelo que tienen en las Administraciones Públicas para modernizarse a través de su transformación digital, en el que, en líneas generales, no se ha tenido en cuenta la gestión efectiva de riesgos de ciberseguridad.

El cambio que se espera en el ENS y la potenciación de todos sus efectos en los pliegos dan una oportunidad, si no fuera porque en el ámbito público se va a precio. Así no hay manera de revisar las plataformas, de evaluar los riesgos de ciberseguridad en el contexto de la digitalización, de diseñar e implantar controles, de auditar… Hay que ser menos reactivos y realmente disponer de entornos seguros.

-Siempre nos quedará innovar.

-Para innovar no solo hace falta poner en los pliegos las expresiones *Machine Learning*, IA y alguna otra más. Ojalá sepamos aprovechar la oportunidad.

– ¿Cree que es correcto el modelo de servicio de ciberseguridad TIC por el que parece que se apuesta en la AGE?

-Sí. Tendremos equipos más preparados, desaparecerán islas y se implantará un modelo de gestión homogéneo y unas evidentes economías de escala. Obviamente, los proveedores de servicios especializados del mercado, particularmente los españoles, estamos expectantes para ver cómo va cristalizando el COCS. Nosotros creemos que con la experiencia que hemos atesorado en nuestra colaboración con el CCN, podemos aportar un gran conocimiento.

– ¿Observa algún cambio significativo en los compradores privados?

– Los usuarios corporativos atesoran gran experiencia en la gestión de riesgos, y en lo que se refiere al que nos ocupa buscan una cierta calidad, porque la experiencia de ir exclusivamente a precio hizo que esta se resintiera.

Además, los procesos de llamamiento al mercado, selección de proveedores, evaluación y compras en el sector privado son mejores que en el sector público para valorar, estimar o desestimar.

– CISOs, proveedores y reguladores andan estremecidos ante el colosal empeño en gestionar los riesgos de ciberseguridad de la cadena de suministro. ¿Se conseguirá?

– Hay algunos proyectos; pero son complejísimos, empezando por el sector del usuario, por su implantación geográfica, su política de adquisiciones y participaciones, y por, en general, su entorno heterogéneo de cumplimiento. Incorporemos, además, en la ecuación la relación contractual con los distintos tipos de proveedores, las cadenas de subcontratación y la estabilidad y estados de la economía en los distintos mercados en los que operan.

En suma, y sin querer entrar por lo menudo en los accesos a la red del cliente y tratamientos de datos del cliente y de terceros, lo que procede aquí es un macroplan y, tras él, establecer un modelo de revisión ligera y automatizada de la cadena de suministro. Importante: todos los implicados deben saber a qué atenerse ante ciertas circunstancias. Si no se consigue esto…

– Una última pregunta. Las *Big Four* tienen una presencia muy destacada en la consultoría TIC y en la provisión de servicios TIC. ¿Qué le parece?

– Creo que las grandes auditoras, por las especiales características de ese servicio, deberían mantenerse en la auditoría. Pero esta es una polémica que se pierde en la noche de los tiempos. ■