“Cuesta hacer llegar a los profesionales la necesidad de una certificación complementaria a su formación”

Alfonso Castaño
Presidente del Capítulo Español de ASIS International

El Capítulo Español de ASIS International eligió en diciembre a Alfonso Castaño como presidente, tras la salida de Juan Muñoz después de seis años en el cargo. Estará al frente de una junta directiva que, aunque es continuista como el propio Castaño indica, también incorpora varias caras nuevas. Pero las novedades no se quedarán en las personas, sino que también se traducirán en proyectos con un enfoque un tanto diferente al de hasta ahora, como por ejemplo la formación de valor dirigida a profesionales de mandos medios del sector con aspiraciones a promocionar en sus empresas. Algo que acompañarán, como no podía ser de otra manera, de las certificaciones de ASIS International, que este año incorpora una nueva, la APP (*Associate Protection Professional*). La formación será, por tanto, una de las prioridades de Castaño durante su etapa en la presidencia.

Por Enrique González Herrero
Fotos: J. S. Arenas

- El pasado diciembre resultó elegido nuevo presidente del Capítulo Español de ASIS International. ¿Cómo han sido estos primeros compases al frente de la organización?

En estos primeros momentos estamos centrándonos en mejorar la gestión administrativa. Para nosotros esta parte supone bastante tiempo los primeros meses del año, y más este en el que la política de ASIS International ha sido renovar a todos sus miembros antes del fin del ejercicio; algo que nos han comunicado en los últimos días de 2018, con lo cual nos hemos visto obligados a agilizar esta gestión. Después se trata de encauzar temas como los patrocinadores, con los que tenemos que contar para organizar nuestros eventos. Nuestra idea es cerrar en el primer trimestre del año todo lo que afecta a la organización desde el punto de vista administrativo.

- Se ha rodeado de una nueva junta directiva en la que hay profesionales que continúan y también caras nuevas. ¿Qué tipo de junta quería conformar?

La junta tiene un carácter continuista en cuanto a los principales perfiles. De hecho, en el *staff* se mantienen el vicepresidente y el secretario, si bien cambiamos el tesorero y yo como presidente.

En cuanto a las vocalías, estamos intentando estructurarlas de una manera diferente. En ASIS International existe una limitación de vocalías técnicas, pero las *policies* internas permiten una cierta flexibilidad de gestión por medio de comisiones de trabajo. Queremos explorar esa posibilidad porque creemos que las vocalías deben ser más cercanas al socio. Al efecto, vamos a proponer que cada vocalía pueda desempeñar unas acciones concretas, que habrá que someter a la junta para que las apruebe. Una de las posibilidades es habilitar un correo electrónico para estar más cerca del socio en aspectos que tienen que ver con su propia vocalía y en los que no tiene por qué interferir tanto la junta directiva. Por ejemplo, estoy pensando en la vocalía de relación con el socio, que podría resolver directamente cosas como que no se ha renovado bien o que figure incorrectamente la dirección de correo sin que escalen al presidente.

- ¿Cuál es su propuesta como nuevo presidente de la asociación? ¿Qué objetivos se ha planteado?

Nuestra idea es trabajar en tres ejes. El primero son los socios; buscamos que entiendan que ASIS es una asociación porque es el formato que se exige en España para que podamos funcionar, pero en realidad somos mucho más que eso. Tenemos una enorme relación con los socios de otros capítulos a nivel global y una gran capilaridad de conocimiento a través de ellos. Por poner un ejemplo, en ASIS es perfectamente factible obtener información y opinión de los miembros de cualquier otro capí-

tulo sobre su país en concreto o acerca de algún aspecto de la seguridad desde la óptica local; es tan sencillo como enviar un correo y recibir respuesta. En ese sentido hay que decir que, aunque existe la idea de que el idioma oficial en ASIS es el inglés, lo cual no deja de ser cierto, tenemos un buen número de capítulos en Iberoamérica que comparten la lengua con nosotros, lo que posibilita una interacción directa con ellos.

Un segundo eje sería compartir experiencias entre nuestros socios y patrocinadores. Debe existir la posibilidad de que ambos tengan una relación de acercamiento más rápida y certera, evidentemente dentro de una política de gestión de privacidad y tutelada desde la vocalía interesada y la propia junta. Para nuestros patrocinadores en España puede ser importante conocer quién sería un buen *partner* en Panamá, por ejemplo, mientras que para los socios sería interesante saber qué posibilidades de desarrollo personal existen en determinado país a través de alguno de nuestros *partners* que operan allí.

Otro eje es buscar que los socios tengan la mayor formación posible, si bien esto hay que matizarlo. En años anteriores hemos propiciado una formación de alto nivel para perfiles elevados en cuanto a conocimientos y posición dentro de la empresa. Este año vamos a prestar atención también a los mandos medios intentando que las formaciones, sin perder el valor añadido, sean más cercanas en contenidos o más fáciles de aplicar en el día a día, tanto parta los socios de alto nivel como para los mandos medios que tengan posibilidad de acceder a posiciones superiores en los próximos años.

Evidentemente, todo esto lo acompañamos de nuestra gestión de certificaciones. Este año añadimos además una nueva, APP, que es una certificación previa al CPP pensada para perfiles menos experimentados, y por supuesto mantenemos las certificaciones PSP, CCP y PSI. En este sentido, hay que decir que el formato de formación en ASIS son las certificaciones, que deben renovarse cada tres años. Eso implica que los profesionales que las obtengan tengan que mejorar sus conocimientos y tenerlos actualizados. Es una manera de entender el desarrollo profesional diferente a la que existe con habilitaciones como la del director de Seguridad en España, que es casi vitalicia.

Un último eje será, por supuesto, mantener al mismo nivel que hasta ahora las relaciones con las Fuerzas y Cuerpos de Seguridad [en adelante, FCS] y otras instituciones.

- ¿En qué consiste, más concretamente, la nueva certificación APP?

Esta certificación tiene un temario más reducido que la de CPP y exige menos experiencia de partida. Es más breve y las exigencias son menores. Está pensada para profesionales que acaban de terminar la carrera y son técnicos, que llevan tres años al frente de un departamento de Seguridad pequeño o que están en una posición de segundo o tercer nivel en un departamento de Seguridad Corporativa pero quieren una formación que les abra paso más adelante.

En el caso de APP se mantiene el mismo sistema de certificación. Y por tanto puede complementarse posteriormente con las de PSP y PCI; no así con la de CPP, que de obtenerse pasa a invalidar la de APP. Si tuviera que recomendar una trayectoria profesional a un joven que trabaje en el mundo de la seguridad, las fases serían terminar su carrera o formación específica, esperar a tener esos dos o tres años para acceder a la certificación de APP y, posteriormente, con ella aspirar a otras como PSP, PSI o CPP.

- Como ha mencionado, ASIS cuenta con los estándares de certificación para profesionales de la seguridad más importantes. ¿Están satisfechos con la cantidad de profesionales certificados en España?

Sin ninguna duda, la respuesta es no. Tendríamos que ser muchos más, y de ahí nuestro empeño en darlas a conocer.

Por otro lado, en España ya tenemos una habilitación para trabajar como director de Seguridad y a veces es difícil hacer llegar a ese profesional que necesitaría una certificación complementaria mucho más amplia en conocimientos y contenidos para formarse mejor

"En el futuro, lo que va a definir un buen sistema de seguridad serán las analíticas y la inteligencia artificial aplicada"

y desarrollar su labor. El profesional que se ve entre una habilitación que ya tiene y otra que no necesita para ejercer toma el camino más cómodo. Por tanto, habría que apelar al deseo de formación, más que al de poder trabajar.

- ASIS ha apostado especialmente en los últimos años por la formación y otros proyectos con la internacionalización como foco. ¿Qué tipo de cursos pondrán en marcha en esta etapa?

Estamos trabajando ahora en una serie de ideas entre las que se encuentra hacer alguna jornada o congreso sobre *Women in Security & Young Professional*, porque entendemos que las mujeres y los jóvenes profesionales no suelen ser los perfiles habituales. Esto nos va a ayudar también a desarrollar iniciativas con las universidades. No estoy pensando ahora mismo en una formación concreta, sino en acciones divulgativas para los estudiantes de los últimos cursos de carrera. Por ejemplo, que los estudiantes de ingenierías vean que la posibilidad futura de certificarse en PSP les permitirá desarrollar su perfil de una forma reglada y con una certificación reconocida internacionalmente.

También tenemos en mente llevar a cabo algún evento formativo sobre gestión de proyectos de seguridad, investigaciones dentro de la empresa, etc. En realidad tenemos preparado un completo porfolio de actividades para este año, a falta solo de concretar fechas.

- ¿Cuál es el principal valor que aporta el Capítulo Español de ASIS International a sus asociados?

Para mí hay un valor clave que son los estándares relacionados con la seguridad, la mayoría traducidos, que están a disposición de los socios. Existen estándares de todas las funciones que se puedan imaginar: seguridad en edificios, frente a incidentes armados, en centros comerciales… Todo eso está tabulado bajo métricas, lo que no quiere decir que sean guías inapelables; pero permiten al profesional que no sea experto acercarse a ello y comenzar su propio proyecto de seguridad, respetando unos estándares reconocidos internacionalmente y que funcionan.

Otro valor de ASIS es la posibilidad de que los socios se relacionen entre sí. Nuestros asociados engloban a fabricantes, vendedores, ingenieros, directivos de seguridad, responsables de ciberseguridad, de IT, miembros de las FCS, militares y detectives; y todos tienen el mismo tratamiento. Todo ese *networking* es tremendamente activo en ASIS International, pero creo que los socios no lo explotan lo suficiente.

- ¿Cree que el sector está preparado para el reto de la digitalización desde el punto de vista de la seguridad?

Tenemos por delante tres tipos de retos. Por un lado estarían los formativos, dado que hemos de tener un cierto nivel de entendimiento, que no de conocimiento, de las tecnologías para sacar provecho de ellas. Las tecnologías son el elemento democratizador en cualquier sistema de seguridad. Es decir, entre un departamento de Seguridad pequeño que posea una tecnología puntera y un departamento muy dotado de personal que maneje una tecnología más antigua puede haber una diferencia sustancial a favor del primero.

El segundo problema que tenemos es estructural, porque no contamos con una carrera profesional en seguridad. No olvidemos que las únicas figuras reconocidas por la Ley de Seguridad Privada son las de vigilante, guarda de campo, escolta, jefe de seguridad, director de seguridad y detective privado. Pero si accediéramos al organigrama de cualquier empresa de seguridad veríamos muchísimos más puestos que no están recogidos en la norma. Por eso tenemos que tener una carrera profesional; no tiene sentido que la única perspectiva de un vigilante sea convertirse en jefe o director de seguridad, cuando laboralmente hay muchas más posibilidades. No obstante, no podemos decir que la ley nos esté cohibiendo, porque aunque se han establecido unas figuras también es cierto que no ha existido por parte del sector un interés especial en ampliarlas.

Un tercer reto es el departamental. Ahora mismo tenemos la figura del director de seguridad, a la que hemos otorgado superresponsabilidades, pero no superpoderes. Muchos departamentos de seguridad son el director y una o dos personas a su alrededor, con lo cual es muy difícil hacer frente a los nuevos desafíos.

Por otro lado, la ciberseguridad es para ASIS otro reto. Este asunto exige una formación muy específica sobre redes y procesos informáticos en la que no suelen estar al día los directores de seguridad, pero no por ello es algo que se pueda abordar simplemente con unos cursos. La ciberseguridad implica que en el futuro los departamentos de Seguridad van a necesitar contar con la ayuda de otros departamentos exter-

nos especializados. Al final los departamentos de Seguridad van a acabar estando estructurados con una parte propia que maneje las estrategias dentro de la compañía y una parte externa que opere las tácticas.

- Usted tiene un perfil profesional tecnológico por las empresas en las que ha trabajado, así como sus propias inquietudes personales. ¿Qué tecnologías o tendencias marcarán más significativamente la evolución de la seguridad privada?

En primer lugar, creo que debería existir un acercamiento a la facilidad del manejo de los sistemas. En los próximos años vamos a encontrarnos, por ejemplo, centros de control muy cercanos al mundo de los videojuegos. Los centros de control actuales, en los que vemos aparecer las alarmas sobre una planilla de Excel, se va a convertir en un entorno más dinámico e intuitivo. De hecho, la tecnología ya permite hacerlo de esa manera, lo que ocurre es que los mejores programadores suelen trabajar, precisamente, para videojuegos porque es más rentable que trabajar en seguridad.

Otra cuestión muy importante van a ser las analíticas. Hoy en día, todo lo que es un sistema de seguridad, es una *commodity*. Hace unos años las cámaras se podían sustituir sin grandes problemas, porque desde el punto de vista de la calidad cualquier fabricante respondía. Sin embargo, en el futuro lo que va a definir un buen sistema de seguridad serán las analíticas y la inteligencia artificial aplicada.

Y sin duda hay que mencionar la evolución de los drones, no tanto por lo que permita la Ley, sino por el uso que puedan hacer de ellos los malos. Hoy en día un dron a cien metros de altura, con un equipo de calidad, puede llegar a hacer análisis de la cara de una persona desde 800 metros de distancia. La normativa regula lo que ya existe, pero los delincuentes no van a utilizar precisamente un dron del mercado, ni van a respetar sus reglas.

Finalmente, el reconocimiento facial abre enormes posibilidades. Esta tecnología ya está madura y, de hecho, ya ha cedido el paso a herramientas capaces de detectar rasgos del comportamiento de una persona. El reto está en hacer que la tecnología trabaje en nuestro beneficio y no para limitar nuestras libertades.

-¿Cuáles cree que son los principales problemas que tiene el sector en la actualidad?

Diría que el principal es encontrar una buena sintonía con la legislación sobre protección de datos. Los procesos de analítica a los que me refería anteriormente están muy vinculados al vídeo, pero puede ser que se desarrollen tecnologías paralelas muy similares para detectar comportamientos mediante controles de acceso, por ejemplo. En el momento en el que la autoridad competente entiende como dato personal para su tratamiento, en caso de que la persona no pertenezca a la propia empresa, la retina, la morfología de la nariz o la huella dactilar, surge el problema; porque el 95 por ciento de los equipos de analítica basan su efectividad en procesos de aprendizaje. Es decir, necesitan datos, pero si no los podemos tratar estamos desaprovechando una tecnología que sin ellos es inútil.

En segundo lugar está la interoperabilidad entre los sistemas de seguridad privados de diferentes usuarios que comparten un mismo espacio, por ejemplo un centro comercial; es decir, conseguir compartir información de una manera rápida y segura, incluso usando bases de datos. Esa connivencia en lo relativo al Reglamento General de Protección de Datos es un reto que está ahí y debemos superar. Si existe esa brecha entre diferentes seguridades privadas, qué no habrá entre estas y la seguridad pública... Hay una enorme oportunidad de acercar esa frontera que separa la seguridad privada de la pública.

En tercer lugar están las amenazas ciber, y lo que implican no solo como fuente de ataque para robar datos, sino como arma de primera línea para desactivar medidas de vigilancia convencionales. Por ejemplo, hoy se puede instalar un reconocimiento facial, pero ya hay quien trabaja para que eso no funcione. Por lo tanto, los nuevos dispositivos deben venir preparados para las amenazas de la Red desde su fabricación.

- En el plano normativo, ¿cómo cree que está afectando al sector la demora del nuevo Reglamento de Seguridad Privada?

Desde ASIS-España hemos tenido la oportunidad de estar presentes en las mesas que han organizado las Fuerzas y Cuerpos de Seguridad del Estado [FCSE] al respecto, y lo que existe es un sentimiento de autorregulación en el sector. El borrador del Reglamento tiene bastantes lagunas que no se han llenado ni se les ha dado continuidad, quizás porque desde la perspectiva de las FCSE está hacerlo posteriormente mediante órdenes ministeriales.

En ese aspecto, como ha habido una continuidad con el reglamento actual, el desarrollo del negocio ha proseguido de manera normal y serena. Con lo cual, no creemos que ningún profesional de la seguridad pueda decir que se encuentra cohibido porque no exista un nuevo reglamento, más allá de los matices que resuelven las unidades de las FCSE cuando se les pregunta. No obstante, evidentemente nos gustaría tenerlo cuanto antes. S

"Uno de los principales problemas del sector de la Seguridad es encontrar una buena sintonía con la legislación sobre protección de datos"