De la seguridad corporativa a la seguridad organizacional

Bajo dicho lema, el pasado mes de abril tuvo lugar el VII Congreso de Directores de Seguridad. Un encuentro, organizado por *Seguritecnia*, AEDS, ADSI y ASIS España con la colaboración de la Fundación Borredá, en el que se abordaron cuestiones de sumo interés relativas a la transformación que se está produciendo en el ámbito de la seguridad corporativa: desde quién debe liderar el modelo implementado en una organización hasta los retos, impactos y amenazas que han de afrontar los directores de Seguridad.

Por B. Valadés, J. Sanz y D. Marchal

En esta ocasión, el escenario elegido para la celebración del congreso fue el auditorio del Colegio Oficial de Odontólogos y Estomatólogos (COEM) de Madrid, en el que se dieron cita más de 300 profesionales del sector. En sus palabras de bienvenida a los asistentes, **Ana Borredá**, directora de *Seguritecnia* y presidenta de la Fundación Borredá, se enorgulleció de ser partícipe de la organización de un evento que calificó de muy especial por su relevancia y condición de punto de encuentro para los directores de Seguridad.

Una breve alocución que dio paso a la de **Carlos Novillo** (en el centro de la imagen superior). El director de la Agencia de Seguridad y Emergencias Madrid 112 manifestó que la seguridad privada es "muy importante" para la organización administrativa que representa de cara a coordinar los diferentes servicios que presta. "Necesitamos el apoyo de todos los actores para ser más eficientes y eficaces", significó. "Y en ese contexto", prosiguió, "la figura del director de Seguridad es fundamental. Se trata del primer eslabón de la cadena, de un gran conocedor de su entorno. Por ello, nuestro deseo es potenciar la relación con los directores de Seguridad a través de congresos, jornadas o actividades formativas", expresó el viceconsejero de Presidencia de la Comunidad de Madrid.

Así daba comienzo el congreso, que contó con el patrocinio de **Panda, Grupo Sia, Johnson Controls, Magal S³, Accenture Security** y **Comstor (distribuidor de Cisco)**, además del copatrocinio de **Axis Communications** e **Ilunion Seguridad**.

Evolución y actualización

Juan Muñoz (CPP) inició el turno de intervenciones de los máximos responsables de las asociaciones organizadoras del evento. El presidente de ASIS España comentó que, allá por 2005, contribuyó decisivamente en la gestación de su primera edición. "Por lo tanto", razonó, "considero que soy un observador privilegiado que puede opinar sobre la evolución tanto del congreso como de nuestra profesión". Una labor, la del director de Seguridad, llamada a liderar la que denominó como "seguridad organizacional", que, a juicio de Muñoz, es un concepto mucho más avanzado que el de seguridad corporativa. "Creo que, de verdad, se están produciendo cambios sustanciales en el enfoque de la seguridad organizacional", opinó.

En cuanto a **Emilio Raduán**, presidente de la Asociación Española de Directores de Seguridad (AEDS), también hizo referencia a la transformación de una figura profesional

Alfonso Castaño (ASIS España), Javier Galván (Policía Nacional), Alberto Ray (ASIS International) y Juan Muñoz (ASIS España).

que no estaba contemplada en la primigenia Ley de Seguridad Privada de 1992. "Pero gracias a su texto reglamentario, el director de Seguridad comenzó a cobrar protagonismo. En el ámbito bancario, por ejemplo, contribuyó decisivamente a reducir los delitos. Las Fuerzas y Cuerpos de Seguridad descubrieron que contaban con un socio leal y su reconocimiento definitivo llegó con la Ley de Protección de Infraestructuras Críticas", ensalzó. Sin embargo, Raduán advirtió sobre la necesidad de mejorar la formación y los conocimientos para que los directores de Seguridad puedan desarrollar con éxito todas sus capacidades.

Y por lo que respecta a **Francisco Poley**, presidente de la Asociación de Directivos de Seguridad Integral (ADSI), basó su discurso en una actividad, la del director de Seguridad, condicionada actualmente por nuevas normas como el Reglamento de Instalaciones de Protección Contra Incendios (RIPCI), aprobado en 2017, o el Reglamento General de Protección de Datos (RGPD), que entrará en aplicación el próximo 25 de mayo. "Teniendo en cuenta las exigencias del desarrollo normativo, los directores de Seguridad deben implementar un modelo basado en la seguridad integral y tener presencia en los órganos de dirección con el objetivo de implicar a estos últimos en las tomas de decisiones relacionadas con la protección de las organizaciones", argumentó.

Autocomplacencia

A continuación, **Juan Muñoz** fue el encargado de inaugurar el ciclo de ponencias y mesas redondas. A través de una enriquecedora exposición, recordó que, en el año 2010, "BP protagonizó uno de los mayores desastres ecológicos de la historia: la explosión de la plataforma Deepwater Horizon provocó el vertido de millones de litros de petróleo en las aguas del golfo de México".

El informe de una comisión de investigación, apuntó Muñoz, señaló a la autocomplacencia en el seno de la compañía como principal causa de la explosión de la plataforma. Y de cara a evitar que no vuelvan a repetirse sucesos similares, hizo hincapié en la necesidad de poner en práctica un nuevo enfoque en la gestión de los riesgos, clasificando a estos últimos en tres grandes categorías: los riesgos evitables, los riesgos estratégicos y los riesgos externos.

"Pero, sin duda, el mayor de los riesgos es la autocomplacencia. Además del ejemplo de BP, la autocomplacencia condujo al derrumbamiento de Lehman Brothers, la derrota de la Armada Invencible o el incendio del dirigible Hindenburg", observó.

Riesgos líquidos

Quien también se refirió a los riesgos bajo un prisma sumamente original fue **Alberto Ray**. En concreto, el consultor venezolano, miembro de ASIS International, se centró en los que bautizó como "riesgos líquidos". "Cada hora que pasa, el mundo es más complejo y líquido. Pero estamos anclados en el pasado, en lo rígido. Y debemos comprender que las cosas pasan ahora. No podemos abordar el porvenir pensando que mañana será igual a hoy", subrayó.

Según Ray, "los riesgos líquidos se manifiestan a través de la globalización, la tecnología y el cambio climático". Una clasificación que ASIS International detalla aún más al identificarlos con la inestabilidad y la polarización política; Internet y el Big Data; la desconfianza, la transparencia y la reputación; la posverdad; los liderazgos emergentes; la inteligencia artificial y, por último, la analítica predictiva.

Los riesgos líquidos, hizo notar, precisan de una serie de requerimientos, desde la necesidad de no aislarse del

El congreso dejó patente el cambio de paradigma de la seguridad de las organizaciones, que se enfrenta a nuevos retos en contextos diferentes a los tradicionales

entorno hasta una aproximación flexible a la adversidad, pasando por el diseño de soluciones robustas, la incorporación de elementos redundantes o la generación de alianzas.

Inteligencia artificial

Precisamente, la inteligencia artificial, uno de los espacios donde se manifiestan los riesgos líquidos, fue el tema elegido por **Alfonso Castaño**, vicepresidente de ASIS España, para su ponencia. En este caso, abordándola desde una visión más constructiva al definirla como "pieza capital" en el ámbito de la seguridad. "Hablar de la inteligencia artificial es hacerlo de un antes y un después. Es como pasar del teléfono móvil al *smartphone*. Utiliza datos, interactúa con los humanos usando su mismo lenguaje, ofrece resultados exactos, aprende de sus errores… Y el hábitat de este animal es el mundo del vídeo. Sin duda, ha llegado para quedarse", reivindicó.

A grandes rasgos, Castaño explicó los conceptos y el funcionamiento de la inteligencia artificial, especialmente útil a la hora de gestionar una emergencia en lugares con grandes concentraciones de personas o vehículos. "Es un producto para directores de Seguridad", resumió. Y de cara al futuro, anticipó que facilitará metadatos en tiempo real que podrán visualizarse en dispositivos móviles y posibilitará realizar estudios forenses basándose en la seguridad en la nube (*cloud security*) y la cadena de bloques (*blockchain*).

Aliados de la UCSP

Antes de realizarse una pausa para que los asistentes pudiesen reponer fuerzas e intercambiar impresiones, **Javier Galván**, comisario jefe de la Brigada Central de Inspección e Investigación de la Unidad Central de Seguridad Privada (UCSP) de la Policía Nacional, puso en valor el papel de los directores de Seguridad en las estructuras organizativas sanitarias.

Respecto al por qué de esa relación existente entre la UCSP y los directores de Seguridad, Galván precisó que la misma se originó a través de una instrucción de la Secretaría de Estado de Seguridad que instaba tanto a la Policía

Magal S3

MAGAL S3
Security, Safety, Site management

El VII Congreso de Directores de Seguridad contó también con la participación de **Miguel Ángel López**, consejero delegado de Magal S3, quien explicó las dos vertientes en las que se mueve el director de Seguridad. La primera de ellas es como gestor técnico-tecnológico, lo que implica estar al tanto de todas las novedades del sector, de conocer las tecnologías y de su aplicación.

En cuanto a la segunda, se trata de la de gerente de departamento, donde el desarrollo de futuro es uno de los puntos más importantes. Como tal, el director de Seguridad "tiene la obligación de acercarse a la alta dirección de la empresa y de alinearse con ella para que llegue a ser su aliado", sostuvo el ponente. No obstante, para López, es el director de Seguridad quien "debe buscar la fórmula de involucrar a la alta dirección a través del lenguaje de los números y de las gráficas", ya que "hay que explicar a sus integrantes qué pueden vender, cómo maximizar el beneficio y cómo controlar el gasto".

López advirtió también del 'cortoplacismo' ya que "la alta dirección en los grandes grupos empresariales es muy temporal, por lo que solo piensan en el corto plazo". Pero en contraposición, "si tienen una visión a largo plazo, otros se beneficiarán de la posterior amortización"..

Miguel Ángel López, consejero delegado de Magal S3.

Imagine poder **controlar una gran instalación,**
abarcando su seguridad física, electrónica, informática, organizativa y personal,
de forma totalmente integrada.

Imagine poder **automatizar la respuesta,**
personalizándola según sus protocolos
y optimizando los tiempos.

E imagine poder hacerlo con sólo
un operador y tres monitores
y a un **precio muy atractivo.**

¿Lo imagina?

Nosotros lo hicimos hace tiempo.

Fortis 4G

*Plataforma integrada de **mando y control** **PSIM+SIEM***

ESTACIÓN DE GESTIÓN

ESTACIÓN GIS 3D

ESTACIÓN DE VIDEO

- **CCTV e IVA**
- **Control de accesos**
- **Intrusión y PCI**
- **Radares**
- **Megafonía**
- **Efectivos**
- **Planes operativos**
- **Ciberseguridad**
- **Fuentes de datos**
- **Etc.**

www.ms3.es

MAGAL S3
Security, Safety, Site management

Nacional como a la Guardia Civil a reducir el número de los incidentes registrados en los centros sanitarios –agresiones a profesionales, intentos de homicidios, etc.–.

"Ello nos obligó a crear un censo de instalaciones, catalogarlas en función del riesgo –alto, medio y bajo– y elegir a un interlocutor, el director de Seguridad, que se ha convertido en un elemento clave, nuestro buque insignia. Para garantizar la normalidad en el ámbito sanitario, las Fuerzas y Cuerpos de Seguridad del Estado y los directores de Seguridad debemos ir de la mano", alentó.

Horizonte 2020

Tras el café, **Maite Boyero**, representante del Centro para el Desarrollo Tecnológico Industrial (CDTI), entidad pública empresarial dependiente del Ministerio de Economía, Industria y Competitividad, dio a conocer el programa marco de investigación e innovación Horizonte 2020 de la Unión Europea. Concretamente, una de las seis áreas esenciales encaminadas a mejorar la vida de los ciudadanos comunitarios: la seguridad.

Mayte Boyero (CDTI).

En su octava edición, el programa se ha centrado en las ciudades seguras, contempla una partida de 1.700 millones de euros para subvencionar proyectos y se articula en torno a tres convocatorias: una reservada a la protección de infraestructuras críticas, otra dedicada a la seguridad –dividida, a su vez, en cuatro apartados: gestión de crisis y desastres, lucha contra el crimen y el terrorismo, seguridad de las fronteras y asuntos generales– y una tercera enfocada en la ciberseguridad.

"Ayuntamientos, ONG, operadores de infraestructuras críticas, etc., pueden beneficiarse de los fondos económicos del programa. Por ello, animo a los profesionales de la seguridad a que participen en él. Debemos intentar que parte del dinero que aporta España vuelva a nuestro país", concluyó.

Mesa impactos normativos

La sesión de la tarde comenzó con el panel "Impactos normativos en la seguridad corporativa", en el que intervinieron cuatro directivos para hablar sobre el Reglamento General de Protección de Datos (RGDP), la normativa NIS, la Ley sobre Protección de Infraestructuras Críticas (Ley PIC) y la nueva legislación en la creación facultativa u obligatoria de los departamentos de seguridad.

Para comentar el primer punto intervino **Elena Mora**, subdirectora de Marco Regulatorio de Seguridad de Ma-

Johnson Controls

La protección contra incendios (PCI) también es una parte importante de la gestión del director de Seguridad. Pese a ello, según lamentó **Luis Sánchez**, *head of Sales Engineered Systems and Water Mist* para el sur de Europa de Johnson Controls, esta especialidad es como "el patito feo de la seguridad, ya que está en un segundo escalón". Esto es debido, tal y como opinó este ponente, a que "la probabilidad de que se produzca un incendio es pequeña", por lo que "los sistemas de prevención no se suelen utilizar".

Teniendo en cuenta tal realidad, este profesional explicó a los asistentes que se dieron cita en el congreso cómo funcionan sistemas de PCI medioambientalmente ecológicos como el Novec presurizado a 70 bar, los cuales vienen a sustituir a la familia de los gases halones y reemplazan en el mercado los fluorados, considerados de efecto invernadero.

En concreto, el punto de ebullición del agente Novec es de 40 grados, "bastante bajo" según Sánchez, por lo que presenta una serie de ventajas. Entre ellas mencionó un transporte y un trabajo mejor, la no conducción de la electricidad, la no liberación en un fuego y la mayor rapidez respecto a otros agentes extintores, entre otras. Además, destacó que este agente funciona por absorción de calor y por enfriamiento, por lo que no elimina el oxígeno y se puede utilizar con la presencia de personas.

Luis Sánchez, *head of Sales Engineered Systems and Water Mist* para el sur de Europa de Johnson Controls.

Francisco Poley (ADSI), Elena Mora (Mapfre) y Alberto Ramos (ISACA Madrid).

pfre, quien dio unas pinceladas de lo que trae el RGPD al marco normativo español, puesto que su aplicación es de transposición directa. "Establece obligaciones desde el momento de la recogida de los datos y afecta a todo el tratamiento de los datos", apuntó.

Además, comentó que introduce conceptos como el de responsabilidad proactiva o *accountability*. "Este es uno de los grandes cambios de paradigma de esta regulación. Partíamos de un entorno en el que tenías que confirmar que cumples con las medidas de seguridad adecuadas. En cambio, ahora hay que demostrar que se han hecho todos los esfuerzos necesarios por garantizar la integridad de los datos. En otras palabras, todo lo que no se pueda demostrar de manera tangible es como si no se tuviera nada", afirmó la directiva.

Igual de importante en este Reglamento es el consentimiento de los dueños de los datos personales para su tratamiento por parte de las empresas. "Ya no sirve el consentimiento tácito. Tendremos que ir a mecanismos que permitan demostrar que el consentimiento sea claro, transparente, explícito y de manera consciente", apuntó Mora.

Finalmente, la directiva abordó la figura del delegado de protección de datos, que es el garante en las organizaciones del cumplimiento de la normativa; y el tema de las sanciones, que puede afectar a la imagen de las empresas.

Seguidamente, **Antonio Ramos**, vicepresidente de ISACA Madrid, fue el encargado de hacer un repaso de los conceptos que introduce la directiva europea NIS, "cuyo espíritu es mejorar la seguridad en las redes y sistemas de información, con el objetivo de potenciar los niveles de seguridad para que se haga un mejor uso de las tecnologías".

Esta normativa se centra en dos colectivos: los operadores de servicios esenciales y los de servicios digitales. En el primer caso, Ramos explicó que afecta directamente a la Ley PIC, por lo que "se va a cambiar y se va a dar un papel más relevante a la seguridad, imponiendo también sanciones", puntualizó. No en vano, la directiva europea establece a este colectivo unas medidas de seguridad mínimas e incide en la notificación de los incidentes.

Accenture Security

Accenture Security

La labor del director de Seguridad desde el punto de vista de la gestión de la información fue el tema central de la ponencia de **Xabier Mitxelena**, director general de Accenture Security para España, Israel y Portugal. Para este profesional, dicha figura tiene que tener en cuenta la información como un activo fundamental y debe trabajar en base a la tecnología.

Las empresas deben "realizar la transformación digital". "Este cambio nos está llevando a una carrera de autos locos, ya que no tenemos un modelo construido para desarrollarla", continuó Mitxelena. En este sentido, el ponente animó a construir este modelo conjuntamente entre todos los actores de la seguridad debido a que "la seguridad corporativa está en constante evolución, por lo que hay que trabajar todos los días en los cambios que se producen". "La transformación digital supone cambiar nuestra forma de pensar; por lo tanto, tenemos que razonar de otra forma a la hora de proteger los activos de la compañía", prosiguió Mitxelena.

Se trata, en definitiva, de un proceso continuo en el que el director de Seguridad tendrá más y nuevas funciones, además de nuevas herramientas, aunque siempre tendrá que hacerse las mismas preguntas respecto a qué hay que proteger y quién es el enemigo.

Xabier Mitxelena, director general de Accenture Security para España, Israel y Portugal.

SMI Server

El Sistema integral para una supervisión global de la seguridad

SMI Server está compuesto por diferentes módulos de software que cubren la totalidad de necesidades de seguridad de las empresas.

Módulo de Control de accesos

Módulo de Intrusión

Módulo de Vídeovigilancia

Gunnebo España S.A., Tel.: 902 100 076 - info.es@gunnebo.com - www.gunnebo.es

GUNNEBO

"Estamos hablando de instalaciones como las industriales, de investigación y docencia, médico-hospitalarias y de comercialización", comentó, y añadió: "la instrucción IS41 establece la identificación del responsable de la instalación con autoridad y capacitación para tomar decisiones en situaciones normales y de contingencia". En total, según el inspector jefe, hay más de 230 instalaciones de este tipo de en España, las cuales deben contar con un departamento de Seguridad.

Estudio sector público

La ponencia de **César Álvarez**, el coordinador de proyectos y miembro del Comité Asesor de la Fundación Borredá, giró en torno a la contratación de servicios de seguridad privada por parte del sector público. La Fundación Borredá ha elaborado un informe al respecto, que verá la luz próximamente, en el que se analiza el periodo comprendido entre 2007 y 2016 para intentar entender cómo ha evolucionado este parámetro. "Lo primero que llama la atención al estudiar esto es la poca información que hay al respecto. Es preciso acudir a portales, contratistas, boletines… y eso dificulta la tarea", explicó.

A pesar de ello, pudo adelantar a los asistentes algunas conclusiones interesantes. Una de ellas es que, debido a la crisis económica, la Administración apostó por contratar servicios de seguridad al precio más bajo, lo que produjo un deterioro en su calidad. "Queriendo comprar barato lo bueno se paga caro lo malo", explicó Álvarez, quien añadió: "La administración no lo ha hecho bien. Los costes no se pueden reducir intentando pagar más baratos los servicios. Hay que planificar mejor y poner los servicios que hagan falta, pero pagados a su precio. Esto ha producido un importante daño a la imagen de la seguridad privada".

César Álvarez (Fundación Borredá).

Por todo ello, el coordinador de proyectos de la Fundación Borredá expresó su deseo de que el nuevo Reglamento de Seguridad Privada establezca una serie de requisitos que busquen "una contratación técnicamente responsable".

Clausura de la jornada

El congreso finalizó con su clausura por parte del director general de la Policía, **Germán López**, quien confirmó que, en los últimos años, España se ha consolidado como uno de los países más seguros de Europa. Este hecho, a juicio de López, es "mérito de todos", tanto de las empresas, las asociaciones, la Administración y los ciudadanos. Y es que, según comentó: "A la seguridad de los españoles contribuimos todos".

Por otro lado, reveló que la Policía se ha marcado el objetivo de colaborar estrechamente con el sector privado, y dentro de este objetivo se encuentra la figura clave con la que tienen que trabajar conjuntamente, la de los directores de seguridad. "Actualmente hay unos 15.000 directores de seguridad y 600 departamentos de seguridad en activo, que son los aliados para el sostenimiento de la seguridad nacional", subrayó el director general, quien añadió: "Son elementos activos del proceso de evolución de la seguridad".

Por último, destacó que también se está avanzando en la implantación de la figura del director de Seguridad en sectores en los que generalmente no había tenido una gran presencia, como el sanitario; y remarcó la importancia de la reestructuración de la actividad inspectora de la Policía Nacional en situaciones como la gestión de la seguridad de las infraestructuras críticas.

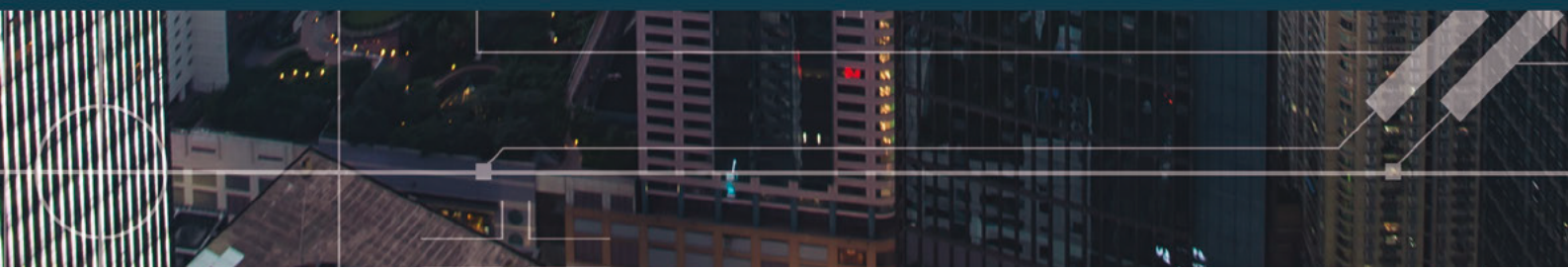
El director general de la Policía, Germán López (en el centro), clausuró el VII Congreso de Directores de Seguridad.

KEDACOM

Especialistas en analítica de video

COREA - SINGAPUR - CHINA

Video Sinopsis - Video Recognitivo - Deep Learning
Reconocimiento Facial - Smart City - Análisis de Video
Cámaras IP Inteligentes - NVRS profesionales - Software de análisis



EUROMA

www.euroma.es

MADRID
C/ Emilia 55 local 4 28029 Madrid
Tel: +34 91 571 13 04 / 15 19
Fax: +34 91 570 68 09
Email: euroma@euroma.es

BARCELONA
C/ Bogatell 43-49 1º 2ª 08930 Sant Adriá de Besos
Tel: +34 93 381 24 58 / 22 12
Fax: +34 93 381 57 34
Email: barcelona@euroma.es

Mesa redonda: "¿Qué perfil liderará el modelo de seguridad corporativa?"

Distintos modelos y un objetivo común: proteger el negocio y sus activos

Si algo quedó claro en la mesa redonda "¿Qué perfil liderará el modelo de seguridad corporativa?" es que, independientemente de cómo se estructuren, los departamentos de Seguridad deben estar dirigidos por profesionales cualificados, conocedores de la organización, cercanos a la alta dirección y, sobre todo, con capacidad para proteger a sus compañías y resolver los problemas que puedan presentarse.

La agenda matinal del VII Congreso de Directores de Seguridad finalizó con la que **Juan Muñoz** consideró la mesa redonda "más potente" de cuantas han tenido lugar en la historia del evento. La misma estuvo moderada por el presidente de ASIS España, quien calificó de *heavy weights* (pesos pesados) a los profesionales que la integraron: **Gianluca D'Antonio**, director de Sistemas de Información de FCC; **Alberto Tovar**, director de Seguridad Corporativa de Cepsa; **Elena Matilla**, directora de Seguridad de la Información de Red Eléctrica de España (REE); **Inés Díaz Ochagavia**, responsable de Seguridad Física del Grupo BBVA; **José Luis Bolaños**, director de Seguridad Corporativa de Gas Natural Fenosa; y **Alberto Torreño**, director de Seguridad de Repsol.

Todos ellos protagonizaron una enriquecedora puesta en escena en la que se trataron tres temas de sumo interés para los asistentes: cómo es el modelo de seguridad de sus respectivas organizaciones –las seis, por cierto, vinculadas a la protección de infraestructuras críticas–, de qué forma se ha materializado la convergencia en ellas y, finalmente, qué perfil debe tener el máximo responsable de un departamento de Seguridad Corporativa.

Seis modelos, seis

En cuanto a la primera cuestión, y sirviéndonos de una expresión taurina, podría afirmarse que Muñoz tuvo que lidiar con seis miuras realmente bravos pero con diferentes hechuras. Dicho de una forma más coloquial, si algo quedó de manifiesto tras escuchar sus exposiciones es que cada uno tiene competencias distintas y están integrados en modelos de seguridad corporativa que poco o nada tienen que ver unos con otros.

Así, si bien es cierto que en ellos suelen cohabitar los mismos perfiles profesionales –director de Seguridad, director de Sistemas de Información, director de Seguridad de la Información, etc.–, la cabeza visible no es idéntica en todos los modelos –de hecho, en algunos no existe un máximo responsable de seguridad corporativa que, como tal, aglutine todas las áreas de protección–. Asimismo, se puso de relieve que unas organizaciones han implementado comités específicos de seguridad, mientras que en otras esta última se aborda en otro tipo de juntas. Y entre las desemejanzas también cabe resaltar que los departamentos de Seguridad no reportan a los mismos directivos o áreas de la compañía. En cuanto al gerente de Riesgos, los participantes afirmaron tener una buena relación con dicha figura, aunque la misma no forme parte de la estructura de seguridad.

"Por lo expuesto, queda claro que no hay un modelo firme. Dependiendo de la organización, este último será liderado por quien esté más preparado para ello, la persona con más conocimiento empresarial y mayor capacidad de liderazgo. Puede ser el director de Seguridad, el director de Sistemas de Información, el director de Seguridad de la Información…", concluyó el presidente de ASIS España.

Ejemplos de convergencia

Y, al hilo de dicha exposición, quedó claro que la convergencia no se ha materializado de la misma forma en todas las empresas. Por ejemplo, Alberto Torreño esclareció que, en el caso de Repsol, las áreas de Seguridad y Ciberseguridad mantienen estructuras independientes. "Pero nos sentimos cómodos porque, en materia de

protección, nos coordinamos y todos estamos muy implicados", manifestó.

Por su parte, José Luis Bolaños afirmó que, en buena medida, el modelo de convergencia implementado en Gas Natural Fenosa fue impulsado por la Ley de Protección de Infraestructuras Críticas. "Y ese mestizaje entre la seguridad física y la ciberseguridad nos ha aportado una enorme riqueza y, no menos importante, ha facilitado acercar el modelo al consejo de administración de la empresa", declaró.

A continuación, Inés Díaz Ochagavia explicó que la convergencia es bastante reciente en el Grupo BBVA. "Sin embargo, aunque no tuviésemos una estructura que soportara el análisis conjunto, considerar los riesgos desde una perspectiva integral es algo en lo que llevamos trabajando desde hace muchos años", reveló.

Seguidamente, Elena Matilla fue rotunda al afirmar que "en REE se trabaja por y para la convergencia", aunque reconoció que esta última aún debe perfeccionarse. "Nuestro modelo será realmente convergente cuando seamos capaces de lograr que la capa operacional trabaje bajo el paraguas de las capas de gobierno y gestión; es decir, que la convergencia se materialice desde arriba hacia abajo", precisó.

En sintonía con este último apunte, Alberto Tovar señaló que en compañías como Cepsa "uno de los principales retos es que converjan los mundos IT y OT", al tiempo que reivindicó el liderazgo de la seguridad física en los modelos de seguridad corporativa. Una defensa no compartida por Gianluca D'Antonio, quien opinó que la misma ha quedado en un segundo plano "en un mundo en el que la cibercriminalidad factura trillones de dólares al año".

Alberto Torreño (Repsol), José Luis Bolaños (Gas Natural), Inés Díaz (Grupo BBVA), Elena Matilla (Red Eléctrica España), Alberto Tovar (Cepsa) y Gianluca D´Antonio (FCC).

Cisco

La sociedad contará con 30.000 millones de dispositivos conectados a Internet en 2020. Pese a ello, solamente al 13 por ciento de las compañías les preocupa la seguridad en el Internet de las Cosas, según datos mostrados en el último informe de Cisco y expuestos en el congreso por parte de Eutimio Fernández, *Cybersecurity Leader* de Cisco España y Portugal.

Es en este contexto en el que el director de Seguridad debe llevar a cabo una inteligencia global para conocer el nivel de las amenazas. Además, tiene que ser capaz de tener un control sobre ellas en un panorama en el que los ciberdelincuentes son diferentes y en el que están evolucionando continuamente. Por lo tanto, "es necesario contar con un nuevo modelo de seguridad dirigido por la ciberinteligencia", tal y como aseguró el ponente.

Además, Fernández avisó de la fragmentación que sufren las organizaciones en relación con los productos de ciberseguridad utilizados. En concreto, tal y como menciona el citado documento, una empresa posee entre 50 y 60 soluciones diferentes de seguridad de la información. "Debido a ello, perdemos mucha visibilidad en la red y mucho conocimiento. Esto es lo que aprovechan los delincuentes para atacar la corporación", concluyó el representante de Cisco.

Eutimio Fernández, Cybersecurity Leader de Cisco España y Portugal.

Mesa redonda: "Análisis de amenazas para la seguridad corporativa"

El criterio de contratación de servicios continúa siendo un reto a mejorar

La última mesa redonda del VII Congreso de Directores de Seguridad, titulada "Análisis de amenazas para la seguridad corporativa", examinó los retos a los que se enfrentan las organizaciones desde el punto de vista de la seguridad, pero no solo en lo que a riesgos se refiere sino también a otros factores que influyen en su desempeño, como el coste y la calidad de los servicios, el nuevo Reglamento de Seguridad Privada o el desarrollo de la ciberseguridad en el ámbito industrial.

Todo parece indicar que atrás han quedado los peores años de la crisis económica. Sin embargo, es cierto que ha dejado un poso que todavía no ha desaparecido. De hecho, esto es lo que sucede con el sector de la seguridad privada, en el que el factor precio tiene todavía un gran peso en la contratación de estos servicios, por encima incluso de la calidad. Precisamente, este es el tema con el que dio comienzo la última mesa redonda del VII Congreso de Directores de Seguridad.

"Durante la crisis, una de las máximas de las organizaciones fue la de reestructurarse en reducción de costes, factor que ha impactado en la seguridad", observó **Jorge Lagares**, vocal de la Confederación Empresarial de Usuarios de Seguridad y Servicios (CEUSS). Tanto es así que los directores de seguridad han perdido peso específico en la elección de sus proveedores, en detrimento de los directores financieros o de compras, según se explicó en la mesa redonda.

En palabras de **Francisco Muñoz Usano**, presidente de la Sociedad Española de Derecho de la Seguridad (SEDS), actualmente "hay mucha preocupación por los números y poco por la letra". Por ello, este experto invitó a todos los asistentes "a reflexionar sobre el concepto mismo de contratar seguridad". Y es que, para Muñoz Usano, un contrato de este tipo "no puede tener el mismo formato que, por ejemplo, la compra de la papelería. La seguridad está para prevenir incidencias y gestionar riesgos, por lo que no hay que perder de vista el aspecto jurídico", afirmó.

En este sentido, los directores de Seguridad tienen un papel importante que desempeñar, como puntualizó Lagares: "Tienen que hacer ver el valor de no contratar a la baja. Además, tanto el departamento de finanzas como el de seguridad han de estar alineados y trabajar en la misma dirección", confirmó.

En este sesntido también se manifestó **Juan Muñoz**, presidente ASIS España, quien ratificó la importancia que están teniendo los departamentos de compras al contratar servicios de seguridad. Sin embargo, esto tiene un inconveniente: "Ahora estas áreas gestionan sus compras a través de una plataforma por Internet, de tal forma que no conocen ni al proveedor". Todo este proceder, junto a la crisis, ha liquidado muchas empresas de seguridad, generando una situación compleja. "Si la Administración contrata mal y a compañías en situación irregular, qué no harán las empresas privadas que se guían solo por la cuenta de resultados", añadió este profesional certificado como CPP.

En la mesa también se destacó otro de los retos a los que debe hacer frente el sector de la seguridad privada: la formación. Según Lagares, de CEUSS, "las empresas de seguridad tienen lo obligación de formar a sus vigilantes en los riesgos actuales, que no son los mismos que los de hace diez años". Para el directivo, se requieren "vigilantes proactivos, en los que se puede depositar la confianza de las empresas, porque ellos son los ojos de las instalaciones".

No en vano, una formación deficiente puede redundar en la calidad de la prestación del servicio. "Cuando las empresas cierran sus puertas por las noches, dejan su patrimonio en manos de alguien que debe estar bien formado y pagado", aseguró Muñoz, de ASIS España.

Nuevos desafíos

Pero estos no fueron los únicos retos que se plantearon durante la mesa redonda. De la mano de Muñoz Usano, de SEDS,

y **Susana Asensio**, responsable de proyectos del Centro de Ciberseguridad Industrial (CCI), también se abordaron temas relacionados con el futuro Reglamento de Seguridad Privada y la seguridad en el ámbito industrial.

En el primer caso, el presidente de SEDS valoró qué se puede esperar del futuro reglamento –en trámite actualmente– en tanto que establecerá una serie de normas de funcionamiento básicas para que los directores de Seguridad puedan ejercer su trabajo con seguridad jurídica. Además, abogó por que cualquier texto que se apruebe "ponga normas nuevas donde haya problemas nuevos; pero donde no hay problemas nuevos, no hacen falta normas nuevas".

Por su parte, la representante del CCI centró su intervención en la necesidad de que tanto las tecnologías de la información como operacionales trabajen y se entiendan conjuntamente para avanzar de forma adecuada en la ciberseguridad industrial. Para ver ese avance, el CCI realiza periódicamente un estudio de evaluación de la situación. "En todos los años que lleva realizándose hay un 80 por ciento más de empresas y de encuestados que afirman que el ámbito de la ciberseguridad industrial se va a incrementar y aumentar exponencialmente", afirmó Asensio.

No obstante, es preciso salvar ciertos obstáculos, porque cada uno de estos equipos "viene con estrategias distintas" que hay que poner en común. A lo que se une también el hecho de que haya pocos profesionales de la ciberseguridad operando en entornos industriales, lo que también complica la relación entre ambos mundos.

En cualquier caso, Asensio confirmó que desde el CCI trabajan en salvar esos obstáculos y en que, en el futuro, se pueda producir una perfecta integración entre los sistemas de la información y las tecnologías operacionales.

Jorge Lagares (CEUSS), Susana Asensio (CCI), Francisco Muñoz Usano (SEDS), Ana Borredá (*Seguritecnia*), Francisco Poley (ADSI) y Juan Muñoz (ASIS España)

Grupo SIA

La evaluación de la resiliencia fue el eje principal de la ponencia de **Roberto Pérez,** director de Desarrollo de Negocio de Ciberseguridad de Grupo SIA. Este profesional explicó en qué consiste un ciberejercicio como método para conocer la reacción de las organizaciones frente a un ciberataque. Se trata de llevar a cabo una serie de prácticas para evaluar de manera objetiva las medidas de detección y respuesta ante ataques informáticos dentro de cualquier entidad.

Para ello, según explicó Pérez, son necesarios dos equipos, uno rojo que ataca y otro azul que defiende, siendo este último el objetivo del ciberataque y al cual se evalúa. También hay un grupo controlador, que tiene el hilo conductor del ciberejercicio, y otro morado, que participa en su diseño y cuyo objetivo es que las técnicas y tácticas estén alineadas con la infraestructura corporativa. Además, recolecta las evidencias de los equipos rojo y azul para recabar conocimiento del atacante y trasladárselo al defensor con el objetivo de implementar medidas de seguridad.

Finalmente, aclaró que para una adecuada ejecución del ciberejercicio hay que tener las infraestructuras específicas para los equipos rojo y morado con la finalidad de que esta herramienta se desarrolle correctamente en cada una de sus fases –diseño, ejecución, evaluación y mejora–.

Roberto Pérez, director de Desarrollo de Negocio de Ciberseguridad de Grupo SIA.

Principales conclusiones del VII Congreso de Directores de Seguridad

Una vez finalizado el VII Congreso de Directores de Seguridad, y analizadas las distintas intervenciones, ponencias y mesas redondas, podemos concluir que:

1. La seguridad está experimentando un cambio de modelo y necesidades dentro de las organizaciones, lo que requiere de una adaptación de los profesionales que lideran esta área.

2. Los representantes de la seguridad pública destacaron el papel del director de Seguridad como primer eslabón de la cadena que vincula a aquella con la seguridad privada.

3. Normas como la Ley de Protección de Infraestructuras Críticas han propiciado tanto reforzar la figura del director de Seguridad como diseñar un modelo de seguridad corporativa marcado por la convergencia. No obstante, esta no se ha materializado de la misma manera en todas las organizaciones.

4. Ante los desafíos actuales, como el cumplimiento de nuevas normas como el RGPD o la normativa NIS, se animó a los directores de Seguridad a continuar formándose de cara a enriquecer sus conocimientos.

5. Más allá de los tradicionales, es preciso hacer frente a los nuevos riesgos derivados del uso de las TIC, así como a los llamados "riesgos líquidos". Para combatirlos, se recomendó a los directores de Seguridad analizar el presente con visión de futuro.

6. Dentro de las capacidades de los directores de Seguridad, se reclamó un mayor conocimiento de las soluciones tecnológicas. Especialmente, la inteligencia artificial está llamada a posicionarse como una herramienta muy útil.

7. En los modelos de seguridad corporativa de grandes compañías no existe una cabeza visible con un perfil definido y la misma, en función de las particularidades de cada organización, puede estar representada por cualquiera de las figuras profesionales existentes: director de Seguridad, director de Sistemas de Información, CISO, etc.

8. En algunos de los modelos de seguridad corporativa expuestos quedó de manifiesto que no existe una comunicación directa entre el director de Seguridad y la alta dirección y que la misma se materializa a través de otras áreas de la organización o de directivos ajenos al departamento.

9. El máximo responsable de Seguridad Corporativa ha de tener un perfil multidisciplinar. Debe estar familiarizado con el negocio, ser capaz de gestionar equipos y crisis, y mantener una comunicación lo más directa posible con la alta dirección.

10. Administración y empresas han de velar por que los criterios de contratación pública de seguridad privada otorguen más peso a la calidad que al precio de la oferta. Una consideración que debería trasladarse también a la contratación privada.